UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORESARAGÓN

"Xplico como herramienta para detectar fugas de información en redes empresariales."

TESIS PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

ALEJANDRO ROMERO REYES

TUTOR:

ING. GRADA HUERTA IVÁN

México, D. F. **Abril 2014**

VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN - UNAM

JEFATURA DE CARRERA DE
INGENIERÍA EN COMPUTACIÓN

OFICIO: FESAR/JACO/195/2014
ASUNTO: Asignación de Jurado

LIC. JOSÉ GUADALUPE PIÑA OROZCO
SECRETARIO ACADÉMICO
P R E S E N T E

Por este conducto me permito presentar a usted el nombre de los profesores que sugiero integren el Sínodo del Examen Profesional de **ROMERO REYES ALEJANDRO**, con el trabajo de titulación: **"XPLICO COMO HERRAMIENTA PARA DETECTAR FUGAS DE INFORMACIÓN EN REDES EMPRESARIALES"**, bajo la modalidad de **TESIS.**

PRESIDENTE:	**ING. JOSÉ ANTONIO AVILA GARCÍA**
VOCAL:	**MTRA. NORMA REYES TECONTERO**
SECRETARIO:	**MTRA. NORMA ROMERO BADILLO**
SUPLENTE:	**ING. RODOLFO VÁZQUEZ MORALES**
SUPLENTE:	**ING. IVÁN GRADA HUERTA**

Quiero subrayar que el Director de Tesis es el **Ing. Iván Grada Huerta**, quien está incluido basándose en lo que reza el Reglamento de Exámenes Profesionales de esta Facultad.

Sin otro particular, me es grato enviarle un cordial saludo.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Nezahualcóyotl, Estado de México, a 19 de marzo de 2014
EL JEFE DE LA CARRERA

M. en C. FELIPE DE JESÚS GUTIÉRREZ LÓPEZ

C.c.p.- Lic. Ma. Teresa Luna Sánchez. Jefa del Depto. de Servicios Escolares.
Ing. Iván Grada Huerta. Asesor
Alumno
FJGL/elo

AGRADECIMIENTOS

A Dios, por darme la serenidad, valor, fuerza y la sabiduría para alcanzar la más importante meta de mi vida.

A la UNAM, por permitirme estudiar en sus instalaciones.

A la Facultad de Estudios Superiores Aragón, por permitirme cursar mis estudios de Licenciatura.

Al Ing. Grada Huerta Iván por su apoyo durante la elaboración de este trabajo.

A los revisores de tesis: Ing. José Antonio Ávila García, Mtra. Norma Reyes Tecontero, Mtra. Norma Romero Badillo e Ing. Rodolfo Vázquez Morales por tomarse el tiempo de revisar mi trabajo para obtener el título de Ingeniero en Computación.

A los profesores de licenciatura, por brindarme sus conocimientos a lo largo de la Licenciatura.

A mis papas, que pusieron todo su empeño para darme la oportunidad de estudiar.

A mi Familia, que me motivaron a cada paso de mi vida.

Al L.I. Neptalí González Gómez por ser el que sembró la semilla de la inquietud y la curiosidad por los programas de licencia libre.

A todos mis compañeros de licenciatura, por brindarme su apoyo en cada una de las materias.

Finalmente quiero agradecer a todas aquellas personas que de una u otra manera me ayudaron durante mi estancia en la licenciatura y durante la elaboración de este trabajo de tesis.

A todos gracias

DEDICATORIAS

Este trabajo está dedicado a mi mamá Carmen Reyes Hernández, por su paciencia, amor y cariño durante toda mi vida.

A mi hermana L.C. Ana María Romero Reyes, por brindarme todo su conocimiento y entusiasmo.

A mis hermanas.

Al L.E. Carlos Alberto Hernández Julián, porque sin él la vida no sería igual.

Al Lic. Trab. Soc. Marco Antonio Benítez Hernández, por brindarme su apoyo y amistad en los momentos difíciles de la vida.

A la Ing. en Computación. Paula Isabel Ortiz Millán, porque sin su presencia la licenciatura no hubiera sido la misma.

A Gerardo Quiroz Salinas, quien fue una gran guía en gran parte de mi vida.

A mi papá Pedro Romero Martínez.

A todos mis compañeros y amigos de la Licenciatura.

A mis amigos, por brindarme eso tan grande que se llama amistad.

INDICE

INDICE DE IMAGENES

INTRODUCCION

ANTECEDENTES Y PLANTEAMIENTO DEL PROBLEMA.

¿Qué tan simple es la instalación y uso de una herramienta de computación forense[1] o informática forense, para detectar filtrado de información en las empresas?

La información en la actualidad es importante para todas las empresas, por medio de ella se llevan a cabo muchos movimientos en las diferentes áreas, ya sea en recursos humanos, contaduría, mercadotecnia, entre otras más. Por ello es muy importante el cuidarla y buscar una herramienta que permita ver lo que transita por la red.

Colombia, México y Chile ocuparon la tercera, cuarta y quinta posición; respectivamente, en el listado de América Latina. Y México se encuentra en la posición 29 a nivel mundial. México es el país con mayor actividad maliciosa en Internet, de acuerdo con el más reciente estudio "Informe sobre Amenazas a la Seguridad en Internet" que elabora Symantec.

