UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

PRAXIS DE LA SEGURIDAD INFORMÁTICA

TESIS PROFESIONAL
PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

ÁREA

REDES Y SEGURIDAD

PRESENTA:
MONROY SUÁREZ DIEGO

DIRECTORA DE TESIS
M.C. Ma. Jaquelina López Barrientos

Ciudad Universitaria, México, 2011

Dedicatoria

A mis padres por su comprensión, por creer en mí y por haberme enseñado a encarar las adversidades ni desfallecer en el intento. Por todo lo que soy como persona y por todo aquello que me han dado con gran paciencia, amor y comprensión, sin pedir nunca nada a cambio.

A mis, primos, tíos, abuelos y amigos por estos años que llevamos de conocernos y apoyarnos en las buenas y en las malas esperando sigan siendo más años de estar juntos.

A todos, por su apoyo, su comprensión y sus consejos en los momentos difíciles.

AGRADECIMIENTOS

A mi Directora de Tesis M.C. Ma. Jaquelina López Barrientos por su presencia incondicional, sus apreciados y relevantes aportes, críticas, comentarios y sugerencias durante el desarrollo del presente trabajo de tesis.

A mis compañeros por estos años que han sido de una u otra forma inolvidables:

David Castro, David Ignacio González, Diego Dante González, Everardo López, Jorge Pantaleón, José Antonio Peña, Josué Joan Méndez, Josué Daniel Escamilla, Juan Sarabia, Luis Ernesto Espinoza, Miguel Ángel, Oscar Monroy, Omar Alejandro García, Pedro Joari Martínez, Rubén, Sergio Becerril.

A mis profesores por compartir sus conocimientos, hacer de mí un ingeniero y una mejor persona; así como aprender de ellos las cosas importantes que no se enseñan en un salón de clases:

Ing. RODRIGUEZ HERNANDEZ VELDA LILIANA, Ing. ORLANDO ZALDIVAR, ING. MA. EUGENIA MACÍAS RÍOS, M.C. MARCO A. VIGUERAS VILLASEÑOR, ING.M.I NORMA ELBA CHÁVEZ, Ing. ARREDONDO GARZA JOSE ANTONIO DE JESUS, M.A. GAYOSSO ESCAMILLA HILARIA NELLY, Ing. CARRANZA TORRES EDUARDO, Ing. RAFAEL SANDOVAL VÁZQUEZ, Ing. LOPEZ HERNANDEZ MARCO ANTONIO, Ing. RAMIREZ TAQUEZ JOEL, Ing. SAMUEL HUERTA, Ing. JAIME MARTINEZ †

A los miembros de las salas de UNICA por estos 2 años de convivencia.

Finalmente una disculpa a aquellas personas que no pude recordar su nombre y que de alguna u otra forma pasamos tiempo conviviendo en todos estos 5 años.

Índice

INTRODUCCIÓN

Hoy en día el creciente uso de las tecnologías de la información es parte de la vida diaria. Entre algunos de los factores que obligan a los países a hacer uso de la tecnología podemos encontrar: el crecimiento económico, la disponibilidad de los recursos, la innovación y mejoras que favorecen el incremento de la productividad y aunado a esto el impulso a la competitividad.

Utilizando eficientemente las tecnologías de la información se pueden obtener ventajas competitivas, sin embargo es necesario encontrar procedimientos inequívocos que nos permitan mantener una mejoría constante, así como disponer de cursos y recursos alternativos de acción para adaptarlas a las necesidades del momento, así mismo, es importante considerar y tener presente que para trabajar eficientemente también es necesario hacerlo de manera segura, ya que en los años recientes el problema de la seguridad de la información ha crecido de manera exponencial afectando a prácticamente todas las actividades de la sociedad.

El uso correcto de las TI (Tecnologías de la Información) puede proporcionar a los administradores una nueva herramienta para distinguir los diferentes tipos de recursos a los que se tiene acceso, sean productos y/o servicios.

En un mundo donde el progreso no se detiene; es necesario permanecer a la vanguardia, para ello se requiere que los especialistas de la información, los sistemas de datos, y los ingenieros en computación actualicen constantemente sus conocimientos, empleando técnicas nuevas que permitan una retroalimentación en un ciclo de avance continuo.

El área de la Ingeniería en Computación presenta una dinámica propia del avance tecnológico y de las condiciones económicas y sociales, las cuales inciden en la formación de recursos humanos. Sin embargo, y debido a situaciones presentes y futuras, es necesario hacer una revisión y mejora de los procesos educativos para seguir manteniendo el liderazgo en la formación de profesionales en esta área.

La Facultad de Ingeniería buscando realizar de manera integral investigación acorde con las necesidades de la sociedad, y difundir ampliamente la cultura Nacional y Universal. Ha revisado y modificado los planes de estudio de las carreras que ofrece aportando nuevos conocimientos para la investigación que impacte en la caracterización de cada especialidad de la ingeniería, el avance científico que se va logrando en las diferentes áreas del conocimiento; así, en la revisión de planes de estudio correspondientes a 2005 se integraron asignaturas en el campo de la seguridad informática creándose el módulo terminal de Redes y Seguridad donde se estudian temas como: Criptografía, Desarrollo de software seguro, Arquitecturas cliente/servidor, Análisis y diseño de redes de datos y Seguridad informática I y II.

La estructura actual que se mantiene en el plan de estudios se ha organizado de tal forma que se han cubierto los temas que son considerados más importantes y agregado otros que representan una introducción a las nuevas tecnologías y tendencias actuales.

Es importante recalcar que aun cuando la carrera de Ingeniería Computación en el módulo de Redes y Seguridad está dedicada a la formación de expertos en la materia, cabe señalar que el número de personas egresadas que se dedican a la investigación científica formal es muy bajo y por el contrario el resto ingresa a un mercado laboral nacional donde es muy importante contar con experiencia en el manejo de las TI.

Por el momento no existe material plenamente enfocado a la revisión e implementación práctica de los conceptos que se presentan en el campo de la seguridad informática lo cual dificulta el aprendizaje y retención de los mismos.

Así, el presente proyecto de tesis tiene por objetivo proponer una serie de prácticas de laboratorio para el estudio de la seguridad informática que contemple conceptos vistos no sólo en una sino en varias de las asignaturas del módulo terminal, dando como resultando un instrumento valioso para el alumno y el maestro.

Esta propuesta parte de la necesidad de crear expertos en la materia con capacidad para resolver problemas de forma rápida y eficaz en su vida profesional.

Para ello en el capítulo 1 se presenta el marco teórico sobre el cual fue desarrollado este proyecto definiendo los elementos teóricos básicos y necesarios para su comprensión.

En el capítulo 2 se presenta la selección de contenidos y las herramientas respectivas tanto de software como de hardware para presentar un acercamiento a la seguridad informática de forma práctica y concisa.

Por consiguiente en el capítulo 3 se presenta la propuesta de 12 prácticas que deberán ser llevadas a cabo para lograr el objetivo del proyecto.

Culminando con el capítulo 4 donde hacemos una revisión extensiva del proyecto verificando el cumplimiento de los objetivos inicialmente planteados.

Finalmente se presentan las conclusiones como resultado de la investigación realizada, puntualizando la importancia que lleva la generación de material para el mejoramiento de la comprensión de conceptos que van más allá de la teoría debido al constante avance tecnológico.

Objetivo General

El propósito de esta tesis es proponer una serie de prácticas de laboratorio para el estudio de la seguridad informática que contemple conceptos vistos no sólo en una sino en varias de las asignaturas del módulo terminal de la carrera de Ingeniería en Computación en el módulo de Redes y Seguridad.

- Adquirir habilidades necesarias en el área de la seguridad informática.
- Capacitación en el uso de diversas herramientas de seguridad informática.
- Integración de diversos conceptos en el área de seguridad informática.

Objetivos Específicos:

- Promover el uso de herramientas de Software Libre.
- Usar entornos virtuales.
- Emplear diferentes herramientas de Software y Hardware.
- Crear una conciencia de la seguridad informática.

La seguridad informática es un proceso continuo en el cuál es de vital importancia identificar aquello que se desea proteger y resguardarlo de aquello que amenaza con alterarlo, dañarlo o destruirlo.

Es por esto que las prácticas propuestas no solo buscan capacitar al estudiante en la adquisición de habilidades requeridas en el área de la seguridad informática si no que también buscan concientizar al estudiante la importancia del uso, manejo, transferencia y almacenamiento de la información que hacen uso las organizaciones para evitan daños mayores y problemas que puede ocasionar algún intruso o los mismos usuarios.

Capítulo I

Antedecentes

En este capítulo de denotan los conceptos básicos para la compresión del proyecto.

1.1 Concepto de la Seguridad Informática

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema automatizado mediante Tecnologías de la Información y sus usuarios, así, la seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

- La información contenida
  Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios no autorizados puedan acceder a ella. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella, que sea manipulada, ocasionando lecturas erradas o incompletas de la misma, o incluso que sea falsamente generada.

- La infraestructura computacional
  La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- Los usuarios
  La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero la implementación de medidas de seguridad informática lógicas, físicas y de redes de datos aunado a la fomentación de una cultura de seguridad informática en los usuarios, evitan daños mayores y problemas que puede ocasionar algún intruso o los mismos usuarios.

1.1.1 Evolución histórica de la Seguridad Informática

Haciendo un breve recorrido por la historia de la informática se observa que conforme se va desarrollando la tecnología se van incrementando las necesidades de resguardar y proteger la información que es de importancia para las organizaciones. Cabe mencionar que el mismo concepto de delito informático ha cambiado a través de los años inicialmente consistía en un reconocimiento de “haberlo hecho” donde el transgresor buscaba ser reconocido como la persona que atacó un sitio sin sustraer información del mismo.

En ocasiones acorde al avance tecnológico van apareciendo amenazas que no se tenían contempladas. He aquí algunas fechas clave:

1958: EE.UU. crea ARPA (Advanced Research Projects Agency), ciencia y tecnología aplicada al campo militar.

1960: Los hackers originales utilizaron los primeros mainframes del MIT para desarrollar habilidades y explorar el potencial de la informática.

1969: La agencia de proyectos de investigación avanzados del Departamento de Defensa (DoD), construyó Arpanet.

1970: Captain Crunch y Phreaking telefónico. El "Creeper" es difundido por la red ARPANET. El virus mostraba el mensaje "SOY CREEPER…ATRAPAME SI PUEDES!". Ese mismo año es creado su antídoto: el antivirus Reaper cuya misión era buscar y destruir al Creeper.

1980: La red ARPANET es infectada por un "gusano" y queda 72 horas fuera de servicio. La infección fue originada por Robert Tappan Morris

1986: Aparecen virus que atacan el sector de arranque

1986: Aparecen virus que atacan archivos

1988: Se funda el CERT (Computer Emergency Response Team). Aparece el primer software antivirus, escrito por un desarrollador de Indonesia.

1989: Primer caso de ciberespionaje en Alemania Occidental. The Mentor lanza el manifiesto Conscience of a Hacker, que finaliza con una frase inquietante: "pueden detener a una persona, pero no pueden detenernos a todos"

1993: Aparecen Virus que atacan virus

1999: Nacimiento del software anti-hacking.

2000: Se producen ataques de denegación de servicio (DoS) sobre los grandes nombres de la Red.

2001: XP, el Windows más seguro, es crackeado antes de su lanzamiento.

2007: Se producen varios ataques phishing específicos contra entidades españolas especialmente agresivos a través de un kit que comprende a muchos bancos españoles.

2008: Se descubre una nueva forma de engañar a los servidores DNS para que den respuestas falsas, gracias a un fallo inherente del protocolo. Hasta ahora, no se han dado detalles técnicos sobre el problema.

Como se observa, algunas de las medidas de seguridad que son utilizadas hoy en día surgieron como respuesta a incidentes que no se tenían considerados o que se desarrollaron a la par de nuevas tecnologías, por ello es importante no descartar todas y cada una de las amenazas de las cuales pudiera ser presa nuestro sistema informático y mantener actualizados tanto a expertos en la materia como a usuarios que hagan uso de la información en una organización; "no hay mejor defensa que una buena preparación".

1.1.2 Objetivos y misión de la Seguridad Informática

Entre los principales objetivos de la seguridad informática se destacan los siguientes:

- Proteger los recursos de los sistemas informáticos, siendo prioritaria la protección a la información, pero abarcando también la infraestructura, y el uso de las aplicaciones, entre otros.
- Garantizar la adecuada utilización de los recursos y aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos en los contratos.

La misión de la seguridad informática se puede plantear como una serie de actividades específicas para una organización que le permitan alcanzar los objetivos de seguridad.

Entre las más importantes están las siguientes:

- Desarrollo e implantación de políticas de seguridad que estén relacionadas directamente con las actividades reales de una organización.
- Mejora constante de los sistemas de seguridad por medio de su monitoreo y análisis, así como la adquisición y actualización de tecnologías.
- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Capacitar al personal encargado de la seguridad del sistema para que cuenten con conocimientos actualizados para desempeñar su labor de manera más eficiente.
- Concienciar a los usuarios del sistema informático sobre la importancia de las políticas de seguridad impuestas.

1.2 Amenazas

Las amenazas son la concepción de un peligro latente o factor de riesgo que pueden causar alteraciones a la información de la organización ocasionándole pérdidas materiales, económicas, de información, y de prestigio. Las amenazas se consideran como exteriores a cualquier sistema, es posible establecer medidas para protegerse de las amenazas, pero prácticamente imposible controlarlas y menos aún eliminarlas. A continuación se presentan los principales tipos de amenazas a la información:

a) Factor humano

   Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos. Esta amenaza surge por descuidos, negligencia, inconformidad y susceptibilidad del ser humano a cambiar su comportamiento. Dentro de las amenazas principales se encuentran:

- Ingeniería Social, es la manipulación de la tendencia humana a la confianza, y el objetivo de la persona que ejerce esta acción es obtener la información necesaria para acceder a la información sensible de una persona u organización.

- Ingeniería Social Inversa, se realiza cuando el atacante suplanta a una persona que se encuentra en una posición con autoridad suficiente para que el usuario o la persona de menor rango proporcione la información necesaria para poder producir un ataque.

  Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados.

b) Hardware

   Se da la amenaza por fallas físicas que presenten en cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

c) Red de datos

   Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta. Cuando la red de comunicación no está disponible, pudiera ser ocasionada por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo (fallas dentro de la planeación). La extracción de la información es cuando un agente pudiera obtener información dentro de la red de comunicación; la amenaza más conocida es un ataque de sniffing en redes Ethernet.

d) Software

   Las amenazas de software incluyen posibles fallas dentro del software de un sistema operativo, software mal desarrollado, mal diseñado o mal implantado, además de que existe software de uso malicioso que representa una amenaza directa contra un sistema.

e) Desastres naturales

   Son eventos que tienen su origen en las fuerzas de la naturaleza. Estos desastres no sólo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al sistema incluso en un estado de inoperabilidad permanente. Este tipo de amenazas también incluye la falta de preparación.

1.3 Vulnerabilidades

Una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo es decir, representan las debilidades o aspectos atacables en el sistema informático. Se trata de una debilidad que puede ser explotada para violar la seguridad. Las vulnerabilidades son también variadas, y con base en esta definición se presentan 6 tipos de vulnerabilidades:

a) Física

La podemos encontrar en el edificio o en el entorno físico de los sistemas de información. Se le relaciona con la posibilidad de entrar o acceder físicamente al lugar donde se encuentra el sistema para robar, modificar o destruir el mismo. Esta vulnerabilidad se refiere al control de acceso físico al sistema.

b) Natural

Se refiere al grado en el que el sistema puede verse afectado por desastres naturales o ambientales. Las vulnerabilidades pueden ser: no disponer de reguladores, no-Breaks, plantas de energía eléctrica alterna; tener una mala instalación eléctrica en los equipos, en caso de rayos, fallas eléctricas o picos de alta potencia. Otra vulnerabilidad es no estar informado de las condiciones climatológicas locales al construir un centro de cómputo o para tomar medidas en determinado tiempo.

c) Hardware

El no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento del equipo. Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, pueden existir algunos sistemas que no cuenten con la herramienta o tarjeta para poder acceder a los mismos.

d) Software

Este tipo de vulnerabilidad incluye todos los errores de programación en el sistema u otros tipos de aplicaciones que permiten atacar al sistema operativo desde la red explotando la vulnerabilidad en el sistema. Hay que tomar en cuenta que no siempre los sistemas son los únicos que traen errores de programación, también los programas hechos por los usuarios son puntos débiles que se deben de cuidar.

e) Red

Este tipo de vulnerabilidad toma a consideración desde la implementación de un mal diseño del cableado estructurado que no es sujeto a estándares, hasta la modificación total o parcial de la interconexión y transmisión de datos entre dispositivos algunos ejemplos son:

- La facilidad que es el acceso no autorizado al sistema de información de manera externa.
- La intercepción y extracción de información.
- La saturación y disponibilidad de servicios dentro de la organización.

f) Humana

Ser vulnerable a la ingeniería social y a la ingeniería social inversa, el no tener el servicio técnico propio de confianza, mala comunicación con el personal, falta de capacitación a los usuarios para responder ante diferentes situaciones de riesgo, no tener un control de registros de entrada y salida de las personas que visitan el centro de cómputo, falta de credenciales que identifiquen al personal, no tener detectores de metales o no contar con algún tipo de sistema biométríco como: huella digital, verificación de voz o verificación de huellas dactilares.

1.4 Sistemas y Mecanismos de Protección

Una vez conocidas las vulnerabilidades y ataques a los que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto es responsabilidad de los administradores detectar, sugerir e implementar medidas que permitan asegurar el sistema informático.

1.4.1 Seguridad Física

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

La seguridad física se complementa con la seguridad lógica.

1.4.2 Seguridad Lógica

La seguridad lógica se refiere a controles lógicos dentro del software y se implementa mediante la construcción de contraseñas en diversos niveles del sistemas donde permita solo el acceso con base en niveles de seguridad de usuarios con permiso, con base en el sistema operativo que use como plataforma el sistema a implantarse, es posible considerar además a nivel código, algoritmos que generen claves para poder cifrar los archivos de contraseñas dentro del sistema lo cual permita mayor seguridad en un entorno de red. Algunos de los objetivos que plantea la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no tengan capacidad de modificar los programas ni los archivos que no correspondan.
- Asegurar que sean utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.4.3 Seguridad en Redes de Datos

La seguridad es más que evitar accesos no autorizados a los equipos y a sus datos. También incluye el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto de la red. En un entorno de red debe asegurarse la privacidad de los datos. No sólo es importante asegurar la información sensible para la organización, sino también, proteger las operaciones de la red de daños no intencionados o deliberados.

El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar el acceso a los datos por parte de usuarios o procesos autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad de los administradores asegurar que la red se mantenga fiable y segura.

1.4.4 Biometría

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.

Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. Sus aplicaciones abarcan un gran número de sectores: desde el acceso seguro a computadoras, redes, protección de archivos electrónicos, hasta el control horario y control de acceso físico a una sala de acceso restringido.

Por esta razón la definen como una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas, tratamientos de enfermedades y otros similares.

Capítulo II

Análisis de las Necesidades

En este capítulo se estudian los contenidos disponibles, se denotan las actividades realizadas, se examinan las herramientas necesarias y útiles para el proyecto y se definen los temas a tratar

2.1 Selección de conceptos

Para una mejor y mayor comprensión del concepto de seguridad informática aunados a las crecientes demandas de seguridad por parte de las organizaciones, es pertinente que los estudiantes de Ingeniería en Computación en el módulo de Redes y Seguridad cuenten con los conceptos presentes que deben ser reforzados durante su formación.

2.1.1 Repaso de conceptos básicos de redes de datos

En el presente proyecto fue importante revisar conceptos clave de Redes de Datos necesarios para las prácticas y tareas de este manual:

Revisión de conceptos básicos de redes basados en la bibliografía, apuntes y referencias digitales:

- Topologías físicas: estrella, anillo, bus y sus características
- Medios físicos de transmisión: par de cobre (UTP), fibra óptica, cable coaxial y frecuencias para transmisión inalámbrica
- Topologías lógicas: las topologías lógicas que se pueden implementar con cada medio físico de transmisión.
- Modelo OSI: características y funciones de las 7 capas del modelo
- Modelo TCP/IP: características y funciones de las 4 capas del modelo
- Comparación entre modelos OSI y TCP/IP: diferencias y correspondencia entre capas de cada modelo.
- Protocolos de TCP/IP: (para que sirven y su funcionamiento): IP, TCP, UDP, ICMP, ARP
- Protocolo Ethernet (funcionamiento, direcciones MAC)
- 3-way-handshake en TCP
- Estados de conexión en TCP (RFC 793): LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK,TIME-WAIT, CLOSED.
- Tipos de aplicaciones comunes sobre TCP/IP: FTP, SMTP, POP3, HTTP, SNMP, TELNET, etc.
- Dispositivos de comunicaciones, características y limitaciones: routers, switches, hubs, bridges, access points.
- Conceptos de ruteo (tablas de ruteo, propagación de la información de ruteo, y protocolos de ruteo)
- Redes inalámbricas 802.11a, 802.11b, 802.11g (características y diferencias entre ellas)

2.2 Elección de contenidos

Se hizo una revisión de los temarios de las asignaturas obligatorias contempladas en el módulo de Redes y Seguridad así como en las asignaturas de carácter optativo. Se encontraron coincidencias dentro del plan de estudios de cada asignatura siendo los principales temas:

- Conceptos básicos de redes
- Conocimientos básicos de LINUX (comandos y estructura del sistema operativo).
- Selección de mecanismos y herramientas de protección, para cuidar la seguridad informática en una organización de manera física y lógica.
- Conocimiento de mecanismos y herramientas que permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.

- Identificación y análisis de los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que los ocasionan.
- Selección y aplicación de técnicas y métodos que permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.
- Comprensión de la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.
- Ubicar las nuevas tendencias en ataques hacia sistemas y redes de cómputo, así como las nuevas tecnologías que puedan minimizar estas amenazas.
- Programación en lenguaje C y java.
- Funciones de los sockets y puertos como sus principales características y estándares.
- Diferentes tipos de sockets para difundir información mediante la red de datos.

Dada la diversidad de lenguajes y formas de programación vistos durante la carrera no se llegó a considerar la realización de una práctica que contenga elementos de programación; así mismo se toma como único requisito con carácter obligatorio el haber cursado la asignatura de Redes de Datos, con el fin de que el estudiante pueda manejar la mayoría de las herramientas usadas durante las prácticas.

2.3 Investigación Bibliográfica

Se consultó la bibliografía disponible en materia de seguridad informática que se encuentra disponible en publicaciones científicas, boletines de seguridad informática, libros en las bibliotecas de la Facultad de Ingeniería, material disponible en centros especializados, tales como la Dirección General de Servicios de Cómputo Académico (DGSCA) o en recursos digitales disponibles en la web.

Se revisó y buscaron libros relacionados, tomando aquellos con contenido referente al área de estudio de la seguridad informática, libros relacionados con:

- Seguridad en redes
- Criptografía
- Seguridad en aplicaciones
- Administración de la seguridad
- Hacking
- Biometría

Se buscó material digital relacionado con:

- Redes de telecomunicaciones
- Sistemas operativos Unix o derivados (Linux por ejemplo)
- Auditoría de sistemas
- Simuladores de redes
- Cómputo forense
- Biometría

2.4 Selección de Herramientas

Conscientes de que las herramientas tecnológicas permiten organizar, comunicar, investigar y ayudan a resolver problemas. La tecnología forma parte integral del proceso para resolver problemas de la seguridad en cómputo, por eso es importante adquirir las habilidades para el uso e implementación de nuevas tecnologías que nos permitan desarrollar mejor herramientas asertivas.

Esta parte es la directriz del manual ya que cada herramienta debe cumplir con un fin acorde al conocimiento a ilustrar, y en este sentido cabe destacar que adicionalmente deben ser acorde, a la capacidad de los equipos que se empleen, para que las herramientas no que sobrepasen la capacidad de los equipos disponibles.

2.4.1 Selección de Herramientas de Hardware

Se eligió una configuración común en los equipos utilizados en salas de cómputo como en laboratorios de la Facultad de Ingeniería:

- Procesador de Arquitectura x86 a 1.0 Ghz
- 1GB de memoria RAM DDR
- Disco duro de 80 GB
- Monitor
- Teclado
- Mouse

Asimismo se eligieron dispositivos externos extraíbles que dan apoyo a la realización de las prácticas tales como:

- GPS con interfaz USB compatible con el protocolo Nmea3
- Lector de huella digital externo
- Tarjeta wireless externa de 1 Watt
- Antena de 10 db de ganancia

Los Dispositivos recomendados son:

- *GPS USB GLOBALSAT ND-100 DONGLE*

Dispositivo compacto y portátil, que permite conectar el receptor GPS para el uso en su laptops, netbooks y dispositivos UMPC. No requiere batería adicional.

Especificaciones:

- Adopt SKYTraq Venus 6 chipset con 65-Channel
- Alta sensibilidad (to -160dBm)
- Tiempo de arranque: 29/1 sec.
- Compatible con NMEA 0183, NMEA0183 V3, GGA, GSA, GSV, RMC, AGPS, WAAS / EGNOS
- Conexión USB
- Dimensiones: 68 x 28 x 14mm
- Peso: 25g

- *Adaptador USB Wireless Alfa Network (awus036h) 54Mbps y antena desmontable de 9dBi*

Permite descubrir redes 802.11 b/g a distancia y con más potencia.

Especificaciones

- Chipset Realtek 8187L (RTL8187L)
- Estándar IEEE 802.11g/b
- Interfaz USB rev. 2.0 B-Type to A-Type
- Banda de Frecuencias 2.400GHz ~ 2.484GHz
- Modulación
  - IEEE 802.11g: OFDM(64-QAM, 16-QAM, QPSK, BPSK)
  - IEEE 802.11b: DSSS(CCK/DQPSK/DBPSK)
- Tasas de Transferencia:
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 & 6Mbps
  - 802.11b: 11, 5.5, 2 and 1 Mbps con auto-rate fall back
- Protocolo de Acceso: CSMA/CA
- Nº de Canales de trabajo:
  - 2.412~2.462GHz (Canadá, FCC) / 11 Canales
  - 2.412~2.484GHz (Japón, TELEC) / 14 Canales
  - 2.412~2.472GHz (Europa, ETSI) / 13 Canales
- Seguridad
  - 64/128bit WEP
  - WPA(TKIP con IEEE 802.1x)
  - WPA2(AES con IEEE 802.1x)
- Potencia de Salida (Típica)
  - 802.11g: hasta 24 ± 1 dBm.
  - 802.11b: hasta 30 ± 1 dBm.
- Sensibilidad
  - 73dBm @ 54 Mbps
  - 85dBm @ 11 Mbps
- Consumo de Energía: Transmisión/ Recepción: 290mA/240mA at 5VDC
- Antena: Una antena desmontable de 5dBi con conector RP-SMA
- Dimensiones (mm.): 95(Largo) x 59(Ancho) x 16(Alto) mm.(antena no incluida)
- Peso: 120g
- Temperatura de Funcionamiento: 0ºC ~ 60ºC Temperatura ambiente
- Humedad 10% ~ 90% (Sin condensación)
- Soporte de controladores: Windows 98SE, ME, 2000, XP 32/64, Vista y Windows 7 32/64 bits, Linux, Wifislax, Backtrack 3

Estas herramientas en conjunto con la paquetería empleada, muestran al estudiante el panorama de lo que es la seguridad informática de manera que sea distinguible el uso específico de cada una de ellas.

2.4.2 Selección de Herramientas de Software

- Microsoft Windows XP

  Es un sistema Operativo que ofrece una interfaz gráfica de usuario amigable, facilitando su uso por usuarios no ambientados. Este sistema operativo de carácter comercial es distribuido bajo una licencia que autoriza sólo el uso del software bajo ciertas condiciones (Microsoft CLUF). Este sistema operativo es actualmente el más popular debido a que muchos de los fabricantes de software en el mundo desarrollan sus productos orientados a esta plataforma.

  A continuación se enumeran algunas ventajas de este Sistema Operativo:

  - Windows dispone de una interfaz gráfica que facilita el manejo de los procedimientos.
  - Es el SO más comercial por lo que dispone de más aplicaciones y mantenimiento.
  - La curva de aprendizaje en el sistema Windows es mucho menor.
  - Los Servicios de actualización de software (SUS) de Microsoft ayuda a los administradores a automatizar las actualizaciones del sistema más recientes.
  - Microsoft ha mejorado a lo largo del tiempo en gran cantidad sus productos y así ha aumentado considerablemente su desempeño en ambientes de red.

  Las desventajas de Windows son las siguientes:

  - Software propietario es decir que la empresa es “propietaria” de los códigos fuente del sistema y sólo ella es capaz de modificar al Sistema Operativo, el usuario sólo tiene permitida la instalación del programa en su máquina.
  - El costo de licencias de Windows es muy elevado por lo que en ocasiones resulta más atractivo desde un punto de vista económico

- AudioBlast

  Es un editor de audio de carácter básico, tiene soporte para archivos en formato WAV, y además puede exportarlos a MP3. Emplea operaciones básicas con archivos de sonido: seleccionar, copiar, cortar, pegar, aplicar filtros, efectos sonoros; edición de parámetros como la velocidad, los tonos, ecualizadores. Permite mezclar varios archivos. AudioBlast realiza diversas funciones de edición al alcance del usuario, en un programa accesible, ligero y de uso gratuito

- Fequency Analizer

  Es un programa que emplea la transformada rápida de Fourier para descomponer en funciones senoidales una señal análoga como es la voz humana la versatilidad de este programa y su licencia libre lo hacen una herramienta muy útil.

- WinRAR

  Es un potente programa compresor y descompresor de datos multi-función, también permite el cifrado de datos empleando el algoritmo AES, Winrar usa también una función de hash especialmente lenta para ralentizar al máximo los intentos de descubrir la contraseña mediante ataques de fuerza bruta que son actualmente la única forma de descubrir una contraseña para archivos con cifrado AES.

Esto lo hace especialmente seguro, incluso mucho más que otros compresores que usan claves de 256 bits, por ejemplo, un ataque a un fichero ZIP cifrado con AES-256 es 10 veces más rápido en las mismas condiciones que el mismo ataque a un fichero RAR cifrado con AES-128.

- GPG4WIN

  Es una herramienta de software libre que permite codificar archivos y correos electrónicos mediante el empleo de un sistema de claves públicas y privadas. El algoritmo de codificación que emplea este programa también es libre y se denomina 'GNU Privacy Guard', la alternativa de código abierto a los sistemas de codificación patentados.

- Wireshark

  Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

  Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

  Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

- Uso del Sistema Operativo Linux Fedora

  Es un sistema Operativo que se ha desarrollado bajo la filosofía del software libre, garantizando ciertas libertades a sus usuarios. Aunque su entorno original era altamente especializado (informática y entornos científicos), con el tiempo se ha desarrollado lo suficiente como para llegar a ser una alternativa viable en entornos domésticos o empresariales donde la interfaz gráfica de usuario y facilidad de uso es altamente valorada. Pese a ello, aún hay muchas aplicaciones de uso especializado pero de amplia demanda (tratamiento de audio, imágenes y aplicaciones de gestión, entre otras) que no han sido desarrolladas para Linux o bien, no existe un símil para esta plataforma. GNU/Linux se distribuye bajo la licencia GNU GPL (GNU General Public License), en la mayoría de sus distribuciones.

  A continuación se describen las principales ventajas de este Sistema Operativo:

  - Está inspirado en Unix, por lo que tanto su gestión de recursos del sistema como la orientación cliente/servidor y multitarea/multiusuario hacen de él un sistema robusto, estable y rápido.
  - Se distribuye bajo licencia GNU GPL, lo que garantiza la libre copia y distribución tanto del software en sí como de su código fuente, permitiendo además su modificación bajo ciertas condiciones como respetar la autoría del programa original.
  - Fue desarrollado desde un comienzo en y para un ambiente de red, por lo que los módulos de protocolos de red forman parte del núcleo del sistema, otorgando un excelente desempeño en ambientes de red.

- Existe gran cantidad de documentación acerca de los programas que componen el sistema, tanto en Internet como en el propio sistema.
- Las principales distribuciones de GNU/Linux (Debian, Suze, CentOS, Fedora) incorporan sistemas de descarga de aplicaciones que facilitan la instalación y actualización de software en el sistema en forma semiautomática.
- Existen distribuciones comerciales de Linux, tales como Suze y RHEL que ofrecen soporte al usuario final.
- GNU/Linux ya no está restringido a personas con grandes conocimientos de informática: Los desarrolladores han hecho un gran esfuerzo por dotar a este sistema de asistentes de configuración y ayuda, además de un sistema gráfico muy potente. Las principales distribuciones de GNU/Linux como Red Hat/Fedora tienen aplicaciones de configuración similares a las de Windows.

- Cisco Packet Tracer

  Es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y estudiantes de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA. Este producto tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando – línea de los dispositivos de Cisco para práctica y aprender por descubrimiento.

  Packet Tracer 5.3.1 es la última versión del simulador de redes de Cisco Systems, herramienta fundamental si el estudiante está cursando CCNA o se dedica al networking.

- VMware. (VM de *Virtual Machine*)

  Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un ordenador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un ordenador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

  Un virtualizador por software permite ejecutar (simular) varios ordenadores (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. No obstante, y al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.

  VMware es similar a su homólogo Virtual PC, aunque existen diferencias entre ambos que afectan a la forma en la que el software interactúa con el sistema físico. El rendimiento del sistema virtual varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales como CPUy RAM, asignados al sistema virtual.

- Zenmap
  Es una herramienta de escaneos de redes muy profunda como la conocida nmap, pero con una agradable interfaz gráfica. Este programa utiliza protocolos como el UDP y TCP. Nmap es una herramienta para escanear redes, ya sea escanear puertos a través de un dominio web o una direccíon IP.

- Nessus
  Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

- Hamachi
  Es una aplicación gratuita (freeware) configuradora de redes privadas virtuales capaz de establecer vínculos directos entre computadoras que están bajo firewalls de NAT sin requerir reconfiguración alguna (en la mayoría de los casos). En otras palabras, establece una conexión a través de Internet y simula una red de área local formada por ordenadores remotos. Actualmente está disponible la versión para Microsoft Windows y la versión beta para Mac OS X y Linux.

  Hamachi es un sistema VPN de administración redondeada que consiste en un cluster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios.

- Dropbpox
  Se trata de un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox. El servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre computadoras y compartir archivos y carpetas con otros. Existen versiones gratuitas y de pago, cada una de las cuales con opciones variadas.

- NetStumbler
  Es un programa para Windows que permite detectar redes inalámbricas (WLAN) usando estándares 802.11a, 802.11b y 802.11g. No sólo se reduce a detectarlas, sino que nos muestra una gran cantidad de información al respecto como el SSID (nombre de la red), el canal por el que emite, la velocidad, el tipo de encriptación e incluso la MAC del punto de acceso y el fabricante.

  La utilidad es máxima, sobre todo para personas que trabajen a menudo con redes inalámbricas y está orientado a la resolución de problemas, localización de interferencias incluso la intrusión de puntos de acceso no autorizados en nuestro rango.

- EarthStumbler
  Es un programa para importar la información marcada con GPS del Netstumbler y visualizarla gráficamente en Google Earth.

- Google Earth
  Es un programa informático similar a un Sistema de Información Geográfica (SIG), que permite visualizar imágenes en 3D del planeta, combinando imágenes de satélite, mapas y el motor de búsqueda de Google que permite ver imágenes a escala de un lugar específico del planeta.

2.4.3 Otras Herramientas

Internet
Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. El uso de este recurso se basa principalmente en la disponibilidad y difusión que permite indistintamente a cualquier usuario compartir información a nivel mundial.

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como:

- CERT/CC (Computer Emergency Response Team Coordination Center) del SEI (Software Engineering Institute) de la Carnegie Mellon University.
  El cual es un prestigioso organismo dependiente de la Universidad Carnegie Mellon de referencia obligada en el terreno de publicación de vulnerabilidades e incidencias en el terreno de la seguridad informática, centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.
  http://www.cert.org/

- Common Criteria
  Es, a pesar de lo polémico y discutido de la certificación obtenida por Windows 2000 en el año 2002, uno de los organismos más prestigiosos en lo tocante a certificaciones de seguridad.
  http://www.commoncriteria.org/

- SANS Institute [SANS (SysAdmin, Audit, Network, Security)]
  Fue fundado en 1989 como un órgano educativo e investigador. Desde entonces hasta nuestros días se ha convertido en el principal punto de referencia dentro de la Seguridad Informática.
  http://www.sans.org/

- CIS, (The Center for Internet Security)
  Organismo dedicado a proporcionar herramientas y métodos para mejorar la seguridad y las prácticas encaminadas a conseguirla.
  http://www.cisecurity.org/

- Security Focus
  Otro de los más prestigiosos organismos dedicados a la seguridad. Particularmente famosa (y útil) es Bugtraq, una lista de correo sobre vulnerabilidades. En agosto de 2002 se anunció su compra por parte de Symantec. Esperemos que no haga cambiar la eficacia de la empresa ni la independencia de sus informes.
  http://www.securityfocus.com/

- Open Source Vulnerability Database
  Base de datos dedicada en exclusiva a la recopilación e información de incidencias de seguridad en código de fuente abierta.
  http://www.osvdb.org/

- ESCERT
  Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas de la Universidad Politécnica de Cataluña.
  http://escert.upc.es/

En México

- UNAM-CERT(Equipo de Respuesta a Incidentes de Seguridad en Cómputo)
  Es un equipo de profesionales en seguridad en cómputo. Está localizado en la Subdirección de Seguridad de la Información (SSI) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, de la UNAM.

  El UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.
  http://www.cert.org.mx/index.html

Capítulo III

Manual de Prácticas

Se presenta la Propuesta del trabajo realizado, el cual está compuesto de 12 prácticas.

3.1 Estructura y desarrollo de las prácticas

Con el fin de garantizar que el alumno perciba las necesidades de seguridad, la protección de las redes y de la información crítica donde ejerza su profesión, en primer lugar debe encontrarse en situaciones que se asemejen a la realidad, por ende se crean escenarios que lo familiaricen con las crecientes amenazas de seguridad.

Es necesario que el alumno se encuentre en un entorno de trabajo en el que de forma segura y práctica se garantice que pueda modificar, analizar y proceder a la ejecución de las herramientas de análisis para el mejoramiento de su formación; dentro de los principales puntos a cubrir están:

- Recolección de los datos
- Entorno del análisis –Descripción de las herramientas–
- Análisis de la evidencia –Información del sistema analizado–
- Aplicaciones
- Servicios
- Vulnerabilidades
- Metodología
- Descripción de los hallazgos
- Herramientas usadas
- Análisis de artefactos
- Conclusiones
- Recomendaciones específicas
- Referencias

Tomando en cuenta la duración de un semestre promedio, se ha planeado para la aplicación de las prácticas durante un lapso de catorce semanas esto con el fin de que no se vea afectado su desarrollo por cambios y ajustes en el calendario escolar.

La estructura básica consiste de una parte introductoria donde se describen los objetivos a alcanzar, después el marco teórico donde quedan definidos los conceptos que emplearemos, algunas preguntas sencillas deberán ser contestadas por el alumno, éstas tienen el fin de brindar una introducción al tema de estudio, después continúa con la descripción de las herramientas físicas y de hardware a emplear, posteriormente la parte de los ejercicios que el alumno debe realizar con preguntas que se van contestando conforme al avance de la práctica.

Finalmente, al término de la práctica el alumno debe escribir una reseña o conclusión para confirmar que tanto los objetivos de la práctica se cumplieron así como los conocimientos fueron adquiridos satisfactoriamente.

3.2 Práctica de laboratorio # 1 - Dispositivos Biométricos

Objetivos de aprendizaje

- El alumno obtendrá muestras biométricas
- Realizará comparativas entre las muestras obtenidas
- Comprenderá la diferencia entre dispositivos biométricos

Introducción

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas, mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo. La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

Identificación por huellas dactilares

Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones.

Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

Son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

Clasificación

La clasificación es útil al momento de la verificación en la identificación electrónica, ya que el sistema sólo busca en la base de datos del grupo correspondiente. Figura 3.1

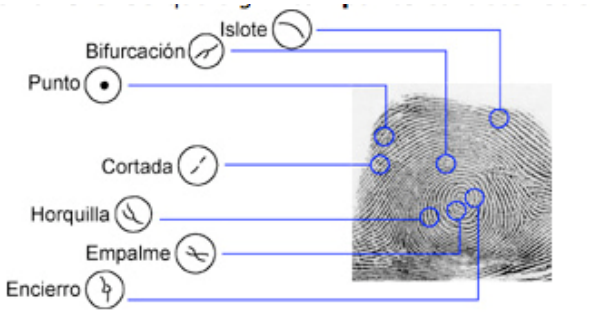


Figura 3.1 Puntos Característicos

En la figura 1 aparecen 8 puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 (por ejemplo 10 orquillas 12 empalmes 15 islotes, etc.). A estos puntos también se les llama minutae, o minucias, término utilizado en la medicina forense que significa "punto característico".

Procedimiento

Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones, según se muestra en el ejemplo. Para ello, la ubicación de cada punto característico o minucia se representa mediante una combinación de números (x,y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible. Para llevar a cabo el proceso inverso o verificación dactilar, se utilizan estos mismos vectores, no imágenes Tabla 3.1

			
El dedo es leído por un lector de huellas.	El dedo es codificado.	Una plantilla matemática es generada.	Se guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

Tabla 3.1 Secuencia de pasos para la verificación Dactilar

Dispositivo para identificación

Para tratar los datos de la huella se utiliza un algoritmo que permite asociar la huella que se desea identificar, con otras de características similares almacenadas en la base de datos.

Existen dos maneras distintas de usar los datos de una huella.

1. Verificación ¿Es la persona quien dice ser?

Se suele pedir un código, una lectura de tarjeta y comparar esa huella almacenada con la huella puesta en el lector, la verificación es un proceso un poco más molesto porque se le pide una información o una acción adicional al usuario, pero como ventaja tiene que es más rápido y más seguro.

2. Identificación. ¿Quién es la persona?

En este proceso directamente se compara una huella capturada contra todas las que están almacenadas en el ordenador, es un proceso algo más lento, pero la interacción con el usuario es mínima.

Es importante remarcar que algunos lectores, no guardan la imagen de la huella, solo almacenan los datos matemáticos explicados anteriormente.

Para comparar huellas se utilizan algoritmos y fórmulas matemáticas que basándose en las bifurcaciones y terminaciones de líneas de cada huella resultan en una serie de "marcadores" en posiciones clave. Además, casi siempre se realizan análisis parciales ya que no es necesaria tanta información como contiene una huella completa para iniciar la comparación.

Para dar un resultado "positivo" el escáner no tiene que encontrar el patrón completo de la huella, simplemente basta con que encuentre el número de marcadores suficiente. El número de marcadores está determinado por el escáner, cuanto más costoso sea, más preciso será.

Defina Dactiloscopia

_____

_____

_____

RECONOCIMIENTO DE VOZ

El reconocimiento por voz, es una modalidad biométrica que utiliza la voz de un individuo con fines de reconocimiento. (Difiere de la tecnología del "reconocimiento de discurso", que reconoce las palabras a medida que van siendo articuladas, éste no es un dispositivo biométrico). El uso de la voz es muy utilizado para reconocimiento biométrico remoto, dada la disponibilidad de dispositivos para tomar las muestras de voz (por ejemplo: la red telefónica y los micrófonos de las computadoras) y su facilidad de integración.

El proceso de reconocimiento de voz depende de las características de la estructura física del tracto vocal de un individuo que consiste de una vía respiratoria y cavidades de tejido blando de donde se originan los sonidos vocales. Para producir sonidos estos componentes trabajan en combinación con los movimientos físicos de la quijada, lengua, laringe y las resonancias de los pasajes nasales.

Las características acústicas del habla provienen de los atributos físicos de las vías respiratorias. El movimiento de la boca y de las pronunciaciones son los componentes de comportamiento para el habla. Las muestras de voz son ondas donde la variable del tiempo se ubica en el vector horizontal y la de volumen en el vertical. El sistema de reconocimiento de quien habla analiza el contenido de frecuencia del discurso y compara las características de calidad, duración, intensidad, dinámica y tono de la señal. Figura 3.2

Figura 3.2 Algoritmo de reconocimiento de voz

La fácil implementación del reconocimiento por voz contribuye con su mayor debilidad: la susceptibilidad al canal de transmisión y a las variaciones del micrófono y su ruido. Los sistemas también pueden enfrentar problemas cuando los usuarios han ingresado una muestra en una línea fija limpia e intentan la verificación contra una muestra tomada de una línea celular con ruido. La incapacidad de controlar los factores que afectan a las entradas puede disminuir el desempeño significativamente.

Los sistemas de verificación de voz, exceptuando a los que utilizan frases dadas, son susceptibles de ataques por spoofing a través de la utilización de una voz grabada.

Desarrollo

Equipo Necesario

Hardware

1 Micrófono
2 Lectores de huella Digital
1 Computadora o Laptop

Software

Microsoft Windows 7
Audioblast
Frequency Analyzer v2.0

Otros Elementos

Diurex
Talco
1 Hoja de acetato tamaño carta
Tinta de color Negro
1 tapa bocas
1 grabadora de voz
Violeta de Genciana
Bote de 1 L de capacidad

Primera Parte Huella Digital

Se dividirá el grupo en dos equipos, cada uno de ellos se le asignará una computadora con un lector de huella. Cada equipo deberá registrar el dedo índice de un individuo para el inicio de sesión **sin permitir** que el otro equipo sepa la identidad del usuario registrado

A continuación cada equipo deberá recolectar la huella de cada uno de los miembros del otro equipo con el fin de iniciar sesión en el equipo protegido con huella digital

Cada equipo deberá usar las siguientes metodologías. (Se recomienda subdividir el quipo en brigadas para realizar la tarea)

- Método 1
  Usando diurex se cortará un trozo de unos 4cm donde se colocará el dedo índice, después cuidadosamente retire la cinta y esparza uniformemente talco, una vez revelada la huella colóquela sobre el sensor.

- Método 2
  Entinte el dedo índice y colóquelo sobre la hoja de acetato, espere a que seque y coloque la hoja sobre el sensor.

- Método 3
  Usando diurex se cortará un trozo de unos 15cm donde se colocarán los dedos índices de los miembros del otro equipo, salga del laboratorio, en un lavabo coloque el bote y vierta en una porción de 50% agua y Violeta de Genciana, mezcle hasta obtener una solución, sumerja la tira de diurex en la solución, remueva el exceso de la solución que se quedó en el diurex con agua en caso de no verse claramente las huellas sumerja de nuevo en la solución, espere a que seque y regrese al laboratorio a realizar la prueba.

Mencione por lo menos 2 formas diferentes de obtener una huella digital

_____

_____

_____

¿Qué tan difícil es la obtención de huellas de una persona, sin que ésta lo sepa? Explique sus razones.

_____

_____

_____

Parte 2 – Voz Humana

Se conformarán equipos de 2 personas.

1. Uno de los miembros de cada equipo grabará una palabra o frase con el grabador de voz

2. Conecte el Micrófono en el conector respectivo (USB o 3.5 mm) y abra la Grabadora de Sonido de Windows.
Figura 3.3

Figura 3.3 Grabadora de Sonidos

Realizaremos 3 grabaciones:

1. La primera diciendo la misma palabra u oración grabada previamente
2. Para la segunda grabación nos colocaremos un tapabocas y repetiremos la misma palabra u oración
3. Reproduciremos la muestra de audio guardada en el grabador de voz y la colocamos en el micrófono

3. Cada grabación se deberá guardar en un archivo individual y deberá almacenarse de la siguiente manera:

1. Seleccionamos el menú Archivo
2. Seleccionamos la opción Guardar como
3. Presionamos el botón cambiar.
4. Seleccionamos en la sección de atributos 48.000KHz, 16 bit, Estéreo 187 Kb/s. Figura 3.4

Figura 3.4 Selección de Formato

5. Etiquetamos cada archivo con nombre referente a su obtención

1. Iniciamos la instalación del programa Audioblast (La aplicación se encuentra en el escritorio).Una vez terminada la instalación ejecutamos el programa

2. Al iniciar la aplicación deberemos abrir las grabaciones previamente hechas, esto lo podemos hacer presionando el botón de **open**. Figura 3.5

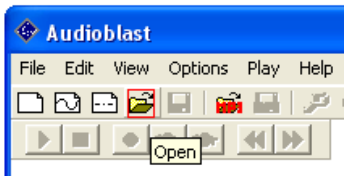


Figura 3.5 Botón de OPEN

3. Aparecerá un cuadro de dialogo donde seleccionaremos la grabación respectiva y daremos click en abrir.

4. Una vez abierto el archivo lo comenzará a reproducir, en esta parte podemos apreciar la gráfica de la grabación a través del tiempo, esta gráfica la importaremos seleccionando el menú **VIEW** y la opción SAVE GRAPHIC AS BMP. Figura 3.6

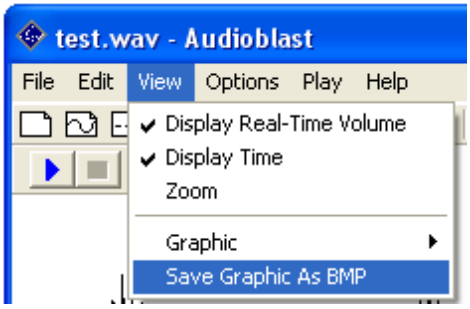


Figura 3.6 Importación de grafica de audio

5. Aparecerá un cuadro de diálogo donde guardaremos la imagen, es importante guardar la imagen con nombres aledaños a la grabación y en una carpeta de fácil acceso.

6. Repita los pasos 5,6,8 y 9 para cada una de las grabaciones

7. Inicie la aplicación de Paint

8. Abra el archivo de la gráfica de la primera grabación.

9. Cambie el color de la gráfica a otro diferente.

10. Abra otra instancia de Paint

11. Abra el archivo de la gráfica de la segunda grabación.

12. Seleccione toda la imagen presionando Ctrl + e.

13. Corte la imagen presionado Ctrl + x

14. Pase a la ventana de la gráfica de la primera grabación. Y seleccione la opción de fondo transparente. Figura 3.7

Figura 3.7 Selección de Fondo Transparente

15. El resultado pudiera semejarse a lo siguiente. Figura 3.8

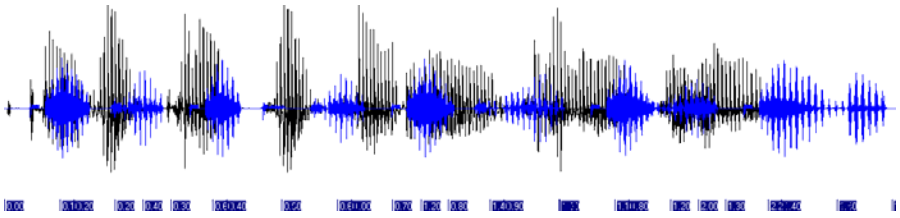


Figura 3.8 Gráficas sobrepuestas

Anote sus observaciones

_____

_____

_____

_____

_____

1. De la misma forma sobreponga la gráfica obtenida de la tercera grabación

Mencione 4 diferencias que encuentre

_____

_____

_____

_____

_____

Algunos sensores de voz solo trabajan ubicando el rango de la amplitud de la voz.

2. Inicie desde el escritorio la aplicación del ícono Fequency Analizer. Figura 3.9

Figura 3.9 Analizador de frecuencias

3. Una vez iniciada la aplicación nos mostrará una pantalla como ésta. Figura 3.10

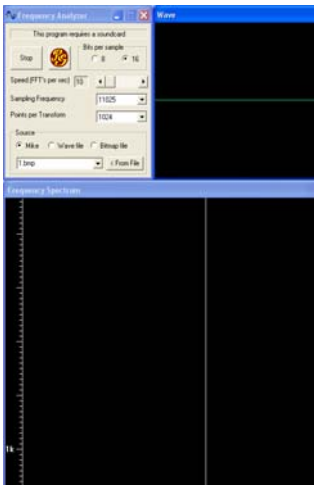


Figura 3.10 Ventana de Fequency Analizer.

4. Seleccionamos la opción de Wave file, abrimos una de las grabaciones realizadas. Figura 3.11

Figura 3.11 Selección de fuente

Fequency Analizer es un programa que utiliza la FFT(Fast Fourier Transform), un proceso matemático que transforma una señal en sus componentes espectrales. Algunas medidas requieren que se preserve la información completa de señal - frecuencia y fase este tipo de análisis se llama vectorial

Dado que el sonido cambia generalmente con el tiempo, la transformada de Fourier se calcula muchas veces por segundo. Es posible ajustar este parámetro a través de la Velocidad (FFT por segundo).

Para interpretar el panel principal del analizador de frecuencia observemos lo siguiente: Hay una línea vertical blanca moviéndose de izquierda a derecha. Se deja atrás un rastro de colores. Los colores corresponden a las intensidades de los distintos componentes del sonido.

Un caso práctico para el Fequency Analizer es usando el micrófono para decir "aaah", se pueden encontrar varias líneas horizontales que corresponden a los armónicos de la voz

Ejercicios

Elabore un mapa mental donde muestre las fortalezas, debilidades e implementaciones de los dispositivos biométricos (utilice por lo menos 4 biométricos diferentes)

1) ¿Qué biométrico considera el más seguro y porqué?

_____
_____
_____

2) ¿El uso de dispositivos Biométricos para el control de acceso es una inversión o un gasto? Fundamente su respuesta.

_____
_____
_____
_____
_____

3) Anote la importancia de cuidar la información biométrica que se pudiera dejar en un área de trabajo.

_____
_____
_____
_____
_____

4) Anote sus conclusiones

_____
_____
_____
_____
_____

3.3 Práctica de laboratorio # 2 - CIFRADO SIMÉTRICO Y ASIMÉTRICO

Objetivo

- El alumno comprenderá las diferencias entre el cifrado simétrico y asimétrico
- Aprenderá a realizar las tareas más sencillas en el manejo de GPG4win
- Usarlo para cifrar y descifrar un documento
- Intercambiar correo cifrado con un compañero
- Generar un par clave pública/privada
- Distribuir nuestra clave pública

Introducción

Los seres humanos siempre han sentido la necesidad de ocultar información, mucho antes de que existieran los primeros equipos de cómputo y calculadoras.

Desde su creación, Internet ha evolucionado hasta convertirse en una herramienta esencial de la comunicación. Sin embargo, esta comunicación implica un número creciente de problemas estratégicos relacionados con las actividades de las empresas en la Web. Las transacciones que se realizan a través de la red pueden ser interceptadas y, sobretodo, porque actualmente resulta difícil establecer una legislación sobre Internet. La seguridad de esta información debe garantizarse: éste es el papel de la criptografía.

¿Qué es la criptografía?

_____
_____
_____
_____
_____
_____

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, también llamado mensaje en claro, texto plano o texto simple.
- asegurarse de que para el receptor sea fácil descifrarlos y para un atacante prácticamente imposible descriptarlos.

El hecho de codificar un mensaje con la firme intención de que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado**.**

El cifrado normalmente se realiza mediante una *clave de cifrado* y el descifrado requiere una *clave de descifrado*. Las claves generalmente se dividen en dos tipos, descríbalos brevemente:

- *Las claves simétricas*:

_____
_____
_____

Las claves asimétricas:

_____
_____
_____

La criptografía se usa tradicionalmente para ocultar mensajes de ciertos usuarios. En la actualidad, esta función es incluso más útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Desarrollo

Equipo Necesario

Hardware

1 Computadora con arquitectura X86

Software

Winrar
GPG4win

Instalación:

Al abrir la aplicación, nos encontramos con la siguiente pantalla inicial (Figura 3.12)

Figura 3.12 Ventana de instalación de winrar

En la misma, podemos modificar el directorio en el cual queremos que se instale el WinRar. Por defecto, utiliza el disco sobre el cual se encuentra instalado Windows, que por defecto es C. Hacemos click en Instalar y veremos el rápido proceso de instalación.

Al finalizar, aparecerá la posibilidad de elegir a cuál/cuáles extensiones queremos que **WinRar** se integre. Si no existe algún otro programa de compresión simplemente dejamos las opciones que vienen por defecto.

Finalmente terminamos la instalación de winrar

Compresión de un documento

1 Creamos un nuevo documento de texto nuevo y escribimos la palabra mensaje.

2 Guardamos el archivo y con el botón derecho del mouse seleccionamos el archivo y elegimos la opción Añadir a Nuevo documento de texto.rar.

3 Una vez creado el nuevo archivo presionamos el botón derecho nuevamente y seleccionamos la opción **abrir con** y seleccionamos el bloc de notas.

Nótese al abrir que veremos el nombre e incluso el contenido en claro de nuestro archivo que comprimimos Figura 3.13

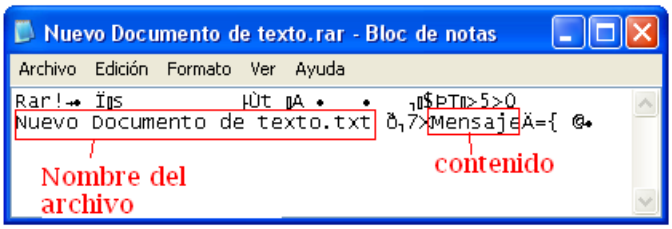


Figura 3.13 Contenido del fichero comprimido

4 Ahora con el botón derecho seleccionamos nuestro archivo original y elegimos la opcion **Añadir al archivo…** aparecerá un recuadro como el siguiente: (Figura 3.14).

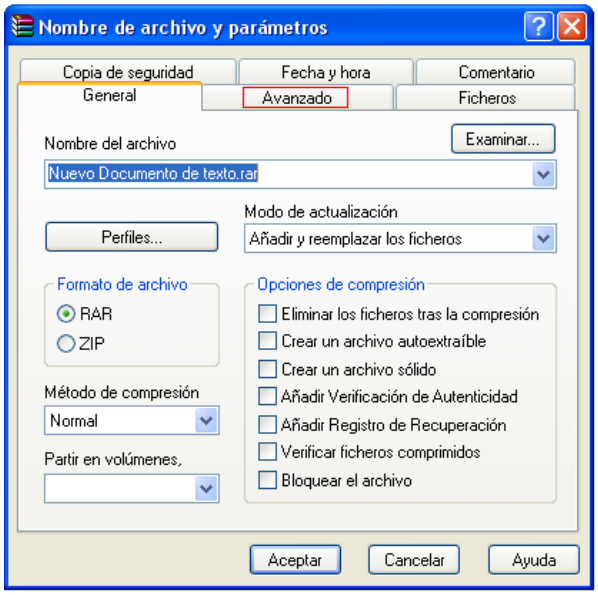


Figura 3.14 Opciones de Winrar

En la pestaña de avanzado presionaremos el botón de **Establecer contraseña** e insertaremos una, dejamos habilitada la opción **codificar nombres de fichero** y presionamos el botón de aceptar.

3 Una vez creado el nuevo archivo presionamos el botón derecho nuevamente y seleccionamos la opción **abrir con** y seleccionamos el bloc de notas.

Observe como el contenido de nuestro archivo comprimido es diferente a cuando no establecimos una contraseña y de que éste **NO** tiene datos en claro Figura 3.15

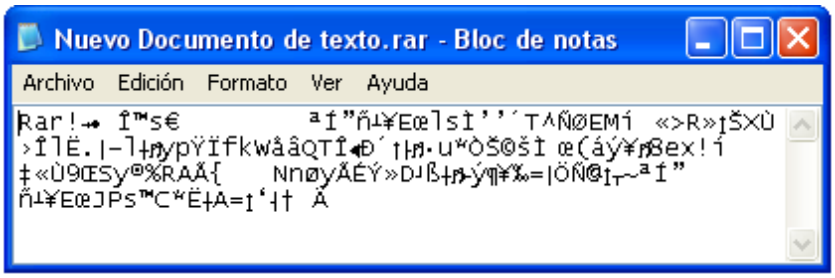


Figura 3.15 Contenido del archivo cifrado comprimido

WinRAR usa el algoritmo de cifrado AES, actualmente considerado el más seguro, con una longitud de clave de 128 bits .

Describa el proceso de cifrado de algoritmo AES, mencione a qué algoritmo sustituyó y las ventajas de su uso actual.

_____

_____

_____

_____

_____

Instalación GPG

Seleccionamos el idioma de la instalación. Figura 3.16

Figura 3.16 Selección de idioma

Presionamos el botón de siguiente. Figura 3.17

Figura 3.17 Pantalla de instalación

Aceptamos el contrato de licencia Figura 3.18

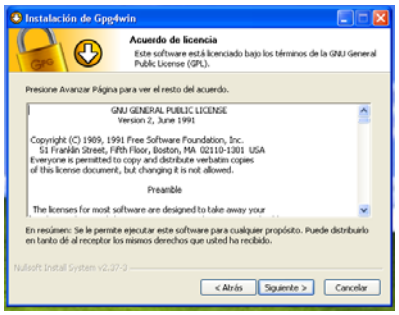


Figura 3.18 Términos de la licencia GPL

Seleccionamos las opciones a instalar Figura 3.19

Figura 3.19 Selección de componentes

Elegimos el directorio destino para la instalación Figura 3.20

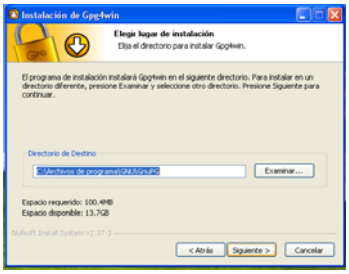


Figura 3.20 Directorio de Instalación

Seleccionamos los accesos directos que emplearemos Figura3.21

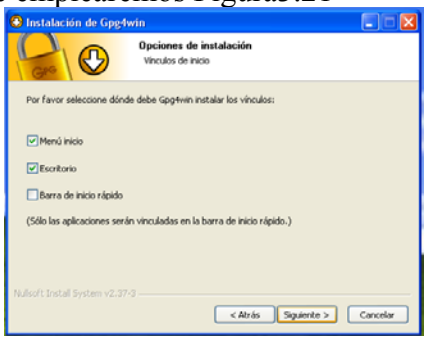


Figura 3.21 Selección de Accesos Directos

Elegimos el menú donde queremos colocar la aplicación Figura 3.22

Figura 3.22 Carpeta de menú de inicio

Completamos la instalación Figura3.23

Figura 3.23 Instalación Completada

1. **Ejecutar gpg**

Al iniciar gpg4win nos deberá aparecer el siguiente recuadro, el cual nos dice que aún no tenemos ningún par de llaves creadas en nuestro equipo, y nos brinda la opción de crear un par de llaves, en nuestro caso damos click en generate key (ya que no poseemos el par de llaves, en caso contrario *do in later*). Figura 3.24

Figura 3.24 Pantalla de inicio Gpg4win

Nos debe aparecer el siguiente cuadro, en el cual debemos indicar como se va a llamar el par de llaves a crear Damos click en forward. Figura3.25

Figura 3.25 Nombre de la nueva llave

Posteriormente nos pedirá el correo, el cual es el que nos va a identificar de otras llaves que lleven el mismo nombre de la nuestra. Y es el lugar donde llegarán nuestros mensajes codificados. Presionamos click en forward. Figura3.26

Figura 3.26 Ingreso de dirección de email

Ahora nos pedirá una contraseña, para nuestro par de llaves. Después de copiada nuestra contraseña damos click en forward. Figura 3.27

Figura 3.27 Ingreso de contraseña

Ahora nos advierte acerca de si estamos seguros en utilizar la contraseña anteriormente escrita por nosotros, damos click en *Take this one*, si estamos seguros de utilizar dicha contraseña, en caso contrario presionamos Enter new password si deseamos cambiarla. Figura 3.28

Figura 3.28 Comprobación de contraseña

Luego nos consulta si queremos crear una copia de seguridad a nuestras llaves, damos en *apply* para crear nuestra respectiva copia.

NOTA:
No se nos olvide que después de pasar esta copia a un medio más confiable (una memoria USB por ejemplo) es necesario eliminarla del sistema en el cual fueron creadas las llaves. Esto por seguridad, en especial la llave privada. Figura3.29

Figura 3.29 Creación de copia de respaldo de la llave

Después de dar Apply nos muestra el proceso de creación del par de llaves. Figura 3.30

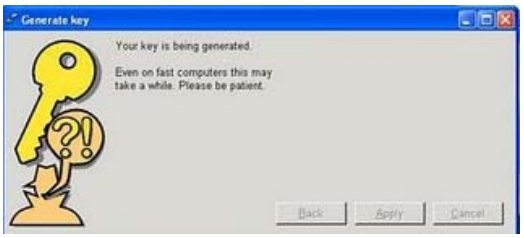


Figura 3.30 Creación Satisfactoria de llave

Terminado el proceso de creación de llaves, nos aparecerá un cuadro de diálogo el cual nos pregunta la ruta y el nombre en el cual será creada la copia de seguridad del par de llaves en nuestro sistema. Figura 3.31

Figura 3.31 Archivo de respaldo de la llave

Listo, ya se creó nuestro par de llaves y su respectiva copia la cual guardaremos en nuestro sistema o en otro medio mucho más confiable en especial la llave privada que es la que nadie pero absolutamente nadie debe saber, finalmente presionamos el botón de close.

Cifrado de Texto plano

Vamos a empezar por el *cifrado de un texto plano.* En la ventana de GNU Privacy, oprime el botón Clipboard (Portapapeles). Figura 3.32

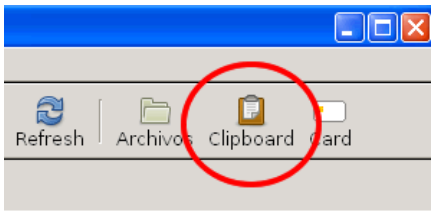


Figura 3.32 Portapapeles

Esta opción abre la ventana de portapapeles, a través de esta ventana, se puede digitar o pegar un texto, no importa la cantidad de caracteres a ingresar, una vez que termine de escribir el texto, debe oprimir el botón **Encryp** (Cifrar). Figura 3.33

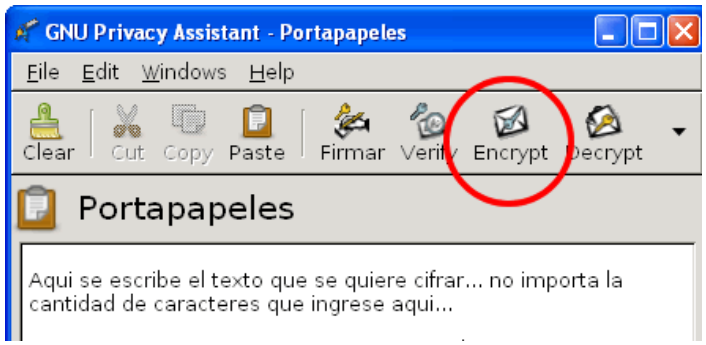


Figura 3.33 Opción de Cifrado

Como estamos cifrando un archivo para uso propio, y al oprimir el botón **Encryp** (Cifrar), se visualizan las llaves o claves que tengamos, en este caso sólo existe la que acabamos de crear.
Seleccionamos nuestra llave y luego click en **OK**. Figura 3.34

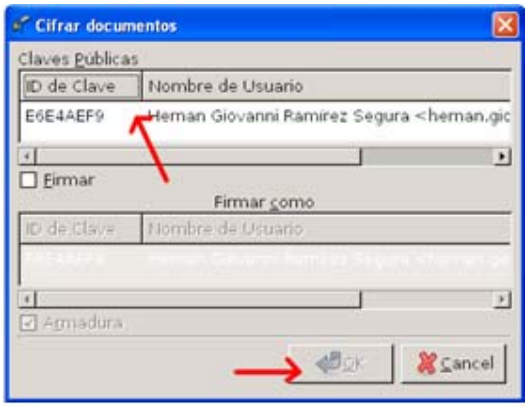


Figura 3.34 Selección de llave a Emplear

El resultado que se obtiene, es un texto cifrado, totalmente ilegible. Este texto se puede copiar y pegar en un documento y ser guardado. El texto cifrado solamente se podrá descifrar con la clave seleccionada (nuestra llave). Figura 3.35

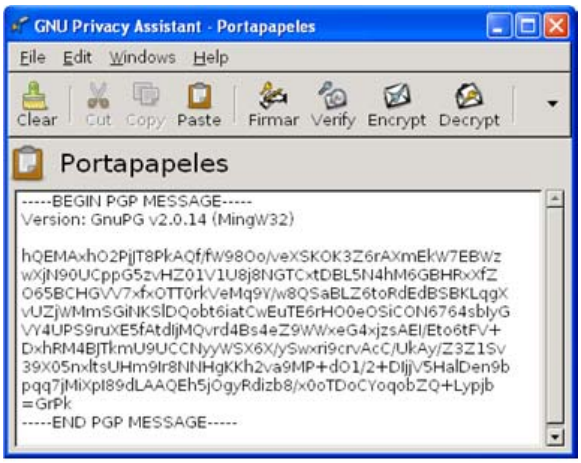


Figura 3.35 Texto Cifrado

Cifrado de un Documento

Ahora continuemos con el ***cifrado de un Archivo.*** En la ventana de GNU Privacy, oprimimos el botón **Archivos**. Refiérase a las figuras 3.36 y 3.37

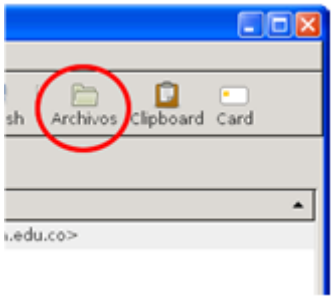


Figura 3.36 Apertura del gestor de Archivo

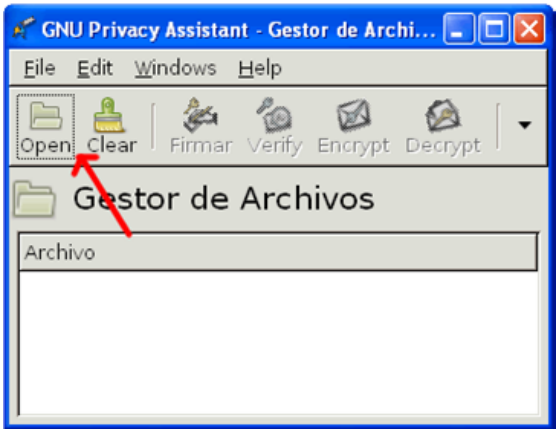


Figura 3.37 Gestor de Archivos

Ahora oprima el botón **Open**, se abre una ventana para buscar el archivo a cifrar, seleccione y de click en **Open**. Una vez escogido el archivo, oprima **Encryp**, seleccione la clave a la cual queremos asignar el archivo y haga click en **OK**. Una vez el archivo se ha cifrado, se obtiene un archivo del mismo nombre del original pero con la extensión **gpg**, el archivo original se puede eliminar, el archivo cifrado, solo podrá ser visto por el usuario para quien fue cifrado y que tenga la clave o frase de contraseña. Figura 3.38

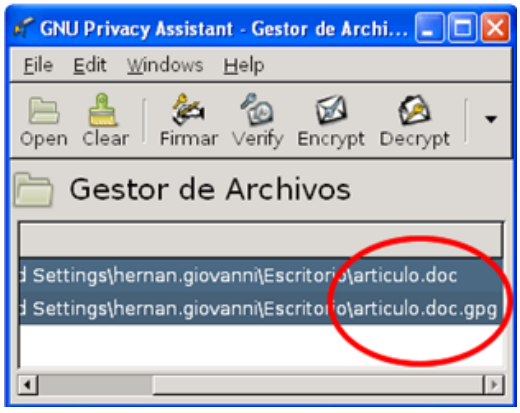


Figura 3.38 Archivo cifrado Creado

En el caso cifrar texto o archivos para otra persona, se debe tener la **llave pública** de esa persona, la forma más segura de tener la llave pública de alguien, es que ésta sea entregada personalmente, así tenemos la seguridad de que esa llave es de quien dice ser. El procedimiento para **exportar** e **importar** llaves públicas, es el siguiente. Figura 3.39

Figura 3.39 Exportación de llaves

Para entregar o dar mi llave pública a mis conocidos, entonces utilizo la opción **Exportar**, un click sobre este botón y se abre la ventana de Exportar clave, ingresamos un nombre, seleccionamos el lugar destino y para terminar click en el botón **Save**. Figura 3.40

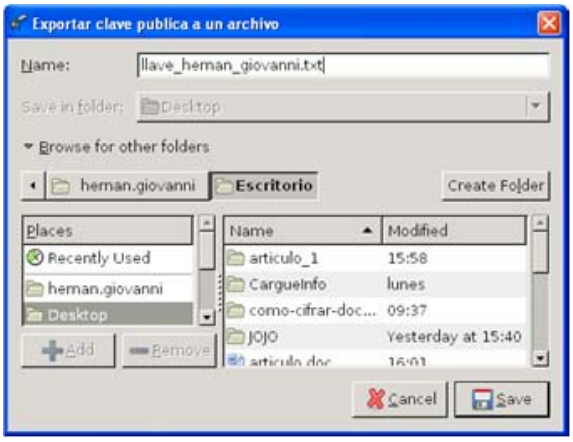


Figura 3.40 Selección destino de la llave a exportar

El archivo generado, es el que se debe compartir con los contactos, ya sea de forma personal (más segura) o a través de correo electrónico seguro. El procedimiento para **Importar** claves o llaves públicas de personas de confianza, es muy similar al proceso de Exportar, presionamos Click sobre el botón **Importar**, se abre la ventana de importar clave, se busca el lugar donde esté el archivo, se selecciona y para terminar se oprime el botón **Open**. Figura 3.41

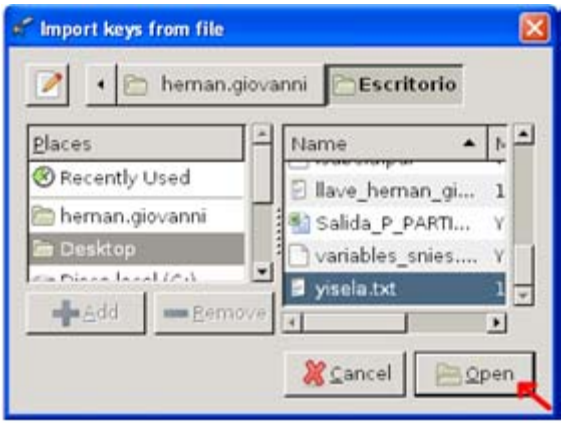


Figura 3.41 Directorio de exportación

Si la importación de la llave pública se ha realizado de forma correcta, se mostrará un mensaje como el siguiente. Figura 3.42

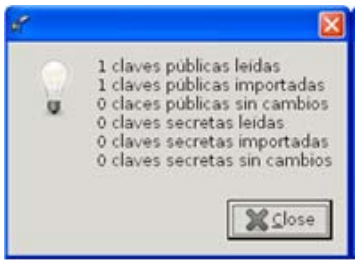


Figura 3.42 Comprobación de operación exitosa

Ahora no solamente está nuestra llave, si no que se mostrarán todas las *llaves públicas* que vamos importando. Figura3.43

Figura 3.43 Llaves importadas

Recuerde, si requiere cifrar un texto plano o archivo para alguien diferente a usted, debe seleccionar la **llave pública** de esa persona y ésta a su vez debe tener su llave pública.
A continuación revisaremos un ejemplo puntual de los casos anteriores haciendo uso del correo electrónico.

Envío de correo electrónico seguro.
Un compañero necesita enviarme un comunicado (texto) que solo me interesa a mí. Él teme que la información sea vista por terceros, siempre existe el riesgo a que hay alguna persona haciendo ***sniffing*** del tráfico de red/Internet, y realmente el riesgo es como disponer de una contraseña débil en tu router o una pregunta de seguridad obvia en tu cuenta de email.

Si un *sniffer* busca en nuestro tráfico de red es muy probable que un email pueda ser leído sin mucho problema, al contener texto plano, sin embargo, si está cifrado realmente lee bits aleatorios tal y como la persona que lo recibe.
Lo primero que necesita es teclear o pegar texto (no importa la cantidad de caracteres) en el Portapapeles del programa **Gpg4win**, una vez tenga todo terminado, oprima el botón **Encrypt**, pero esta vez seleccione su llave pública o las llaves públicas de las personas que solamente le interesa lean el mensaje.

Como resultado se obtiene un texto ilegible, el cual lo seleccionamos y pegamos en nuestro programa habitual de correo electrónico (Escribir o Redactar Nuevo mensaje) y se envía. Figura 3.44

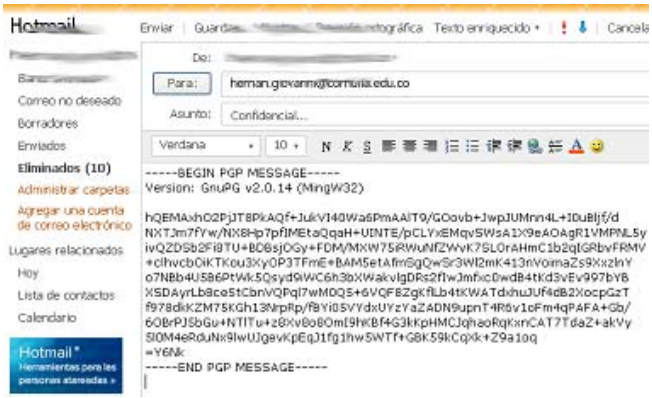


Figura 3.44 Mensaje cifrado

Así, si alguien empleando técnicas ***sniffing*** logra ver el email, no podrá entender de qué se trata. El correo electrónico llega a su destino (su propio email) y el procedimiento para ***descifrar*** el mensaje es el siguiente: Seleccione el texto recibido en el correo electrónico, cópielo y péguelo en el portapapeles de su programa Gpg4win, debe asegurarse de seleccionar todo el texto, desde el inicio hasta el final. Ahora oprima el botón **Decrypt**. Figuras 3.45 y 3.46

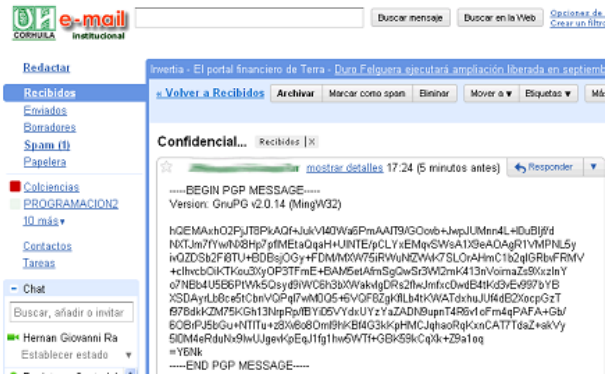


Figura 3.45 Envío de Mensaje cifrado

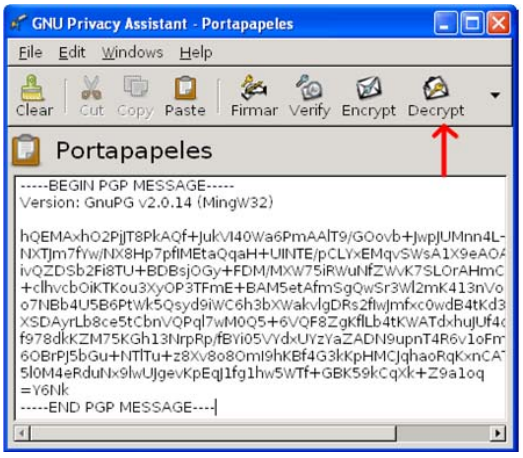


Figura 3.46 Descifrado del mensaje

Cuando se oprime el botón **Decrypt**, se abre una ventana donde se le solicitará su clave, con el objetivo de verificar que la persona a ver el mensaje es la persona a la cual se le envió.
Una vez haya digitado la contraseña, de click en **OK**. Figura3.47

Figura 3.47 Solicitud de contraseña

Si la clave es correcta, el mensaje es descifrado y se muestra el mensaje en claro que fue enviado. Figura 3.48

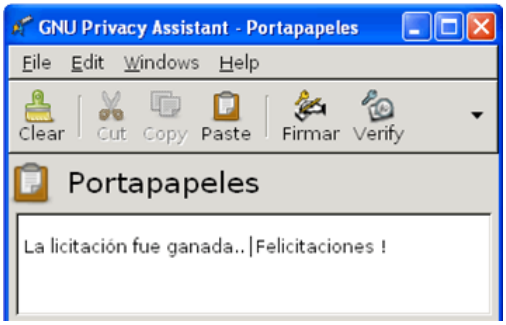


Figura 3.48 - Mensaje en Claro

El procedimiento es igual para el envío de archivos. De esta manera podrás cifrar tus comunicaciones de forma tradicional, un método realmente recomendable para realizar intercambio de archivos de forma personal o en organizaciones.