La actividad maliciosa; analizada en el estudio de Symantec, incluye actividades de amenazas, phishing, código malicioso, zombis de spam, computadoras infectadas por bots y orígenes de ataques a redes.

Las empresas más afectadas por ciberataques han sido La Secretaría de la Defensa Nacional (SEDENA), TV Azteca y Televisa (que se encuentran ubicadas en México), The New York Times, The Washington Post, Facebook, Google, Twitter y Monsanto (en Estados Unidos de América).

A veces, los autores de este tipo de actos ilegales quieren causar daño a la imagen y reputación de sus víctimas para promover sus propias causas. En otras ocasiones, los

[1]Son programas computacionales basados en técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos, dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

perpetradores de estos fraudes quieren fanfarronear sus habilidades, como fue el caso de la Secretaría de la Defensa Nacional (SEDENA).

“Estados Unidos es el primer lugar en Norteamérica y primero a nivel mundial, que junto con Brasil, fueron la principal fuente de actividad maliciosa para cada una de sus regiones”, explica el estudio.

En las últimas ediciones de su Informe sobre Amenazas a la Seguridad en Internet, Symantec reveló que mientras el número de vulnerabilidades disminuyó un 20 % respecto a otros años, la cantidad de ataques maliciosos aumentó 81 %.

Destaca que los ataques dirigidos se están expandiendo a organizaciones de todos los tamaños, incluyendo pequeñas y medianas empresas.

“En el caso del correo electrónico, en 2011, uno de cada 239 mensajes enviados contenía un virus”, detalló la empresa creadora del antivirus ***Norton***.

En el 2011, empresas como Mitsubishi Heavy Industries, Lockheed Martin, L-3 Communications y Northrupo Grumman sufrieron ciberataques selectivos y pese a las diferentes herramientas como Firewalls, antivirus, etc.; colocados en dichas empresas, ha sido imposible evitar al 100% los ataques informáticos; eso sí, han menguado las instrucciones.

Aunque los ataques contra empresas de seguridad e instituciones gubernamentales atrae la atención de los medio de comunicación, las empresas normales también sufren este tipo de ataques con fines económicos o de espionaje para obtención de secretos corporativos importantes.

Estos ataques suelen aprovechar técnicas de ingeniería social; envían mensajes de correo electrónico con el nombre de contactos conocidos para incitar a las víctimas a que los abran. Con los mecanismos de entrega selectiva, los ciber delincuentes pueden utilizar documentos maliciosos para aprovechar agujeros en la seguridad e instalar programas maliciosos. Por lo cual es importante conocer qué tipo de información transita por la red de una empresa.

Xplico es una de estas herramientas para la decodificación de datos en la red. Y puede ser de mucha ayuda para detectar en que parte de la empresa hay algún pilar débil.

JUSTIFICACIÓN

Es importante analizar el tráfico de red. En estos días donde la tecnología avanza a pasos agigantados es necesario saber en las empresas que tipo de información circula en las redes privadas. Ya que nunca se sabe qué tipo de ataques puede sufrir. Esto puede ser

un seguro para poder realizar un contra ataque o bien una detención oportuna de una intrusión.

Además puede ser una buena práctica de seguridad y un seguro que comprobara (en caso de tener un problema) quien y de donde se realizó cualquier práctica inusual.

La computación forense es la aplicación de la ciencia de la computación a la investigación criminal, ofrece la posibilidad de, metodológicamente identificar, recuperar, preservar, reconstruir, validar, analizar, interpretar, documentar y presentar evidencia digital como parte de la investigación de un incidente informático.

De acuerdo con el Departamento de Justicia de los Estados Unidos el procedimiento forense debe tener en cuenta 2 tipos de evidencia digital:

1. Evidencia generada por un computador, es decir los registros generados por un firewall.
2. La información que es producida por una persona, pero almacenada en un computador.

En este caso se pondrá especial atención al primer grupo que se menciona.

Xplico es una herramienta que formara parte de la seguridad para conocer qué tipo de datos entran y salen.

¿Por qué utilizar un programa de licencia Open Source como lo es Xplico? La principal razón es porque los programas de licencia Libre son más estables, ya que por tener el código fuente como parte de la documentación es más fácil que programadores, analistas y usuarios puedan modificar dicho código para mejorarlo aún más. Es como tener millones de programadores analizando y mejorando a cada momento el mismo programa. Esto provoca mayor estabilidad en el código.

En segundo lugar tenemos que estos programas son realmente económicos. UBUNTU o Xplico piden aportaciones voluntarias para poder seguir con estos grandes proyectos; pero por su naturaleza Open Source, no exigen este tipo de pagos. Por lo cual para las pequeñas empresas es realmente económico poder adquirir programas de este estilo. Y no realizar pagos forzosos anuales como con los de licencia cerrada.

Objetivos generales.

Estudiar y comprender el funcionamiento de la herramienta Xplico de computación forense.

Instalaren un equipo y generar una simulación con características de un sistema real.

Objetivos específicos.

Dar una idea general de como se establece una políticas de seguridad Informática. Para poder implementar a la pequeña empresa un sistema así.

Analizar como instalar un firewall y que opciones tenemos para implementarlo.

Mostrar cómo se instalar el sistema operativo UBUNTU.

Traducir y mostrar cómo está constituida la herramienta forense Xplico y cuáles son sus principales funciones.

1er CAPITULO

Marco teórico.

La idea de crear programas capaces de competir con las producciones comerciales de Software comienza en el año de 1991 con Linus Torvalds[2], al comenzar la creación de una versión reducida del sistema operativo UNIX®.

Con el fin de mejorar el software, decide lanzar el código con la comunidad desarrolladora de Software fuera de la Universidad de Helsinkien[3] Finlandia. Esta comunidad aprovecho el desarrollo de Linux y dio un verdadero impulso a lo gratuito y la Filosofía del Open Source (FOSS). El primer lanzamiento de Linux (en combinación del sistema operativo y el soporte a aplicaciones) de Torvalds en 1994 ha conducido a una explosión de nuevas aplicaciones de Linux basadas en el sistema operativo de licencia Open Source.

La filosofía FOSS desafía lo establecido para el desarrollo de Software establecido por las empresas. La forma tradicional del desarrollo de Software consiste en que todos los programas tienen que ser completamente terminados y probados antes de salir al mercado.

Cuando este Software sale al mercado, estén o no terminados no puede ser cambiado en su código fuente y si tiene errores es problema de la empresa. Esta forma de trabajo marcada en el desarrollo de nuevo Software, es un proceso largo. Con el desarrollo de Software Open Source marca otro camino.

La programación está diseñada para que otras personas prueben el Software, lo usen y/o lo modifiquen. Los errores no se consideran un problema, porque son aceptados. Desde que el código fuente es distribuido, toda la ingeniería de Software puede realizar cambios o agregar características al original. Así todo es desarrollado en casa y luego puesto en

[2]Nace el 28 de diciembre de 1969. Helsinki (Finlandia)

[3]Fundada en la cuidad de Turku en 1640 y después trasladad a la nueva capital Helsinki en 1828.

libertad, FOSS está en constante desarrollo por que cualquier persona en el mundo puede cambiar el código.

Un aspecto importante en pro de FOSS es el precio. No todo el FOSS está libre de no ser cobrado, y algunos tienen algún precio, pero en muchos de los casos es más barato que un Software propietario.

"Los programas OSS/FS son programas cuyas licencias dan a los usuarios la libertad de correr los programas con diferentes propósitos, para el estudio y modificación del programa y redistribuir copias de la original o de la versión modificada del programa. (Sin tener que pagar derechos de autor)."[4]

La búsqueda de una definición de Free and Open Source Software es complicado, pero la definición según David Wheeler[5] proporciona una buena descripción de la esencia de lo que es FOSS. *"La comunidad FOSS promueve el crecimiento del conocimiento para otros miembros, con ayuda de gigantes que pertenecen a esta comunidad."*

Los programas Open Source son producidos y emitidos a la comunidad que le gusta tener sus productos libres y compartirlos con otros miembros de la comunidad. La idea de una comunidad que le guste aprender sin dejar a personas fuera es excelente.

Se conocen dos grandes escuelas en el mundo de FOSS: la más antigua es la Free Software Foundation (FSF) fundada por Richard Stallman[6]. En el otro extremo se encuentra un enfoque más empresarial en el Open Source Initiative; OSI.

El inicio del Software libre; FSF, tiene un largo historial iniciado en las principales academias del conocimiento. El FSF surge en los primeros días de la industria de la computación, al compartir códigos de programas convirtiéndose en un problema y el software gradualmente se convirtió en "cerrado".

Antes la prioridad de los programas fue tratarlos como productos académicos. Las personas compartían código, algoritmos o todo tipo de programas con sus compañeros. El intercambio hizo la base para poder usarlo, pero se reconoció el origen de la información, el mismo camino del mundo académico aun funciona.

Al aumentar la industria y la comercialización de la computación, cambio la actitud. El intercambio gradualmente fue reemplazado por la protección y las academias que promovían la apertura tuvieron que dar paso a las empresas que convirtieron los programas en "cerrado/propietario". William (Bill) H[7]. Gates, es considerado único en este

[4]David Wheeler, 2003

[5]Nace en Birmingham (Inglaterra) en el año de 1927.

[6]Nace en Manhattan (Nueva York) en el año de 1953.

[7]Nace en Seattle (Washington) en el año de 1955.

cambio, en la carta "*An Open Leather to Hobbyists*" fechado el 3 de febrero de 1976, arremete contra la imperante cultura del compartir Software.

"¿Por qué? Como la mayoría de los aficionados deben ser conscientes, la mayoría de ustedes roban sus programas. El hardware debe ser pagado, pero el software es algo para distribuir. ¿A quién le importa si la persona trabaja para obtener una paga?"[8]

La gradual destrucción de la cultura de compartir programas a la que refiere Gates, es la razón de que Richard Stallman; investigador del MIT laboratorio de Inteligencia Artificial, promueve el desarrollo y la licencia del Free and Open Source Software. Y crea el Free Software Foundation.