¿Cuál es la importancia del intercambio de llaves?

_____
_____
_____
_____

¿Con qué llave se cifra el mensaje y con cuál se descifra?

_____
_____
_____

Anote sus conclusiones

3.4 Práctica de laboratorio # 3 - Análisis de Tráfico

Objetivos de aprendizaje

- El alumno aprenderá a realizar capturas básicas de la unidad de datos del protocolo (PDU) mediante el uso de Wireshark.
- Realizara un análisis básico de la PDU en un tráfico de datos de red simple.
- Experimentara con las características y opciones de Wireshark, como captura de PDU y visualización de filtrado.

Desarrollo

Equipo Necesario

HARDWARE
1 Computadora arquitectura X86

SOFTWARE
Wireshark

Detalles de la herramienta

Un analizador de red o analizador de protocolos, es un software que puede interceptar y registrar tráfico de datos pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el programa "captura" cada unidad de datos del protocolo (Protocol Data Unit,PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Wireshark está programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado.

Características del Programa

Para capturar las PDU, la computadora donde está instalado Wireshark debe tener una conexión activa a la red y Wireshark debe estar activo antes de que se pueda capturar cualquier dato. Cuando se inicia Wireshark, se muestra la siguiente pantalla. Figura 3.49

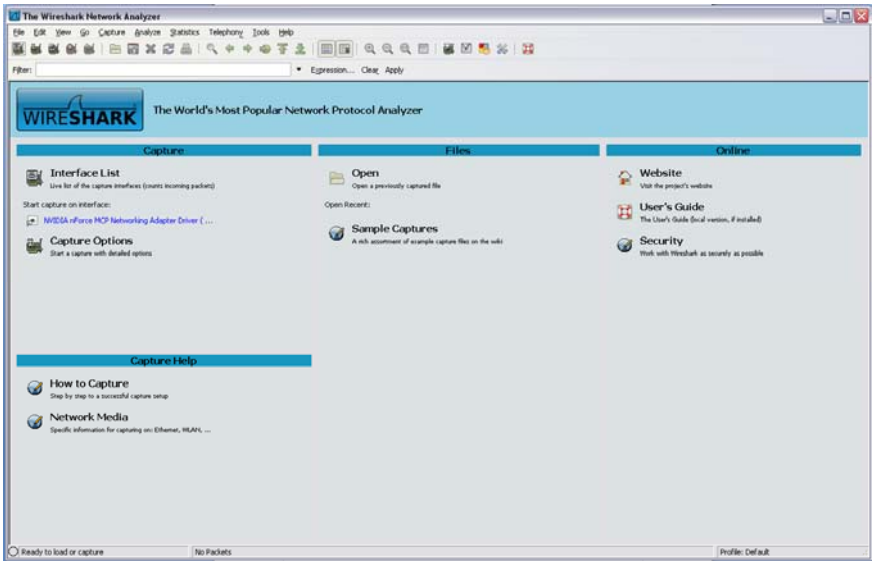


Figura 3.49 Pantalla de Wireshark

Para empezar con la captura de datos es necesario ir al menú Captura y seleccionar Opciones. Figura 3.50

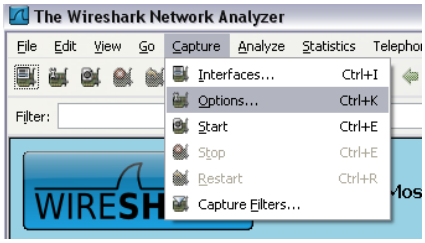


Figura 3.50 menú de captura

El cuadro de diálogo Opciones provee una serie de configuraciones y filtros que determinan el tipo y la cantidad de tráfico de datos que se captura. Figura 3.51

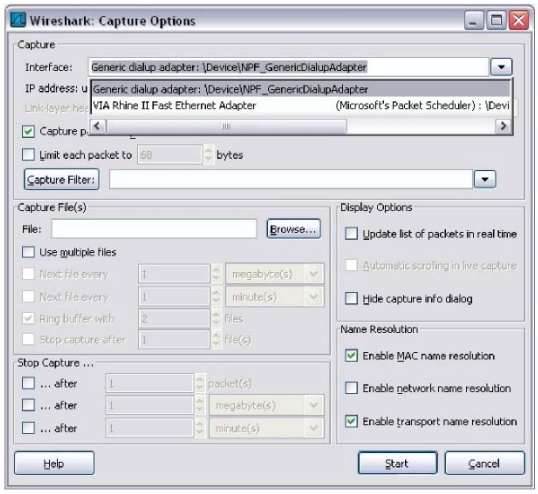


Figura 3.51 Ventana de opciones de captura

Primero, es necesario asegurarse de que Wireshark está configurado para monitorear la interfaz correcta. Desde la lista desplegable Interfaz, seleccione el adaptador de red que se utiliza. Generalmente, para una computadora, será el adaptador Ethernet conectado.

Luego se pueden configurar otras opciones. Entre las que están disponibles en Opciones de captura, merecen examinarse las siguientes dos opciones resaltadas. Figura 3.52

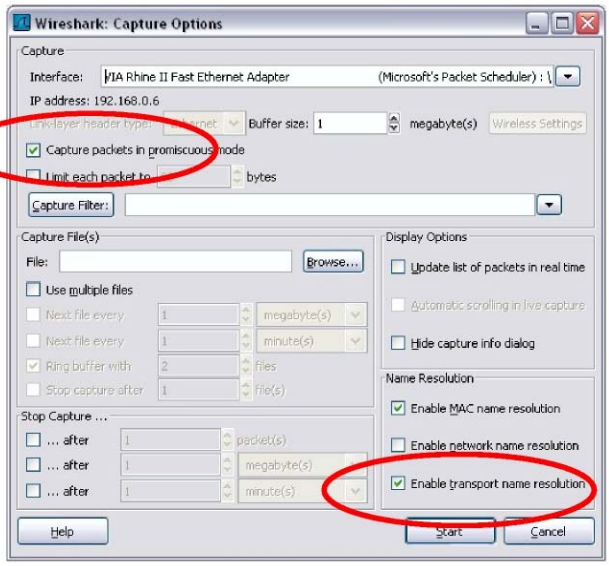


Figura 3.52 Opciones a seleccionar

Configurar Wireshark para capturar paquetes en un modo promiscuo.

Si esta característica NO está verificada, sólo se capturarán las PDU destinadas a esta computadora. Si esta característica está verificada, se capturarán todas las PDU destinadas a esta computadora y todas aquellas detectadas por la NIC de la computadora en el mismo segmento de red (es decir, aquellas que "pasan por" la NIC pero que no están destinadas para la computadora).

Configurar Wireshark para la resolución del nombre de red

Esta opción le permite controlar si Wireshark traduce a nombres las direcciones de red encontradas en las PDU. A pesar de que esta es una característica útil, el proceso de resolución del nombre puede agregar más PDU a sus datos capturados, que podrían distorsionar el análisis.

También hay otras configuraciones de proceso y filtrado de captura disponibles.

Haga clic en el botón Iniciar para comenzar el proceso de captura de datos y una casilla de mensajes muestra el progreso de este proceso. Figura 3.53

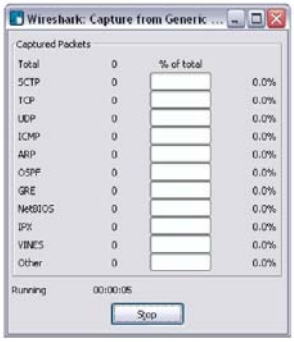


Figura 3.53 Captura de PDU

Mientras se capturan las PDU, los tipos y números se indican en la casilla de mensajes.

Si hace clic en el botón Detener, el proceso de captura termina y se muestra la pantalla principal. La ventana de visualización principal de Wireshark tiene tres paneles. Figura 3.54

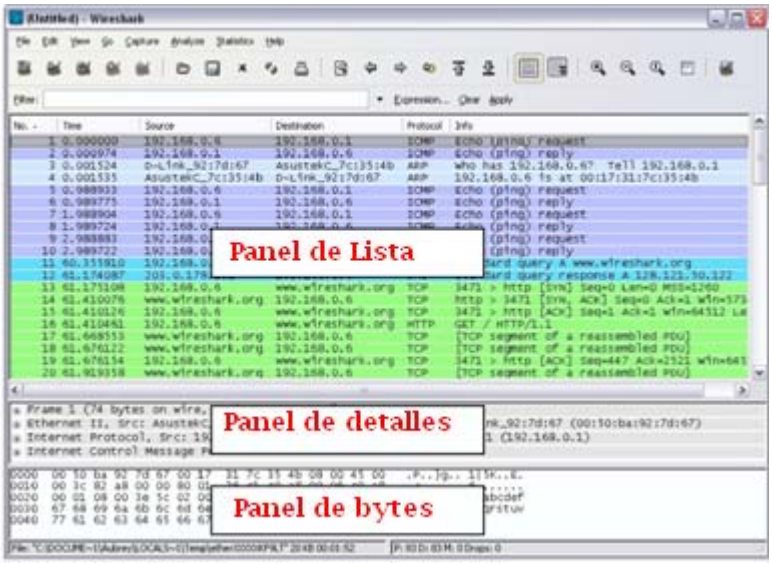


Figura 3.54 Ventana de Visualización principal

El panel de Lista de PDU (o Paquete) ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado. Si hace clic en los paquetes de este panel, controla lo que se muestra en los otros dos paneles.

El panel de detalles de PDU (o Paquete) ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de bytes de PDU (o paquete) ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete.

Cada línea en la Lista del paquete corresponde a una PDU o paquete de los datos capturados.

Si seleccionó una línea en este panel, se mostrarán más detalles en los paneles “Detalles del paquete” y “Bytes del paquete”. En la figura 3.54 muestra las PDU capturadas cuando se utilizó la utilidad ping y cuando se accedió a http://www.Wireshark.org.

El panel Detalles del paquete muestra al paquete actual (seleccionado en el panel “Lista de paquetes”) de manera más detallada. Este panel muestra los protocolos y los campos de protocolo de los paquetes seleccionados. Los protocolos y los campos del paquete se muestran con un árbol que se puede expandir y colapsar.

El panel Bytes del paquete muestra los datos del paquete actual (seleccionado en el panel “Lista de paquetes”) en lo que se conoce como estilo “hexdump”. En esta práctica de laboratorio no se examinará en detalle este panel. Sin embargo, cuando se requiere un análisis más profundo, esta información que se muestra es útil para examinar los valores binarios y el contenido de las PDU.

La información capturada para las PDU de datos se puede guardar en un archivo. Ese archivo se puede abrir en Wireshark para un futuro análisis sin la necesidad de volver a capturar el mismo tráfico de datos. La información que se muestra cuando se abre un archivo de captura es la misma de la captura original.

Cuando se cierra una pantalla de captura de datos o se sale de Wireshark se le pide que guarde las PDU capturadas. Figura 3.55

Figura 3.55 Guardado de PDU capturadas

Si hace clic en Continuar sin guardar se cierra el archivo o se sale de Wireshark sin guardar los datos capturados que se muestran.

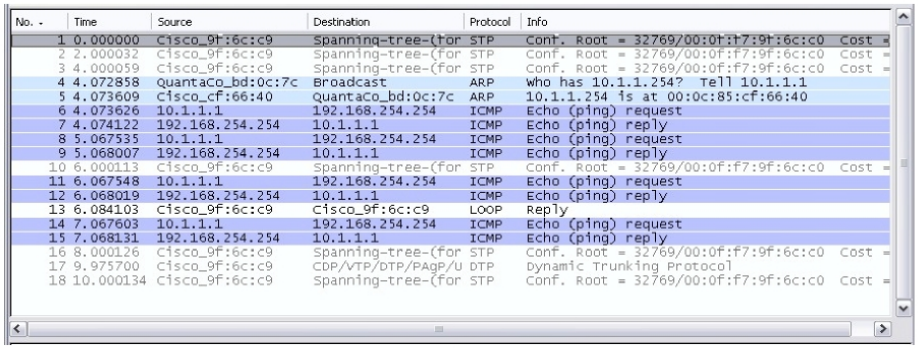
Ejercicio 1: Captura de PDU mediante ping

Paso 1: Después de asegurarse de que la configuración del equipo de laboratorio es correcta y hay conectividad, inicie Wireshark.

Configure las opciones de captura como se describe arriba en la descripción general e inicie el proceso de captura.
Desde la línea de comando del equipo, haga ping en la dirección IP de otra red conectada y encienda el dispositivo final en la topología de laboratorio. En este caso, haga ping utilizando el comando ping 192.168.**22**.254.
Después de recibir las respuestas exitosas al ping en la ventana de línea de comandos, detenga la captura del paquete.

Paso 2: Examine el panel Lista de paquetes.

Observe los paquetes de la lista de arriba. Nos interesan aquellos que son ICMP. Localice aquellos que aparecen en la lista de paquetes de su equipo. Figura 3.56



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Figura 3.56 Lista de paquetes

Si el usuario realizó el Paso de arriba, haga coincidir los mensajes que se muestran en la ventana de línea de comandos cuando el ping se ejecutó con los seis paquetes capturados por Wireshark. Responda lo siguiente desde la lista de paquetes Wireshark:

¿Qué protocolo se utiliza por ping?

_____

_____

¿Cuál es el nombre completo del protocolo?

_____

_____

¿Cuáles son los nombres de los dos mensajes ping?

_____

_____

¿Las direcciones IP de origen y destino que se encuentran en la lista son las que esperaba? Sí / No
¿Por qué?

_____

_____

Paso 3: Seleccione (resalte) con el mouse el primer paquete de solicitud de eco en la lista.

El panel de Detalles del paquete mostrará ahora algo parecido a:

Haga clic en cada uno de los cuatro "+" para expandir la información.

Como puede ver, los detalles de cada sección y protocolo se pueden expandir más. Revise esta información. En esta etapa del curso, puede ser que no entienda completamente la información que se muestra, pero tome nota de la que sí reconozca.

Localice los dos tipos diferentes de “Origen” y “Destino”. ¿Por qué hay dos tipos?

_____

_____

¿Cuáles son los protocolos que están en la trama de Ethernet?

_____

_____

Si selecciona una línea en el panel de Detalles del paquete, toda o parte de la información en el panel de Bytes del paquete también quedará resaltada.

Por ejemplo, si la segunda línea (+ Ethernet II) está resaltada en el panel de detalles, el panel de Bytes resalta ahora los valores correspondientes.

Esto muestra los valores binarios particulares que representan la información de la PDU. En esta etapa del curso no es necesario entender esta información en detalle.

Paso 4: Vaya al menú Archivo y seleccione Cerrar.

Haga clic en Continuar sin guardar cuando se muestre esta casilla de mensaje.

Ejercicio 2: Captura de FTP PDU

Paso 1: Inicie la captura de paquetes.
Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción Iniciar en el menú Captura de Wireshark.

Ingrese **ftp ftp.members.multimania.co.uk** en la línea de comandos del equipo donde se ejecuta Wireshark.

Cuando se establezca la conexión, ingrese **skfidj**
Password: **s3gur1d@d**

Una vez que inició sesión con éxito, ingrese:

```
get wireshark-win32-1.4.2.exe
```

y presione la tecla Enter. Con esa operación comenzará la descarga del archivo desde el servidor ftp.

Una vez que la descarga del archivo se haya completado, ingrese quit
Una vez que los archivos se hayan descargado exitosamente, detenga la captura PDU en Wireshark.

Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice y tome nota de las PDU asociadas con la descarga del archivo.

Éstas serán las PDU del protocolo TCP de Capa 4 y del protocolo FTP de Capa 7.

Identifique los tres grupos de PDU asociados con la transferencia del archivo.

Si realizó el paso de arriba, haga coincidir los paquetes con los mensajes y las indicaciones en la ventana de línea de comandos FTP.

El primer grupo está asociado con la fase "conexión" y el inicio de sesión en el servidor. Haga una lista de ejemplos de mensajes intercambiados en esta fase.

_____

_____

Localice y haga una lista de ejemplos de mensajes intercambiados en la segunda fase, que es el pedido de descarga real y la transferencia de datos.

_____

_____

El tercer grupo de PDU está relacionado con el cierre de sesión y la "desconexión".

Haga una lista de ejemplos de mensajes intercambiados durante este proceso.

_____

_____

Localice los intercambios TCP recurrentes a través del proceso FTP.

¿Qué característica de TCP indica esto?

_____

_____

Paso 3: Examine los Detalles del paquete.

Seleccione (resalte) un paquete de la lista asociada con la primera fase del proceso FTP. Observe los detalles del paquete en el panel de Detalles.

¿Cuáles son los protocolos encapsulados en la trama?

_____

_____

Seleccione los paquetes que contengan el nombre de usuario y contraseña. Examine la porción resaltada en el panel Byte del paquete.

¿Qué mensaje aparece al inicio de sesión FTP?

_____

_____

Seleccione un paquete asociado con la segunda fase.

Desde cualquier panel, localice el paquete que contenga el nombre del archivo. El nombre del archivo es:

_____

Seleccione un paquete que tenga el contenido real del archivo. Observe el texto simple visible en el panel Byte. Resalte y examine en los paneles Detalles y Byte; algunos de los paquetes intercambiados en la tercera fase de la descarga del archivo.

¿Qué características distinguen al contenido de estos paquetes?

_____

_____

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Ejercicio 3: Captura de HTTP PDU

Paso 1: Inicie la captura de paquetes.
Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción Iniciar en el menú Captura de Wireshark.

Inicie un navegador Web en el equipo donde ejecuta Wireshark.
Ingrese la dirección IP 192.168.254.254. Una vez que la página Web se haya descargado por completo, detenga la captura del paquete Wireshark.

Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.
Localice e identifique los paquetes TCP y HTTP asociados con la descarga de la página Web. Observe el parecido entre este intercambio de mensajes y el intercambio FTP.

Paso 3: En el panel Lista de paquetes, resalte un paquete HTTP que tenga la notación "(text/html)" en la columna Información.
En el panel Detalles del paquete, haga clic en "+" al lado de "Datos de texto basado en línea: html"

¿Cuándo esta información expande lo que se muestra?

_____

_____

Examine la porción que resaltó en el panel Byte.
Esto muestra los datos HTML que contiene el paquete.

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Reflexión

Considere lo que puede proveer Wireshark sobre la información de encapsulación referida a los datos de red capturados. Relacione esto a los modelos de la capa OSI y TCP/IP. Es importante que el usuario pueda reconocer y relacionar tanto los protocolos representados como la capa de protocolo y los tipos de encapsulación de los modelos con la información provista por Wireshark.

Ejercicio 4

Elabore un mapa mental de cómo podría utilizar un analizador de protocolos como Wireshark para:
(1) Diagnosticar fallas de una página Web para descargar con éxito un navegador en un equipo,
(2) Identificar el tráfico de datos en una red requerida por los usuarios.

A menos que el profesor indique lo contrario, salga de Wireshark y apague el equipo correctamente.

Anote sus conclusiones

_____
_____
_____
_____
_____
_____

3.5 Práctica de laboratorio # 4 - FIREWALL

Objetivos

- El alumno comprenderá el concepto de firewall
- Aprenderá las diferentes políticas que se emplean para el uso del firewall
- Hará uso de IPTABLES para la creación de un firewall

Introducción

La seguridad es una de las preocupaciones principales del administrador de red. Hay muchas páginas inseguras en Internet y la mayor parte de nosotros desconoce lo que realmente pasa durante la transmisión de datos, o si éstos pueden venir acompañados de virus o intrusos. Así pues, es necesario desarrollar un sistema que proteja a la red interna de la externa, esto es, de Internet, mediante el uso de filtros equipados para evitar automáticamente que un usuario no autorizado ataque al equipo.
En la actualidad los mecanismos de defensa se basan en tres grandes apartados:

- Utilización de aplicaciones seguras.

- Utilización de tecnología de cifrado.

- Utilización de cortafuegos (Firewall).

Firewall

Mencione ¿Qué es un firewall?

_____
_____
_____
_____
_____

Hoy en día un firewall es un hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.

Dependiendo de las necesidades de cada red, pueden ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a Internet (como es el caso de un servidor Web, un servidor de correo, etc.), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es colocar ese servidor en un lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada.

Defina lo que es un DMZ y mencione su función

_____
_____
_____
_____

Los firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de Internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior; esto último se hace con el firewall o frecuentemente con un Proxy.

¿Cuál es el uso de un servidor Proxy y en que capa del modelo OSI opera?

_____
_____
_____
_____

También, en empresas de hosting con muchos servidores alojados lo normal es encontrarnos uno o más firewalls ya sea filtrando toda la instalación o parte de ella:
Sea el tipo de firewall que sea, generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo TCP/IP. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los TCP, también los UDP, los ICMP y otros protocolos vinculados a VPNS.
Es necesario tener una política establecida a la hora de montar un sistema de seguridad:

Describir para qué es el servicio.

Describir el grupo de personas a las que va dirigido el servicio.

Describir a qué servicio necesita acceder cada grupo.

Describir para cada grupo de servicio cómo se puede mantener seguro el servicio.

Hay dos maneras de implementar un firewall. Mencione ¿Cuáles son? y ¿En qué consisten?

_____
_____

_____
_____

Como es obvio imaginar, la primera política facilita mucho la gestión del firewall, ya que simplemente nos tenemos que preocupar de proteger aquellos puertos o direcciones que sabemos que nos interesa; el resto no importa tanto y se deja pasar. El único problema que podemos tener es que no controlemos que es lo que está abierto, o que en un momento dado se instale un software nuevo que abra un puerto determinado, o que no sepamos que determinados paquetes ICMP son peligrosos.

Si la política por defecto es ACEPTAR y no se protege explícitamente, tendríamos una falla de seguridad.

En cambio, si la política por defecto es DENEGAR, a no ser que lo permitamos explícitamente, el firewall se convierte en un auténtico muro infranqueable.

El problema es que es mucho más difícil preparar un firewall así(permitiendo solo servicios específicos), y hay que tener muy claro cómo funciona el sistema (sea iptables o el que sea) y qué es lo que se tiene que abrir sin caer en la tentación de introducir reglas demasiado permisivas.

Un firewall es inútil si el sistema en el que está instalado es vulnerable a ataques externos. No proporcionan seguridad absoluta. Son un mecanismo más y deben combinarse con otras medidas de seguridad, tanto en redes como en sistemas operativos, para hacer el sistema lo más seguro posible.

El orden en el que se ponen las reglas de firewall es determinante. Normalmente cuando hay que decidir qué se hace con un paquete se va comparando con cada regla del firewall hasta que se encuentra una que le afecta (match), y se hace lo que dicte esta regla (aceptar o denegar); después de eso no se miran más para ese paquete. Si se añaden reglas muy permisivas entre las primeras del firewall, puede que las siguientes no se apliquen y no sirvan de nada.

Desarrollo

Equipo Necesario

Hardware

3 Computadora con arquitectura X86
2 Tarjeta de red PCI

Software

FEDORA

Defina IPTABLES

_____
_____
_____
_____

Cuando llega un paquete el kernel mira si es para él o para otra máquina y consulta las reglas del firewall para decidir qué hacer con él.
Mencione los tres tipos de reglas en iptables:

_____
_____

_____
_____

_____
_____

Para los paquetes (o datagramas, según el protocolo) que van a la propia máquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o máquinas se aplican simplemente reglas FORWARD. INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT, que se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino; incluso antes de las reglas de NAT se pueden incorporar reglas de tipo MANGLE, destinadas a modificar los paquetes; son reglas poco conocidas.

Para alterar paquetes recibidos por medio de una interfaz de red cuando llegan, se usa la cadena *Prerouting*. Por otro lado, tenemos la cadena Output, la cual altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.

Finalmente la cadena *Postrouting* altera paquetes antes de que sean enviados a través de una interfaz de red.

Mencione el objetivo de las reglas:

ACCEPT

_____

_____

DROP

_____

_____

QUEUE

_____

_____

REJECT

_____

_____

Estructura de las reglas:

Table-name: permite especificar una tabla diferente a la predeterminada filter.

Command: acción específica a realizar (anexar, eliminar, …).

Chain-name: regla sobre la que se aplica.

Parameter/option: parámetros y opciones que definen que pasará cuando un paquete coincide con la regla.

Opciones de comando

-A: añade la regla iptables al final de la cadena especificada. El orden de las reglas en la cadena no importa.

-F: libera la cadena seleccionada, que borra cada regla de la cadena. Si no se especifica ninguna cadena, este comando libera cada regla de cada cadena.

-P: configura la política por defecto para una cadena en particular de tal forma que cuando los paquetes atraviesen la cadena completa sin cumplir ninguna regla, serán enviados a un objetivo en particular.

-X: borra una cadena especificada por el usuario.

-Z: pone ceros en los contadores de byte y de paquetes en todas las cadenas de una tabla en particular.

-t: indica el nombre de una tabla.

Parámetros

-d: configura el nombre de la máquina destino, dirección IP o red de un paquete que coincide con la regla.

-i: configura la interfaz de red entrante.

-j: le dice a iptables que salte a un objetivo particular cuando un paquete coincide con una regla.

-o: configura la interfaz de red saliente.

-p: configura el protocolo ip para la regla.

-s: configura la fuente para un paquete particular.

-dport: configura el puerto destino para el paquete.

-sport: configura el puerto origen para el paquete.

EJERCICIO 1

El primer ejercicio marcado, es implementar las reglas para llevar a cabo una política de "*denegación por defecto*". Este tipo de políticas restringen todo aquello que intente acceder al ordenador o de igual manera salir de él.

A medida que se vayan añadiendo mas reglas la permisividad del cortafuego irá disminuyendo en función de los requerimientos del administrador del sistema.

Las reglas necesarias para llevar la política mencionada anteriormente son las mostradas a continuación:

iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

Las reglas expuestas anteriormente, cortan todo tipo de acceso o salida por los diferentes medios de comunicación: salida (output), entrada (input), interno (forward).

A continuación se explicará una de estas reglas, omitiendo el resto ya que el significado es el mismo:
iptables –P INPUT DROP

iptables: Es el comando que se utiliza cuando se quiere hacer mención a una regla del servicio iptables.

-P: Este parámetro nos indica el tipo de canal sobre el que se quiere llevar un control mediante una regla.

INPUT: Canal sobre el cual se aplicará la regla.

DROP: Permiso que se quiere dar, en este caso *denegado*.

EJERCICIO 2

a) Denegar Echo Request a máquinas internas

REGLAS:

1. iptables -A INPUT -s 192.168.22.0/24 -p icmp --icmp-type echo-request -j ACCEPT

2. iptables -A FORWARD -i eth1 -p icmp --icmp-type
echo-request -j ACCEPT

A partir de las dos reglas mostradas para este apartado, se controla la solicitud de echo para las máquinas internas. En estas reglas, se tiene como parámetro nuevo el "-p", el cual indica el protocolo de encapsulamiento de los paquetes. Dentro de cada protocolo especificado, se extiende una serie de opciones dependientes del protocolo especificado. En este caso como se quiere restringir este paquete, se utiliza el tipo especificado en la regla.

MENCIONE CÓMO SE DARÍA LECTURA DE LAS REGLAS:

_____
_____
_____
_____
_____
_____

b) Permitir Telnet solo hacia fuera.

REGLAS:

1. iptables -A OUTPUT -p tcp --dport 23 -j ACCEPT

2. iptables -A FORWARD -s 192.168.22.0/24 -p tcp --dport 23 –j ACCEPT

3. iptables -A INPUT -p tcp --sport 23 -m state
--state 'ESTABLISHED,RELATED' -j ACCEPT

4. iptables -A FORWARD -d 192.168.22.0/24 -i eth0 -p tcp
--sport 23 -m state --state 'ESTABLISHED,RELATED'-j ACCEPT

Con este conjunto de reglas se permite telnet sólo hacia fuera. Con la opción --dport especificamos el campo de puerto de destino del paquete. Con –m state podemos indicar el estado del paquete (seguido de --state 'ESTADO').

MENCIONE CÓMO SE DARÍA LECTURA DE LAS REGLAS:

_____
_____
_____
_____
_____
_____
_____

No es posible comprobar si nuestro firewall funciona correctamente para el servicio Telnet. Ello es debido a que Telnet debe utilizar dos conexiones, una para datos y otra para comandos. Se necesitaría tener un equipo escuchando por el puerto 23 mientras que el otro accede por dicho puerto.
Para comprobar que el servicio Telnet funciona correctamente se debe proceder comprobando el comportamiento antes y después de activar el firewall.

Cuando el firewall está desactivado, aparecerá que la dirección sobre la que se quiere realizar una conexión Telnet, no es reconocida, mientras que si el firewall se activa, se observará cómo el equipo se queda bloqueado a la espera de la respuesta del otro equipo.
Ambas situaciones han sido mostradas en las imágenes superiores.

c) Permitir FTP solo hacia fuera.

REGLAS:

1. iptables -A OUTPUT -p tcp --dport ftp -j ACCEPT
2. iptables -A FORWARD -s 192.168.22.0/24 -p tcp --dport ftp -j ACCEPT
3. iptables -A INPUT -p tcp --sport ftp –m state –state 'ESTABLISHED,RELATED' -j ACCEPT
4. iptables -A FORWARD -d 192.168.22.0/24 -i eth0 -p tcp --sport ftp –m state --state 'ESTABLISHED,RELATED' -j ACCEPT

MENCIONE CÓMO SE DARÍA LECTURA DE LAS REGLAS:

Como se observa, el firewall funciona correctamente a la hora de permitir un acceso a una dirección la cual no pertenece a nuestra propia red.

Por el contrario, podemos comprobar que si se intenta realizar un acceso ftp sobre una dirección perteneciente a nuestra red, el firewall dejará el equipo bloqueado a la espera de una respuesta.

En caso de desactivar el firewall el resultado de un acceso ftp sobre una dirección de nuestra red es el mismo que para el Telnet.

Restauramos la configuración inicial y apagamos el equipo.

Anote sus conclusiones

3.6 Práctica de laboratorio # 5 - IPv6

Objetivos

- Conocer las principales características de la nueva versión del protocolo de red de la arquitectura TCP/IP: IP versión 6 (de forma abreviada IPv6).

- Comprender su funcionamiento y aplicar los conocimientos adquiridos a la configuración de un escenario de red sencillo compuesto por dos routers, tres segmentos Ethernet y varios sistemas finales.

- Conocer las técnicas básicas diseñadas para la migración hacia IPv6 de redes basadas en el protocolo IP actual (IPv4) y experimentar con ellas sobre el escenario anterior.

Conceptos

Defina el protocolo IPv6

Mencione al menos 5 diferencias entre IPV6 e IPV4 y menciones las características principales de cada una.

Dibuje un esquema de la trama de IPV6 y uno de trama IPv4

En IPv6 las direcciones son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en IPv4 en los nodos se asignan a interfaces.
Mencione los tres tipos de direcciones que se emplean:

_____
_____
_____

Al igual que con IPv4 en IPv6 contamos con direcciones de uso restringido:

- Dirección virtual de auto-retorno o loopback.

Esta dirección se especifica en IPv4 con la dirección 127.0.0.1. En IPv6 esta dirección se representa como ::1.

- Dirección no especificada (::).

Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección.

- Túneles dinámicos/automáticos de IPv6 sobre IPv4.

Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre redes IPv4, de forma transparente. Se indican como ::, por ejemplo ::156.55.23.5.

- Representación automática de direcciones IPv4 sobre IPv6.

Nos permite que los nodos que sólo soportan IPv4 puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4". Se indican como ::FFFF:, por ejemplo ::FFFF:156.55.43.3.

¿Qué es un túnel IPv6 en IPv4?

_____
_____
_____

¿Qué características proporciona IPSEC y ¿En qué consiste cada una de ellas?

_____
_____
_____

Desarrollo

Equipo Necesario

Hardware

1 Computadora con arquitectura X86

Software

Packet Tracer
Microsoft Windows XP

DESARROLLO

Ejercicio #1 RUTEO ESTÁTICO EN Ipv6

DESARROLLO

1. Configurar la siguiente topología: (véase figura 3.57)

Topología de la red

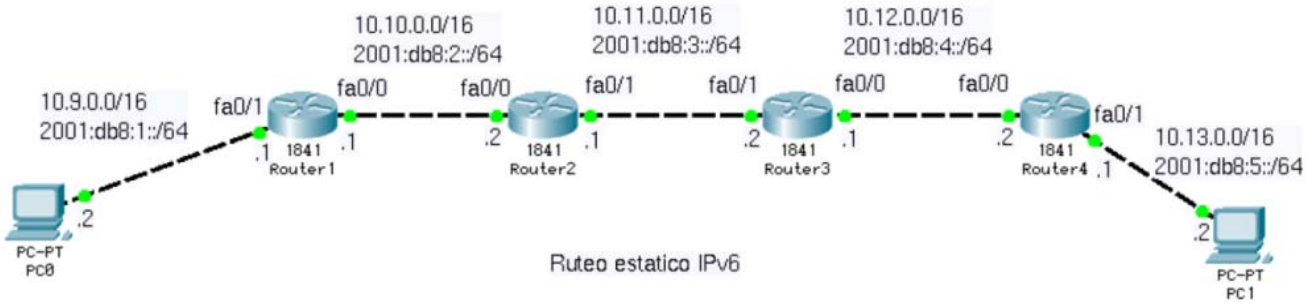


Figura 3.57 Ruteo Estático

2. Colocar nombres a los routers
Router> enable
Router# configure terminal
Router(config)# hostname <nombre_del_router>
Router1(config)#

3. Configurar Ipv6 en cada interfaz FastEthernet, e ipv4 (opcional) en los routers:
Router> enable
Router# configure terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 enable
Router(config-if)# ip address <Dirección_IPV4> <MASCARA_SUBRED>

Router(config-if)# ipv6 address <Dirección_IPv6>/<Longitud_del_prefijo>
Router(config-if)# exit
Router(config)#

"Repetir el paso anterior para las dos interfaces, FastEthernet 0/0 y 0/1 , de los cuatro routers"

3. Realizar una prueba de conexión entre routers **directamente** conectados
Router2#ping 2001:db8:2::1

 En caso de una conexión exitosa debe aparecer:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/10 ms

4. OPCIONAL: Agregar las rutas estáticas Ipv4 a cada router, hacia cada red no directamente conectada.
Router2# configure terminal
Router2(config)# ip route <prefijo_destino> <mascara_subred> <interfaz_o_gateway>

5. Agregar las rutas estáticas Ipv6 en cada router.
Router2# configure terminal
Router2(config)# ipv6 route <prefijo_IPv6>/<longitud_del_prefijo> <interfaz_o_gateway>

6. verificar las configuraciones
Router2# show run
Router2# ping <direccion_ipv6>
Router2# show ipv6 interface
Router2# show ipv6 route
Router2# show ipv6 neighbors

Ejercicio #2 RIP IPv6

Investigue a qué se refiere el protocolo RIP

_____
_____
_____

1.Con la misma topología, configuramos en cada router el encaminamiento de paquetes ipv6
Router1(config)# ipv6 unicast-routing

2. Configurar Ipv6 en cada interfaz FastEthernet, en los routers:
Router> enable
Router# configure terminal

Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 address <Dirección_IPv6>/<Longitud_del_prefijo>
Router(config-if)# exit
Router(config)#

3.Repetir el paso anterior para las dos interfaces, FastEthernet 0/0 y 0/1 , de los cuatro routers

4. Realizar una prueba de conexión entre routers **directamente** conectados
Router2#ping 2001:db8:2::1

5. Habilitar RIP en cada router usando el comando:
Router2# configure terminal
Router2(config)# ipv6 router rip <numero_de_proceso>

6. Habilitar RIP en ambas interfaces de cada router
Router2(config)# interface f 0/0
Router2(config-if)# ipv6 rip <numero_de_proceso> enable
Router2(config)# interface f 0/1
Router2(config-if)# ipv6 rip <numero_de_proceso> enable

7. Verificamos las configuraciones tecleando
Router2# show run
Router2# ping <direccion_ipv6>
Router2# show ipv6 interface
Router2# show ipv6 route rip
Router2# show ipv6 neighbors

Ejercicio #3 OSPFv3
Explique a qué se refiere el protocolo OSPF

_____
_____
_____

1. Configurar en cada router el encaminamiento de paquetes ipv6
Router1(config)# ipv6 unicast-routing

2. Configurar Ipv6 en cada interfaz FastEthernet, en los routers:
Router> enable
Router# configure terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 address <Dirección_IPv6>/<Longitud_del_prefijo>
Router(config-if)# exit
Router(config)#

3.Repetir el paso anterior para las dos interfaces, FastEthernet 0/0 y 0/1 , de los cuatro routers

4. Realizar una prueba de conexión entre routers **directamente** conectados

Router2#ping 2001:db8:2::1

5. Habilitar OSPF en cada router usando el comando:

Router2# configure terminal
Router2(config)# ipv6 router ospf <numero_de_proceso>

6. Habilitar OSPF en ambas interfaces de cada router
Router2(config)# interface f 0/0
Router2(config-if)# ipv6 ospf 1 area 0

7. Verificamos las configuraciones tecleando
Router2# show run
Router2# ping <direccion_ipv6>
Router2# show ipv6 interface
Router2# show ipv6 route ospf
Router2# show ipv6 neighbors

Ejercicio # 4 Túnel 6to4

¿Qué es un Túnel 6to 4?

_____

_____

_____

DESARROLLO

1. Configure la siguiente topología:
Topología de la red(véase figura 3.58)

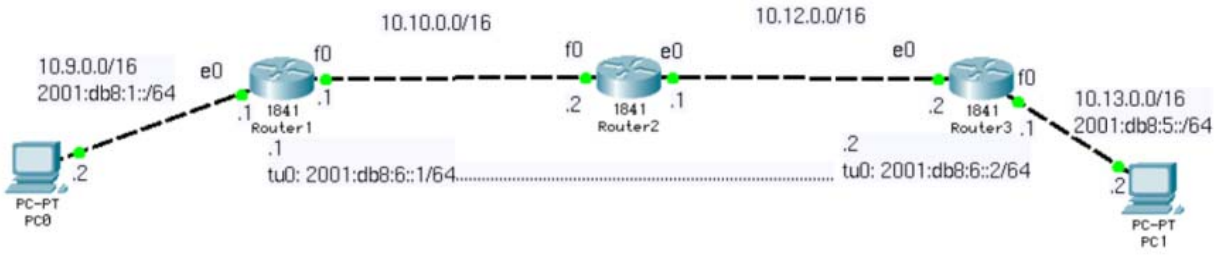


Figura 3.58 Túnel 6to4

2. Colocar nombres a los routers
Router> enable
Router# configure terminal
Router(config)# hostname <nombre_del_router>
Router1(config)#

3. Configurar en cada router el encaminamiento de paquetes ipv6
Router1(config)# ipv6 unicast-routing

3. Configurar Ipv4 entre los tres routers
Router> enable
Router# configure terminal
Router(config)# interface Ethernet 0
Router(config-if)# ip address <Dirección_IPV4> <MASCARA_SUBRED>
Router(config-if)# exit
Router(config)#

4. Configurar Ipv6 en las interfaces LAN de los 2 routers de frontera
Router> enable
Router# configure terminal
Router(config)# interface Ethernet 0
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 address <Dirección_IPv6>/<Longitud_del_prefijo>
Router(config-if)# exit
Router(config)#

5. Agregar ruteo ipv4 entre los 3 routers, use ruteo estático, rip u ospf.

6. Realizar pruebas de ping de ipv4 de extremo a extremo

7. Crear uNa interfaz túnel entre los dos routers de frontera
Router2(config)# interface tunnel0
Router2(config-if)# no ip address
Router2(config-if)# ipv6 address <direccion_ipv6_del_tunnel>/<Longitud_del_prefijo>
Router2(config-if)# tunnel source <direccion_ipv4_local_origen_del_tunnel>
Router2(config-if)# tunnel destination <direccion_ipv4_local_destino_del_tunnel>
Router2(config-if)# tunnel mode ipv6ip
Router2(config-if)# no shutdown

7. Verificamos las configuraciones tecleando
Router2# show run
Router2# ping <direccion_ipv6>
Router2# show ipv6 interface
Router2# show ipv6 route

CONFIGURACIONES DE LOS 3 ROUTERS
ROUTER 1
```
conf t
int e0
ip add 10.9.0.1 255.255.0.0
ipv6 add 2001:db8:1::1/64
no sh
int f0
ip add 10.10.0.1 255.255.0.0
no sh
interface Tunnel0
no ip address
ipv6 address 2001:db8:6::1/64
tunnel source 10.10.0.1
tunnel destination 10.12.0.2
tunnel mode ipv6ip
no sh
ip route 0.0.0.0 0.0.0.0 10.10.0.2
ipv6 route ::/0 2001:db8:6::2
```
ROUTER R2
```
conf t
int f0
ip add 10.10.0.2 255.255.0.0
no sh
int e0
ip add 10.12.0.1 255.255.0.0
no sh
ip route 10.9.0.0 255.255.0.0 10.10.0.1
ip route 10.13.0.0 255.255.0.0 10.12.0.2
```

ROUTER R3
```
conf t
int e0
ip add 10.12.0.2 255.255.0.0
no sh
int f0
ip add 10.13.0.1 255.255.0.0
ipv6 address 2001:db8:5::1/64
no sh
interface Tunnel0
no ip address
ipv6 address 2001:db8:6::2/64
tunnel source 10.12.0.2
tunnel destination 10.10.0.1
tunnel mode ipv6ip
no sh
ip route 0.0.0.0 0.0.0.0 10.12.0.1
```

ipv6 route ::/0 2001:db8:6::1

Anote sus conclusiones

_____
_____
_____
_____
_____
_____

3.7 Práctica de laboratorio # 6 - Códigos Maliciosos

Objetivos de aprendizaje

El alumno conocerá y comprenderá las diferencias que existen entre varios tipos de malware.

El estudiante observará y analizará las acciones que realizan los códigos maliciosos bajo diferentes esquemas.

Se removerán códigos maliciosos con herramientas anti-malware y anti-virus.

Introducción

En seguridad informática, código malicioso es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso. Esta definición incluye tanto programas malignos compilados, como macros y códigos que se ejecutan directamente, como los que suelen emplearse en las páginas web (scripts).

Los códigos maliciosos pueden tener múltiples objetivos como:

- Extenderse por la computadora, otras computadoras en una red o por internet.
- Robar información y claves.
- Eliminar archivos e incluso formatear el disco duro.
- Mostrar publicidad invasiva.

Mínimos cambios en un código malicioso, pueden hacer que ya no sea reconocido como malicioso por un programa antivirus; es por esta razón que existen tantas variantes de los virus, los gusanos y otros malwares. Además, los antivirus todavía no tienen la suficiente "inteligencia" como para detectar códigos maliciosos nuevos.
Los tipos más conocidos de malware, virus y gusanos, se distinguen por la manera en que se propagan más que por otro comportamiento particular

Defina Virus informático

_____
_____
_____
_____

Defina Gusano

_____
_____
_____
_____
_____

Teniendo en cuenta esta distinción, las infecciones transmitidas por e-mail o documentos, que dependen de su apertura por parte del destinatario para infectar su sistema, deberían ser clasificadas más como virus que como gusanos.

Nótese que un virus necesita de la intervención del usuario para propagarse mientras que un gusano se propaga automáticamente.

Para que un software malicioso pueda completar sus objetivos, es esencial que permanezca oculto al usuario. Por ejemplo, si un usuario experimentado detecta un programa malicioso, terminaría el proceso y borraría el malware antes de que este pudiera completar sus objetivos. El ocultamiento también puede ayudar a que el malware se instale por primera vez en la computadora.

Defina Troyano

_____
_____
_____
_____
_____

Defina Rootkit

_____
_____
_____
_____
_____

Defina Backdoor

_____
_____
_____
_____
_____

Hay muchos más tipos de malware algunos son producidos con fines de lucro, por ejemplo el spyware, el adware intrusivo y los hijacker tratan de mostrar publicidad no deseada o redireccionar visitas hacia publicidad para beneficio del creador. Estos tipos de malware no se propagan como los virus, generalmente son instalados aprovechándose de vulnerabilidades o junto con software legítimo como aplicaciones P2P.

Malware para mostrar publicidad: Spyware, Adware y Hijackers

Los programas spyware son creados para recopilar información sobre las actividades realizadas por un usuario y distribuirla a agencias de publicidad u otras organizaciones interesadas. Algunos de los datos que recogen son las páginas web que visita el usuario y direcciones de email, a las que después se envía spam. La mayoría de los programas spyware son instalados como troyanos junto a software deseable bajado de Internet. Otros programas spyware recogen la información mediante cookies de terceros o barras de herramientas instaladas en navegadores web. Los autores de spyware que intentan actuar de manera legal se presentan abiertamente como empresas de publicidad e incluyen unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender.

Por otra parte los programas adware muestran publicidad al usuario de forma intrusiva en forma de ventanas emergentes (pop-up) o de cualquier otra forma.
Los hijackers son programas que realizan cambios en la configuración del navegador web. Por ejemplo, algunos cambian la página de inicio del navegador por páginas web de publicidad o pornográficas, otros redireccionan los resultados de los buscadores hacia anuncios de pago o páginas de phishing bancario.

Ciertos tipos de malware se dedican al robo de información. Mencione y describa por lo menos dos tipos de malware que roben información personal del usuario

_____
_____
_____
_____
_____

Como los ataques con malware son cada vez más frecuentes, el interés ha empezado a cambiar de protección frente a virus y spyware, a protección frente al malware, y los programas han sido específicamente desarrollados para combatirlos.

Los programas anti-malware pueden combatir el malware de dos formas:

1. Proporcionando protección en tiempo real (real-time protection) contra la instalación de malware en una computadora. El software anti-malware escanea todos los datos procedentes de la red en busca de malware y bloquea todo lo que suponga una amenaza.
2. Detectando y eliminando malware que ya ha sido instalado en una computadora. Este tipo de protección frente al malware es normalmente mucho más fácil de usar y más popular. Este tipo de programas anti-malware escanean el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en la computadora. Al terminar el escaneo muestran al usuario una lista con todas las amenazas encontradas y permiten escoger cuáles eliminar.

La protección en tiempo real funciona idénticamente a la protección de los antivirus: el software escanea los archivos al ser descargados de Internet y bloquea la actividad de los componentes identificados como malware. En algunos casos, también pueden interceptar intentos de ejecutarse automáticamente al arrancar el sistema o modificaciones en el navegador web. Debido a que muchas veces el malware es instalado como resultado de exploits para un navegador web o errores del usuario, usar un software de seguridad para proteger el navegador web puede ser una ayuda efectiva para restringir los daños que el malware puede causar.

Desarrollo

NOTA: ESTA PRÁCTICA SE LLEVARÁ A CABO SOBRE UN EQUIPO VIRTUAL QUEDA ESTRICTAMENTE PROHIBIDO EL CAMBIO EN LA CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Equipo Necesario

HARDWARE
1 Computadora arquitectura X86

SOFTWARE
Windows XP
VMWARE WORKSTATION 6.0
3 Equipos virtuales

Parte 1 Infección

1. Se abrirá la carpeta en el escritorio que lleva por nombre malware.

2. Contaminamos el sistema con el primer programa.

3. Apagamos y reiniciamos el sistema.

4. verificamos el comportamiento del equipo abriendo el administrador de tareas (Ctrl+Alt+Supr).

5. Liste los procesos que se están ejecutando con la sesión del usuario.

_____
_____
_____

a) ¿Encuentra algún proceso sospechoso, diga cuál?

_____
_____

b) ¿Qué comportamiento inusual presenta?

_____
_____
_____

6. Por observación, determine el posible malware que está afectando el equipo

_____

7. Pausamos el equipo y abrimos la siguiente máquina virtual

8. Se abrirá la carpeta en el escritorio que lleva por nombre malware.

9. Contaminamos el sistema con el segundo programa.

10. Apagamos y reiniciamos el sistema.

11. verificamos el comportamiento del equipo abriendo el administrador de tareas (Ctrl+Alt+Supr).

12. Liste los procesos que se están ejecutando con la sesión del usuario.

_____
_____
_____

c) ¿Encuentra algún proceso sospechoso, diga cuál?

_____
_____

d) ¿Qué comportamiento inusual presenta?

_____
_____
_____

13. Por observación, determine el posible malware que está afectando el equipo

_____

14. Pausamos el equipo y abrimos la tercera máquina virtual

15. Se abrirá la carpeta que está en el escritorio y que lleva por nombre malware

16. Contaminamos el sistema con el tercer programa

17. Apagamos y reiniciamos el sistema

18. verificamos el comportamiento del equipo abriendo el administrador de tareas (Ctrl+Alt+Supr)

19. Liste los procesos que se están ejecutando con la sesión del usuario

_____
_____
_____

e) ¿Encuentra algún proceso sospechoso, cuál?

_____
_____
_____

f) ¿Qué comportamiento inusual presenta?

_____
_____

20. Por observación, determine el posible malware que está afectando el equipo.

_____

21. Pausamos el equipo

Parte 2 Desinfección

Abrimos la primera máquina virtual

1. Instalamos el antivirus AVG que se encuentra en la carpeta del escritorio

2. Ejecutamos un análisis rápido

3. ¿Se detectó la amenaza, (si/no) indique porqué?

_____
_____
_____

4. En caso de detectarse busque información en internet y liste los principales atributos de ese malware
5. En caso de no detectarse, instale Ad-Aware y ejecute un análisis rápido

6. Liste el nombre de la amenaza y confirme si su deducción inicial fue correcta

_____
_____

Abrimos la segunda máquina virtual

7. Instalamos el antivirus AVG que se encuentran en la carpeta del escritorio

8. Ejecutamos un análisis rápido

9. ¿Se detectó la amenaza, (si/no) indique porqué?

_____
_____
_____

10. En caso de detectarse busque información en internet y liste los principales atributos de ese malware

11. En caso de no detectarse, instale Ad-Aware y ejecute un análisis rápido

12. Liste el nombre de la amenaza y confirme si su deducción inicial fue correcta

_____
_____

Abrimos la tercera máquina virtual

14. Instalamos el antivirus AVG que se encuentran en la carpeta del escritorio

15. Ejecutamos un análisis rápido

16. ¿Se detectó la amenaza, (si/no) indique porqué?

_____
_____
_____

17. En caso de detectarse busque información en internet y liste los principales atributos de ese malware

18. En caso de no detectarse instalamos Ad-Aware y ejecutamos un análisis rápido

19. Liste el nombre de la amenaza y confirme si su deducción inicial fue correcta

_____
_____

Parte 3 Análisis

1 Haga un cuadro comparativo entre las 3 amenazas encontradas: tipo, objetivo, propagación. Mencione cuáles fueron detectadas por el antivirus y cuáles fueron detectadas por la herramienta especializada.

2 Haga un mapa mental de las principales prevenciones que se deben tomar ante este tipo de amenazas

3. Anote sus conclusiones

_____
_____
_____
_____
_____
_____

3.8 Práctica de laboratorio # 7 - Perímetro de Seguridad

OBJETIVO

Se definirán las pautas mínimas que permitan implementar controles de seguridad que posibiliten el cumplir con los objetivos generales sobre seguridad física.

- Se identificarán las posibles amenazas sobre las instalaciones de servicios informáticos y de resguardo físico de copias de respaldo.

PROCEDIMIENTO

Se hará un recorrido por las instalaciones (edificio Ing. Bernardo Quintana Arrioja) haciendo un análisis de los elementos de procesamiento de sistemas de información que considere sean críticos o sensitivos para la organización (en este caso una sección de la Facultad de Ingeniería), deberán ubicarse áreas seguras, protegidas por un perímetro de seguridad definido.

Desarrollo

Equipo Necesario

1 Hoja de papel
1 Pluma

PERÍMETRO DE SEGURIDAD FÍSICA

La protección física puede ser lograda creando varias barreras físicas alrededor de las instalaciones de procesamiento de sistemas de información.
Cada barrera establece un perímetro seguro, incrementando la protección total provista, siendo una barrera de seguridad, (una pared, una puerta de entrada controlada por una tarjeta o una mesa de recepción).
La ubicación y fortaleza de cada barrera depende de los resultados de una evaluación de riesgo.
Elabore una lista de por lo menos 5 de los elementos existentes y de aquellos que se deben considerar para la creación de barreras efectivas:

1.CONTROLES FÍSICOS DE ENTRADA

Un área segura puede ser una o varias habitaciones dentro de un perímetro de seguridad físico, el cual puede ser cerrado y puede contener gabinetes bloqueables o seguros.

Para la selección y diseño de un área segura se debe tener en cuenta la probabilidad de ocurrencia de amenazas como fuego, agua, explosión, conflicto civil, y otras formas de desastres naturales o realizados por el hombre que amenace la seguridad.

Elabore una lista de de por lo menos 5 de los elementos existentes y de aquellos que se deben considerar para asegurar que solo personal autorizado tenga permitido el acceso

2.SEGURIDAD CIRCUNDANTE

En esta práctica no se hará hincapié, sin embargo es importante evaluar los riesgos potenciales que rodean las instalaciones de la organización, tales como almacenes de materiales inflamables u otros potencialmente peligrosos, también tomar en consideración aquellas zonas próximas que pudieran afectar las telecomunicaciones tales como radiodifusoras, aeropuertos.

3. ACCESO DE VISITAS

Consiste en asegurar que todos los individuos que entran al edificio y al área restringida se identifiquen, sean autenticados y autorizados para entrar.

Se recomienda el uso de tarjeta de identificación personal magnética u otra identificación específica, y proceder al requerimiento automático o manual de ellos cada vez que se ingrese a áreas de servicios informáticos, para determinar la razón de la visita. Dicho requerimiento será realizado ya sea por un sistema automatizado o por una persona apropiada en su manejo, que llevará un registro permanente de todos los tiempos de entrada y salida de cada visitante.

Cabe señalar que estas medidas pueden brindar diferentes niveles de seguridad, un control biométrico ofrece más seguridad y confianza que una simple tarjeta magnética, que es susceptible al robo o pérdida. Lo más recomendable no es el uso exclusivo de métodos de autenticación automatizados,(estos pudieran presentar fallas ante una pérdida de energía o una variación de voltaje), sino una combinación de manuales y automáticos, así teniendo lo mejor de cada uno de ellos haciendo más robusta la seguridad en el control de acceso.

SEGURIDAD DE RECURSOS

Para prevenir pérdidas, daños o compromisos de los activos y la interrupción de las actividades de negocio, los equipos deberán ser protegidos físicamente de las amenazas de seguridad y peligros ambientales.
La protección de equipamiento (incluyendo los que se usan fuera del sitio) es necesaria para reducir el riesgo por accesos no autorizados a los datos y para proteger contra la pérdida o daños.
Se deberá considerar también el equipamiento instalado y el desechado.
Controles especiales pueden ser requeridos para proteger contra peligros o accesos no autorizados y para salvaguardar las instalaciones de soporte como la provisión de energía y la infraestructura de cableado.

LOCACIÓN Y PROTECCIÓN DE LOS EQUIPOS

El equipamiento deberá estar situado y protegido para reducir el riesgo de materialización de amenazas y peligros ambientales, así como las oportunidades para accesos no autorizados.

Elabore una lista de por lo menos 10 controles que deberán ser considerados:

1.EQUIPOS DE DETECCIÓN.

Para contrarrestar los efectos de las amenazas enumeradas precedentemente, las organizaciones deben considerar:

a. Instalar sistemas de detección adecuados como detectores de humo, calor, fuego, agua, etc., para proteger los elementos dentro del área de servicios y en cualquier área donde los medios magnéticos de computación, discos y otros registros se almacenan (incluyendo áreas de almacenamiento fuera del lugar habitual).

b. Asegurar por parte del responsable del área de servicios y sus dependencias la remoción inmediata de material inflamable del interior y alrededores del mismo.

c. Limitar el almacenamiento de papel y otros materiales combustibles en el sector de operaciones.

d. Observar el orden y limpieza y hacer cumplir las reglas de prohibición de fumar, comer y beber en el sector de equipos.

e. Verificar y Aprobar por personal técnico de los organismos de seguridad de las instalaciones de detección de incendios, calor, humo y agua.

2.SUMINISTRO DE ENERGÍA ELÉCTRICA

Los equipos de tecnología de la información deben ser protegidos de fallas de energía y otras anomalías eléctricas. La provisión de energía debe ser provista conforme a las especificaciones del fabricante de equipos.

Elabore una lista de por lo menos 10 elementos que deberán ser considerados para lograr una provisión continua de energía.

3.EXPOSICIÓN AL FUEGO

Los sistemas de detección y extinción deben estar funcionando correctamente, ya que su objetivo es proteger las instalaciones y equipos en caso de fuego.

a) Debe existir un sistema de detección de fuego, calor o humo que actúe en forma automática sobre el sistema de extinción.
b) Debe existir un sistema manual que actúe sobre el sistema de extinción de incendios.
c) Inspeccionar el sistema de extinción de fuego en forma periódica.
d) Probar el sistema en forma periódica.
e) Conservar los planos de la instalación y el acceso a los mismos debe ser para personal autorizado.
f) Instruir al personal del área de servicios informáticos en particular y al resto de la organización en general, sobre medidas de detección y extinción de incendios.

4. AMENAZAS POR ACCIÓN DE AGUA

Se implementarán medidas para prevenir y reducir daños por acción del agua o líquidos.

5.MANTENIMIENTO DE EQUIPOS

El equipamiento debe ser mantenido correctamente para asegurar su continua disponibilidad e integridad. Los siguientes controles deben ser considerados para los equipos de cómputo:

a) Deben ser mantenidos de acuerdo con las especificaciones de servicio recomendados por el vendedor.
b) Las reparaciones y servicios deben ser realizados sólo personal de mantenimiento autorizado.
c) Deberán conservarse registros de las fallas y todos los mantenimientos preventivos y correctivos realizados.

6. SISTEMAS DE AMBIENTACIÓN

Evaluar la calidad del sistema de acondicionamiento de aire considerando:

a) Velar por el cumplimiento de las normas de control y seguridad para que no se produzcan hechos que afecten al medio ambiente donde deben procesarse los datos del organismo.
b) Asegurar que la cantidad de contaminación que se encuentra habitualmente en el aire no interfiera en la operación de los equipos. Para ello deben existir sistemas de detección que permita actuar a los sistemas de acondicionamiento de aire, encendido/apagado automático a cierta temperatura, y renovación del aire del ambiente, debiéndose administrar en los equipos:

    - Temperatura
    - Ventilación
    - Filtros
    - Protección.
    - Sistema alternativo de Back-Up
    - Aprobar por personal técnico de la organización las instalaciones.

7. PROCEDIMIENTOS DE BACK-UP

Se deben realizar copias de resguardo de los archivos de datos, software de base y de aplicaciones, documentación de operaciones y de sistemas de aplicación

8. CONTROL DE AMENAZAS

Determinar la existencia de procedimientos para controlar riesgos originados entre otros por:

- Combustibilidad de materiales de uso diario.
- Contaminación y suciedad del aire.
- Estática de los equipos.

9. PLAN DE CONTINGENCIA

Asegurar la existencia del Plan de Contingencias y que el personal esté capacitado para su aplicación.

10. CAPACITACIÓN DE PERSONAL

Revisar el entrenamiento del personal y políticas que aseguren alcanzar el nivel de conocimiento sobre seguridad para el caso de accidentes.

Controles y directivas adicionales pueden ser requeridas para ampliar la seguridad de un área segura.

Esto incluye controles para el personal o terceras partes trabajando en el área segura, así como actividades de terceras partes que tienen lugar aquí.

Elabore una lista de por lo menos 10 controles que deberán ser considerados:

11. SEGUROS

Se debe verificar la existencia de cobertura de seguros, sobre los equipos de tecnología de la información.

a) Verificar la existencia de coberturas de seguro contra desastres producidas por amenazas naturales, fuego, fraude y robo, cubriendo las pérdidas directas e indirectas.

SEGURIDAD DE EQUIPOS FUERA DE LAS INSTALACIONES

Sin tener en cuenta la propiedad, el uso de cualquier equipo fuera de los sitios organizacionales para el procesamiento de la información debe ser autorizado por la dirección o gerencia.
La seguridad provista deberá ser equivalente a aquella proporcionada a los equipos on-site usados para el mismo propósito, tomando en cuenta los riesgos del trabajo fuera de las locaciones de la organización.
El equipamiento de procesamiento de la información incluye todas las formas de computadoras personales, organizadores, teléfonos móviles, papeles u otros formularios, los cuales son soporte para trabajo en casa o son transportados fuera del sitio normal de trabajo.

Elabore una lista de por lo menos 5 directivas que deben ser consideradas:

ÁREAS DE ENTREGA Y CARGA

Las áreas de entrega y carga de insumos deberán ser controladas y si es posible, aisladas de las instalaciones de procesamiento de la información para evitar accesos no autorizados. Los requerimientos de seguridad para tales áreas deberán ser determinadas por una evaluación de riesgos.

Elabore una lista de por lo menos 10 controles que deberán ser considerados:

SEGURIDAD DE CABLEADOS

El cableado de energía y comunicaciones que transportan datos o soportan servicios de información deberán ser protegidos para evitar una intercepción o daño. Los siguientes controles deben ser considerados:

a) Las líneas de energía y telecomunicaciones dentro de las instalaciones de procesamiento de la información deberán estar bajo tierra, cuando sea posible, o sujetos a una protección alternativa adecuada.
b) El cableado de redes debe estar protegido para evitar intercepciones no autorizadas o daños, por ejemplo usando canaletas o evitando el tendido a través de áreas públicas.
c) Los cables de energía deberán estar separados de los cables de comunicaciones para prevenir interferencias, de acuerdo a las recomendaciones del fabricante y de los estándares en vigencia.
d) Para sistemas críticos o sensitivos se debe considerar incluir controles adicionales:

- La instalación de conductores armados y armarios o habitaciones bloqueadas en los puntos de terminación e inspección.
- Uso de rutas o medios de transmisión alternativos.
- Uso de cableado de fibra óptica.
- Iniciadores de barrido deberán ser conectados a los cables para detección de dispositivos no autorizados.

CONTROLES GENERALES

La información y las instalaciones de procesamiento de la información deben ser protegidas para evitar la divulgación, modificación o el robo por parte de personas no autorizadas a su manejo y se deben implementar controles para minimizar las perdidas o daños.
Se deben adoptar políticas que mantengan el orden en los ambientes de trabajo, con el propósito de reducir el riesgo de accesos no autorizados, pérdida de documentación y daño a la información durante y fuera de las horas normales de trabajo. La información dejada sobre los escritorios es también probable de ser dañada, destruida o robada.
La política debe tener en cuenta las clasificaciones de la información, los riesgos correspondientes y aspectos culturales de la organización.

Elabore una lista de por lo menos 5 controles que deberán ser considerados:

RESPONSABLES

Todo el personal de la organización está encargado de la seguridad física de los recursos relacionados a los sistemas de información a los que tienen acceso y los que están a su cargo.

El responsable de seguridad debe velar por el cumplimiento de las definiciones de seguridad.

Investigue el nombre del responsable del área de servicios informáticos del laboratorio de redes y seguridad.

_____

Con sus propias palabras indique la importancia de los controles de acceso para cumplir los objetivos de una organización.

_____
_____
_____
_____

Anote sus conclusiones

_____
_____
_____
_____
_____
_____

3.9 Práctica de laboratorio # 8 - Análisis de Vulnerabilidades

Objetivos de aprendizaje

- Que el alumno tome conciencia acerca de la importancia que tienen las vulnerabilidades en los sistemas de cómputo (personales y a nivel de red).
- Que el alumno se familiarice con las capacidades de una herramienta de Análisis de vulnerabilidades y comprenda su forma de operar.
- Que el alumno sea capaz de interpretar los resultados obtenidos luego de haber llevado a cabo un Análisis de Vulnerabilidades en una PC objetivo.
- Comprender la importancia de contar con un ciclo de administración de vulnerabilidades en infraestructuras de red.

Materiales y Equipo

HARDWARE
1 Computadora arquitectura X86

SOFTWARE
Windows XP

Nessus **4.4.0**
Zenmap 5.00

Introducción

Los análisis de vulnerabilidades son un componente esencial dentro de la seguridad informática, son capaces de descubrir y definir una guía para el aseguramiento de los datos; sin embargo, el escaneo periódico provee información actualizada acerca de la administración de las vulnerabilidades en un ambiente de red, son capaces de generar tendencias y reportes de cumplimiento con políticas.

Las herramientas utilizadas para la ejecución de análisis de vulnerabilidades proveen los fundamentos de seguridad para una infraestructura de red desde una base de datos de vulnerabilidades conocidas, la cual se actualiza periódicamente.

Existen tres tipos de herramientas de Análisis de Vulnerabilidades, explique cada una de ellas:

Escaneo de red activo

_____
_____
_____
_____

Observación del tráfico de red pasivo

Basado en Agentes

Para obtener resultados más exactos sobre las vulnerabilidades en los sistemas, se requieren de credenciales y permisos administrativos sobre los mismos (ya sea a través de la red o con la utilización de agentes).

Las Organizaciones de Seguridad TI (Tecnologías de la Información) requieren que el análisis de las vulnerabilidades se ejecute a través de la red para que de forma precisa se descubran y evalúen las vulnerabilidades tanto en sistemas administrados como en no administrados. De cualquier forma, para que un Análisis de Vulnerabilidades sea utilizado para mejorar la seguridad y satisfacer los requerimientos de auditoría, ellos deben contar con capacidades de priorización de eventos y de reportes.

Las Organizaciones también necesitan implementar un ciclo de vida (véase Figura 3.59) para la administración de vulnerabilidades para hacer el ambiente más seguro.

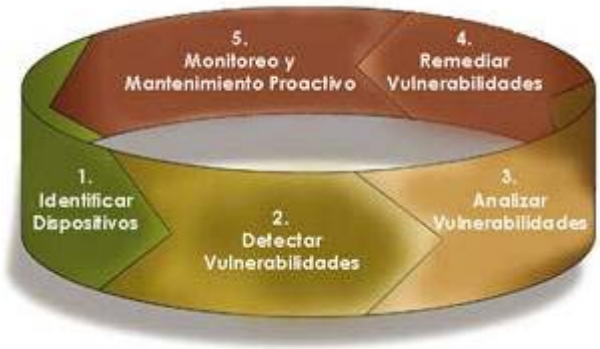


Figura 3.59- Ciclo de Vulnerabilidades

Escaneo de Red con ZENMAP

Utilizando ZENNMAP for Windows 5.2.1, el cual ya se encuentra instalado en la PC asignada, realizar los escaneos que se describen a continuación. (véase Figura 3.60)

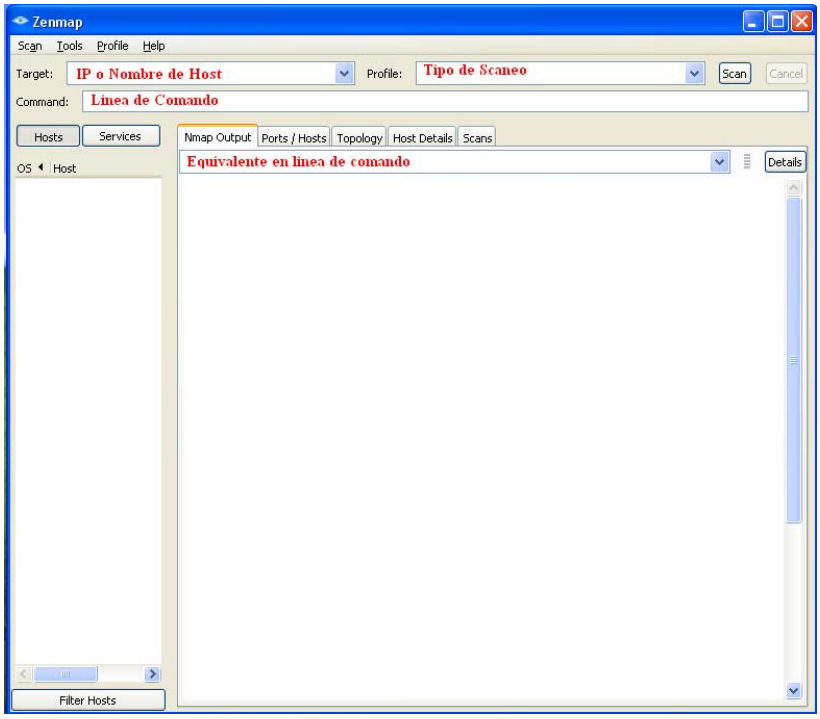


Figura 3.60- Pantalla de ZENMAP

Ejercicio 1

1. Escaneo de red (ICMP)

Utilizando ZENNMAP realizaremos un escaneo "PING SCAN" de la red local para obtener el número de direcciones IP disponibles para esta red.

Anote el resultado obtenido

_____
_____
_____
_____
_____

2. Escaneo de red (Intense scan) a servidor remoto

Utilizando ZENNMAP, realizar un escaneo "Intense scan" de un equipo en la red local y obtener protocolos y puertos abiertos disponibles para ese host. Anote Al menos 10 puertos con diferentes servicios

Anote el resultado obtenido

_____
_____
_____
_____

3. Escaneo ZENNMAP de host

Utilizando Nmap y las dos primeras direcciones IP detectadas en el punto 1, realizar un escaneo de puertos TCP de estas dos máquinas, y realice una tabla donde indique dirección IP, puerto, estado y servicio del puerto asociado.

	dirección IP	purto	estado	servicio
Máq 1				
Máq 2				

4. Detección de Sistema Operativo

Utilizando ZENNMAP, realizar un escaneo de sistema operativo de la red local que se está ejecutando en la máquina e indique la dirección IP y el sistema operativo utilizado.
Anote el resultado obtenido

_____
_____
_____

5. Escaneo ZENNMAP de host remoto

Solicite al profesor la dirección de host remoto a analizar.

Anote el resultado obtenido

_____
_____
_____
_____
_____

¿Qué diferencias se presentan entre el escaneo a equipos de la red local y a un host remoto? Mencione al menos 5 diferencias

_____
_____
_____
_____
_____

Escaneo de Red y Vulnerabilidades con Nessus

1. Iniciaremos creando nuestros perfiles para el uso de la herramienta dando click en el icono del escritorio "Nessus Server Manager". Figura 3.61

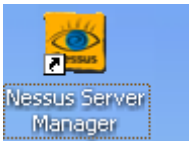


Figura 3.61 – icono de la aplicación

A continuación se debe seleccionar la opción de Manage Users. Figura 3.62

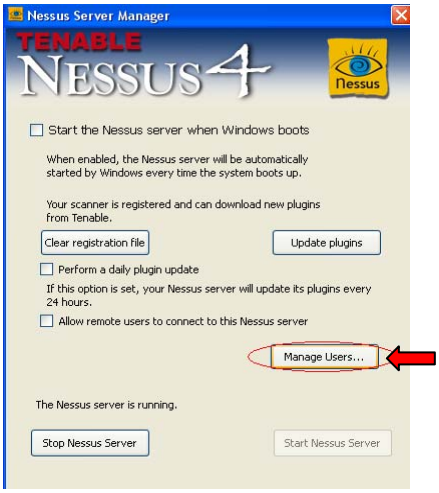


Figura 3.62 – Nessus Server Manager

2. A continuación aparecerá el administrador de usuarios donde crearemos un nuevo usuario para el programa presionando el botón [+]. Figura 3.63

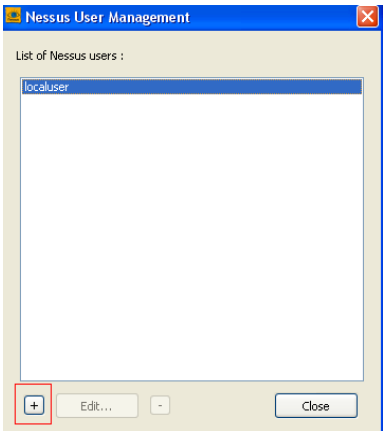


Figura 3.63 - Nessus User Manangement

3. Ingresamos datos como nombre de usuario y contraseña en la nueva caja de dialogo que aparece sin olvidar habilitar la casilla de Administrador. Véase figura 3.64

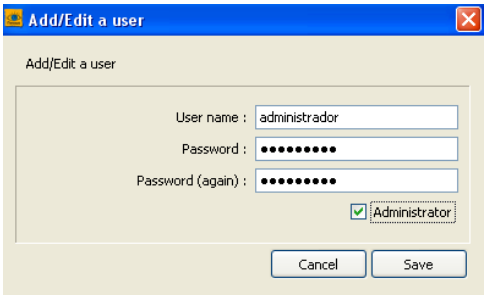


Figura 3.64 – Agregar / editar usuario

4. Presionamos el botón de SAVE y acontinuacion presionamos el boton de CLOSE. (Figura 5)

Una vez creado el nuevo usuario, iniciamos la aplicación dando click en el icono del escritorio NESSUS CLIENT. (Figura 3.65)

Figura 3.65 NESSUS CLIENT

5. Al dar click nos abrirá una ventana del navegador por defecto del equipo dirigiéndonos a la dirección https://localhost:8834/

6. Una vez abierta la página aparecerá una página donde podremos loguear con nuestra cuenta previamente creada(Figura 3.66)

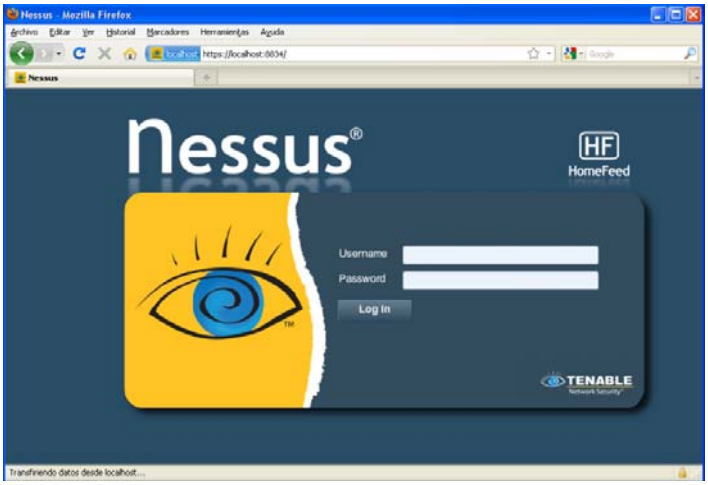


Figura 3.66 Ventana de logueo

7. Una vez iniciada la sesion tenemos el siguente panel de herramientas(ver figura 3.67)

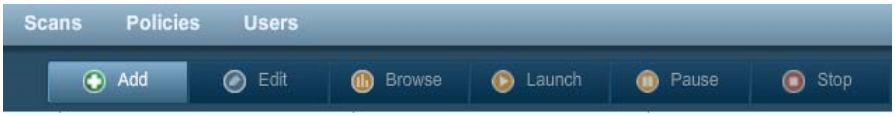


Figura 3.67 - Opciones del Nessus

Antes de iniciar el escaneo debemos configurar las políticas seleccionando el botón de POLICIES y después el botón de ADD

8. A continuación seleccionaremos las opciones para el escaneo tal y como se muestra en la figura 3.68

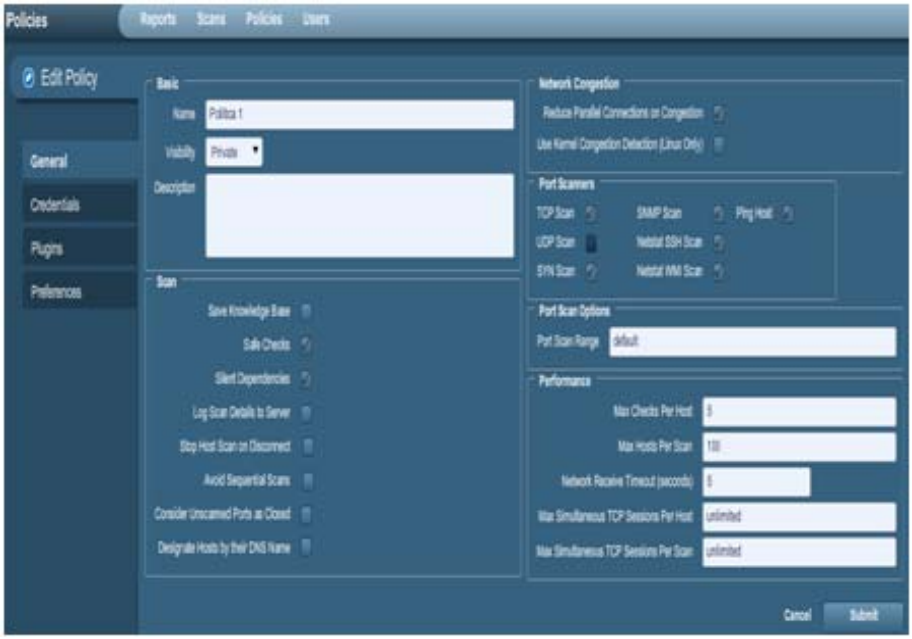


Figura 3.68 – opciones de NESSUS

10. Presionamos el Botón de SUBMIT

11. En la siguiente ventana nos pedirá que escribamos las credenciales de Windows, no ingresamos ningún dato y a continuación NEXT.

12. En la siguiente ventana en el cuadro FAMILIES desplazamos la barra de navegación hasta encontrar la opción de Windows, la seleccionamos, después presionamos el botón ENABLE ALL y a continuación NEXT.

13. Finalmente presionamos el botón SUBMIT.

14. En la barra de herramientas seleccionamos la opción de SCANS y después el botón de ADD.

15. Ingresamos los datos correspondientes como se muestra en la Figura3.69

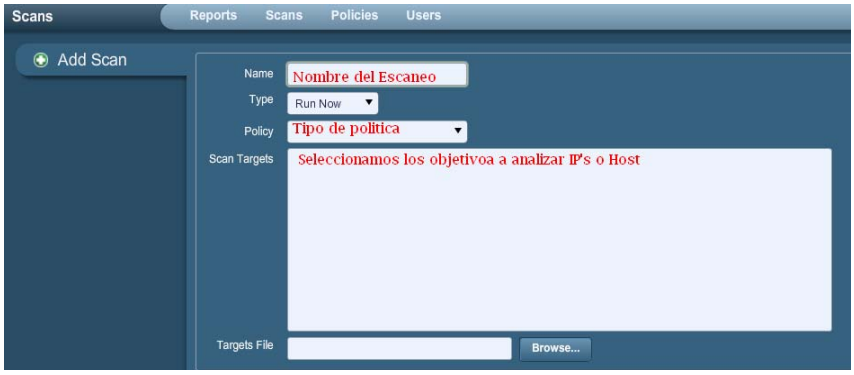


Figura 3.69 – Opciones del escaneo

Para realizar la comparativa respectiva revisaremos dos direcciones IP de nuestra red local

16 Presionamos el botón de LAUNCH SCAN

17. Una vez terminado el escaneo debemos seleccionar la opción de REPORTS y el nombre que le habíamos puesto a nuestro escaneo

18. Para desplegar la información obtenida simplemente damos click en el nombre de los host analizados para obtener los resultados

Ejercicio # 2

1. Utilizando Nessus realizar un escaneo de puertos de los host analizados. Con los datos obtenidos, elaborar una tabla que indique, dirección IP del host, puertos TCP y UDP disponibles y riesgos de seguridad detectadas con Nessus.

dirección IP	puerto TCP	puerto UDP	riesgos

2. Escaneo de Vulnerabilidades de servidor Web (según indique el profesor)

Utilizando Nessus, realizar un escaneo de las vulnerabilidades de dos servidores WEB cualquiera, analizando los puertos comprendidos entre el 15 y el 85, donde se realice una detección de Sistema Operativo. Con los datos obtenidos se realizará una tabla donde se indiquen: el servidor WEB, puertos disponibles, Sistema Operativo utilizado, y riesgos de seguridad.

Servidor WEB	Puertos disponibles	Sistema operativo	Número de riesgos

3. Utilizando la información proporcionada por Nessus y los boletines de seguridad disponibles en Internet, indicar para tres de los riesgos y agujeros de seguridad detectados la siguiente información:

a. Identificación del riesgo/agujero de seguridad.

b. Descripción del problema.

c. Exploits disponibles para dicha vulnerabilidad.

d. Solución a los problemas detectados.

4. Compare los resultados obtenidos al analizar los puertos y su uso en los host locales con ZenNmap y Nessus, indique si existe alguna diferencia entre ambos resultados. REVISAR

Anote sus conclusiones

_____
_____
_____
_____
_____
_____

3.10 Práctica de laboratorio # 9 - VLAN

Objetivos

En esta práctica se realizarán las configuraciones básicas del switch:

- Se definirá el direccionamiento en los equipos PC.
- Se creará una red de Frame Relay
- Se establecerá el enrutamiento entre VLAN.

Introducción

Defina lo que es una VLAN

La comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según lo defina el administrador de la red (direcciones MAC, números de puertos, protocolo, etc.).

La VLAN permite definir una nueva red por encima de la red física.