Conforme con el FSF, se trata de proteger cuatro aspectos de los usuarios:

- La libertad de ejecutar programas, para cualquier propósito.
- La libertad de estudiar cómo trabaja un programa y adaptarla a las necesidades personales.
- Acceso al código fuente; es una condición.
- La libertad de redistribuir copias de modo que pueda ayudar a su prójimo.
- La libertad de promover un programa y realizar mejoras para el público, de modo que la comunidad se mejore.

La esencia del FSF es la libertad para cooperar y colaborar. Porque lo que no es libre Software restringe la libertad de cooperar, FSF considera una ética de software propietario. FSF es también opuesto a las patentes de software y restricciones que puedan existir de las leyes de derecho de autor. Estas leyes restringen las libertades fundamentales mencionadas anteriormente.

La filosofía OSI es por lo tanto diferente de la FSF:

"La idea básica detrás del Open Source es simple: cuando el programador pueda leer, redistribuir y modificar el código fuente del Software en una pieza, el programa evoluciona. Las personas pueden mejorar, adaptar y corregir errores. Y esto puede suceder a mucha velocidad, es sorprendente que estemos acostumbrados a la lentitud del software convencional."

El modelo OSI se centra en la idea de hacer poderoso y seguro el software, por lo tanto es favorable para las empresas que el FSF. Este menos centrado en las cuestiones morales de programas libres y más en las ventajas del FOSS del método del desarrollo distribuido .998, un grupo asociado con el software libre introduce el término "Open Source" que se empeña con romper con el termino de Hacker, que en el pasado se asociaba con GNU u otros proyectos de programación libre, para darle un nuevo énfasis

[8] William Bill H. Gates.

en la comunidad sobre las posibilidades de extender el modelo de software libre en el mundo del comercio.

OSI Open Source define al software los siguientes derechos y obligaciones:

- Sin derechos u otro cargo impuesto a la distribución.
- Disponibilidad del código fuente.
- Derecho de crear modificaciones y trabajos derivados.
- Puede requerir modificaciones a las versiones distribuidas de la versión original además de parches.
- No discriminar entre personas o grupos.
- No discriminar entre las diferentes áreas.

FOSS es más que una filosofía, es también un enfoque en el desarrollo de Software que tiene resultados en nuevos programas estables, que dominen el aspecto del software actual. Discutir sobre las ventajas o desventajas del FOSS es complicado, por la falta de información objetiva.

El Asesor Nacional Consultor en Innovación de submarinos en África del sur, ve los beneficios del FOSS y adopta los estándares del código abierto, las ventajas más importantes son:

1. Reduce costos y es menos dependiente de la tecnología e importa habilidades.
2. Programas accesibles para las personas, empresas y gobierno.
3. Acceso universal a través de la masiva implementación de programas sin costo de licencia.
4. Acceso a los datos del gobierno sin barreras de software o formatos de datos.
5. Genera la personalización de programas en lenguajes locales o culturas.
6. Disminuye barreras entre empresas.
7. Participación en la red global del desarrollo de Software.

Una ventaja adicional que identifica la organización gubernamental de comercio (OCG, 2002) es: Provee independencia, limita el encadenamiento con proveedores.

Los parches y actualizaciones salen más rápidamente por lo que disminuyen las averías y los riesgos de inseguridad.

Al mismo tiempo tiene también limitaciones e inconvenientes el uso de FOSS. La organización de comercio gubernamental identifica los siguientes factores que limitan con éxito su implementación:

1. *Apoyo disponible para el FOSS*. En años pasados ha faltado el apoyo profesional. En años recientes ha mejorado la nueva intervención de compañías de Software como IBM, SUN y HP han comenzado a unirse a los convenios de FOSS.

2. *Encontrar los programas adecuados*: desde que el FOSS no se difunde tiene dificultades para seleccionar las correctas aplicaciones que tiene que apoyar. Un papel más activo aprovecharía las necesidades de los usuarios.
3. *Documentación:* la documentación que acompañan los programas FOSS es a menudo idiosincrático y en ocasiones inexistentes. El desarrollo con FOSS es motivado hacia los aspectos técnicos o aplicaciones de fácil uso. Limitado en las mejores prácticas: hay poco conocimientos y casos documentados de migración a gran escala de programas propietarios a FOSS.
4. *Ajustes de Hardware – Software*: FOSS a menudo se queda atrás del nuevo hardware. Esto pasa por el hecho de que la manufactura del Hardware no libera las especificaciones en tiempo para la comunidad FOSS.

El proyecto GNU nace en 1991 en la Universidad de Helsinkien Finlandia, consistía en desarrollar un Kernel de licencia libre, con las herramientas que existían en los repositorios del GNU, pero faltaba una pieza central en el sueño de Richard Stallman para culminar su objetivo de crear un sistema parecido a UNIX® pero completamente libre.

Linus Benedict Torvalds[9] de 19 años de edad, crea una propuesta en el IRC[10] (Internet Relay Chat); de hacer un Kernel para la plataforma Intel x386.