Mencione al menos tres ventajas que ofrece el uso de las VLANS y explíquelas:

Defina lo que es Frame-Relay y su funcionamiento

Mencione ¿qué es un DLCI?

_____

_____

_____

En la especificación Frame-Relay básica, los DLCI son significativos a nivel local (los dispositivos conectados pueden usar distintos valores para especificar la misma conexión).

Desarrollo

Equipo Necesario

Hardware

1 Computadora con arquitectura X86

Software

Microsoft Windows XP
Packet tracer versión 5.0

Desarrollo

Mediante el programa de packet tracer crearemos el siguiente escenario. Figura 3.70

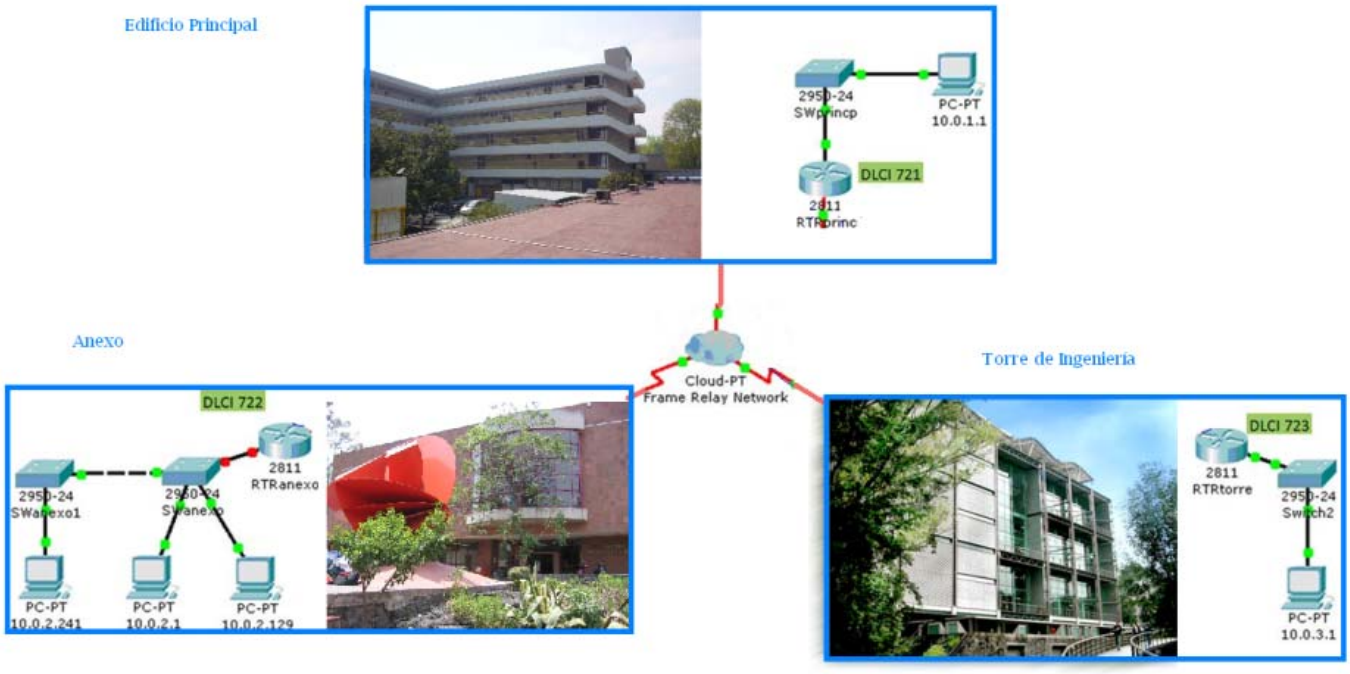


Figura 3.70 Conexión Física

Se contratarán con la compañía telefónica dos circuitos virtuales frame relay de 128 kbps; uno entre el edificio principal y el anexo y el otro entre el edificio principal y la torre de ingeniería (Figura 3.71)

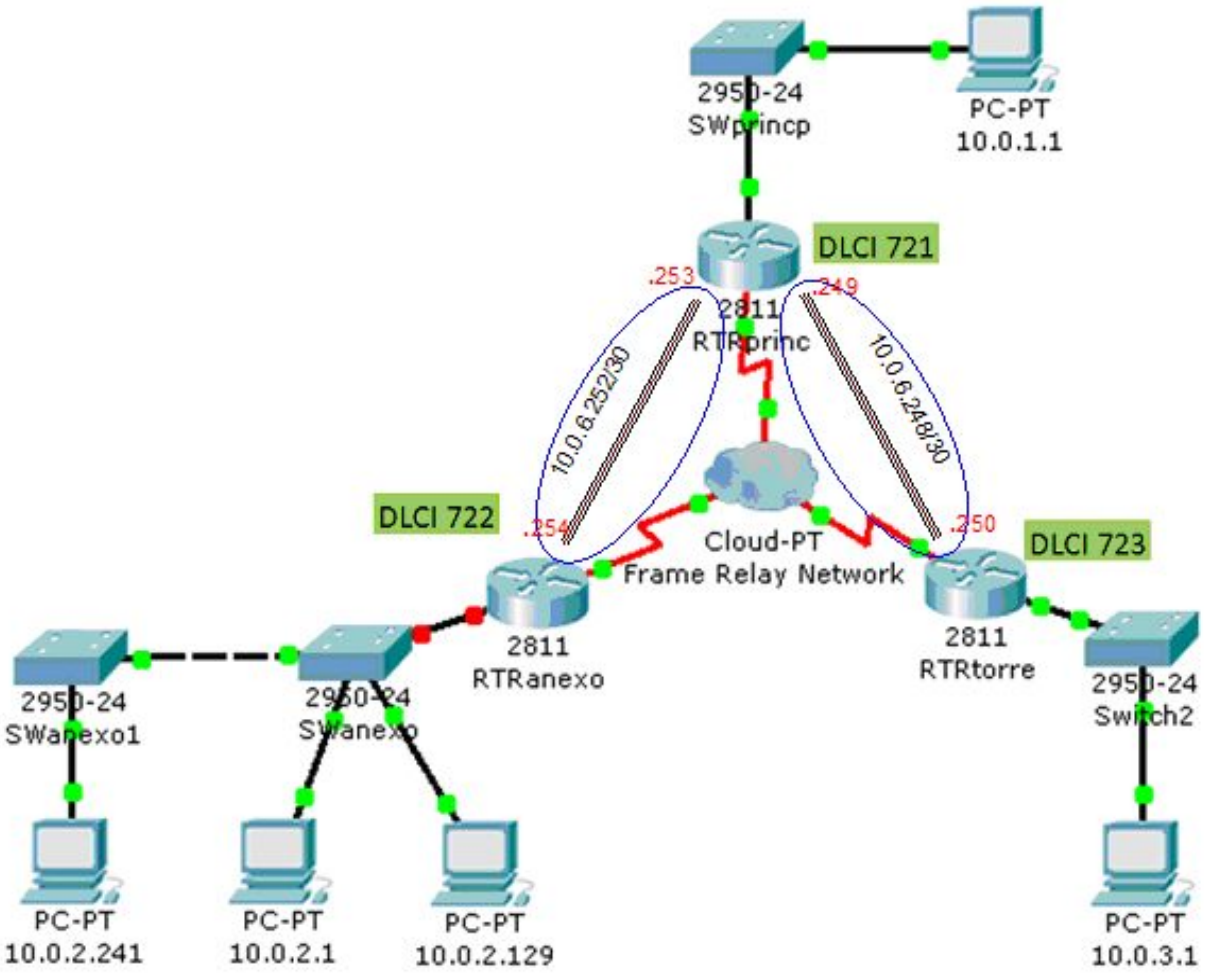


Figura 3.71 Construcción de la red

Se tomarán en cuenta las siguientes configuraciones:

- 5 Equipos PC Terminales
- 4 Switches 2950-24
- 3 Router 2811
- 2 Enlaces Frame Relay a 128 kbps
- Direcciones IP
- RTRanexo
- RTRtorre
- RTRprincipal

Parte 1.

Configurar los ruteadores para conectarse a la red frame relay utilizando los DLCI que se indican. Para la configuración de las interfaces serie de los ruteadores, definir la subnet 10.0.6.252/30 en el enlace entre el principal y el anexo. Definir la subnet 10.0.6.248/30 en el enlace entre el principal y la torre.

Defina qué es un CSU/DSU y en qué capa del modelo OSI opera

_____
_____
_____
_____
_____

El primer paso dentro de la configuración de Frame-Relay es el de la activación de la interfaz que conecta a dicho router con una CSU/DSU, conectada a su vez con el switch del proveedor.

Accedemos a configurar los routers, en el Router0 damos un clic y de la misma forma que en las pc's, se abrirá una ventana. Esta nueva ventana constará de tres pestañas denominadas Physical, Config y CLI. Como ya mencionamos, en Physical se muestra la información relacionada con cada interfaz del dispositivo al igual que las imágenes relacionadas.

En Config, aparece la configuración por botones del router, y en la parte inferior aparecen las instrucciones de consola. En CLI, se presenta la consola del router, en esta parte debemos ingresar los comandos del IOS para configurar el router. Nota: Pueden mezclarse las opciones de configurar el router por botones o por comandos de consola.

En CONFIG, tenemos las opciones Static y RIP, de enrutamiento Estático y Dinámico (RIP). No modificaremos hasta que indiquemos las interfaces, esto es en el siguiente paso. En INTERFACE aparecen las interfaces disponibles, Serials y FastEthernet (Seriales y FastEthernet). Por ser un router genérico se nos provee cuatro interfaces FastEthernet y dos interfaces Seriales.

Router(config)#interface Serial 1

Router(config-if)#ip address [direction IP+máscara]

Router(config-if)#encapsulation frame-relay

Router(config-if)#bandwidth [valor del ancho de banda en Kbps]

Si fuera necesario, según la versión de IOS, configurar LMI:

Router(config-if)#frame-relay lmi-type [cisco/anci/q933a]

Mencione que es el protocolo ARP inverso(InARP)

_____

_____

_____

ARP inverso está activado por defecto, si fuera necesario activarlo:

Router(config-if)#frame-relay inverse-arp [protocolo] [dlci]

Donde:

protocolo: IP, IPX, appletalk, decnet, etc

dlci: numero de dlci de la interfaz local, valor entre el 16 y 1007.

Configuración estática de Frame-Relay

Cuando un router no soporta ARP inverso, o cuando se quiere controlar el tráfico sobre los circuitos virtuales se debe definir estáticamente una tabla de dirección remota y su DLCI.

A partir de la configuración básica se agrega le mapeo estático:

Router(config-if)#frame-relay map [protocolo][dirección destino][DLCI local][broadcast][ietf/cisco][payload-compress paket-by-paket]

Donde se define el tipo de protocolo, la dirección IP del destino y el DLCI local. Con dispositivos Cisco no es necesaria la configuración de la encapsulación, mientras que con dispositivos no Cisco se debe utilizar IETF. Los parámetros restantes son opcionales y habilitan el envío de difusiones y la compresión de sobrecarga.

Pruebe la conectividad haciendo un ping del ruteador en el principal a los ruteadores del anexo y la torre y viceversa.

Parte 2.- Configurar el protocolo de ruteo OSPF en los ruteadores.

Mencione que es el protocolo OSPF

_____

_____

_____

_____

_____

Para habilitar OSPF por medio del comando:

Router(config)#router ospf process-id

Router(config-router)#network address wildcard-mask area area-id

Donde:

process-id es el número que se usa internamente para identificar si existen múltiples procesos OSPF en ejecución dentro del router.

network identifica las redes directamente conectadas, identificadas por medio de su correspondiente máscara de wildcard

area para cada red, deberá identificar además a qué área pertenece. El área principal o de Backbone es el área 0.

La modificación del ID de router OSPF en una dirección loopback implica definirla de la siguiente manera:

Router(config)#interface loopback number

Router(config-if)#ip address ip-address subnet-mask

La modificación de la prioridad de router implica cambiar la prioridad OSPF de una interfaz por medio del siguiente comando:

Router(config-if)#ip ospf priority number

Router#show ip ospf interface type number

Parte 3

Defina TRUNKING

_____

_____

_____

Configure el ruteador para realizar 802.1q trunking entre las 2 VLAN´s conectadas. Para que las Vlans puedan establecer comunicación entre ellas deben ser necesarios los servicios de un router. Para esto se deben establecer Subinterfaces FastEthernet, encapsulación y dirección IP correspondiente de manera que cada una de éstas pertenezca a una vlan determinada. Figura3.72

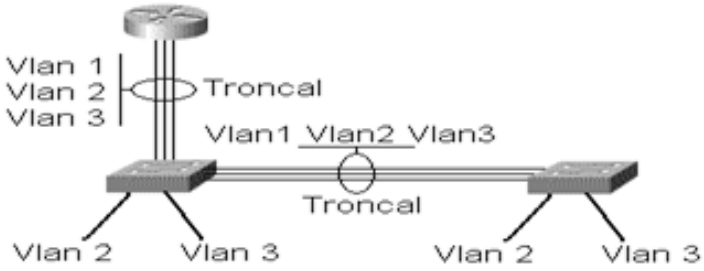


Figura 3.72 Trunking entre vlans

Los pasos que siguen permiten establecer las configuraciones de una Subinterfaz FastEthernet

Router(config)#interface fastethernet Nºde slot/Nºde interfaz.Nºde subinterfaz
Router(config-subif)#encapsulation [dot1q|ISL] Nºde vlan
Router(config-subif)#ip address direccion IP+mascara
Router(config-subif)#exit
Router(config)#interface fastethernet Nºde slot/Nºde interfaz
Router(config-if)#no shutdown

Pruebe la conectividad entre las dos VLAN´s haciendo un ping entre las PC´s en el anexo 10.0.2.241 y la 10.0.2.1

También configure 2 VLAN´s en el anexo: sistemas y telecoms con las subnets 10.0.2.0/25 y la 10.0.2.128/25.

Parte 4

Defina el protocolo TELNET, ¿Qué puerto emplea? y su uso

_____

_____

_____

Configure el switch anexo1 para poder acceder a su configuración desde la PC 10.0.3.1. Pruebe la conexión listando la tabla ARP del switch. Para poder acceder al switch anexo 1 a través de la red (telnet), deberá configurársele una dirección IP y un password.

---Configuración de la IP en el Switch anexo1---

SWanexo1(config)#interface vlan 3

SWanexo1(config-if)#ip address 10.0.2.242 255.255.255.128

SWanexo1(config-if)#exit

SWanexo1(config)#ip default-gateway 10.0.2.254

---Configuración de contraseñas---

```
SWanexo1(config)#enable password contraseña
SWanexo1(config)#enable secret usuario
SWanexo1(config)#line console 0
SWanexo1(config-line)#login
SWanexo1(config-line)#password 12
SWanexo1(config-line)#exit
SWanexo1(config)#line vty 0 4
SWanexo1(config-line)#login
SWanexo1(config-line)#password 456
SWanexo1(config-line)#
```

¿El uso del protocolo TELNET es seguro?, ¿Por qué?

_____
_____
_____

¿Qué protocolo es empleado actualmente en sustitución del telnet?

_____
_____
_____

Anote sus conclusiones

_____
_____
_____
_____
_____

3.11 Práctica de laboratorio # 10 - VPN y Cloud Computing

Objetivos

- Se establecerá una VLAN a través del Internet
- Realizará acceso a la nube
- Compartirá recursos en una VLAN y en una nube

Introducción

VPN (siglas en inglés de Virtual Private Network)
Una red privada virtual o VPN, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Figura 3.73

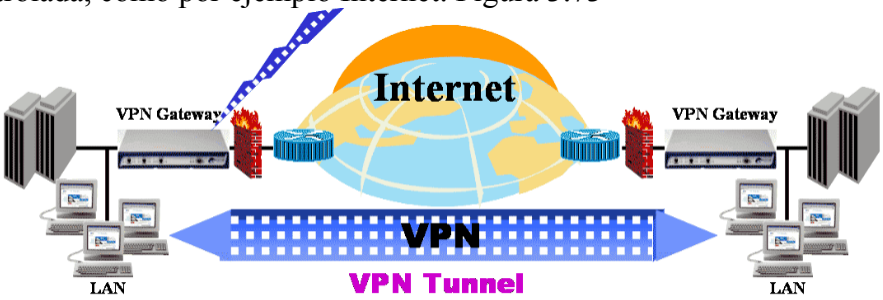


Figura. 3.73 VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU(*Protocol Data Units*) con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que pudiera ser SSH.

VPN sobre LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Cloud Computing

La computación en nube o informática en nube, del inglés "Cloud Computing", es un paradigma que permite ofrecer servicios de computación a través de Internet. La "nube" es una metáfora de Internet.

En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicial, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan.

Esta clase de servicio no es totalmente nueva, ya que uno de los primeros servicios con esta idea es el email en la web, como por ejemplo Yahoo, Hotmail, etc.

La idea tras una aplicación “cloud” es que el usuario tenga acceso a su información, que está almacenada en Internet (la nube), en cualquier lugar y desde cualquier computadora, sin importar el sistema operativo, o incluso desde un Smartphone. Figura 3.74

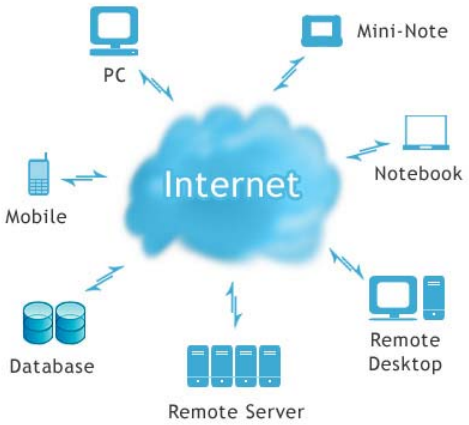


Figura.3.74 Accesos a la nube

La computación en nube se sustenta en tres pilares fundamentales: software, plataforma, e infraestructura. Cada pilar cumple un propósito diferente en la nube y cubre distintas áreas de productos y servicios para empresas y particulares de todo el mundo. Defina cada uno de ellos:

Software

_____
_____
_____

Plataforma

_____
_____
_____

Infraestructura

_____
_____
_____

Ventajas

Los usuarios de la nube no deberán preocuparse por gestionar el software o hardware, ahora la responsabilidad de la administración queda en manos de un proveedor, quienes son expertos en las herramientas brindadas y en los recursos de hardware ofrecido. Las actualizaciones de software y hardware son automáticas, en la gran mayoría de casos transparentes para el usuario, y este último, solo debe preocuparse por ampliar o reducir el servicio de acuerdo a sus necesidades.

Los costos de la computación en nube son menores frente a un servicio similar como Grid Computing, en algunos casos estos servicios son gratuitos como Google Apps.

Defina Grid Computing

_____
_____
_____

Los servicios se pueden acceder casi desde cualquier parte del mundo donde se destaca su alta disponibilidad para la gran mayoría de servicios.

La Escalabilidad puede ser manejada muy rápidamente y de acuerdo a la necesidad del usuario, ejemplo: aumentando el número de nodos de procesamiento requeridos(a un costo adicional). Un ejemplo práctico de esta situación son los sitios de noticias que colapsan con sucesos muy populares. Otro ejemplo puede darse ser en el sector financiero, cuando algunos servicios experimentan un picos de procesamiento en las fechas límite de pago, estos casos, en su mayoría, pueden ser solventados aumentando los nodos de procesamiento.

En algunos casos, la nube puede tener redundancia localizada en distintos puntos geográficos, en estas situaciones, existen servicios especializados que redireccionan el tráfico dependiendo de la ubicación geográfica de quien los solicita, disminuyendo los tiempos de respuesta.

Desventajas

Al depender de los servicios de un tercero, si nuestro proveedor presenta inconvenientes técnicos, nos veríamos imposibilitados para acceder el servicio, claro está, como mencioné antes, muchos de estos servicios se han convertido en servicios de alta disponibilidad lo que reduce considerablemente el tiempo de inactividad o downtime del servicio en caso de una falla.

Acceso de nuestra información por parte de terceros dado que nuestra infraestructura de software y hardware, y, la administración de la misma, queda en manos de un proveedor.

Al depender de un servicio en línea(Internet), nuestra disponibilidad del servicio depende de nuestra capacidad para accesar la web, que como sabemos, en algunos sitios no se presenta cobertura o simplemente la calidad de la conexión no es la adecuada.

Ejemplos de servicios de Cloud Computing

Google Apps: ofrece servicios como Google mail, Google Docs y Google Calendar entre otros.

AWS (Amazon Web Services): ofrece servicios como Amazon S3 (Amazon Simple Storage Service), Amazon EC2 (Amazon Elastic Compute Cloud) y Amazon RDS (Amazon Relational Database Service) entre otros.

Microsoft Cloud Services: entre los servicios más reconocidos se encuentran Microsoft Exchange Online, Microsoft SQL Azure y Microsoft Sharepoint Online.

Dropbox: es el ejemplo más práctico de computación en nube, donde el proveedor ofrece un servicio de almacenamiento en línea que permite la sincronización sus archivos en línea y con otros computadores.

VPS.net: ofrece un servicio de hosting en nube, y un servicio de hosting de contenidos. Estos servicios poseen redundancia en dos continentes distintos que entregan el contenido de acuerdo al nodo que más convenga según la ubicación geográfica.

Desarrollo

Equipo Necesario

HARDWARE
1 Computadora arquitectura X86

SOFTWARE
Windows XP
Hamachi
Dropbox

Parte 1 VPN

Hamachi es una aplicación gratuita configuradora de redes privadas virtuales capaz de establecer vínculos directos entre computadoras que están bajo firewalls de NAT sin requerir reconfiguración alguna (en la mayoría de los casos). En otras palabras, establece una conexión a través de Internet y simula una red de área local formada por ordenadores remotos.

1. Iniciamos la instalación del programa ejecutando el instalador que se encuentra en el escritorio

2. Seleccionamos el idioma para la instalación de Hamachi
3. A continuación nos muestra información acerca de la versión en este caso la 2.0.3.89. Seleccionamos el botón de siguiente.
4. Aparecerán los términos de la licencia, seleccionamos el botón de Acepto.
5. Seleccionamos el directorio de instalación y oprimimos el botón de instalar.
6. Terminada la instalación damos click en el botón de terminar.

7. Al iniciar nos mostrara una ventana como la siguiente: Figura 3.75

Figura 3.75 Ventana de inicio Hamachi.

8. Al presionar el botón de encendido nos aparecerá una ventana donde debemos asignar un nombre para que sea identificado el host en Hamachi. Presionamos el botón crear

9. Aparecen 2 opciones de configuración:

a) Crear una nueva red
b) Unirse a una red existente

10. En grupos de 4 personas elegirán un nombre para la red a la cual se conectarán.

11. Solo una persona registrara el nombre de la nueva red, seleccionará la opción de crear una nueva red, esto con el fin de que los demás miembros del grupo se unan posteriormente.

12. Se debe escribir una contraseña para la red creada con el fin de restringir la cantidad de usuarios que tengan acceso a ella. Dará click en el botón crear.

13. Los demás miembros del equipo deberán unirse a la red recién creada seleccionado la opción Unirse a una red existente

14. Ingresara los datos de acceso respectivos

15. Una vez completado el acceso arriba del nombre aparecerá la dirección IP asignada a la VPN. Indique ¿de qué tipo es?

_____

16. Inicie un pequeño chat para comprobar la comunicación presionando botón derecho sobre el equipo que desee conectarse, si desea mandar un mensaje global hágalo sobre el Id de la red.
17. Comparta una carpeta dentro de Hamachi y exporte contenido a otros usuarios (imágenes, música, documentos).

19. Anote sus Observaciones.

_____
_____
_____
_____

Parte 2 Nube

Dropbox es un servicio de alojamiento en la nube (Internet), el cual nos permite almacenar y sincronizar archivos en línea y entre computadoras, compartir archivos y carpetas con otros, etc. El cliente de Dropbox permite a los usuarios dejar cualquier archivo en una carpeta designada. Ese archivo es sincronizado en la nube (Internet) y en todas las demás computadores con el cliente de Dropbox. Los archivos en la carpeta de Dropbox pueden entonces ser compartidos con otros usuarios de Dropbox o ser accedidos desde la página Web del servicio. De igual manera permite agregar archivos manualmente por medio del navegador web.

1. Para bajar e instalar el programa de Dropbox, debemos acceder a la página electrónica http://www.getdropbox.com

a) Una vez que accedemos a la página, localizamos el botón “Download Dropbox” y presionamos una vez sobre el mismo.

b) En la pantalla que se despliega, Presionamos el botón de RUN para comenzar a descargar el programa. Puede tardar varios minutos, dependiendo de la velocidad de Internet. Cuando termine de bajar, presionamos el botón de Run.

2. Durante la instalación aparecerán varias pantallas como las mostradas a continuación:

a). Esta pantalla nuestra el acuerdo de la licencia y debemos presionar “I Agree” para poder continuar. Figura 3.76

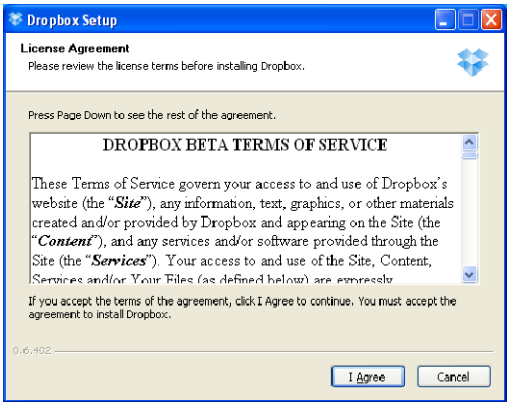


Figura 3.76 Términos de servicio

b). En la siguiente pantalla, presionamos el botón de Install, sin hacer ningún cambio. Figura 3.77

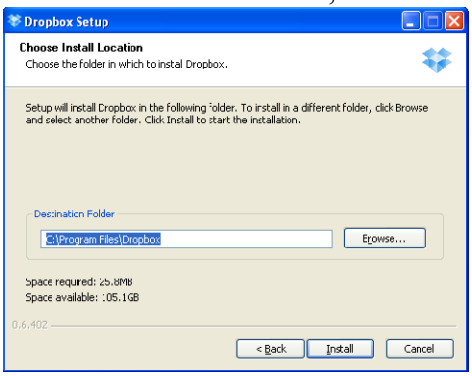


Figura 3.77 Directorio de instalación

c). Después, aparecerá una pantalla en la que debemos seleccionar una de las siguientes dos alternativas: Figura 3.78

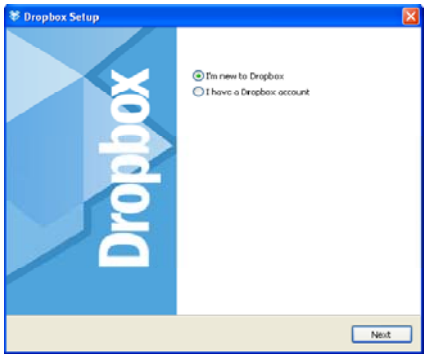


Figura 3.78 Alternativas de instalación

- I'm new to Dropbox: Seleccionamos esta alternativa si nunca has creado una cuenta en Dropbox. Figura 7

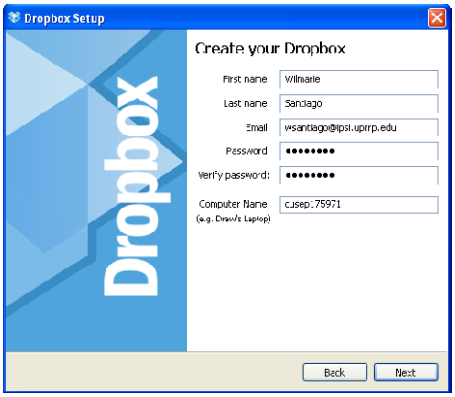


Figura 3.79 Creación de cuenta

- I have a Dropbox account: Seleccionamos esta alternativa si se tiene creada una cuenta en Dropbox.

- Presionamos NEXT para Continuar.

- Para crear y compartir una carpeta con otros usuarios, primero debemos localizar el archivo de My Dropbox, localizado en la carpeta de Mis Documentos de la computadora. Presionamos dos veces sobre el mismo para accederlo. Figura 3.80

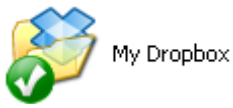


Figura 3.80 Carpeta de Dropbox

1. Creamos una nueva carpeta, dentro de My Dropbox, y escribimos un nombre representativo a su contenido.

2. Guardamos dentro de la carpeta aquellos documentos que se desean compartir con otras personas.

3. Seleccionamos la carpeta a compartir y presionamos una vez con el botón derecho del mouse, localizamos la alternativa de Dropbox y presiona la opción de Share…

4. Se abrirá una página de Internet en donde nos aparecerá un encasillado para escribir la/s dirección(es) electrónica(s) de la(s) persona(s) con la(s) que quieres compartir la carpeta y su contenido.

Las direcciones de email deberán estar separadas por coma (,). Presionamos el botón de Share folder para terminar.

d. Si seleccionamos la primera alternativa para crear una nueva cuenta, se deben completar todos los espacios provistos en la pantalla presentada. El espacio de Computer Name puede dejarse igual a como aparece. Presionamos Next para continuar.

Importante:
Recuerde el correo electrónico y el password que registro ya que éste es el mismo que se va a utilizar para autenticar la cuenta de acceso.

e. Luego aparecerán una serie de pantalla en las cuales se puede presionar el botón de Skip tour and finish o Next para tener una vista previa del programa.
f. En la última pantalla, presionamos Finish and go to My Dropbox para terminar.

Creación una carpeta para compartir archivos

1. Luego de que alguna persona haya compartido una carpeta, recibiremos un correo electrónico en el cual debe acceder el enlace presentado para lograr acceso al Sharing.

2. Luego de localizar la carpeta a compartir, debemos presionar uno de los dos botones presentados en la página electrónica de la carpeta que se ha compartido. Al presionar el botón de Acept., automáticamente se añadirá la carpeta compartida en su cuenta, no se añadirá ninguna carpeta en caso de presionar el botón de Decline.

3. Luego acceda a la carpeta de My Dropbox, localizada dentro de Mis Documentos, para acceder la carpeta compartida.

El espacio disponible para almacenar la información en la cuenta de Dropbox, es de 2GB. Para verificar la disponibilidad de espacio, realice lo siguiente:

1. Accedemos la dirección: http://getdropbox.com
2. En la parte superior derecha de la página electrónica, aparecerán los encasillados donde se deberá escribir el username y password para lograr acceso a la cuenta, se debe presionar Sign in.

3. Luego, en la parte superior derecha de la pantalla, Presionamos el enlace de Account.

4. En la primera pestaña, Account Info, aparece una gráfica y el porcentaje de uso de la cuenta.

Finalmente para desvincular el equipo que estamos usando presionamos una vez sobre el icono de Dropbox en la barra de tareas (localizado al lado del reloj del sistema) y luego seleccionamos la opción de Preferences…, presionamos sobre el botón Unlink this computer…, y terminamos presionando OK para terminar

1. ¿Qué diferencia existe entre una carpeta compartida con Hamachi y otra con Dropbox?

_____
_____
_____
_____

2. ¿Cuál forma encuentra más eficiente para compartir archivos?

_____
_____
_____

3. ¿Cuál forma encuentra más segura para la compartición de archivos y porqué?

_____
_____
_____

Anote sus conclusiones

_____
_____
_____
_____
_____
_____

3.12 Práctica de laboratorio # 11 - Redes Inalámbricas

Objetivos

- El alumno realizará un escaneo de redes Wi-Fi
- Aprenderá los diferentes tipos de seguridad implementados en una red 802.11
- Ubicará en un mapa las redes descubiertas

Introducción

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). **Wi-Fi** (que significa "Fidelidad inalámbrica", a veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la Wi-Fi Alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11.

Por el uso indebido de los términos (y por razones de marketing) el nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11.

El estándar 802.11 establece los niveles inferiores del modelo OSI para las conexiones inalámbricas que utilizan ondas electromagnéticas, por ejemplo:

- La capa física (a veces abreviada capa "PHY")
- La capa de enlace de datos compuesta por dos subcapas: **control de enlace lógico** (**LLC**) y **control de acceso al medio** (**MAC**).

Modulación

Las modulaciones que se utilizan son DBPSK (Differential Binary Phase Shift Keying) y DQPSK (Differential Quadrature Phase Shift Keying) para velocidades de transmisión de 1 y 2 Mbps respectivamente. Todas las estaciones en una red 802.11 usan la misma secuencia de 11 bits. En el transmisor una función EX-OR combina la trama con la secuencia Barker para que cada bit de la trama se combine con la secuencia de 11 bits. En el receptor la señal DSSS se convoluciona con la secuencia Barker para recuperar la trama y evitar las interferencias.

Mencione la Secuencia Barker

_____

_____

_____

_____

Canales WiFi

Cada canal ocupa 22 MHz de ancho de banda y la forma espectral de los canales se representa por una función sinc(X). La máscara de transmisión del canal DS, en el estándar IEEE 802.11, especifica que en recepción los primeros productos de intermodulación deben ser filtrados a -30dBr y el resto de productos a -50dBr. Esto solamente permite tres canales no interferentes espaciados 25MHz en la banda de 2.4GHz, a pesar de que se definen 14 canales de operación en esa banda.

En los productos comerciales actuales, la potencia nominal de transmisión es 100mW.

Mencione qué canales son los que se emplean en México

_____
_____

Existen varias clases de hardware que se pueden utilizar para implementar una red inalámbrica WiFi.

Mencione por lo menos 2 de ellos

_____
_____

_____
_____

Explique los dos modos operativos (topologías de interconexión e nodos) del estándar 802.11

_____
_____
_____
_____
_____

- El modo de infraestructura en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso común. Éste es por lo general el modo predeterminado para las tarjetas 802.11b.
- El modo ad-hoc en el que los clientes se conectan entre sí sin ningún punto de acceso en común.

¿En qué casos conviene utilizar una arquitectura sobre la otra?

Identificación de un nodo

Cada nodo se identifica mediante los 6 bytes de su dirección MAC. Cada nodo receptor reconoce su propia dirección MAC.

Búsqueda (Scanning)

El estándar 802.11 define tanto la búsqueda activa como pasiva, sistemas que utilizan un adaptador de red para localizar puntos de acceso. La búsqueda pasiva es obligatoria donde cada adaptador de red busca canales individuales para encontrar la mejor señal del punto de acceso. Periódicamente, cada punto de acceso difunde señales como si fuera un faro, y el adaptador de red recibe estas señales (beacon) mientras busca tomando nota de sus datos. Estas beacon (señales de faro) contienen datos sobre el punto de acceso incluyendo por ejemplo el SSID, tasas de transmisión admitidas, etc. El adaptador de red puede usar esta información para compararla y determinar junto con otras características, como la fuerza de la señal, qué punto de acceso utilizar.

En tanto la búsqueda activa se refiere a que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red. Este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea conectar. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de sondeo. Se completan los pasos de autenticación y asociación.

Autenticación (Authentication)

La autenticación es el proceso para comprobar la identidad de un adaptador en la red para aceptarlo o rechazarlo. El estándar 802.11 especifica dos formas de autenticación, el sistema abierto y el sistema basado en una clave compartida.

El sistema abierto es obligatorio y consta de dos pasos, mencione cuáles son:

_____

_____

_____

_____

La autenticación de clave compartida es opcional y básicamente comprueba si la clave WEP es la correcta. El hecho de ser opcional para el protocolo no impide que esté en la práctica en la totalidad de los adaptadores y puntos de acceso. Este proceso consta de cuatro pasos Mencione en que conste cada uno de ellos.

Asociación

La asociación es un proceso por el cual el punto de acceso reserva recursos y sincroniza con una estación cliente. Una vez que el adaptador de red se ha autenticado, también tiene que asociarse al punto de acceso antes poder transmitir tramas de datos. La asociación es importante para sincronizar a ambos elementos con información importante como por ejemplo las tasas de transmisión admitidas.

Los estándares 802.11b, 802.11g y 802.11n, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Complete la siguiente tabla

Estándar	**Frecuencia**	**Velocidad**	**Rango**
WiFi B (802.11b)	2,4 GHz	11 Mbit/s	
WiFi G (802.11g)		54 Mbit/s	100 m
WiFi G (802.11n)			

Mencione las características principales de cada estándar.

_____
_____
_____

_____
_____
_____

_____
_____
_____

Seguridad

Las ondas de radio tienen en sí mismas la posibilidad de propagarse en todas las direcciones dentro de un rango relativamente amplio. Es por esto que es muy difícil mantener las transmisiones de radio dentro de un área limitada. La propagación radial también se da en tres dimensiones. Por lo tanto, las ondas pueden pasar de un piso a otro en un edificio (con un alto grado de atenuación).

La consecuencia principal de esta "propagación desmedida" de ondas radiales es que personas no autorizadas pueden escuchar la red, posiblemente más allá del confinamiento del edificio donde se ha establecido la red inalámbrica.

El problema grave es que se puede instalar una red inalámbrica muy fácilmente en una compañía sin que se entere el departamento de IT. Un empleado sólo tiene que conectar un punto de acceso con un puerto de datos para que todas las comunicaciones en la red sean "públicas" dentro del rango de transmisión del punto de acceso.

Medidas preventivas

La seguridad de las transmisiones inalámbricas puede ser difícil de lograr. Donde existen redes inalámbricas, la seguridad es reducida. Esto ha sido un problema desde los primeros días de las WLAN.

En la actualidad, muchos administradores no se ocupan de implementar prácticas de seguridad efectivas como lo mencionaremos a continuación.

1. Filtrado de direcciones MAC

Las interfaces de configuración de los puntos de acceso les permiten, por lo general, mantener una lista de permisos de acceso (llamada ACL; Lista de control de acceso) que se basa en las direcciones MAC de los dispositivos autorizados para conectarse a la red inalámbrica.

Esta precaución algo restrictiva le permite a la red limitar el acceso a un número dado de equipos. Sin embargo, esto no soluciona el problema de la seguridad en las transferencias de datos.

2. WAP **Wireless Application Protocol** (protocolo de aplicaciones inalámbricas)

Es un estándar seguro que permite que los usuarios accedan a información de forma instantánea a través de dispositivos inalámbricos como PDAs, teléfonos móviles, buscas, walkie-talkies y teléfonos inteligentes (smartphones).

3. WEP

Para solucionar los problemas de seguridad de transferencia en redes inalámbricas, el estándar 802.11 incluye un sencillo mecanismo de cifrado llamado **WEP** (Privacidad equivalente al cableado). Para subsanar problemas de seguridad WEP surge WPA – (acceso inalámbrico protegido)

La seguridad en "WEP" se basa en claves, sin embargo se considera una seguridad débil ¿Por qué?

_____

_____

_____

4 .WPA

El funcionamiento de WPA se basa en la implementación de un servidor de autenticación (en general un servidor RADIUS) que identifica a los usuarios en una red y establece sus privilegios de acceso. No obstante, redes pequeñas pueden usar una versión más simple de WPA, llamada WPA-PSK, al implementar la misma clave de cifrado en todos los dispositivos, con lo cual ya no se necesita el servidor RADIUS.

El WPA (en su primera construcción) sólo admite redes en modo infraestructura, es decir que no se puede utilizar para asegurar redes punto a punto inalámbricas (modo "ad-hoc").

5. 802.1X

El estándar 802.1x es una solución de seguridad ratificada por el IEEE en junio de 2001 que puede autenticar (identificar) a un usuario que quiere acceder a la red (ya sea por cable o inalámbrica). Esto se hace a través del uso de un servidor de autenticación.

6. EAP

La forma en que opera el protocolo EAP se basa en el uso de un controlador de acceso llamado *autenticador*, que le otorga o deniega a un usuario el acceso a la red. El usuario en este sistema se llama *solicitante*. El controlador de acceso es un firewall básico que actúa como intermediario entre el usuario y el *servidor de autenticación*, y que necesita muy pocos recursos para funcionar. Cuando se trata de una red inalámbrica, el punto de acceso actúa como autenticador.

Equipo Necesario

Hardware

1 Laptop o Netbook
1 Tarjeta de red inalámbrica Alfa AWUS036H
1 Antena 9dbi
1 GPS Garmin eTrex Legend H (recomendado) ó
1GPS USB Dongle MD -100

Software

Earth Stumbler
Netstumbler
Google Earth

Desarrollo

Instalamos la tarjeta de red externa en la laptop, que será la que llevará a cabo el descubrimiento de las redes, cabe destacar que hacemos uso de ésta ya que es más sensible que la que posee integrada el equipo. También instalamos los controladores del GPS para que éste sea detectado por NetStumbler una vez instalado.

Una vez instalado el controlador procedemos a descargar el programa de la página web:
www.netstumbler.com/downloads

Buscando redes

Una vez instalado, ya se puede ejecutar el programa, al iniciarlo, aparecerá un mensaje que informa que con la configuración actual de nuestra tarjeta de red. Elegimos Yes para que el programa la reconfigure adecuadamente. Esto te llevará a otra ventana que te pedirá que extraigas y vuelvas a introducir la tarjeta (Eject and re-insert it), habilites y deshabilites (Enable and desable it) o reinicies el sistema (Reboot the system)(ver figura 3.81).

Figura 3.81 Ventana de Notificación de Nestumbler

En cuanto lo hayas hecho (cualquiera de las tres opciones), deberás presionar en **Aceptar** y se mostrará la pantalla de inicio del programa (véase figura 3.82)

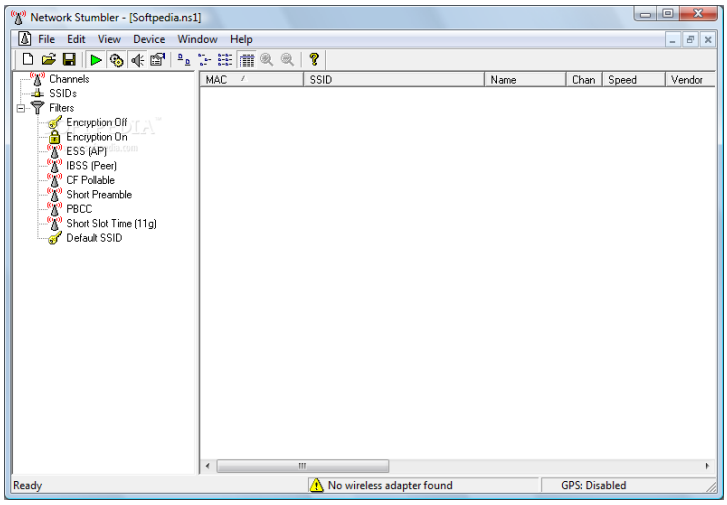


Figura 3.82 Ventana de Netstumbler

En ese momento comprobaremos que se ha dividido en dos partes. En la de la izquierda aparecen las redes clasificadas por distintos parámetros que comentaremos más adelante, mientras que la derecha se muestran los detalles de cada una de ellas. Ahora nos fijaremos en el icono con forma de flecha de color verde de la parte superior de la pantalla. **Es el que inicia el escaneo.** Es posible que cuando lo localice ya esté presionado. Eso significa que la búsqueda de nuevas redes comenzará automáticamente sin tener que hacer nada. En cuanto el programa detecte las redes inalámbricas a las que se puede conectar, se mostrarán en pantalla.

Configuración

Además de encontrar redes inalámbricas con la configuración que NetStumbler trae por defecto, también es posible modificar algunos parámetros de la conexión. Todos ellos se encuentran en la ventana denominada **Network Stumbler Options**, que aparecerá al pulsar en el menú **View** y a continuación **Options**. En ella se muestra una ventana con cuatro pestañas: **General, GPS, Scripting y MIDI**. Pruebe cada una de las opciones

En la primera puedes establecer la velocidad del escaneo (**Scan Speed***)* a través de la barra deslizante que va desde **Slow** (Lento) hasta **Fast** (Rápido). Aparte, tiene cinco opciones para señalar: **Auto adjust using GPS**, que permite variar la velocidad del escaneo en función de la velocidad soportada por el receptor GPS que se utilice (si no usas ninguno, no hace falta marcarlo); **New document starts scanning**, para que comience el escaneo en un nuevo documento; **Reconfigure card automatically**, si deseas que la tarjeta inalámbrica se reconfigure por sí sola nada más iniciar el programa; **Query APs for names**, para que el programa intente recoger las direcciones IP del punto de acceso a la red, y **Save files automatically**, en caso de que quiera que la aplicación grabe los cambios en la configuración de la red cada diez minutos sin pedir confirmación.

GPS

La segunda pestaña que encontraremos es la de GPS, que facilitará la configuración de un dispositivo de estas características. Se trata de una herramienta realmente útil para **detectar en un mapa el punto de acceso a una red inalámbrica**. Ahora bien, para ello es necesario tener conectado un receptor GPS al ordenador e indicar a NetStumbler el protocolo de comunicación que utiliza por defecto.

Eso lo hay que seleccionarlo en la primera opción que encontrarás en la ventana **Protocol**, así como el puerto utilizado para la conexión en **Port**.
Por último, los datos que se muestran más abajo, **Bits per second, Data bits, Parity, Stop bits** y **Flow control**, son los parámetros de comunicación de datos del GPS, que te vendrán en el manual que hallarás adjunto a éste. Así pues, selecciona lo que te indique en cada caso(véase Figura 3.83)

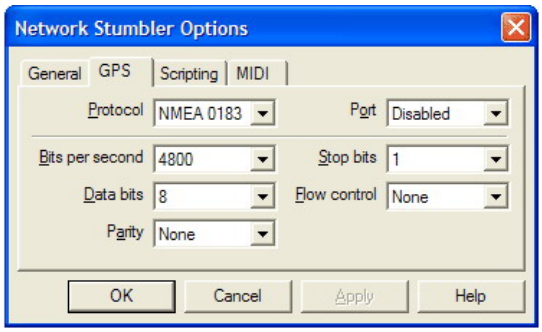


Figura 3.83 – configuración del GPS

Una vez configurado el equipo procedemos a recorrer el campus para la obtención de datos

Visualización de resultados

El símbolo de un candado que aparece justo al lado del número de identificación de la red significa que esa red está protegida y que, a menos que conozcamos su contraseña, **no podremos conectarnos a ella**. También pudiera suceder, por supuesto, que apareciera una red sin ningún candado, lo que le permitiría establecer una conexión con ella sin tener que introducir una clave. Así, simplemente pulsando con el botón derecho del ratón sobre ella y eligiendo su nombre en el menú emergente, se conectará.

El color del icono indica la intensidad de la conexión a la red. En verde la conexión es óptima, si cambia a amarillo o naranja sería regular, y si se pusiera roja, muy mala.

Si pulsamos con el botón derecho del ratón sobre cada una de ellas, veremos cómo aparece un menú emergente con algunos datos. Por ejemplo, si el sistema lo sabe, mostrará la dirección IP a la que está conectada la red, dependiendo del lugar donde se encuentre: Norteamérica (ARIN), Europa (RIPE) y Asia (APNIC). Además, ofrece la posibilidad de seleccionar todas las redes (**Select All**) o deshabilitarlas (**Delete Selected**). Ahora bien, si optas por esta segunda opción, debes saber que después no podrás recuperarlas y será necesario volver a iniciar el programa.

Detalles

En la columna de la derecha aparecen tres nombres: **Channels**, **SSIDs** y **Filters**, con tres signos "+" al lado. Al desplegarlos haciendo clic sobre ellos, el primer apartado hace referencia a **los canales en donde se ha encontrado la red**. En nuestro caso corresponden al 11 y al 12. El segundo se refiere al **número de identificación.** Ambos puntos te servirán para comprobar el estado de la conexión. Dentro de este menú, el último será el número de identificación de nuestra red. Si pulsamos sobre él la pantalla principal cambiará de aspecto y se mostrará la actividad de la red en dos colores (verde y rojo), tal y como puedes apreciar en la imagen. En la coordenada "Y" (la horizontal) muestra la fecha y la hora en la que se encuentra en el momento de realizar la consulta, mientras que en la "X" (la vertical) tiene el nivel de la señal. En verde aparece el grado más alto de conexión registrada en cada momento, mientras que en rojo se hace referencia al más bajo. Ahora bien, la mejor forma de hacerse una idea exacta de la evolución de ésta es acudir a la parte superior de la pantalla. Allí está el icono de una lupa con un signo "+" y otra con uno "–". Pulsando sobre la primera, se agrandará el gráfico; mientras que si haces clic sobre la segunda, lo reducirá.

En la tercera sección, **Filters**, encontrarás nueve apartados que actúan a modo de filtro según el parámetro elegido: **Encryption Off** mostrará todas las redes encontradas que no necesiten una clave para conectarse a ellas; **Encryption On** justo lo contrario; **ESS** para las redes que utilicen un mismo punto de acceso para conectar varios dispositivos; **IBSS** para las de extremo a extremo; **CF Pollable** para las 802.11; **Short Preamble y PBCC** para las 802.11b en diferentes frecuencias; **Short Slot Time** para las 802.11g, y **Default SSID** para las que tienen por defecto un identificador de configuración de la red.

Exportación de Datos

Guardamos los resultados de búsqueda en un archivo txt
A continuación disponemos de 2 formas para pasar los datos GPS a un formato compatible con Google Earth

Opción 1

Ingresamos al sitio web www.gpsvisualizer.com y subimos el archivo del NetStumbler, y de output seleccionamos "Google Earth"

Opción 2

Instalamos el programa Earth Stumbler el cuál es un programa para importar la información marcada con GPS del Netstumbler y visualizarla gráficamente en Google Earth.

Una vez exportados los datos a un archivo .kml. Finalmente ejecutamos Google Earth e importamos el .kml, quedarán todos los Access Points en My Places, divididos por abiertos y seguros.

El resultado obtenido deberá asemejarse a la siguiente imagen (véase figura3.84)

Figura 3.84 – Access Points Localizados

Una vez exportados los datos y localizados en el mapa conteste las siguientes preguntas.

1. ¿Qué SSID cuenta con la mayor cantidad de AP(Access Points)?

2. ¿Cuáles son los canales de transmisión más utilizados?

3. Mencione los tipos de cifrado más empleados
4. ¿Cuántas redes se encuentran sin seguridad (abiertas)?

5. ¿Cuáles tienen seguridad más robusta y porqué?

6. Mencione la importancia de tener cifrado WPA y no el comúnmente usado WEP

Anote sus conclusiones

_____
_____
_____
_____
_____

3.13 Práctica de laboratorio # 12 - El Valor de la Información

Objetivos de aprendizaje

- El alumno establecerá una mesa de discusión para los casos reales presentados
- El alumno tomará conciencia del valor de la información

Introducción

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto mediante una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática se resume, por lo general, en seis servicios de seguridad los cuales representan los objetivos principales:

- **Integridad:** Se encarga de salvaguardar la precisión y exactitud de la información en todo momento. La integridad está relacionada con la garantía de la exactitud y la exhaustividad de los datos del sistema de información.
- **Confidencialidad**: asegurar que sólo los individuos y los procesos autorizados tengan acceso a los recursos que se intercambian
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información a fin de que usuarios y procesos autorizados accedan a la información cuando así lo requieran.
- **No repudio**: garantizar que no se pueda negar una operación realizada sobre la información o los elementos que la contienen, procesan o transportan.
- **Autenticación**: asegurar que sólo los individuos y los procesos autorizados tengan acceso a los recursos
- **Control de acceso**: limitar el acceso autorizado solo a entidades autenticadas.

Frecuentemente, la seguridad de los sistemas de información es objeto de metáforas. A menudo, se la compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas.

Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad a nivel global y que debe constar de los siguientes elementos:

- Seguridad física, o la seguridad de infraestructuras materiales: consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

  Las principales amenazas que se prevén en la seguridad física son:

  - Desastres naturales, incendios accidentales tormentas e inundaciones.
  - Amenazas ocasionadas por el hombre.
  - Disturbios, sabotajes internos y externos deliberados.

- Seguridad lógica, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.

- Usuarios, se trata de concienciar a los usuarios acerca de los problemas de seguridad de la información

La seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control de acceso que aseguran que los usuarios de estos recursos sólo posean los derechos que les sean otorgados.

Por consiguiente, la seguridad informática debe estudiarse, analizarse y llevarse a la práctica de modo que no interfiera con las actividades que los usuarios deban realizar ni con el flujo de datos necesarios para que así puedan utilizar los sistemas de información de manera adecuada y en forma segura.

El primer paso en la conservación de la seguridad debe ser la determinación de lo que es importante para la organización, es decir ¿Qué quiere proteger?, ¿de qué lo quiere proteger? Y ¿cómo lo va a proteger?

Las necesidades de una organización para proteger sus activos se pueden determinar mediante la redacción de un inventario del sistema de información y luego estudiar los diferentes riesgos y las distintas amenazas que representan para implementar una política de seguridad apropiada.

La etapa de definición se compone entonces de tres etapas:

- Identificación de las necesidades
- Análisis de los riesgos
- Definición de la política de seguridad

La etapa de identificación de las necesidades consiste en realizar en primer lugar un inventario del sistema de información, en particular de la siguiente información:

- Personas y funciones
- Materiales, servidores y los servicios que éstos brindan
- Esquematización de la red (esquema de direcciones, topologías físicas y lógicas, etc.)

- Lista de los nombres de dominio de la empresa.
- Infraestructura de la comunicación (routers, switches, etc.)
- Información delicada

La mejor forma de analizar el impacto de una amenaza consiste en calcular el costo de los daños que causaría (por ejemplo, un ataque a un servidor o un daño de los datos de vital importancia de la compañía).

Partiendo de esta base, es necesario elaborar una tabla de riesgos y de sus potencialidades (es decir, la probabilidad de que existan) dándoles niveles escalonados de acuerdo con una escala que debe definirse. Por ejemplo:

- Infundado (o improbable): la amenaza es insostenible
- Débil: la amenaza tiene pocas probabilidades de existir
- Moderada: la amenaza es real
- Alta: la amenaza tiene muchas probabilidades de existir

Los efectos de las diversas amenazas pueden ser muy variados de manera que también se debe considerar para cada una de ellas el nivel de impacto que causen, por ejemplo:

- Notable: Los daños son al mínimo o imperceptibles, no altera significativamente el funcionamiento de la organización, pueden o no tomarse contramedidas.
- Menor: Se llevan a cabo contramedidas contempladas en un plan de riesgo, la recuperación es pronta
- Grave: Se altera el funcionamiento de la organización, la recuperación toma un largo periodo de tiempo.
- Irreparable: El daño es tal que, no existe recuperación para la organización.

Algunos pueden comprometer la integridad de la información o de los sistemas, otros pueden degradar la disponibilidad de los servicios y otros pueden estar relacionados con la confidencialidad de la información.

Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costos, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones.

Existe un gran abanico de medidas de seguridad que pueden reducir el riesgo de pérdidas debidas a la aparición de incidentes en los sistemas informáticos. Muchas veces al hablar de medidas de seguridad, solo se mencionan las meramente técnicas, como cortafuegos, antivirus o sistemas de copias de respaldo. Sin embargo, las medidas más efectivas suelen ser las medidas de gestión planteadas a mediano y largo plazo desde un punto de vista estratégico y táctico.

Es importante señalar que no existe medida de seguridad absoluta contra todo riesgo pero sí podemos tener mecanismos que reduzcan el impacto a niveles menores

Desarrollo

Lea los siguientes artículos, elabore una lista de los puntos principales y conteste en equipo las preguntas

Material

1 Hoja de papel
1 Pluma
1 Marcador de pizarrón

Lectura 1

La mayor filtración de la historia deja al descubierto los secretos de la política exterior de EE UU
Vicente Jiménez / Antonio Caño - Madrid –

EL PAÍS, en colaboración con otros diarios de Europa y Estados Unidos, revela el contenido de la mayor filtración de documentos secretos a la que jamás se haya tenido acceso en toda la historia. Se trata de una colección de más de 250.000 mensajes del Departamento de Estado de Estados Unidos, obtenidos por la página digital Wikileaks, en los que se descubren episodios inéditos ocurridos en los puntos más conflictivos del mundo, así como otros muchos sucesos y datos de gran relevancia que desnudan por completo la política exterior norteamericana, sacan a la luz sus mecanismos y sus fuentes, dejan en evidencia sus debilidades y obsesiones, y en conjunto facilitan la comprensión por parte de los ciudadanos de las circunstancias en las que se desarrolla el lado oscuro de las relaciones internacionales.
Estos documentos recogen comentarios e informes elaborados por funcionarios estadounidenses, con un lenguaje muy franco, sobre personalidades de todo mundo, desvelan los contenidos de entrevistas del más alto nivel, descubren desconocidas actividades de espionaje y exponen con detalle las opiniones vertidas y datos aportados por diferentes fuentes en conversaciones con embajadores norteamericanos o personal diplomático de esa nación en numerosos países, incluido España.

Queda en evidencia, por ejemplo, la sospecha norteamericana de que la política rusa está en manos de Vladimir Putin, a quien se juzga como un político de corte autoritario cuyo estilo personal machista le permite conectar perfectamente con Silvio Berlusconi. Del primer ministro italiano se detallan sus "fiestas salvajes" y se expone la desconfianza profunda que despierta en Washington. Tampoco muestra la diplomacia estadounidense un gran aprecio por el presidente francés, Nicolas Sarkozy, a quien se sigue con gran meticulosidad acerca de cualquier movimiento para obstaculizar la política exterior de Estados Unidos.

Los cables prueban la intensa actividad de ese país para bloquear a Irán, el enorme juego que se desarrolla en torno a China, cuyo predominio en Asia se da casi por aceptado, o los esfuerzos por cortejar a países de América Latina para aislar al venezolano Hugo Chávez.

En ocasiones, las expresiones usadas en estos documentos son de tal naturaleza que pueden dinamitar las relaciones de Estados Unidos con algunos de sus principales aliados; en otras, pueden ponerse en riesgo algunos proyectos importantes de su política exterior, como el acercamiento a Rusia o el apoyo de ciertos Gobiernos árabes.

El alcance de estas revelaciones es de tal calibre que, seguramente, se podrá hablar de un antes y un después en lo que respecta a los hábitos diplomáticos. Esta filtración puede acabar con una era de la política exterior: los métodos tradicionales de comunicación y las prácticas empleadas para la consecución de información quedan en entredicho a partir de ahora.

Todos los servicios diplomáticos del mundo, y especialmente de Estados Unidos, donde esta filtración se suma a otras anteriores de menor trascendencia con papeles relativos a Irak y Afganistán, tendrán que replantearse desde este momento su modo de operar y, probablemente, modificar profundamente sus prácticas.

Intensas gestiones

Tratando de anticiparse a ese perjuicio, la Administración de Estados Unidos lleva varios días, desde que supo la existencia de esta fuga de documentos, realizando intensas gestiones ante el Congreso norteamericano y los Gobiernos de gran parte de las naciones ante los que tiene representación diplomática para informarles sobre el previsible contenido de las filtraciones y sus posibles consecuencias. El Departamento de Estado envió a principio de esta semana un informe a los principales comités de la Cámara de Representantes y del Senado previniéndoles sobre la situación.

La propia secretaria de Estado, Hillary Clinton, ha telefoneado en las últimas horas a los Gobiernos de los países más importante afectados por esta fuga de información, entre otros los de China, Alemania, Francia y Arabia Saudí, para alertarles de lo sucedido y ofrecer algunas justificaciones

En Reino Unido, Israel, Italia, Australia y Canadá, entre otros socios de Estados Unidos, portavoces de sus respectivos ministerios de Relaciones Exteriores confirmaron que habían recibido información de parte de los embajadores norteamericanos, aunque no revelaron detalles sobre los datos precisos que habían sido puestos en su conocimiento. No ha habido, sin embargo, comunicación directa entre la Embajada en Madrid y el Gobierno español acerca de este asunto.

El portavoz del Departamento de Estado, P. J. Crowley, ha reconocido que no conoce con exactitud las informaciones que aparecerán en los papeles filtrados, aunque ha adelantado que "estas revelaciones son dañinas para los intereses de Estados Unidos". "Van a crear tensiones entre nuestros diplomáticos y nuestros amigos alrededor del mundo", declaró este fin de semana.

El Departamento de Estado, que ha negociado con uno de los periódicos que hoy publican los cables algunos contenidos particularmente lesivos para sus intereses o peligrosos para ciertas personas, está especialmente preocupado por el daño que esto puede causar en la guerra contra Al Qaeda en algunas regiones en la que la libran de forma encubierta, como Yemen o Pakistán, así como los efectos que puede tener para las difíciles relaciones con otras potencias, como Rusia y China.

Los dos últimos años

Los documentos -251.287 mensajes que cubren un periodo hasta febrero de 2010 y, en su mayor parte, afectan a los dos últimos años- fueron facilitados por WikiLeaks hace varias semanas, además de a EL PAÍS, a los diarios The Guardian, de Reino Unido; The New York Times, de Estados Unidos; Le Monde, de Francia, y al semanario Der Spiegel, de Alemania. Estos medios han trabajado por separado en la valoración y selección del material, y pondrán a disposición de sus lectores aquellas historias que cada uno considere de mayor interés; en algunos casos serán coincidentes, en otros no.

Ese proceso se ha llevado a cabo bajo una exigente condición de no poner en peligro en ningún momento fuentes protegidas de antemano o personas cuya vida podría verse amenazada al desvelarse su identidad. Al mismo tiempo, todos los medios han hecho un esfuerzo supremo por evitar la revelación de episodios que pudieran suponer un riesgo para la seguridad de cualquier país, particularmente de Estados Unidos, el más expuesto por estas revelaciones. Por esa razón, algunos de los documentos que serán puestos a disposición de nuestros lectores a partir de hoy aparecerán parcialmente mutilados.

EL PAÍS no ha estado en el origen de la filtración y, por tanto, desconoce los criterios con los que se ha llevado a cabo la selección del paquete que finalmente ha llegado a manos del diario. Resulta evidente que los papeles analizados no son todos los emitidos en el mundo por el Departamento de Estado en el periodo de tiempo comprendido, pero ignoramos si esos son todos a los que ha tenido acceso WikiLeaks.

Pese a eso, el lector comprobará el valor que en sí mismo encierra el conjunto de documentos facilitados, al margen de que puedan existir otros muchos que aún se desconocen. Se trata de un material que aporta novedades relevantes sobre el manejo de asuntos de gran repercusión mundial, como el programa nuclear de Irán, las tensiones en Oriente Próximo, las guerras de Irak y Afganistán y otros conflictos en Asia y África.

Terrorismo y radicalismo islámico

También se recogen los movimientos entre Estados Unidos y sus aliados para hacer frente al terrorismo y al radicalismo islámico, así como detalles reveladores sobre episodios de tanta trascendencia como el boicot de China a la empresa Google o los negocios conjuntos de Putin y Berlusconi en el sector del petróleo. De especial interés son las pruebas que se aportan sobre el alcance de la corrupción a escala planetaria y las permanentes presiones que se ejercen sobre los diferentes Gobiernos, desde Brasil a Turquía, para favorecer los intereses comerciales o militares de Estados Unidos.

Entre los primeros documentos que hoy se hacen públicos, se descubre el pánico que los planes armamentísticos de Irán, incluido su programa nuclear, despiertan entre los países árabes, hasta el punto de que alguno de sus gobernantes llega a sugerir que es preferible una guerra convencional hoy que un Irán nuclear mañana. Se aprecia la enorme preocupación con la que Estados Unidos observa la evolución de los acontecimientos en Turquía y la estrecha vigilancia a la que se mantiene al primer ministro, Erdogan.

Y, sobre todo, esta primera entrega revela las instrucciones que el Departamento de Estado ha cursado a sus diplomáticos en Naciones Unidas y en algunos países para desarrollar una verdadera labor de espionaje sobre el secretario general de la ONU, sus principales oficinas y sus más delicadas misiones.

Los lectores descubrirán al acceder a las sucesivas crónicas detalles insospechados sobre la personalidad de algunos destacados dirigentes y comprobarán el papel que desempeñan las más íntimas facetas humanas en las relaciones políticas. Eso resulta particularmente evidente en América Latina, donde se dan a conocer juicios de diplomáticos norteamericanos y de muchos de sus interlocutores sobre el carácter, las aficiones y los pecados de las figuras más controvertidas.

Mañana EL PAÍS ofrecerá detalles, por ejemplo, sobre las sospechas que la presidenta de Argentina, Cristina Fernández de Kirchner, despierta en Washington, hasta el punto de que la Secretaría de Estado llega a solicitar información sobre su estado de salud mental. El mismo día se darán a conocer algunas de las gestiones que la

diplomacia norteamericana ha realizado para repatriar a los presos de Guantánamo, así como la intensa actividad en Asia para frenar el peligro que representa Corea del Norte.

Cables controvertidos

Entre los cables con los que ha trabajado este periódic o se encuentran informes extraordinariamente controvertidos, como los mensajes del embajador norteamericano en Trípoli en los que cuenta que el líder libio, Muamar el Gadafi, usa botox y es un verdadero hipocondríaco que hace filmar todos sus exámenes médicos para analizarlos posteriormente con sus doctores, y relatos con meticulosas descripciones del paisaje local, como el que hace un diplomático estadounidense invitado a una boda en Daguestán que sirve para ilustrar el grado de corrupción en la zona.

Hay cables de gran valor histórico, como el que revela la apuesta de la diplomacia norteamericana por el derrocamiento del general panameño Manuel Antonio Noriega o el que detalla ciertos movimientos de Estados Unidos durante el golpe de Estado que destituyó a Manuel Zelaya en Honduras, y cables de enorme interés sobre acontecimientos actuales, como el que precisa la presión ejercida sobre el presidente de Afganistán, Hamid Karzai, para que contenga los abusos de sus allegados y facilite la gobernabilidad del país.

En lo que respecta a España, estos documentos registran el enorme acceso de la Embajada de Estados Unidos a personalidades destacadas del ámbito político y judicial, y su influencia en algunos acontecimientos que han marcado la actualidad de los últimos años. También se descubre el punto de vista que funcionarios estadounidenses tienen de la clase política española, así como el que algunos políticos expresan sobre sus compañeros y adversarios.

En determinados casos, estas revelaciones tienen el estrictamente el valor que tiene la opinión de una persona de posición influyente. En otros casos, se trata de relatos que aportan pistas sobre acontecimientos importantes pero que son narrados por una sola fuente: el servicio diplomático de Estados Unidos. EL PAÍS no ha podido corroborar todos esos relatos y ha prescindido de algunos que ha considerado de dudosa credibilidad. Pero sí ha certificado otros y ha operado de forma responsable con el país objeto de la filtración con la intención de causar el menor daño posible. Entre otras precauciones, se ha decidido aceptar los compromisos a los que The New York Times llegue con el Departamento de Estado para evitar la difusión de determinados documentos.

No todos los papeles obtenidos por Wikileaks han sido utilizados para la elaboración de nuestras informaciones, y solo una parte de ellos serán expuestos públicamente, independientemente de lo que la propia WikiLeaks o los demás medios que han recibido el material decidan hacer. Se han seleccionado tan solo aquellos que consideramos imprescindibles para respaldar la información ofrecida.

Las informaciones han sido preparadas y escritas únicamente por redactores de nuestro periódico atendiendo a nuestras particulares exigencias de rigor y calidad. A lo largo de varios días se irán ofreciendo las crónicas que recogen la sustancia de esos documentos, añadiéndoles el contexto y la valoración requeridos, así como sus posibles reacciones y consecuencias.

Algunas de esas reacciones estarán, seguramente, dirigidas a examinar las causas por las que puede haberse producido una fuga de semejante magnitud. El origen de este problema puede remontarse a los días posteriores al ataque terrorista del 11 de septiembre de 2001, cuando se detectaron unos fallos de coordinación entre los servicios de inteligencia que recomendaron la necesidad de un modelo de comunicación que permitiera a los diferentes responsables de la seguridad compartir datos extraídos por el Departamento de Estado.

Un sistema de Internet del Ejército

Se extendió, por tanto, a partir de esa fecha el uso de un sistema de Internet del Ejército norteamericano denominado SIPRNET, un acrónimo de Secret Internet Protocol Router Network. Todos los cables que se incluyen en esta filtración fueron enviados por ese medio, como se comprueba por la etiqueta que cada uno de ellos lleva en su cabecera, la palabra SIPDIS, que son las siglas para Secret Internet Protocol Distribution.

Al menos 180 embajadas norteamericanas alrededor del mundo utilizan actualmente ese sistema de comunicación, según informes elaborados por el Congreso norteamericano. Aunque se exigen fuertes medidas de seguridad para el uso de ese sistema, como la de mantenerlo abierto únicamente cuando el usuario está frente a la pantalla, la exigencia de cambiar la clave cada cinco meses o la prohibición de utilizar cualquier clase de CD u otro método de copia de contenidos, el número de personas que ahora acceden a la información ha crecido considerablemente.

A ese crecimiento ha ayudado también la necesidad de ampliar el número de personas trabajando en cuestiones de seguridad y, como consecuencia, la del número de personas a la que se da acceso a documentos clasificados. El Departamento de Estado clasifica sus informes en una escala que va del Top Secret al Confidential. En los documentos facilitados a EL PAÍS no hay ninguno clasificado como Top Secret, aunque sí más de 15.000 situados en la escala inferior, Secret.

Según se puede deducir de datos elaborados por la Oficina de Control del Gobierno, perteneciente al Congreso norteamericano, y otros expuestos recientemente por medios de comunicación de ese país, más de tres millones de estadounidenses están autorizados al acceso a ese material Secret. Eso incluye decenas de miles de empleados del Departamento de Estado, funcionarios de la CIA, del FBI, de la DEA, de los servicios de inteligencia de las fuerzas armadas y de otros departamentos implicados en la búsqueda de información. En Estados Unidos funcionan 16 agencias con responsabilidades de espionaje.

Será muy costoso, por tanto, para ese país reparar el daño causado por esta filtración, y llevará años poner en pie un nuevo sistema de comunicación con plenas garantías. Lo más importante, sin embargo, es el valor informativo que esos documentos tienen actualmente. Estamos ante una serie de relatos, sin precedentes en el periodismo español, que servirán para una mejor comprensión de algunos conflictos y de personalidades que afectan determinantemente a nuestra vida y que pueden abrir a nuestros lectores a una nueva interpretación de la realidad que les rodea.

Extraído del Periódico El País en su edición del Domingo 28 de Noviembre de 2010.

http://www.elpais.com/articulo/internacional/mayor/filtracion/historia/deja/descubierto/secretos/politica/exterior/EE/UU/elpepuint/20101128elpepuint_25/Tes

Responda en equipo las siguientes Preguntas

1. ¿Qué es WikiLeaks?

2. ¿Qué impacto social tiene la divulgación de opiniones personales de personas de alto rango?

3. ¿Qué trascendencia tiene este evento en el campo de la seguridad informática?

4. ¿Qué medidas debiera tomar el gobierno de EU, para evitar otra fuga de información similar?

5. ¿Qué acciones tomaría usted para reducir el impacto causado por ésta fuga se redujera lo más posible?

Lectura 2

Facebook dejará a anunciantes aprovechar contactos
AP | El Universal

NUEVA YORK.- Los usuarios de **Facebook** que entren a una tienda virtual o señalen que una marca les "**gusta**" con el botón para ese fin podrían empezar a ver pronto que los **negocios** retransmitan esas acciones a las páginas de sus **amigos** como un "artículo patrocinado".

Por ahora, Facebook no ofrece una manera de desactivar esta función.

Según la compañía, la función permitirá a los anunciantes promocionar las recomendaciones que la gente ya hace en el sitio. Así pueden dar realce a las actividades de los usuarios que podrían perderse en la montaña de vínculos, fotos, actualizaciones de estatus y otros contenidos que circulan por la red social más grande del mundo.

Los nuevos artículos patrocinados retendrían el nivel de privacidad marcado por el usuario para el contenido original. Por ejemplo, si un usuario limita a sus amigos la información sobre las tiendas que visita, sólo ellos podrían ver más tarde la versión pagada por la compañía.

El contenido promocional aparecerá del lado derecho de la pantalla del usuario, no en su columna principal de noticias. Es la ubicación que suelen tomar los anuncios comunes, los pedidos de contacto y otros contenidos.

Involucrar a los usuarios en anuncios comerciales sin su consentimiento es un tema peliagudo para Facebook.

Marc Rotenberg, director ejecutivo del Centro de Privacidad de la Información Electrónica, dijo que en este caso la compañía estaría ganando dinero gracias al nombre o imagen de una persona que no aprobó la transacción. Lo consideró una decisión "sutil y engañosa" y afirmó que los usuarios deberían oponerse.

Otra de las principales redes sociales, Twitter, ofrece a sus anunciantes mensajes patrocinados. Los negocios pagan para aparecer en los resultados de búsqueda y en las listas de los temas populares del momento, pero estos son anuncios escritos por las compañías, mientras que los de Facebook son mensajes creados por los usuarios.

Ambos son parte de los intentos de que la publicidad se parezca cada vez más a lo que la gente hace en las redes sociales, en lugar de colocar carteles virtuales a los que los usuarios pueden no prestar atención o considerar de mal gusto.

Extraído del Periódico El Universal en su edición del día Jueves 27 de enero de 2011.

http://www.eluniversal.com.mx/articulos/62656.html

Responda en equipo las siguientes Preguntas

1. Elabore una lista de 7 posibles usos de las redes sociales para el marketing

2. ¿Son las redes sociales un canal de difusión o una fuga de información?

3. ¿Es usuario de Facebook?, ¿Porqué?

4. ¿Ha leído la Política de privacidad de Facebook, en caso negativo explique el porqué?

5. Elabore una lista de por lo menos 5 aspectos a favor y 5 aspectos en contra del uso de las redes sociales

Lectura 3

Tepito vende bases de datos oficiales

Por María de la Luz González

Bases de datos que contienen información personal de millones de mexicanos están a la venta en 12 mil dólares en el barrio de Tepito.

EL UNIVERSAL comprobó que en tres memorias externas, cada una de 160 gigabytes, el comprador recibe el padrón electoral de todo el país, el registro de todos los vehículos y de licencias de conducir, entre otros "productos".

La información la han adquirido tanto grupos del crimen organizado como agentes policiacos que la utilizan para trabajar, ya que en sus corporaciones no tienen esa disponibilidad de datos.

Un agente que tiene los datos en su poder explicó: "Cuando le comentamos al jefe de grupo que se estaba vendiendo, nos cooperarnos para comprarla, cada uno de nosotros puso 10 mil pesos, porque la verdad agiliza el trabajo".

Mencionó que uno de los archivos, denominado "Casetas Telmex", con los números de todos los teléfonos públicos del país, les permite rastrear llamadas relacionadas con secuestros o extorsiones, un trámite que les tomaría unos cinco días, si lo hacen ante la compañía.

Otro archivo incluye datos de las policías del país, con fotografía de sus elementos, número de placa y el lugar donde están adscritos.

El agente consultado advirtió del riesgo de esta última información: “Los delincuentes ya saben con quién llegar, a quién amenazar, pues cruzando datos con la lista del padrón [electoral], obtienen hasta sus domicilios y ubican a su familia, para presionarlos”.

La información que se adquiere contiene también la identificación de todo el parque vehicular del Servicio Federal, donde está incluido el transporte de carga. Ahí se detallan marca, modelo, placas y tipo de carga que transportan, desde electrodomésticos y abarrotes hasta material explosivo y las rutas.

Especialistas del Instituto Nacional de Ciencias Penales y de la Universidad Autónoma Metropolitana reconocieron que las bases de datos almacenadas por el gobierno no son 100% confiables debido a la falta de control, que las hace vulnerables a robos y fugas de información.

Extraído del Periódico El Universal en su edición del día Lunes 19 de abril de 2010.

http://www.eluniversal.com.mx/notas/673768.html

Responda en equipo las siguientes Preguntas

1. ¿Qué valor tiene su información personal (en forma cuantitativa)?

2. Elabore una lista con 10 medidas preventivas para proteger su información personal

3. ¿Qué es la ingeniería social?

4. ¿Qué medidas hay para contrarrestar la ingeniería social?

5. Investigue si en México existe algún organismo encargado de vigilar la protección de los datos y privacidad

Finalmente después de haber analizado diferentes herramientas de seguridad informática, sus usos y aplicaciones, revisado algunos casos reales donde la seguridad se ve afectada. Responda individualmente la siguiente pregunta:

6. ¿De quién es la responsabilidad de la Seguridad Informática?

Anote sus conclusiones

Capítulo IV

Resultados

En este capítulo se muestran los resultados obtenidos.

4.1 Pruebas de realización

Se realizó una cordial invitación a estudiantes de la carrera de Ingeniería en Computación para participar en las pruebas técnicas de las prácticas de Seguridad Informática; dadas las diferentes condiciones académicas de cada participante se optó por dar libertad de horario, así mismo, del número de prácticas a realizar por cada participante a fin de que esta actividad no interfiriera con sus actividades académicas ó laborales.

Para llevar a cabo un control sobre las pruebas de campo se definieron 2 términos:

- Política de privacidad: Para el uso de los datos personales recabados de cada participante.
- Condiciones de uso: Se establecieron los términos para el préstamo y distribución de material digital y electrónico para la realización de las prácticas.

Se establece lo siguiente:

Condiciones de Uso
Se provee al participante con material electrónico, impreso y digital para la consulta y realización de prácticas de seguridad informática. Algunos elementos tales como dispositivos físicos están sujetos únicamente a préstamo durante la realización de determinadas prácticas, el uso de estos dispositivos se encuentra sujeto a disponibilidad.

Política de Privacidad
La recopilación de datos tales como: información personal y resultados obtenidos mediante el presente cuestionario sólo se utilizan con fines estadísticos y de mejora de las prácticas realizadas.

Una vez definidos ambos términos, a cada participante se le pidió leyera y en caso de aceptar participar firmara el documento acatando dichos términos; se optó por la realización de un cuestionario de opción múltiple para una mejor y organizada recolección de datos, el cual se encuentra en el Anexo II.

Finalmente al término de las pruebas se recabó información valiosa que permitió complementar el presente trabajo así como algunas correcciones a fallas que se presentaron durante las pruebas.

4.2 Estadísticas e interpretación

A continuación se muestran los datos recabados de las pruebas técnicas

De los participantes

Se presentan los datos estadísticos de cada participante Tabla 4.1

	SEMESTRE	Prácticas Realizadas	Tiempo Total
Participante 1	Pasante	12	20:00
Participante 2	Pasante	12	20:30
Participante 3	9	12	20:15
Participante 4	9	12	20:00
Participante 5	8	10	17:45
Participante 6	8	9	15:45
Participante 7	9	8	13:30
Participante 8	8	8	13:30
Participante 9	8	8	13:45
Participante 10	8	7	12:30
Participante 11	Pasante	5	7:45
Participante 12	8	5	8:30

Tabla 4.1 Información de los Participantes

De la información presentada podemos concluir que la mayoría de los participantes promedia el octavo semestre de la carrera y ha gastado alrededor de 15:18 horas promedio en esta actividad así mismo se denota que en promedio se realizaron 9 prácticas como lo muestra a detalle la tabla4.2

Prácticas vs Tiempo	SEMESTRE	Prácticas	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	Total
Participante 1	10	12	1:45	1:45	1:45	1:45	1:45	1:45	1:30	1:45	1:45	1:30	1:30	1:30	20:00
Participante 2	10	12	1:45	1:45	1:45	2:00	1:45	1:45	1:30	2:00	1:45	1:30	1:30	1:30	20:30
Participante 3	9	12	1:45	1:45	1:45	2:00	1:45	1:45	1:30	1:45	1:45	1:30	1:30	1:30	20:15
Participante 4	9	12	1:30	1:45	1:45	2:00	1:45	1:45	1:30	1:45	1:45	1:30	1:30	1:30	20:00
Participante 5	8	10	1:45	2:00	1:45		1:45	2:00	1:45	1:45		1:45	1:45	1:30	17:45
Participante 6	8	9		1:45	1:45		2:00	2:00	1:30	1:45		1:45	1:45	1:30	15:45
Participante 7	9	8		1:45			1:45	1:45	1:30	1:45		1:45	1:45	1:30	13:30
Participante 8	8	8		1:45			1:45	1:45	1:30	1:45		1:45	1:45	1:30	13:30
Participante 9	8	8		1:45	1:45			1:45	1:45		1:45	1:45	1:45	1:30	13:45
Participante 10	8	7		2:00	2:00			1:45	1:45		1:45		1:45	1:30	12:30
Participante 11	10	5		1:45					1:30			1:30	1:30	1:30	7:45
Participante 12	8	5		1:45					1:45			1:45	1:45	1:30	8:30

Tabla 4.2 Número de prácticas realizadas

Cada práctica tomó diferentes tiempos de realización; así mismo sale a relucir que participantes de semestres avanzados realizaron cada práctica en un tiempo menor que aquellos que cursan el octavo semestre(ver Tabla 4.3); esto se ve reflejado en el nivel de dificultad denotado para cada practica (ver Tabla 4.4).