El nombre propuesto por Torvalds fue Freax, pero Aris al colocarlo en el FTP (File Transfer Protocol) lo renombró Linux y lo puso a disposición de descarga para probar y mejorar. Después de un tiempo y de constantes mejoras, el Kernel llego a su versión 1.0 y la licencia GPL (General Public License) fue la garantía que siempre será libre y más programadores se involucraron.

Cuando la comunidad empezó a probar y analizar el Kernel causo todo un revuelo y el Kernel que fue pensado solo para la plataforma Intel, pronto fue migrado para decenas de arquitecturas, mainframes y supercomputadoras han sido reportadas ejecutando sobre GNU/Linux.

Algunas de las características de GNU/Linux son:

- Su licencia GPL, garantiza que permanecerá **LIBRE**, los documentos que se produzcan siempre estarán disponibles y no son objeto de políticas corporativas.
- Acceso a los códigos de fuentes y derecho a modificación. Esto motiva a la participación de miles de programadores. Además es muy útil en el momento de eliminar errores o bugs y mejorar la seguridad.
- GNU/Linux es realmente un sistema operativo multiusuario, multitarea que permite que múltiples usuarios trabajen con múltiples aplicaciones. Y a hoy día la mayoría de los servidores de empresas medianas y pequeñas se ejecutan sobre

[9]Nace en Helsinki (Finlandia) en el año de 1969.

[10]Creada por Jarkko Oikarinen en agosto de 1988 para reemplazar al programa MUT (talk multiusuario) en Finlandia.

GNU/Linux.

- Es extremadamente estable, robusto, escalable y seguro. Puede ser actualizado sin necesidad de reiniciar y sus actualizaciones son fáciles y prontas.
- Su naturaleza de Libre permite que los administradores sepan con exactitud la capacidad de un programa y los riesgos de seguridad. Aplicaciones libres no mantienen secreto de marcas ni colectan información. La naturaleza de la disponibilidad del código fuente nos garantiza que el código no vulnere nuestra privacidad.
- Un gran número de aplicaciones disponibles para su uso.
- Compatibilidad con aplicaciones comerciales que ayudan a abaratar costos de operaciones, sin sacrificar calidad ni seguridad.

Todas las distribuciones tienen utilerías, aplicaciones y Kernel GNU en común y lo que diferencia una de otra es la configuración y las aplicaciones que incluyen esto depende de la configuración que maneje su creador y crea que son las mejores y más necesitadas, dentro del GNU. Existen más de un navegador y lector de correo, por cada aplicación existen varias; esta elección y la personificación de la configuración de estas es que diferencian una distribución de otra.

La seguridad en internet no es muy diferente a otras formas de seguridad. El mismo concepto de los castillos se usa para construir sitio web que ofrece acceso a bases de datos. El concepto y la forma de construirlos aprovechan el rol que juega.

Internet es un maravilloso avance en la tecnología para proporcionar acceso a la información y publicarla de formas innovadoras. Pero también es muy peligroso proporcionar cierto tipo de información en este medio de difusión.

Existen diferentes modelos de seguridad para que las personas puedan tener privacidad de sus datos y recursos en internet, un firewall es una forma de protección que permite a la red conectarse a Internet mientras mantiene un grado de seguridad.

Lo primero que se tiene que saber antes de instalar un firewall es lo que vamos a proteger, cuando nos conectamos a internet ponemos tres cosas en riesgo:

1. Los datos; la información que tiene en sus computadoras.

Los datos tienen tres características para separar la necesidad de protegerlos:

- Secretos: no necesitamos que ninguna persona sepa de nosotros
- Honradez: no necesitamos que otra persona se haga pasar por nosotros
- Disponibilidad: necesitamos usar nuestra propia información en cualquier momento.

Algunas organizaciones tienen algunos de los más importantes secretos en sus computadoras.

Es muy serio perder la confianza en el sistema de datos y consecuentemente perder la confiabilidad en su organización.

2. Los recursos; los componentes en sí mismos

Las personas que rentan equipos o solicitan espacios para guardar datos en los mismos agradecen por este servicio; por lo que no quieren ser víctimas de los intrusos. Gastamos buen tiempo y dinero en la construcción de computadoras y lo mejor es saber quién hace uso de ellas. Algunos intrusos argumentan que ellos solo usan los recursos excedentes, por lo que la intrusión no les cuesta. Existen dos problemas con ese argumento.

Primero; es posible para un intruso determinar con éxito que recursos son excedentes y usarlos. Esto puede observarse como si su sistema tiene océanos de discos y horas que se utilizan en la computadora. De hecho un intruso no puede ignorar los recursos que usamos.

Segundo; si se usan los recursos de manera correcta incluso si usted simplemente siente un poco lenta su equipo checa el espacio en el disco duro, o incluso si se perciben luces parpadeando en el equipo no está feliz en su computadora. Los recursos informáticos no son recursos naturales que pertenezcan al mundo en general. Ni son recursos ilimitados que si no son aprovechados o se destruyen si no son usados.

3. La reputación.

Cuando un intruso aparece en internet con su identidad. Todo hombre o mujer no parece él. ¿Cuáles con las consecuencias?