S vs T	Semestre	Prácticas	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	Tiempo Total
Participante 1	Pasante	12	1:45	1:45	1:45	1:45	1:45	1:45	1:30	1:45	1:45	1:30	1:30	1:30	20:00
Participante 2	Pasante	12	1:45	1:45	1:45	2:00	1:45	1:45	1:30	2:00	1:45	1:30	1:30	1:30	20:30
Participante 11	Pasante	5		1:45					1:30			1:30	1:30	1:30	7:45
Participante 3	9	12	1:45	1:45	1:45	2:00	1:45	1:45	1:30	1:45	1:45	1:30	1:30	1:30	20:15
Participante 4	9	12	1:30	1:45	1:45	2:00	1:45	1:45	1:30	1:45	1:45	1:30	1:30	1:30	20:00
Participante 7	9	8		1:45			1:45	1:45	1:30	1:45		1:45	1:45	1:30	13:30
Participante 5	8	10	1:45	2:00	1:45		1:45	2:00	1:45	1:45		1:45	1:45	1:30	17:45
Participante 6	8	9		1:45	1:45		2:00	2:00	1:30	1:45		1:45	1:45	1:30	15:45
Participante 8	8	8		1:45			1:45	1:45	1:30	1:45		1:45	1:45	1:30	13:30
Participante 9	8	8		1:45	1:45			1:45	1:45		1:45	1:45	1:45	1:30	13:45
Participante 10	8	7		2:00	2:00			1:45	1:45		1:45		1:45	1:30	12:30
Participante 12	8	5		1:45					1:45			1:45	1:45	1:30	8:30

Tabla 4.3 Tiempo de realización de las prácticas realizadas

Dificultad	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
Participante 1	Normal	Normal	Normal	Difícil	Normal	Normal	Fácil	Normal	Normal	Normal	Normal	Fácil
Participante 2	Normal	Normal	Normal	Difícil	Normal	Normal	Fácil	Normal	Normal	Normal	Normal	Fácil
Participante 3	Normal	Normal	Normal	Difícil	Normal	Normal	Fácil	Normal	Normal	Normal	Normal	Fácil
Participante 4	Normal	Normal	Normal	Difícil	Normal	Normal	Fácil	Normal	Normal	Normal	Normal	Fácil
Participante 5	Normal	Normal	Normal		Normal	Normal	Fácil	Normal		Normal	Normal	Fácil
Participante 6		Normal	Normal		Normal	Normal	Fácil	Normal		Normal	Normal	Fácil
Participante 7		Normal			Normal	Normal	Fácil	Normal		Normal	Normal	Fácil
Participante 8		Normal			Normal	Normal	Fácil	Normal		Normal	Normal	Fácil
Participante 9		Normal	Normal			Normal	Fácil		Normal	Normal	Normal	Fácil
Participante 10		Normal	Normal			Normal	Fácil		Normal		Normal	Fácil
Participante 11		Normal					Fácil			Normal	Normal	Fácil
Participante 12		Normal					Fácil			Normal	Normal	Fácil

Tabla 4.4 Dificultad de las prácticas realizadas

Con esta información podemos ver que tomando en cuenta un tiempo teórico de 2hrs destinado a cada práctica y tomando en cuenta los tiempos experimentales obtenemos la siguiente Figura 4.1

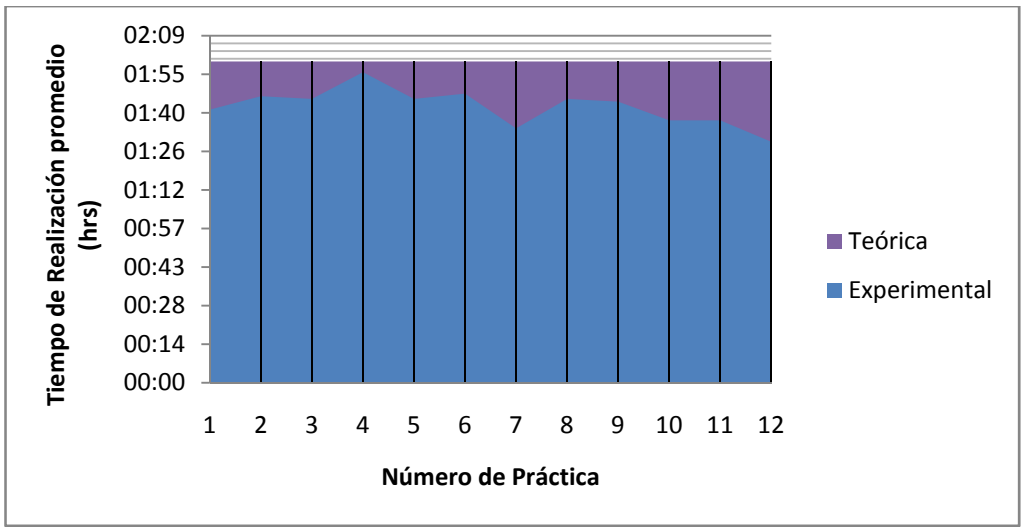


Figura 4.1 Tiempos de realización de la práctica

Como se observa, al asignar a cada práctica 2hr queda cubierto un tiempo suficiente para la realización con un ligero margen adicional de tiempo para el cumplimiento de las actividades

Cada actividad requirió de diferentes elementos, se pidió a los participantes calificar el tipo de material usado en cada práctica tomando en cuenta la siguiente escala Tabla 4.5
Útiles 2 | Adecuados 1 | Inadecuados 1

Material	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	Promedio Total
Promedio	2,00	2,00	2,00	2,00	2,00	2,00	2,00	2,00	2,00	2,00	1,90	1,40	1,92

Tabla 4.5 Opinión acerca del material usado en las prácticas realizadas

Se tomó en cuenta el nivel de interés de los estudiantes hacia cada práctica de manera individual, señalando aquellas que tuvieron cierto grado de popularidad tomando en cuenta la siguiente escala: (ver tabla 4.6)
4 Muy interesante | 3 Interesante | 2 Poco Interesante | 1 Aburrido

Interés	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	Promedio Total
Promedio	4,00	3,11	3,00	3,00	3,00	3,00	3,00	3,00	2,40	3,00	3,00	3,22	3,04

Tabla 4.6 Popularidad de las prácticas realizadas

Esto nos permite ver el interés de los estudiantes en el uso de los dispositivos biométricos

Se preguntó a los participantes fuentes adicionales de información tomando en cuenta apuntes, diapositivas, el internet y material recolectado a través de los años Figura 4.2

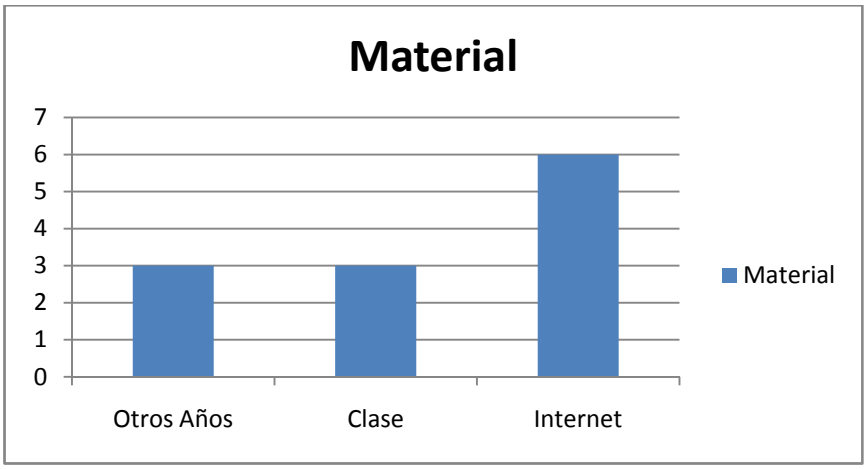


Figura 4.2 Recursos informáticos adicionales a la proporcionada por las prácticas

Finalmente se cuestionó a los participantes acerca del tipo de actividades y práctica que realizaron mostrando que las prácticas complementan lo visto en clase de teoría Figuras 4.3

Figura 4.3 Consideraciones respecto a las actividades de las prácticas con respecto a las clases teóricas.

Así se preguntó a los estudiantes su preferencia a la hora de realizar prácticas en ambientes simulados o con equipos físicos (figura.4.4)

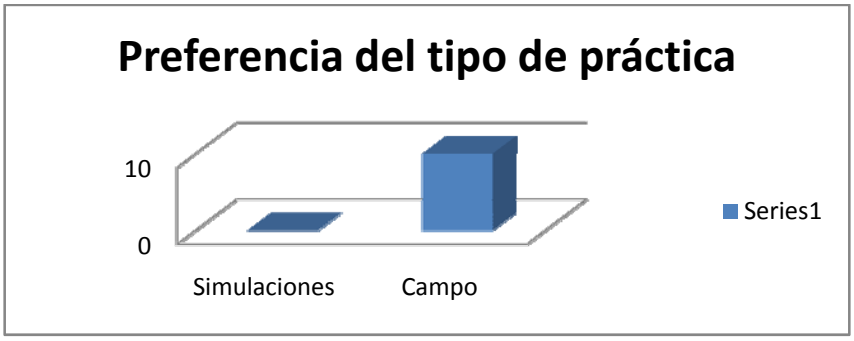


Figura 4.4 Consideraciones respecto a la preferencia del tipo de prácticas.

De esto se puede concluir que la preferencia absoluta es realizar las prácticas con equipos físicos, sin embargo no siempre es posible contar con ellos, pese a esto se considera mayoritariamente que las actividades realizadas en cada práctica son adecuadas a cada tema.

Para terminar, es pertinente anotar que el objetivo de todas las actividades a realizar y que es brindar el conocimiento e ilustrar la importancia que tiene la seguridad informática hoy en día se logra con el trabajo realizado.

4.3 Correcciones

Dentro de la realización de las prácticas se encontraron algunos problemas en el manejo del equipo y material, tal es el caso de la práctica #1 en la cual la solución de Nitrato de Plata al 3% debe realizarse con cuidado extremo; al ser una sustancia altamente corrosiva se optó por retirarla de los materiales de uso, debido a que el más mínimo error en su preparación o manejo puede ocasionar severos daños a los usuarios y al material que se emplea en dicha práctica.

Conclusiones

Conclusiones

En base en el objetivo planteado al inicio del presente trabajo, se desarrollaron 12 prácticas que permiten el estudio de la seguridad informática en diversas áreas o enfoques entre los que están: El enfoque físico de la red y los dispositivos que la conforman, el enfoque lógico mediante el cual se comparten recursos, se establecen rutas de direccionamiento y se distribuye información. Asimismo la valía de la información que es de vital importancia para la empresa así como la preservación y cuidado de sus activos, de esta manera, cabe resaltar que se diseñaron 12 prácticas a fin de que sean cubiertos los conocimientos esenciales en materia de seguridad de la información en el período correspondiente a un semestre escolar, y que sea acorde a las actividades que se programan en el laboratorio del área.

En cada una de las prácticas desarrolladas se estudian temas vistos en diferentes asignaturas que componen el módulo, de tal forma que:

- Para la asignatura de Análisis y diseño de Redes se estudian los temas de VLAN, IPv6 y VPN; éstos se encuentran en las prácticas 5,9,10
- Para la asignatura de Arquitecturas Cliente-Servidor se estudia el tema de Análisis de tráfico; mismo que se presenta en la práctica 3
- Para la asignatura de Criptografía se estudian los temas de cifrado Simétrico y Asimétrico; éstos se trabajan en la práctica 2.
- Para la asignatura de Redes Inalámbricas se estudia el tema de WI-FI; el cual se ubica en la práctica 11.
- Para la asignatura de Seguridad Informática I se estudian los temas de Perímetro de seguridad y Controles de Acceso; éstos se revisan en las prácticas 1 y 7.
- Para la asignatura de Seguridad Informática II se estudian los temas de Firewall, vulnerabilidades, Perímetro de seguridad, y Códigos maliciosos; éstos se encuentran en las prácticas 4,6,7, 8 y 12.

Lo anterior da un amplio enfoque, permitiendo entender y correlacionar conceptos que parecieran distantes en primera instancia. Para poner a prueba la presente propuesta se realizaron pruebas las cuales fueron realizadas por estudiantes de Ingeniería en Computación de diferentes semestres, y en opinión de los estudiantes participantes demostraron su preferencia por usar equipos físicos sobre el uso de ambientes virtuales; considerando que éstos permitirían una mayor práctica durante el ejercicio profesional.

Con base en lo desarrollado en el capítulo 4 se puede concluir que los objetivos a cumplir fueron cubiertos, no sólo al quedar programadas actividades sujetas a un horario sino que también los estudiantes consideraron que los conocimientos revisados son acordes al módulo de estudio de Redes y Seguridad así como las actividades y materiales desarrollados para este fin.

Cabe mencionar que con la finalidad de crear expertos en la materia fue fundamental considerar a empresas como Symantec, Kaspersky y Bitdefender las cuales se dedican al desarrollo de soluciones en materia de seguridad informática y para ello les es imprescindible contar entre sus colaboradores con profesionales de la seguridad, así, al preparar profesionales especializados en esta área, la Facultad de Ingeniería hace más

competitivos a sus egresados en el mercado laboral dotándolos de capacidades para afrontar los retos que se exigen día a día en este mundo competitivo.

Es necesario crear de material como lo es el presente trabajo de tesis, que permita a los estudiantes mantenerse al día con las nuevas tecnologías existentes en materia de seguridad informática, así como el proveer conocimiento para el uso responsable de los recursos e información, que estén a su cargo durante su vida profesional.

Por último, se dejan un par de sugerencias con el fin de mejorar y actualizar el presente trabajo para que éste no se vuelva obsoleto y represente un instrumento valioso para el estudiante y el profesor.

Recomendaciones

- Con el constante avance tecnológico no es fácil mantener intacto un material de este tipo, por lo que la recomendación es que se revisen y actualicen semestralmente.

- Se sugiere la adquisición de equipo físico que permita afianzar los conocimientos en aquellas prácticas que se realizaron mediante el uso de ambientes virtuales.

- Se recomiendan la promoción de herramientas de seguridad informática usando Software Libre.

Finalmente espero que el presente material sea de gran apoyo a las siguientes generaciones.

Anexo I

Instalación de software necesario para la realización de la práctica # 7

Guía rápida de instalación de los programas NMAP y NESSUS

Instalación de NMAP

1. Iniciamos el instalador de la aplicación permitiendo la ejecución del programa. Presionamos el botón Ejecutar Figura AI.1

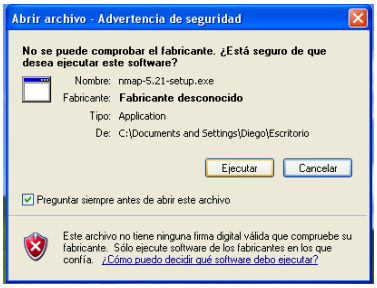


Figura AI.1 Ejecución del instalador

2. En este paso aceptamos los términos de la licencia (I AGREE) Figura AI.2

Se recuerda que NMAP tiene una licencia tipo GNU

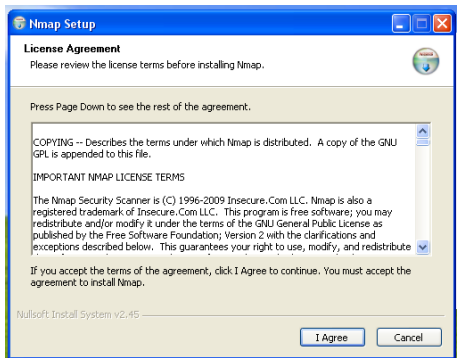


Figura AI.2 Términos de la licencia de NMAP

3. Seleccionamos los componentes a instalar, para fines de esta práctica dejaremos todos los componentes seleccionados. Pulsamos el botón NEXT Figura AI.3

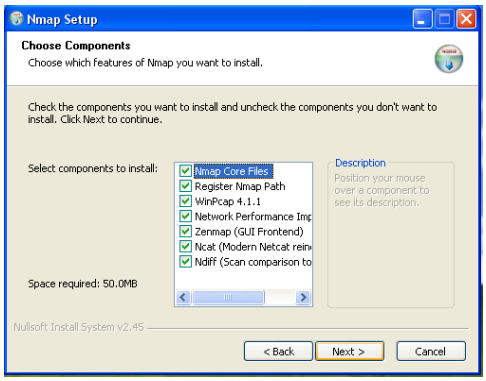


Figura AI.3 Selección de componentes de NMAP

4. Seleccionamos la ubicación donde quedaran instalados los archivos de ésta aplicación. Presionamos el botón INSTALL Figura AI.4

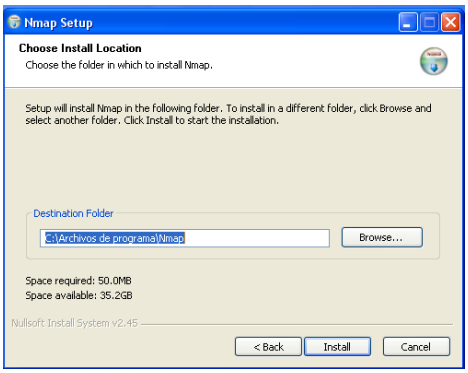


Figura AI.4 Selección del directorio de instalación de NMAP

5. Uno de los paquetes que vienen incluidos en ésta distribución de NMAP es WinPcap, ésta solicitará la configuración de preferencias de inicio, por el momento deseleccionáremos ambas casillas. Presionamos el botón NEXT. Figura AI.5

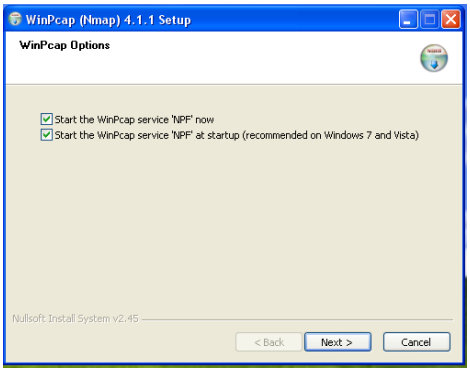


Figura AI.5 Preferencias de NMAP

6. Seleccionamos los accesos directos al programa. Presionamos el botón NEXT Figura AI.6

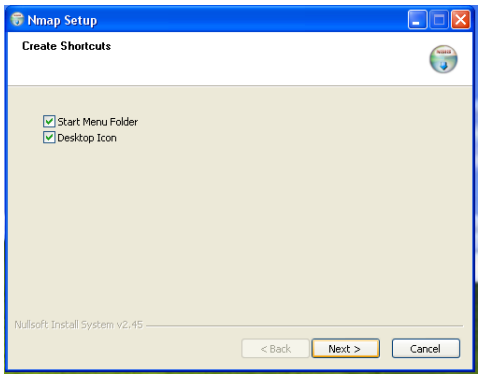


Figura AI.6 Creación de Accesos de NMAP

7. Finalizamos la instalación del programa presionado el botón de FINISH Figura AI.7

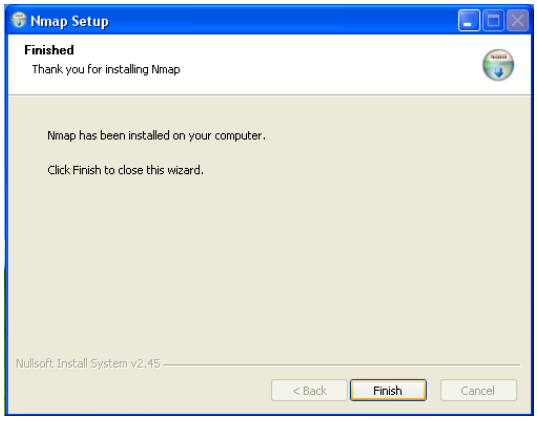


Figura AI.7 Finalización de la instalación de NMAP

Instalación de Nessus

1. Ejecutamos el instalador de la aplicación. Presionamos el Botón NEXT Figura AI.8

Figura AI.8 Instalador de NESSUS

2. Aceptamos los términos de la licencia. Presionamos el botón NEXT. Figura AI.9

NOTA a diferencia de NMAP NESSUS tiene una licencia COMERCIAL

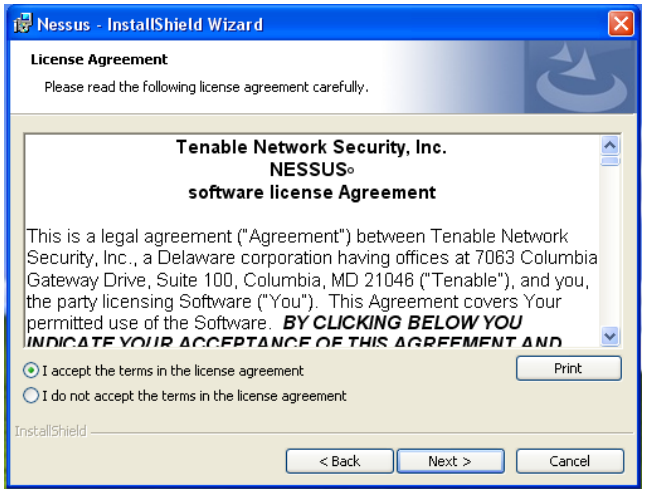


Figura AI.9 Términos de la licencia de NESSUS

3. Seleccionamos la ubicación donde quedaran instalados los archivos de ésta aplicación. Presionamos el botón NEXT. Figura AI.10

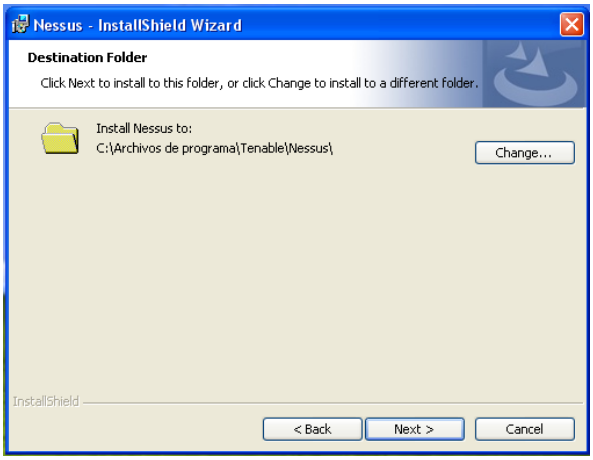


Figura AI.10 Selección del directorio de instalación de NESSUS

4. Seleccionamos el tipo de instalación que queremos llevar a cabo. Para fines de esta práctica elegimos COMPLETE. Presionamos el botón NEXT Figura AI.11

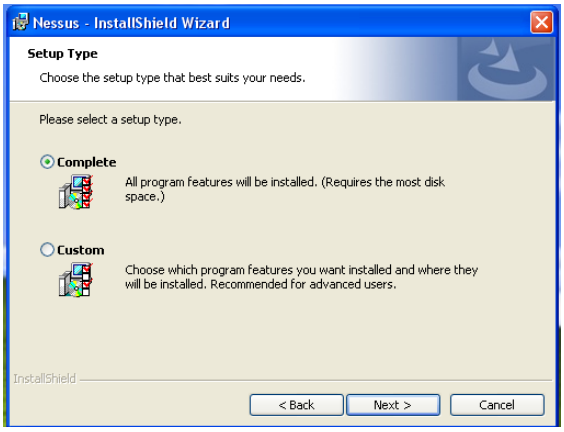


Figura AI.11 Tipo de instalación de NESSUS

Al termino de la instalación nosmostrará la sigueinte pantalla. Terminamos la instalación presionando el Botón FINISH Figura AI.12

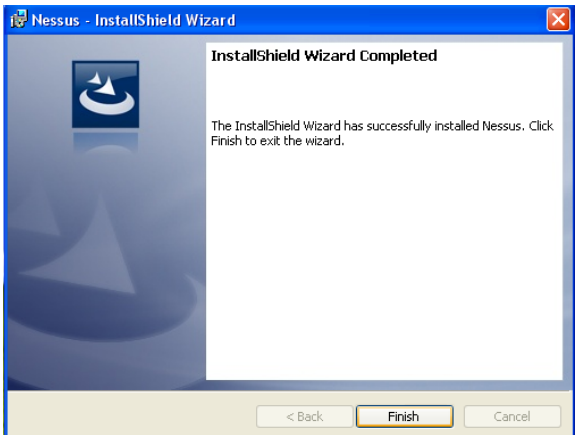


Figura AI.12 Instalación terminada de NESSUS

Configuración de NESSUS

1. Iniciamos la aplicación de Nessus Server Manager Figura AI.13

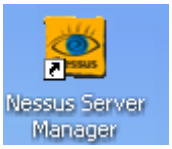


Figura AI.13 NESSUS Server Manager

2. Al iniciar nos aparecerá una ventana como la siguiente: Figura AI.14

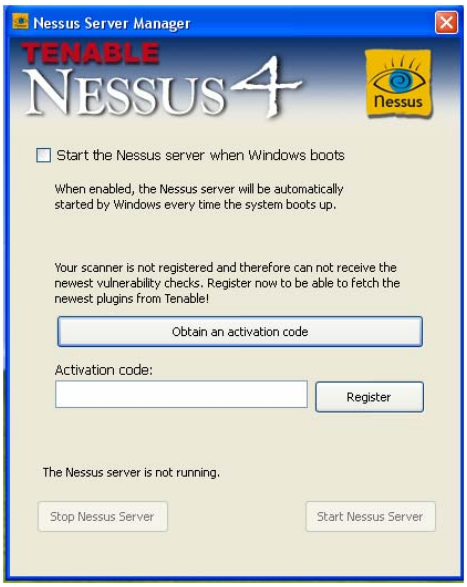


Figura AI.14 Configuraciones del servidor de NESSUS

Damos click en el botón OBTAIN AN ACTIVATION CODE

3. Se abrirá una ventana del navegador predeterminado de internet mostrando las 2 opciones de suscripción para el uso de ésta herramienta, para fines de la práctica seleccionaremos HomeFeed Figura AI.15

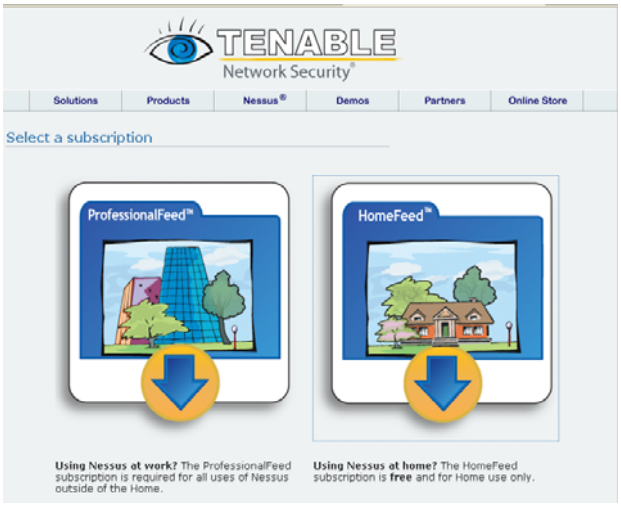


Figura AI.15 Selección de la suscripción de NESSUS

4. Aceptamos los términos de uso Figura AI .16

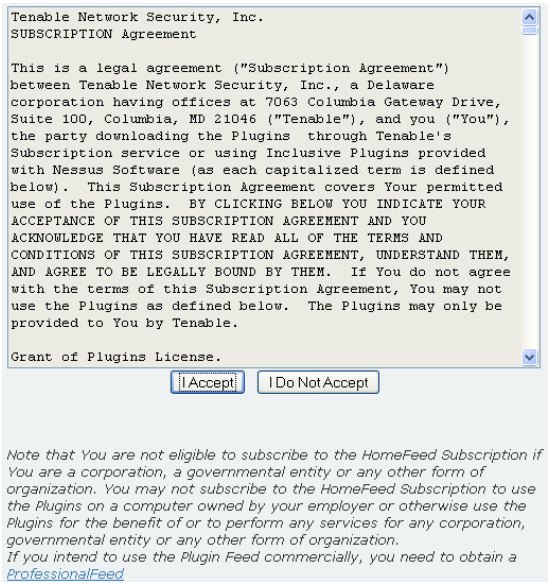


Figura AI.16 Licencia de NESSUS

5. A continuación escribimos una dirección de correo válida donde recibiremos la llave para usar el producto Figura AI.17

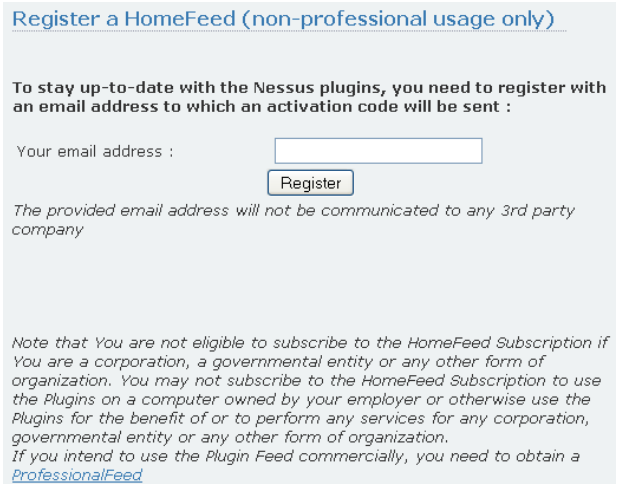


Figura AI.17 Registro de email para recibir clave de activación de NESSUS

6. Revisamos nuestra bandeja de entrada de nuestro correo y buscamos un mensaje con el encabezado "Nessus Plugin Feed" abrimos el correo y verificamos la clave adjunta en él Figura AI.18

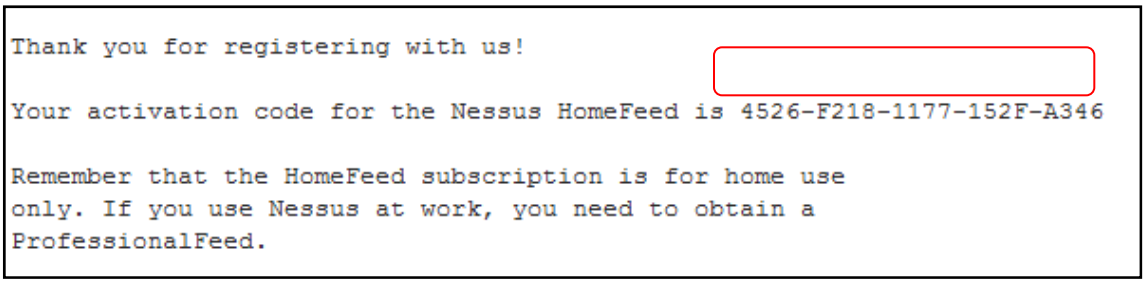


Figura AI.18 Clave de validación para NESSUS

7. Insertamos la clave y presionamos el botón Register para validar el producto. Después de ser activado iniciara la actualización de plug-ins de la aplicación, puede que tome varios minutos realizar la operación. Figura AI.19

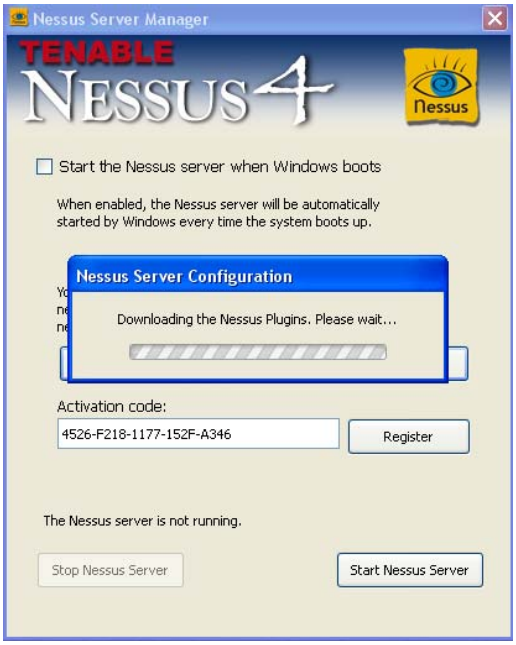


Figura AI.19 Registro de clave de NESSUS

8. Una vez que aparezca ésta pantalla podemos iniciar la práctica # 7 Figura AI.20

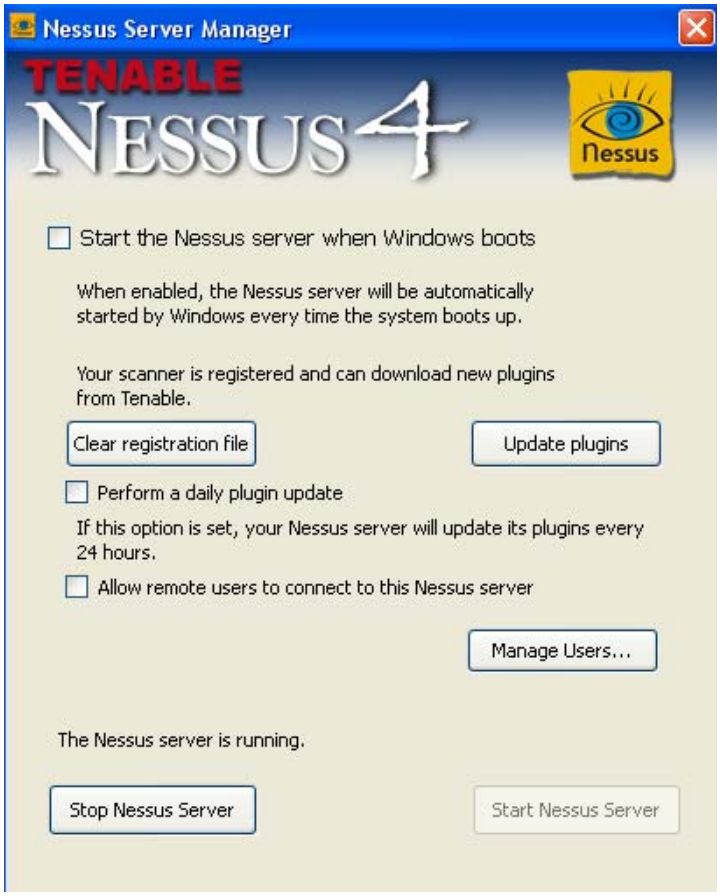


Figura AI.20 Panel de Control del servidor de NESSUS

Anexo II

Cuestionario Práctico

Cuestionario implementado para la obtención de datos estadísticos

Universidad Nacional Autónoma de México
Facultad de Ingeniería
División de Ingeniería Eléctrica

Cuestionario Estadístico

Condiciones de Uso

Se proveerá al participante material electrónico, impreso y digital para la consulta y realización de prácticas de seguridad informática. Algunos elementos tales como dispositivos físicos serán sujetos únicamente a préstamo durante la realización de determinadas prácticas, el uso de estos dispositivos estará sujeto a disponibilidad. Se brindará asesoría gratuita en caso de ser requerida.

Política de Privacidad

La recopilación de datos tales como: información personal y resultados obtenidos mediante el presente cuestionario solo serán con fines estadísticos y de mejora de las prácticas realizadas.

Acepto condiciones de uso y política de privacidad

_____
Nombre y Firma del Participante

Datos del Participante

Nombre del Alumno_____
Número de Cuenta_____ ¿Es Ud. pasante (si/no)?_____
Semestre Actual (aprox.)_____

Anexo II

Llena la siguiente tabla marcando con una x cada una de las preguntas:

Indica qué práctica(s) has realizado y ¿cuánto tiempo te ha llevado aproximadamente?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	45 min	1hr	1.25hr	1.5hr	1.75hr	2hr	2.5hr
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente contestar el cuestionario inicial?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente leer la introducción de la práctica?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									

7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente la toma de datos?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente rellenar el informe y terminar el cuestionario final?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

Selecciona una de las siguientes Opciones:

¿Por qué medio recibiste las prácticas?

1.-USB 2.-Email 3.-Prácticas impresas 4.-Otro

Anexo II

¿Cuál es tu principal fuente de información adiciona para realizar las prácticas de laboratorio de Seguridad Informática?

1. Soy pasante, tengo la información de otros años
2. En clase (apuntes, diapositivas, etc.)
3. Internet

¿Requeriste asesoría durante la realización de las prácticas?

1.-Si 2.-No

En tu opinión, ¿son útiles las actividades y prácticas en el laboratorio de Seguridad informática?

1.- Útiles 2.- Adecuadas 3.- Inútiles

¿Prefieres las prácticas virtuales o las de campo?

1.-Simulaciones 2.-De campo (con equipo físico)

¿Son útiles las prácticas para consolidar lo que se estudia en la teoría, o son complementarias?

1.- Refuerzan conocimiento 2.- Complementan

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando su consideración personal acerca de la información presentada en introducción.

1.- Suficiente 2.- Adecuada 3.-Deficiente

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando su consideración personal acerca del material empleado

1.- Suficiente 2.- Adecuada 3.- Deficiente

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando el nivel de dificultad de cada práctica

4 Muy difícil | 3 Difícil | 2 Normal | 1 Fácil

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando el nivel interés en las prácticas que hayas realizado

4 Muy interesante | 3 Interesante | 2 Poco Interesante | 1 Aburrido

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Índice de figuras y tablas

Listado indexado de figuras y tablas que aparecen en el presente trabajo

Índice de figuras

Tablas

Glosario

Definiciones de conceptos utilizados en el marco de la seguridad informática

802.11

802.11: Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas (wireless). Permite la conexión de dispositivos móviles (laptop, PDA, teléfonos celulares a una red cableada, por medio de un Punto de Acceso (Access Point). La conexión se realiza a través de ondas de Radio Frecuencia. Originalmente ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de 2.4 GHz Se le conoce popularmente como WIFI. Tiene un área de cobertura aproximada de 100 ms.

802.11a: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz Utiliza la tecnología OFDM (Orthogonal Frecuency División Multiplexing. Esta banda de 5GHz no se pudo utilizar en muchos países, al comienzo, por estar asignada a las fuerzas y organismos de seguridad.

802.11b: Estándar de conexión wireless que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. Fue ratificado en 1999. No es compatible con el 802.11a pues funciona en otra banda de frecuencia.

802.11g: Estándar de conexión wireless que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz Se basa en la tecnología OFDM, al igual que el estándar 802.11a. Fue ratificado en Junio de 2003. Una de sus ventajas es la compatibilidad con el estándar 802.11b.

802.11n: Estándar en elaboración desde Enero 2004. Tiene como objetivo conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps Hay 2 propuestas distintas. En 2006 se aprobará una de las dos. La de TGn Sync o la WWiSE.

• 802.16: Estándar de transmisión wireless conocido como WIMAX (Worldwide Interoperability for Microwave Access). Es compatible con WIFI. Se originó en Abril de 2002 con la finalidad de cubrir inalámbricamente distancias de hasta 50 Km. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz La interoperabilidad es certificada por el WIMAX FORUM

• 802.16d: Estándar de transmisión wireless (WIMAX*) que suministra una velocidad de entre 300 K y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Ratificado a finales de 2004. Se utiliza para el cubrimiento de la “primer milla”.

• 802.1x: Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

A

AAA: Abreviatura de autenticación, autorización y accounting, sistema de redes IP para a qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

Autenticación es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

Autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.

Accounting es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeamiento de capacidad, billing, auditoría y cost allocation.

A menudo los servicios AAA requieren un servidor dedicado. RADIUS es un ejemplo de un servicio AAA.

ACCESS POINT (PUNTO DE ACCESO): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

ACCESO REMOTO (REMOTE ACCESS): Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

ACREDITACIÓN VOLUNTARIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (1): Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

ACTIVE-X: Los denominados controles Active-X son componentes adicionales que se pueden incorporar a las páginas web, para dotar a éstas de mayores funcionalidades (animaciones, video, navegación tridimensional, etc.). Escritos en un lenguaje de programación como Visual Basic, C o C++, que no es el propio de las páginas web (HTML) y podrían estar infectados con virus.

AD HOC: Una WLAN bajo una topología “Ad Hoc” consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones “Ad Hoc” son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal

ADWARE: Es una variante comercial del Spyware. Se trata de un pequeño trozo de código que tiene como finalidad recolectar datos a efectos de marketing. Es difícil distinguirlo del malware.

AES: Estándar de cifrado avanzado (Advanced Encryption Standar): También conocido como “Rijndael”, algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST).

AGUJERO (HOLE): Una vulnerabilidad en el diseño del software y/o hardware que permite engañar a las medidas de seguridad

ALIAS (ALIAS): Nombre diferente por el cual se conoce un virus.

ALGORITMO DE ENCRIPTACIÓN (ENCRIPTYON ALGORITHM): Codificaciones de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma / producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños.