La mayor parte del tiempo, las consecuencias son simplemente que los sitios donde se intenta entrar preguntan el por qué tratamos de tener acceso a ellos. Un sitio tiene personal de seguridad y políticas de seguridad, un intruso es un disgusto para todos, toma la identidad de personas desconocidas, puede cambiar un sitio web, envía correos electrónicos o postean nuevos mensajes que simulan venir de nosotros. Toda acción creíble puede hacer daño a tu reputación.

Las políticas de seguridad son para establecer decisiones que establezcan, determinen y organicen posturas de seguridad. O lo que es lo mismo; los límites aceptables de comportamiento y que respuesta debe haber ante las violaciones. Naturalmente las políticas de seguridad serán diferentes de empresa a empresa.

Estas políticas también determinan las acciones legales en contra de un ataque. Además, tales políticas pueden determinar si los registros específicos son admisibles como prueba ante las autoridades.

Un firewall es una forma de protección que permite en una red conectarse a internet mientras se mantiene en un rango de seguridad. También es considerado como; cualquier dispositivo colocado entre una red privada e internet que bloquea cierto tráfico de la red.

Pero; ¿cuáles son las funciones básicas de un firewall?

- Filtrar el tráfico: los encabezados de toda la red pasan por un filtro en el firewall. El firewall hace una inspección para permitir o bloquear el paquete.
- Hacer un NAT (Network Address Translation): Fuera de la red se ven uno o muchos rangos de direcciones IP. En una red privada solo tenemos un rango de red. La dirección destino y origen en la red. Un firewall cambia la dirección IP cuando sale y cuando entra.
- Aplicación proxy: el Firewall es capaz de inspeccionar más que solo el encabezado del paquete de red, esta capacidad es necesaria para entender la aplicación específica que se utiliza para enviar un paquete.
- Monitoreo y registro: incluso con un conjunto solido de normas, todo lo registrado en la red es importante. Al hacerlo le es posible analizar una posible intrusión en la red, da información sobre el rendimiento y los filtros reales que realiza el firewall.

Porque un firewalls es el punto de entrada entre una red interna e internet, es importante tener algunas funciones importantes, algunos firewalls modernos tienen las siguientes características:

- El almacenamiento de datos: porque algunos datos o el contenido de algunos sitios de la Web pueden pasar por el Firewall repetidamente en respuesta a los usuarios. El firewall puede almacenar los datos y las respuestas más rápidamente sin tener que obtenerlas del sitio Web.
- Filtrar el contenido: un Firewall puede ser usado para restringir el acceso a ciertos sitios web basados en URL, palabras clave y otros contenidos.
- Detección de intrusos: ciertos patrones de red pueden indicar una intrusión que se esté llevando en proceso; en lugar de bloquear los paquetes de red sospechosos, el Firewall puede tomar medidas para limitar aún más la intrusión.
- Balancear la carga: desde el punto de vista de la seguridad un solo punto de entrada es bueno, pero desde el punto de vista de la disponibilidad un único punto puede llevar a un fallo. La mayoría de los firewalls permiten la solicitud de redes entrantes y salientes para ser distribuidos entre uno o más Firewalls.

FreeBSD es uno de estos nuevos tipos de Firewalls. Nace en el año de 1993 como una extensión de un oficial 386BSD Patch kit, sus desarrolladores son: Nate Williams, Rod Grimes y Jordan Hubbard. El objetivo principal era obtener una réplica de 386BSD para arreglar una serie de problemas que no podían solucionar los parches.

386BSD era el sistema operativo de Bill Jolitz, que hasta este punto había estado sufriendo de consecuencias. Los creadores adoptan el nombre de FreeBSD (bautizado así por David Greenman) tras quitarles el respaldo de Bill Jolitz.

La primera distribución en CD-ROM (y disponible en la red) fue FreeBSD 1.0 publicado en diciembre de 1993. Estaba basado en la cinta de U.C. Berkeley del 4.3 BSD-lite ("Net/2"), con bastantes componentes de 386BSD y trabajos provenientes de la Free Software Foundation. Cinco meses después surge FreeBSD 1.1 en mayo de 1994.

Novel y la Universidad de Berkeley[11]resolvieron un largo juicio acerca del estatus legal de la cinta de Berkeley Net/2. Una condición de acuerdo fue la concesión por parte de Berkeley de que una gran parte de Net/2 era código gravado y propiedad de Novel, quien a su vez lo había adquirido de AT&T anteriormente. Berkeley obtuvo a cambio de Novell el beneplácito para que 4.4BSD-Lite, fuera declarado como no gravado y se instara a los usuario de Net/2 a cambiar.

Esto repercutió sobre el proyecto FreeBSD, a quienes se dio hasta julio de 1994 para dejar de sacar su producto basado en Net/2. Bajo los términos de aquel acuerdo se permitía al Proyecto sacar una última versión antes de la fecha límite: esa versión fue FreeBSD 1.1.5.1.

FreeBSD tuvo entonces que acometer la ardua tarea de reinventarse a sí mismo a partir de partes nuevas y bastante incompletas de 4.4BSD-Lite. Las versiones Lite eran ligeras en parte porque el CSRG de Berkeley quito grandes partes del código necesario para construir un sistema que pudiera arrancar y porque la versión de 4.4 para Intel era muy incompleta.

Hasta noviembre de 1994 el proyecto al fin realizo esa transición; apareció FreeBSD 2.0 en la red y CD-ROM. A pesar de no estar suficientemente pulida esta distribución fue un éxito significativo, al cual siguió el más robusto y fácil de instalar FreeBSD 2.0.5 en junio de 1995.

El objetivo del proyecto FreeBSD es producir software que pueda usarse con cualquier propósito y sin ningún tipo de restricción. El código fuente de nuestro árbol se halla bajo la GNU (General Public License), GPL y LGPL (Library General Public License).

Algunas de las distribuciones más conocidas del proyecto Linux son Fedora, RedHat, Suse, Mandriva, Debian, Gentoo, Slackware y por último Ubuntu. Muchas de ellas pueden ser descargadas de sitios como http://www.linuxiso.org.ar y http://www.distrowatch.org.

Aunque Ubuntu es de fácil adquisición, es uno de los más populares de estas distribuciones, desde su portal podemos pedir copias originales que nos envían a nuestras puertas sin ningún costo. Ubuntu viene en un solo CD lo que lo hace muy efectivo en costo de copia, a diferencia de Debian por ejemplo que es distribuido en 14 DVD. Ubuntu es un Debian lo que lo hace (basado en paquetes DEB) muy fácil de

[11]Inaugurada en 1868 en los Ángeles.

actualizar y mantener. Ubuntu puede ser usado como USB LIFE, estación de trabajo o como servidor. La versión más estable hasta la fecha es la 12.04 LTS[12].

Xplico es una Herramienta de Análisis Forense para redes. Su objetivó es extraer del tráfico de red el contenido de las aplicaciones.

Xplico es un decodificador IP con licencia implícita en GNU General Public License.

DeMa; que es una utilería para el funcionamiento de Xplico, también tiene licencia GNU

Los manipuladores, que se encargan de manipular el tráfico de red y los archivos pcap son: **msite, mpaltalk, mfbc, mlile** y **mwmail** también están escritos bajo esta licencia.

Sin embargo **mimedump.pyc, session_mng.pyc, wbm_aol_v2.pyc, wbm_gmail.pyc, wbm_yahoo_android.pyc** y **wbm_yahoo_v2.pyc** están bajo la licencia CC-BY-NC-SA 3.0[13], estos son los despachadores que presentan los datos a los usuarios.

La interfaz de Xplico (XI por sus siglas en inglés) está bajo tres tipos de licencias dando a elegir entre una o las tres o bien por los términos del software libre y abierto.

Estas licencias son;

- Mozilla Public License, versión 1.1
- GNU General Public License, versión 2.0 o superior
- GNU Lesser General Public License, versión 2.1 o superior

Xplico está construido con los leguajes C, Python, PHP y JavaScript.

El lenguaje C evolucionó a partir de B; dicha evolución estuvo a cargo de Dennis Ritchie en los laboratorios AT&T Bell y en 1972, se implementó en una computadora DEC PDP-1I. C utiliza muchos conceptos importantes de BCPL y B cuando agrega tipos de datos y otras características. Inicialmente, C se hizo popular como lenguaje de desarrollo para el

[12]Según la página oficial de UBUNTU en su última edición que es el 2014-02-03 17:56:07 por cjwatson

[13] Esta licencia nos dice que;

1. Se puede copiar y redistribuir el material en cualquier medio o formato.
2. Se puede remezclar, transformar y crear a partir del material.
3. Y que el licenciador no puede revocar estas libertades mientras cumpla con los términos de la licencia.

Pero las condiciones indican que;

1. Se debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios.
2. Puede hacerse de cualquier manera razonable, pero no de manera que se diga que se tiene apoyo del licenciador o lo recibe por el uso que hace.
3. No se puede utilizar el material para una finalidad comercial. Si mescla, transforma o crea a partir del material, deberá distribuir sus contribuciones bajo la misma licencia que la original.

sistema Operativo UNIX. En la actualidad, la mayoría de los sistemas operativos están escritos en C y/o C++. C se encuentra disponible para la mayoría de los computadores, y es independiente del Hardware. Con un diseño cuidadoso, es posible escribir programas en C que sean portables para la mayoría de las computadoras.

Con la popularidad; que aumentaba, de C comenzaron a surgir variantes (aunque similares en ocasiones incompatibles entre sí) lo que obligo a crear una versión estándar. En 1983 se creó el comité técnico X3J11 bajo la supervisión de American National Standards Committee on Computers and Information Processing (X3), para "proporcionar una definición cara del lenguaje e independientemente de la computadora". En 1989, el estándar fue aprobado; este estándar se actualizo en 1999. Al documento del estándar se le conoce como INCITS/ISO/IEC 9899-1999.

C proporciona las construcciones fundamentales de control de flujo que se requieren en programas bien estructurados: agrupación de proposiciones, toma de decisiones (if – else), selección de un caso entre un conjunto de ellos (switch), interacción con la condición de paro en la parte superior (while, for) o en la parte inferior (do) y terminación prematura de ciclos (break).