AMPLIFICADOR (AMPLIFIER): Produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido preamplificado y un amplificador lineal de salida de radio frecuencia (RF).

ANTENA (ANTENNA): Dispositivo generalmente metálico capáz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia qué punto se emita la señal podemos encontrar direccionales u omnidireccionales.

APPLIANCE SERVER: Servidores (dedicados a Internet sharing servicios FTP, e-mail, conexiones VPN, servicios de cortafuegos, de impresora y archivo y también operan como servidores web) que incorporan hardware y software en el mismo producto de modo que las aplicaciones se encuentran pre instaladas. El appliance está plug-in dentro de una red existente y puede comenzar a funcionar casi de inmediato con una mínima configuración y mantenimiento.

ANÁLISIS EURÍSTICO (HEURISTIC ANALIST): Se trata de un análisis adicional que solamente algunos programas anti-virus pueden realizar para detectar virus que hasta ese momento son desconocidos.

ANALIZADOR DE COMPORTAMIENTO (BEHAVIOR BLOCKER): Un programa anti-virus emplea una técnica para comprobar si un archivo incorpora los comportamientos habituales de un virus. Un Behavior blocker trabaja bajo un conjunto de reglas de funcionamiento que legitima programas bajo las reglas de comportamiento que siguen los virus. Además analiza y determina las tareas y comportamientos que han sido diseñadas para un archivo y averigua si el éste contiene algún virus.

ANCHO DE BANDA (BANDWIDTH): Este término define la cantidad de datos que pueden ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado.

ANTI-VIRUS: Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos

APPENDER (APPENDER): Es un virus que afecta una copia de su código al final del archivo de la víctima.

ARMOURING (ARMOURING): Mediante esta técnica el virus impide ser examinado. Para conocer más datos sobre cada uno de los virus, éstos son abiertos como archivos, utilizando programas especiales que permiten descubrir cada una de las líneas de su código. De un virus que utilice esta técnica no se podrá leer su código.

ATAQUE ACTIVO (ACTIVE ATTACK): Ataque al sistema para insertar información falsa o corromper la ya existente.

ATAQUES A PASSWORDS (PASSWORD ATTACK): Es un intento de obtener o descifrar un password legítima de usuario. Las medidas de seguridad contra estos ataques son muy limitadas, consistiendo en una política de passwords, que incluye una longitud mínima, palabras no reconocibles y cambios frecuentes.

ATAQUE DE DICCIONARIO (DICCIONARY ATTACK): Método empleado para romper la seguridad de los sistemas basados en passwords (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático. Generalmente no se introducen manualmente las posibles contraseñas sino que se emplean programas especiales que se encargan de ello.

ATAQUE DE FUERZA BRUTA (BRUTE FORCE ATTACK): Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.

AUDITORÍA: Análisis de las condiciones de una instalación informática por un auditor extremo e independiente que realiza un dictamen sobre diferentes aspectos. Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

AUTENTIFICACIÓN (AUTHENTICATION): Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

AUTO – ENCRIPTACIÓN (AUTO – ENCRYPTION): Capacidad de algunos virus para esconderse de posibles programas anti-virus. Las soluciones anti-virus se encargan de encontrarlos buscando determinadas cadenas de caracteres (firma del virus), identificativas de cada una de ellos. Para evitar este mecanismo de búsqueda, algunos virus consiguen codificar o cifrar estas cadenas de texto de forma diferente en cada nueva infección. Esto supone que en la nueva infección, el anti-virus no encontrará la cadena que busca para detectar a un virus en concreto, pues éste la habrá modificado. No obstante, existen otros mecanismos alternativos para detectarlos.

AUTORIZACIÓN (AUTHORISATION): Proceso por el que se acredita a un sujeto o entidad para realizar una acción determinada.

B

BACKGROUND (BACKGROUND): Se dice que una aplicación funciona “en background” cuando está trabajando sin afectar la actividad del usuario.

BIOMÉTRICA (BIOMETRIC): Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc.…) para su aplicación a la seguridad informática como medio de identificación del usuario.

BLOWFISH: es un codificador simétrico de bloques. Toma una clave de longitud variable, entre 32 y 448 bits.

BRIDGE (PUENTE): elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

BOMBA DE E-MAIL (MAILBOMB): son mensajes de correo electrónico excesivamente largos enviados a la cuenta de correo de un usuario con el propósito de provocar la caída del sistema o evitar que los mensajes verdaderos sean recibidos.

BOMBA DE TIEMPO (TIME BOMB): Programa que se activa en una determinada hora.

BOMBA LÓGICA (LOGIC BOMB): programa que se ejecuta cuando existen condiciones específicas para su activación. Los suelen utilizar muchos virus como mecanismo de activación.

BOTS (BOTS): Término utilizado en Internet y que se deriva de la palabra “robot”. Con él se denomina a pequeños trozos de software que tienen la finalidad de actuar de manera independiente en un computador, como un “robot” controlado remotamente.

BUGTRAG: lista de correo de divulgación completa, moderada para la discusión detallada y anuncio de vulnerabilidades en seguridad informática; qué son, cómo explotarlas y cómo solucionarlas.

BÚSQUEDA EXAUSTIVA DE CLAVE (EXHAUSTIVE KEY SEARCH): Consiste en descubrir la clave empleada en un sistema de encriptación, probando todas las posibles.

C

CADENA (CHAIN): Una consecución de caracteres de texto, dígitos, números, signos de puntuación o espacios en blanco consecutivos. Alguna de las técnicas empleadas por los anti-virus para la detección de virus es buscar determinadas cadenas de texto (o código) que estos incluyen de manera frecuente.

CENTRINO: Tecnología móvil desarrollada por Intel compuesta por un procesador Pentium M, chipset 855 y conectividad inalámbrica integrada.

CHAP – CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL: Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP. Una vez efectuado el enlace, el servidor envía un mensaje de desafió al solicitante de la conexión, el cual responde a un valor hash que será comparado por el servidor con sus cálculos de valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario0 finaliza. En cualquier momento el servidor puede solicitar un mensaje de desafió. Debido a que los identificadores cambian frecuentemente y por que la autenticación puede ser solicitada en cualquier momento.

CLIENTE INALÁMBRICO (WIRELESS CLIENT): Todo dispositivo susceptible de integrarse en una red wireless como PDAs, portátil, cámaras inalámbricas, impresoras, etc.…

CERTIFICADO DIGITAL (1) (CERTIDFICATE): Es la certificación electrónica que emiten las Autoridades Certificadoras donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma digital del

emisor. Los Certificados Digitales siguen las estipulaciones del estándar X.509. Este documento sirve para vincular una clave pública a una entidad o persona.

CHEQUEADOR DE INTEGRIDAD (INTEGRITY CHECKER): Es un programa que determina si otro programa ha sido alterado. Para que una infección de virus ocurra, el código ejecutable necesita haber sido alterado por un virus. Un chequeador de integridad investiga tales cambios y los marca como sospechosos.

CHECKSUM CRIPTOGRÁFICO (CRYPOGRAPHIC CHECKSUM): Checksum calculado mediante la utilización de un algoritmo como base criptográfica. Es imposible cambiar unos datos sin que el checksum criptográfico cambie.

CHECSUMMER: Herramienta que calcula un único número asociado a determinados archivos que habitualmente no cambia para protegerlos. Checksummer recalculará periódicamente dicho número y si se detecta que ha cambiado, será un indicio de infección.

CLAVE DE ENCRIPTACIÓN (ENCRYPTION KEY): Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

CLAVE DE REGISTRO (REGISTRY KEY): El registro (Registry) de Windows es un elemento en el que se guardan las especificaciones de configuración del PC mediante claves. Estas claves cambiarán de valor y/o se crearán cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.

CODIFICADOR OR BLOQUES (BLOCK CIPHER): Ciencia que estudia las características biológicas del ser humano (el iris, huella dactilar, la voz, etc.…) para su aplicación a la seguridad informática como medio de identificación del usuario.

COMPSEC: Abreviatura de COMPuter SECurity (Seguridad Informática).

CONFIDENCIALIDAD (CONFIDENTIALITY): Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

CONTROL DE ACCESOS (ACCESS CONTROL): Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web, etc.,… El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de usuario y password, certificados del cliente, protocolos de seguridad de redes, etc.

COPIA DE SEGURIDAD (BACKUP): Es una copia de todos los datos originales contenidos en redes y PC’s que puede ser usado en caso de que estos se destruyan por diversas causas.

CORTAFUEGOS (FIREWALL): Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc.…

CRACKER: Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.

CRIPTOANÁLISIS (CRYPTANALYSIS): Estudio de un sistema de encriptación con la intención de detectar cualquier punto débil dentro de su algoritmo clave.

CRIPTOLOGÍA (CRYPTOLOGY): Ciencia que estudia el arte de crear y utilizar sistemas de encriptación.

CRON (UNIX): En el sistema operativo Unix, cron es un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero crontab.

CROSSTALK (RUIDO, INTERFERENCIA): Ruido o interferencia que fluye entre los cables de comunicación o dispositivos.

D

DELITO INFORMÁTICO (COMPUTER CRIME): Delito cometido utilizando una PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

DENEGACIÓN DE SERVICIOS (Denial of Service) (DoS): O ataque DoS. Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

DES: algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmos DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

DESBORDAMIENTO DE BÚFFER (BUFFER OVERFLOW): Error de software que se produce cuando se copia una cantidad más grande de datos sobre un área más pequeña sin interrumpir la operación sobre-escribiendo otras zonas de datos no previstas. En algunas ocasiones eso puede suponer la posibilidad de alterar el flujo del programa pudiendo hacer que este realice operaciones no previstas. Si el programa que tiene el error en cuestión tiene privilegios especiales se convierte además en un fallo de seguridad. El código copiado especialmente reparado para obtener los privilegios del programa atacado se llama shellcode.

DESENCRIPTAR (DESCRYPTION): Proceso de transformación en cyphertext – texto encriptado o cifrado – a plaintext (Es la acción inversa de encriptar).

DESINFECCIÓN (DISINFECTION): Acción que realizan los programas anti-virus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan o restauran la información infectada.

DHA (DIRECTORY HARVEST ATTACK): Llamado el "Asesino Silencioso". Este ataque consiste en el envío masivo de emails a un dominio determinado con el fin de "cosechar" y recolectar direcciones válidas de emails, para ser incorporadas a las listas de spam.

RELLAMADA (DIALBACK): Rasgo de seguridad que asegura que las personas sin autorización no conecten con módems a los que no deben tener acceso. Cuando se pide una conexión, el sistema verifica el nombre del usuario para validarlo, e inicia una re llamada al número asociado con ese nombre de usuario.

DIALER: Programa que permite cambiar el número de acceso telefónico automáticamente de acuerdo a la situación geográfica del usuario. Estos códigos (que se descargan de sites a veces sin darnos cuenta) toman el control sólo de la conexión telefónica vía módem, desviando las llamadas normales que efectúas a través de tu proveedor hacia una número del tipo 908, 906, etc.…, números de tarifa especial y bastante cara por lo general. Últimamente se han detectado un aumento de incidentes relativos a “dialers porno” que permiten visualizar páginas pornográficas de forma gratuita pero que sin embargo se pagan cuando llega la escandalosa factura telefónica.

DISPOSITIVO MOVIL (MOBILE DEVICE): Ya sea una tarjeta PCMIA, USB, PCI (Slot de un PC de sobremesa), Centrino, que sustituyen a las tarjetas de red. Su función es la de recibir/enviar información desde la estación en que están instaladas (portatileslaptops, netbooks, PDAs, móviles, cámaras, impresoras)

DSSS- ESPECTRO AMPLIO MEDIANTE SECUENCIA DIRECTA (DIRECT SEQUENCE SPREAD SPECTRUM): A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos. Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b

DISPOSITIVO DE CREACIÓN DE FIRMA ELECTRÓNICA (1): Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma (electrónica).

DISPOSITIVO DE VERIFICACIÓN DE FIRMA ELECTRÓNICA (1): Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma (electrónica).

DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA ELECTRÓNICA (1): Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

DONGLE: Hardware de seguridad que se debe conectar al sistema informático antes de que se ejecute una determinada aplicación; previene las copias ilegales de los programas informáticos.

DROPPER: Usado como portador de virus, un dropper es un programa ejecutable que instala el virus en memoria, en el disco o en un archivo (aunque un dropper por sí mismo no tiene capacidades de infección ni de replicación).

E

EAP – PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE (EAP – EXTENSIBLE AUTHENTICATION PROTOCOL): Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por

clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

ECHELON: Sistema internacional de interceptación mediante satélites de las telecomunicaciones iniciado como proyecto en 1947 e implementado en 1960. Desde su nacimiento en plena Guerra Fría ha evolucionando con los tiempos incluyendo actualmente actividades de espionaje industrial. Su dirección está al cargo de la NSA (National Security Agency, Estados Unidos) y de la GCHQ (Government Communications Headquarters, Gran Bretaña) aunque también tiene estaciones de control en Australia, Canadá y Nueva Zelanda.

ENCRIPTACIÓN (ENCRYPTION): Proceso para transformar la información escrita en plaintext a ciphertext.

ENCRIPTACIÓN ASIMÉTRICA (ASYMMETRIC ENCRYPTION): Encriptación que permite que la clave utilizada para encriptar sea diferente a la utilizada para desencriptar. El algoritmo de encriptación asimétrico más difundido es RSA.

ENCRIPTACIÓN DE ARCHIVOS (FILE ENCRYPTION): transformación de los contenidos plaintext de un archivo (texto sin cifrar) a un formato ininteligible mediante algún sistema de encriptación.

EN EL TERRENO (IN THE WILD): Clasificación utilizada por la organización Wildlist que recoge todos aquellos virus sobre los que más de una persona ha notificado alguna incidencia.

EN EL ZOO (IN THE ZOO): Describe un virus que únicamente existe dentro de un entorno de investigación.

ENGAÑO (HOAX): No se trata de virus, sino de falsos mensajes de alarma (bromas o engaños) sobre virus que no existen. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet. Los mensajes no suelen estar fechados, con lo que se pretende que los mensajes siempre parezcan recientes. En ocasiones, los Hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas. , mensajes que simulan a los reales, alertas de nuevos virus, anuncios de nuevas soluciones, cadena de correos a reenviar,…, etc. Por otra parte, suele ser frecuente la inclusión del nombre de ciertas agencias de prensa (CBS…) en el encabezamiento de estos mensajes. Con todo esto se pretende dar un aspecto verídico a los mensajes.

ESCÁNER (SCANNER): Programa que busca virus en la memoria del PC o en los archivos.

ESCÁNER BAJO DEMANDA (SCANNER ON DEMAND): Programa escáner antivirus que el usuario ejecuta manualmente cuando lo estima conveniente.

ESCÁNER HEURÍSTICO (HEURISTIC SCANNER): Programa escáner antivirus que busca virus nuevos y desconocidos.

ESCÁNER RESIDENTE (RESIDENT SCANNER): Programa escáner antivirus que está buscando virus recursivamente en background.

ESTÁNDAR (STANDAR): Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc.…

ETHERNET: Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

EXCEPCIONES (EXCEPTIONS): Una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso, lo que el programa anti-virus puede chequear es el cambio en las cadenas (excepciones).

EXPLOTAR (EXPLOIT): Método de utilizar un bug o fallo para penetrar en un sistema.

F

FALLO (BUG): O error en un programa. Cuando uno de ellos tiene errores, se dice que tiene Bugs. Como los virus son programas, también pueden contener bugs. Esto implicaría que, si el virus debe realizar determinadas acciones, podría no realizarlas, o no hacerlo bajo las condiciones que su programador ha establecido inicialmente.

FALSO NEGATIVO (FALSE NEGATIVE): Evento que se da como inexistente cuando realmente si existe, por ejemplo, decir que un sistema está limpio de virus cuando realmente está infectado.

FALSO POSITIVO (FALSE POSITIVE): Evento que se da como existente cuando realmente no existe, por ejemplo, decir que un sistema está infectado de virus cuando realmente está limpio.

FAST – FLEXIBLE AUTHENTICATION SECURE TUNNELING : Protocolo de seguridad WLAN del tipo EAP. Desarrollado por Cisco y presentado a la IETF como borrador a principios de 2004. Impide los denominados ataques de diccionario por fuerza bruta enviando una autenticación de contraseña entre el cliente WLAN y el punto de acceso inalámbrico a través de un túnel cifrado seguro. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).

FHSS – ESPECTRO AMPLIO MEDIANTE SALTOS DE FRECUENCIA (FHSS – FREQUENCY HOPPING SPREAD SPECTRUM): Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar a cabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este “Hopping Pattern”. El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth.

FICHERO (FILE): Todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.

FILTRADO (FILTERING): Proceso mediante el cual un puente o conmutador Ethernet lee el contenido del paquete y descubre que éste no necesita volver a ser enviado, por lo que lo desprecia. La velocidad de filtrado es la velocidad a la que un dispositivo puede recibir paquetes y desecharlos sin ninguna pérdida de paquetes entrantes o demoras en su procesado.

FILTROS ANTI-SPAM (ANTI-SPAM FILTERS): Son herramientas para filtrar el spam o correo basura no solicitado en los programas de correo.

FIRMA ELECTRÓNICA O FIRMA DIGITAL (DIGITAL SIGNATURE): El conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.

FIRMA ELECTRÓNICA AVANZADA (ADVANCED DIGITAL SIGNATURE) : Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

FIRMWARE: Software (programas o datos) escritos en la memoria de sólo lectura (ROM). El firmware es una combinación de software y hardware. ROMs, PROMs e EPROMs que tienen datos o programas grabados dentro son firmware.

ENTRAMADO (FRAMING): División de datos para su transmisión en grupos de bits a los que se les añade una cabecera y un código de verificación para formar una trama.

FTP – PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP – FILE TRANSFER PROTOCOL) : Protocolo de transferencia de archivos que permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.

G

GALLETA (COOKIE): Rastro que el servidor de un sitio web deja en nuestro PC cuando lo visitamos por primera vez; cada vez que volvemos a dicho sitio, la señal se actualiza, dando información al servidor de nuestro paso por la página. Con estas señales, los servidores pueden saber por dónde navegamos, cuáles son nuestros intereses, etc.…

GATEWAY (PASARELA/PUERTA): Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas.

GPS – SISTEMA DE POSICIONAMIENTO GLOBAL (GPS – GLOBAL POSITION SYSTEM): Sistema de navegación por satélite con cobertura global y continua que ofrece de forma rápida y temporalmente bastante precisa una posición geográfica de un elemento. El primer satélite para esta técnica de seguimiento se lanzó en

1978, pero sin embargo el sistema no estuvo operativo hasta 1992 y fue desarrollado por las fuerzas aéreas de los EE.UU.

GESTIÓN DE CLAVES (KEY MANAGEMENT): Proceso para generar, transportar, almacenar y destruir claves de encriptación de modo seguro.

GNU: Es un acrónimo recursivo que significa **GNU No es Unix** (*GNU is Not Unix*). Puesto que en inglés "*gnu*" (en español "ñu") se pronuncia igual que "*new*", Richard Stallman recomienda pronunciarlo "*guh-noo*". En español, se recomienda pronunciarlo ñu como el antílope africano o fonéticamente;[2] por ello, el término mayoritariamente se deletrea (G-N-U) para su mejor comprensión. En sus charlas Richard Stallman finalmente dice siempre «Se puede pronunciar de cualquier forma, la única pronunciación errónea es decirle 'linux'».

GPL: Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en Inglés como copyleft -'copia permitida'- (en clara oposición a copyright -'derecho de copia'-), y está contenida en la Licencia General Pública de GNU

H

HACKER: Persona que accede a un sistema informático sin autorización para “cotillear”, ver su funcionamiento interno y explotar vulnerabilidades. Este término se suele utilizar indistintamente con el término cracker (intruso), pero supuestamente hacker no implica necesariamente malas intenciones, mientras que cracker sí.

HASH: Un valor hash, también conocido como “message digest”, es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

HONEYPOTS (TARROS DE MIEL EN CASTELLANO): Un servidor diseñado para ser atacado y que actúa como señuelo para hackers los cuales piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del “pirata” con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, etc.

HOTSPOT (PUNTO CALIENTE): Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc.…) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.

I

IRC WORMS (GUSANOS DE INTERNET RELAY CHAT): Infectan solamente a usuarios del software MIRC para acceder a los canales IRC (Internet Relay Chat). El gusano se aprovecha de cualquier desperfecto en el diseño de seguridad del software mIRC PARA sobre-escribir el archivo Script omitido (Script.ini) cuando los archivos son transferidos utilizando el protocolo DCC.

IEEE – INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS (- INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS)
Formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo (http://www.ieee.org).

IETF – THE INTERNET ENGINEERING TASK FORCE: Grupo principal auto-organizado comprometido en el desarrollo de nuevas especificaciones estándares para Internet (http://www.ietf.org).

INFRAESTRUCTURA (INFRAESTRUCTURE): Topología de una red inalámbrica que consta de dos elementos básicos: estaciones cliente wireless y puntos de acceso

IPSEC – IP SECURITY: Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

INFECCIÓN (INFECTION): Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo.

INTEGRIDAD DE ARCHIVOS: Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).

ISO 17999: Estándar para la gestión de la seguridad de la información.

L

LAN – RED DE ÁREA LOCAL (LOCAL AREA NETWORK): Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)… Sus características son: Topología en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.

LDAP – Protocolo de Acceso Ligero a Directorio (Lightweight Directory Access Protocol): Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más

simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet. Aunque no está ampliamente extendido, debería poderse implementar en la práctica mayoría de aplicaciones que se ejecutan virtualmente sobre plataformas informáticas para obtener información de directorios tales como direcciones de correo y llaves públicas. Ya que es un protocolo abierto, no afecta el tipo de servidor en el que se aloje el directorio.

LEAP – LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL: Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

M

MAC – DIRECCIÓN DE CONTROL DE ACCESO A MEDIOS (MEDIA ACCESS CONTROL ADDRESS): Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexadecimal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.

MALWARE (CÓDIGO MALICIOSO): Es un término genérico utilizado para describir el software malicioso tales como: virus, troyanos, etc.

MBPS (MEGABITS POR SEGUNDO): Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

MD5: Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función hash de una dirección, se puede comparar un valor hash frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en Nombre de Usuario y Contraseña, EL PRIMERO SE ENVÍA sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

MHZ (MEGAHERTZIO): Unidad empleada para medir la “velocidad bruta” de los microprocesadores equivalente a un millón de hertzios.

MS-CHAP – PROTOCOLO DE AUTENTICACIÓN POR DESAFÍO MUTUO (MS-CHAP – CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL): Protocolo de autenticación utilizado por el acceso remoto de Microsoft y conexiones de red y de acceso telefónico. Con CHAP los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autenticación a un servidor de acceso remoto. Microsoft ha creado una variante de CHAP específica de Windows denominada MS-CHAP. Challenge Handshake Authentication Protocol se llama también CHAP.

N

NCSC – CENTRO NACIONAL DE SEGURIDAD INFORMÁTICA (NATIONAL COMPUTER SECURITY CENTER): Institución de EEUU responsable de fomentar el desarrollo de sistemas informáticos seguros y de su implantación en las oficinas del gobierno para la clasificación de la información.

O

OFDM – ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING: Técnica de modulación FDM (empleada por el 802.11a wi-fi) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

P

PAP – PROTOCOLO DE AUTENTICACIÓN DE CLAVES (PASSWORD AUTHENTICATION PROTOCOL): El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión. Típicamente, las contraseñas almacenadas en la tabla se encuentran encriptadas. El principal defecto de PAP es que tanto el nombre de usuario como la clave se transmiten sin codificar, a diferencia de sistema CHAP.

PAYLOAD: Efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos secundarios de dicha infección (cambios en la configuración del sistema, reenvío de e-mail, ejecución del virus en el arranque del sistema o de Windows,…).

PEAP – PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL: Protocolo del tipo EAP desarrollado conjuntamente por Microsoft, RSA Security y Cisco para la transmisión datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wi-fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS encriptado entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

PHISHING: Técnica en auge que consiste en atraer mediante engaños a un usuario hacia un sitio web fraudulento donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y passwords de las cuentas, números de seguridad social, etc.… Uno de los métodos más comunes para hacer llegar a la “víctima” a la página falsa es a través de un e-mail que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una web en la que el “phiser” ha reemplazado en la barra de dirección del navegador la verdadera URL para que parezca una legal.
Una de las consecuencias más peligrosas de este fraude es que la barra “falsa” queda en memoria aún después de salir de la misma pudiendo hacer un seguimiento de todos los sitios que visitamos posteriormente y también el atacante puede observar todo lo que se envía y recibe a través del navegador hasta que éste sea cerrado.
Una manera para el usuario de descubrir el engaño es que no se muestra la imagen del candado en la parte inferior del navegador que indica que la navegación es segura.

PIN – PERSONAL IDENTIFIER NUMBER (NÚMERO DE IDENTIFICACIÓN PERSONAL): Número generalmente de 4 dígitos que actúa como contraseña de acceso para el uso de una diversidad de servicios: cajeros automáticos, conexión de teléfono móvil, etc..

PKI – INFRAESTRUCTURA DE CLAVE PÚBLICA (PUBLIC KEY INFRASTRUCTURE): Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet. Los estándares de PKI siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico. La infraestructura de claves públicas se llama también PKI.

POLIMORFISMO (POLYMORPHISM): Característica que presentan algunos virus consisten en que su código no siga un patrón fijo de caracteres de modo que es muy difícil detectarlo.

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (CERTIFICATE SERVICE PROVIDER): Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

PROCEDIMIENTO DE DISOCIACIÓN: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

PRODUCTO DE FIRMA ELECTRÓNICA (PRODUCT OF DIGITAL SIGNATURE): Es un programa o aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

PROTECCIÓN CONTRA COPIADO (COPY PROTECTION): Método para impedir hacer copias de programas de software. Es una forma de evitar el robo de aplicaciones informáticas.

PROTECCIÓN DE DATOS (DATA PROTECTION): Conjunto de técnicas utilizadas para preservar la confidencialidad, la integridad y la disponibilidad de la información.

PROTOCOLO (PROTOCOL): Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

PUERTA TRASERA (BACKDOOR): No se trata de un virus, sino de una herramienta de administración remota. Si es instalada por un hacker tiene la capacidad de dar a un atacante privilegios como administrador. Puede incluso buscar passwords y datos confidenciales y enviarlos vía mail a un área remota.

R

RADIUS – REMOTE AUTHENTICATION DIAL-IN USER SERVICE: Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISP's) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y

contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

RAS – SERVIDOR DE ACCESO REMOTO (REMOTE ACCESS SERVER): Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

ROUTER: Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LAN's o WAN's o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.

ITINERANCIA (ROAMING): En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

S

SECTOR DE ARRANQUE (BOOT SECTOR): Todo disco tiene un sector de arranque que el PC lee cuando se enciende. Este sector contiene todos los códigos necesarios para cargar los archivos de sistema DOS.

SECTOR DE PARTICIÓN (PARTITION SECTOR): Todo disco duro o disquete tiene un sector de partición que es leído después de que se ha arrancado el PC. Contiene datos sobre el disco tales como el número de sectores de cada partición y la ubicación de las particiones.

SECTORES DEFECTUOSOS (BAD SECTORS): Aquellos que, tras formatear el disco duro en MS-DOS, se revelan inutilizables. Algunos virus tienen la capacidad de renombrar sectores útiles como “defectuosos” para almacenar en ellos su código, de modo que el usuario y el sistema operativo no accedan a él y garantizando así la infección del PC.

SERVIDOR DE AUTENTICACIÓN (AUTHENTICATION SERVER): Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.

SHELLCODE: En términos underground, shellcode son una serie de órdenes de ensamblador que, beneficiándose de fallos informáticos, que ejecutan un código después de sobrescribir la dirección de retorno (ret) de un programa o función mediante un desbordamiento (overflow) u otro método válido. Si el atacante consigue insertar su shellcode sobre el ret, cuando se produzca el desbordamiento y el salto, se ejecutará sus órdenes.

SIGNATARIO (SIGNATORY): Persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

SISTEMA DE ENCRIPTACIÓN (CRYPTOSYSTEM): Colección completa de algoritmos que tienen su propia denominación en función de las claves que utilizan para encriptar.

SOBREPASAMIENTO (TUNNELING): Técnica diseñada para impedir que las aplicaciones anti-virus trabajen correctamente.

SPYWARE (SPYWARE): Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se dé cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

STEALTH: Característica que tienen los virus para pasar inadvertidos ante el usuario al que infectan.

TARJETA INTELIGENTE (SMART CARD): Pequeño dispositivo electrónico del tamaño de una tarjeta de crédito que contiene memoria digital y posiblemente un circuito integrado, llamándose entonces Integrated Circuit Cards (ICCs). Sus usos son variados: para almacenar historiales médicos, como monedero digital, para generar IDs (similar a un Token). Para utilizarla, y bien capturar los datos en ella almacenada o bien añadirlos, es necesario un pequeño lector especial para estos dispositivos.
SNIFFER: Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas sniffers conocidas son: WepCrack, Airsnort o NetStumbler, entre otras…

SPAM: También conocido como junk-mail o correo basura, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

SPOOFING: Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Otros ataques de falseamiento conocidos son:
• DNS Spoofing: En este caso se falsea una dirección IP ante una consulta de resolución de nombre (DNS) o viceversa, resolver con un nombre falso una cierta dirección IP.
• ARP Spoofing: Hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que un determinado equipo de una red local envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.
• Web Spoofing: El pirata puede visualizar y modificar una página web (incluso conexiones seguras SSL) solicitada por la víctima.
• E.mail Spoofing: Falsifica la cabecera de un e-mail para que parezca que proviene de un remitente legítimo. El principal protocolo de envío de e-mails, SMTP, no incluye opciones de autenticación, si bien existe una extensión (RFC 2554) que permite a un cliente SMTP negociar un nivel de seguridad con el servidor de correo.

SSID: Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

SSL – SECURE SOCKETS LAYER : Aprobado como estándar por el Internet Engineering Task Force (IETF), es un protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor. Trabaja empleando una llave privada de encriptación de datos que es transferida a través de la conexión SSL. Los navegadores Netscape y Explorer soportan SSL, y muchas páginas web emplean el protocolo para obtener información confidencial del usuario, como números de tarjeta de crédito, etc. Por convención, las URLs que precisen una conexión SSL comienzan con https, en lugar de http.

T

TARJETA DE RED INALÁMBRICA: Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: Compact Flash, PCI, PCMCIA, USB

TEXTO CODIFICADO (CIPHERTEXT): Se dice que un texto está escrito en ciphertext cuando es necesario decodificarlo para poder leerlo.

TEXTO SIMPLE (PLAINTEXT): Se dice que un texto está escrito en plaintext cuando puede ser leído sin tener que realizar ninguna operación, es decir, no está codificado.

TKIP – PROTOCOLO DE INTEGRIDAD DE CLAVE TEMPORAL (TEMPORAL KEY INTEGRITY PROTOCOL): Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS – TRANSPORT LAYER SECURITY: Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS – situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el

TOKEN: En lenguaje de programación un elemento simple de un elemento de programación. Por ejemplo un token podría ser una palabra clave, un operador una marca de puntuación.
En redes, un token es una serie especial de bits que viajan a través de una red token-ring y a los cuales tiene acceso cualquier equipo perteneciente a esa red. El token actúa como un ticket, permitiendo a su propietario enviar un mensaje a través de la red. Existe sólo un token para cada red de modo que no sea posible que dos equipos intenten transmitir mensajes al mismo tiempo.
En sistemas de seguridad, un pequeño dispositivo del tamaño de una tarjeta de crédito que muestra un código ID que cambia constantemente (cada x minutos). El usuario primero introduce una clave y luego la tarjeta muestra un ID que puede ser utilizado para acceder a la red. Un mecanismo similar de generación de IDs son las smart card.

TRATAMIENTO DE DATOS(2): Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

TROYANO (TROJAN): Programa informático cuya ejecución tiene unos efectos imprevistos y, generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

TTLS – TUNNELES TRANSPORT LAYER SECURITY: Protocolo de seguridad para redes inalámbricas del tipo EAP propiedad de la multinacional norteamericana Funk Software. Se trata de una extensión de EAP-TLS, protocolo utilizado por Windows XP en sistemas inalámbricos que proporciona los servicios de autenticación entre los usuarios y el servidor de la red basados en certificados. EAP-TTLS sólo requiere certificados al servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión es mucho más tediosa y pesada. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada cliente de la red

inalámbrica. Además, EAP-TTLS autentica al cliente en el sistema con las credenciales ya existentes basadas en password, y encripta credenciales y password para garantizar la protección de la comunicación inalámbrica.

V

VARIANTE DE UN VIRUS: Se conoce como variante de un virus ya existente a otro virus básicamente igual al primero pero con algún pequeño cambio en su programación.

VIRUS: Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

VIRUS DE ARCHIVO: Virus que infecta los archivos ejecutables de los programas. Al abrir un programa infectado, primero se ejecuta el virus y luego se abre la aplicación. Cuando se ejecuta el virus se copia a sí mismo en otros archivos o en otro disco.

VIRUS DE COMPAÑÍA : Virus que crea un archivo para esconderse cuyo nombre es igual al de otro de extensión .EXE de algún programa legítimo y con extensión .COM. MS-DOS siempre lee primero los archivos con la extensión .COM, antes que los de extensión .EXE.

VIRUS DE INGENIERÍA SOCIAL (SOCIAL ENGINEERING): Este término es utilizado frecuentemente para describir los trucos utilizados por los virus de correo masivo para atraer a los receptores de los mensajes con archivos adjuntos infectados para ejecutarlos o visualizarlos.

VIRUS DE MACRO (MACRO VIRUS): Virus que infecta las macros de Word y Excel, principalmente, de modo que cuando se abre un archivo que tenga una macro infectada, infectará el sistema.

VIRUS DE SECTOR DE ARRANQUE Y DE PARTICIÓN (BOOT AND PARTITION SECTOR VIRUS): Los virus de esta categoría infectan el sector de arranque y sector de partición. La mayoría de las PCs están configurados para intentar arrancar de la unidad a: antes que del disco duro, por lo que si se ha introducido un disquete infectado en la disquetera en el momento de arrancar, el PC se infectará.

VIRUS DE SCRIPT (SCRIPT VIRUS): Estos virus son escritos en lenguajes de programación script, tales como Visual Basic Script o Java Script.

VIRUS DE SOBRE-ESCRITURA (OVERWRITTING VIRUS): Virus que sobrescribe cada archivo que infecta: el programa maligno copia su propio código sobre el archivo de modo que los programas dejan de funcionar. Aunque la desinfección es viable, no es posible recuperar la información de los archivos infectados.

VIRUS MULTIPARTITO (MULTIPARTITE VIRUS): Virus que utiliza una combinación de técnicas para expandirse infectando archivos ejecutables, de sector boot y de partición

VIRUS RESIDENTE EN MEMORIA (MEMORY-RESIDENT VIRUS): Virus que permanece en memoria después de que ha sido ejecutado e infecta otros objetos bajo determinadas circunstancias.

VLAN – RED DE ÁREA LOCAL VIRTUAL (VIRTUAL LOCAL AREA NETWORK): Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares

VPN – RED PRIVADA VIRTUAL (VPN – VIRTUAL PRIVATE NETWORK): Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (LAN).

W

WPA – PROTOCOLO DE SEGURIDAD EN REDES INALÁMBRICAS (WIRELESS PROTECTED ACCESS): Protocolo de Seguridad para redes inalámbricas.
Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i.

WPA2 – PROTOCOLO DE SEGURIDAD WIFI PARA REDES INALÁMBRICAS (WIRELESS PROTECTED ACCESS): Protocolo de seguridad para redes wi-fi, definido en el estándar 802.11i.
Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.

WARCHALKING – ATAQUE A REDES INALÁMBRICAS: Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.
Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

WARDRIVING – ATAQUE A REDES INALÁMBRICAS: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless.
Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc.…

WARSPAMMING: Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

WI-FI(ALIANZA): Alianza sin ánimo de lucro formada por diversos fabricantes de redes inalámbricas en agosto de 1999 para certificar la interoperabilidad de productos WLAN basados en la especificación 802.11 así como la promoción del estándar WLAN en todos los segmentos del mercado.

WEP – WIRED EQUIVALENT PRIVACY: Protocolo para la transmisión de datos “segura”.
La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red.

También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

WI-FI – TECNOLOGÍA UTILIZADA EN REDES INALAMBRICAS: Abreviatura de Wireless Fidelity. Es el nombre “comercial” con el que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

WIMAX: Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

WLAN – RED DE ÁREA LOCAL INALÁMBRICA (WIRELESS LOCAL AREA NETWORK): También conocida como red wireless.
Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado.
Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA – ACCESO WI-FI PROTEGIDO (WI-FI PROTECTED ACCESS): Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WWWD – THE WORLDWIDE WARDRIVE: Evento internacional que durante una semana reúne a expertos de todo el mundo que buscan y catalogan nodos inalámbricos en sus ámbitos geográficos.

Bibliografía y Mesografía

Recursos Digitales e impresos utilizados en la realización del presente trabajo

Bibliografía

19 deadly sins of software security : programming flaws and hot to fix them
Howard, Michael
New York ; Mexico City : McGraw-Hill/Osborne, 2005

Análisis de la calidad de señal en una red WIFI con la herramienta netstumbler
Umbral científico 2005 N7 dic P61-71

Hack attacks testing [recurso electrónico] : how to conduct your own security audit
John Chirillo.
Indianapolis, Indiana : Wiley, c2003.

Hacking ético
Shon Harris ... [y otros.] ; traducción Elisabeth Sánchez León
Madrid : Anaya Multimedia, 2005

Historia y criptografía: reflexiones a propósito de dos cartas cortesianas
Narváez, Roberto
Estudios de historia novohispana 2007 N36 ene-jun P17-62

Investigación sobre seguridad informática : delitos informáticos, hackers, crackers y noticias relacionadas en la actualidad
Martos Rodríguez, María del Carmen
Almería : Procompal : 2010

IT-security and privacy : design and use of privacy-enhancing security mechanisms
Simone Fischer-Hubner
Berlin : Springer Verlag, c2001

La máquina sabe quién soy. La tecnología biométrica ya no es ciencia-ficción en América Latina
Fernández, Juan
América economía N206 abr P46-47

Network security tools
Dhanjani, Nitesh
Sebastopol, California : O'Reilly Media, 2005

Redes virtuales con soporte para IPv6 usando software libre
Amaya González, Luis Enrique
Tesis Licenciatura (Ingeniero en Computación)-UNAM, Facultad de Ingeniería México, 2011

Sistema de seguridad en redes locales utilizando sistemas multiagentes distribuidos net-mass
Horfan Alvarez, Daniel, Mark Bailey, Andrew Gómez Blandón, Lucas Adrián
Revista Facultad de Ingeniería. Universidad de Antioquia 2005

The software vulnerability guide
Herbert H. Thompson, Scott G. Chase
Hingham, Massachusetts : Charles River Media, 2005

Mesografía

CENTRAL DE LA ISO 17799
http://www.17799central.com/spain.htm

CERT/CC (Computer Emergency Response Team Coordination Center)
http://www.cert.org/

Cisco Packet Tracer
http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

Common Criteria
http://www.commoncriteria.org/

Community Emergency Response Teams (CERT)
http://www.citizencorps.gov/cert/

Dropbox
http://www.dropbox.com/

FIREWALL PENETRATION TESTING
http://www.wittys.com/files/mab/fwpentesting.html

GoogleEarth
http://www.google.es/intl/es/earth/index.html

GPG4WIN
http://www.gpg4win.org/

Hack hispano
http://www.hackhispano.com/

La Comunidad Dragonjar
http://www.dragonjar.org/

LogMeIn Hamachi
https://secure.logmein.com/products/hamachi2/

MANUAL DE PACKET TRACER 4.0
http://fcp.unach.mx/manuales/download/packet4.pdf

NESSUS
http://www.tenable.com/products/nessus

NetStumbler
http://www.netstumbler.com/

NMAP
http://nmap.org/zenmap/

Red Temática de Criptografía y Seguridad de la Información
http://www.criptored.upm.es/

Seguridad Informática. Qué, por qué y para qué
http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/seguridad/intro.htm

Seguridad Informática
http://facundovazquez.wordpress.com/

Security by default
http://www.securitybydefault.com/

Shibbo - Seguridad informática
http://passreminder.blogia.com/

Top 100 Network Security Tools
http://sectools.org/

UNAM-CERT
http://www.cert.org.mx/index.html

US – CERT: control systems
http://www.us-cert.gov/control_systems/

VMware
www.vmware.com

Winrar
http://www.winrar.es/

Wireshark
http://www.wireshark.org/