Las funciones pueden entregar valores de tipo básicos, estructuras, uniones o apuntadores. Cualquier función puede ser llamada recursivamente. Las variables locales son normalmente "automáticas" o creadas de nuevo con cada invocación. La definición de una función no puede estar anidada, pero las variables pueden estar declaradas en una modalidad estructurada por bloques. Las funciones de un programa en C pueden existir en archivos fuente separados, que se compilan de manera separada. Las variables pueden ser internas a un función externas pero conocidas solo dentro de un archivo fuente o visibles al programa completo.

C es un lenguaje de "bajo nivel". C trata con el mismo tipo de objetos que la mayoría de las computadoras, llámense caracteres, números y direcciones. Estos pueden ser combinados y cambiados de sitio con los operadores aritméticos y lógicos implantados por maquinas reales.

C no proporciona operaciones para tratar directamente con objetos compuestos, tales como cadenas de caracteres, conjuntos, listas o arreglos. No existen operaciones que manipulen un arreglo o una cadena completa, aunque las estructuras pueden copiarse como una unidad. El lenguaje no define ninguna facilidad para asignación de almacenamiento que no se la definición estática y la disciplina de pilas provista por las variables locales de funciones.

De otra manera podemos decir que C solamente ofrece un control de flujo franco y lineal: condiciones, ciclos, agrupamientos y subprogramas, pero no multiprogramación, operaciones paralelas, sincronización no co-rutinas.

Aunque la ausencia de alguna de esas capacidades puede parecer como una grave deficiencia, el mantener al lenguaje de un tamaño modesto tiene beneficios reales. Puesto que C es relativamente pequeño, se puede describir en un pequeño espacio y aprenderse con rapidez. Un programador puede razonablemente esperar conocer, entender y utilizar en verdad la totalidad del lenguaje.

A continuación se listan algunas características del lenguaje C que lo definen. Estas características dan una idea de por qué C se ha convertido en el lenguaje más usado.

- Los programas en C son relativamente pequeño y sencillo.
- Permite una mecanografía suelta. Como PASCAL.
- Es un lenguaje estructurado.
- Es un lenguaje compilado, es decir, si se escribe en C, tenemos que correrlo en un compilador para que este no regrese un ejecutable. Los compiladores de C son comúnmente disponibles.
- Tiene una implementación de soporte. Extenso uso de soporte para memoria, orden, estructuras y funciones.
- Está incorporado en un gran número de funciones. Es recomendado el uso de llamada de funciones.
- Puede manejar actividades de bajo nivel. El lenguaje de bajo nivel es altamente disponible.
- Da eficiencia y programación rápida.
- Puede ser compilado en gran variedad de computadoras.
- Es altamente portable. Esto significa que un programa escrito en C en alguna computadora puede ser corrido en otra con diferente sistema operativo con unos pocos cambios.

Python es el más popular lenguaje de programación Open Source usado por los estándares de programas y aplicación de scripts con amplia variedad de dominios. Es libre, portable, poderoso y por lo tanto relativamente fácil y extraordinarias funciones Python se centra en desarrollar productividad y software rápido siendo estratégicamente avanzado en proyectos como largos como cortos.

Para muchos, Python se centra en la legibilidad, coherencia y la calidad del Software en general que lo distingue de otras herramientas en el mundo de los scripts. El código de Python es designado a ser legible y por lo tanto reusable y manipularle – mucho más que un script tradicional. La uniformidad del código de Python marca la facilidad de entenderlo, incluso si usted no la escrito. Adicionalmente, Python tiene un profundo soporte para los más avanzados mecanismos, tal como orientado a objetos y funciones de programación.

Python aumenta el motor de productividad muchas veces más allá de los lenguajes estéticos y compilados como lo son C, C++ y Java. El código en Python es típicamente un

tercio o un cuarto del tamaño del equivalente en C++ o Java. Eso significa que hay que escribir menos, depurar menos y para mantenerlo.

Mas programas hechos con Python corren sin alterare en las mejores plataformas de computadoras. La portabilidad del código de Python entre Linux y Windows, es usual solo con cuestión de copiar el código entre maquinas. Por otra parte, Python ofrece múltiples opciones de código grafico portable usando interfaces, acceso de programas a bases de datos, sistemas basados en Web y más. Incluso interfaces de sistemas operativos, incluso lanzamiento de programas y procesamiento de directorio, es muy portable y ofrece Python muchas posibilidades.

Python es un derivado de ABC, un lenguaje designado para enseñar programación en la época de los 80´s por Lambert Meertens, Leo Geurts y otros en la CWI (Nacional Research Institute for Mathematics and Computer Science) en Amsterdam.

PHP es un lenguaje de alto nivel que se ejecuta en el servidor donde están alojadas las páginas, al contrario que otros lenguajes que son ejecutados en el propio navegador.

La ventaja de que el lenguaje se ejecute en el servidor es que las paginas van a poder ser vistas en cualquier ordenador, independientemente del navegador que tenga; en cambio, el gran problema de que se ejecute el código en el navegador es que muchos navegadores no son capaces de entender todo el código, lo que presentara errores al mostrar el resultado de las páginas.

PHP es un lenguaje de programación gratuito, por lo que todo el mundo puede utilizarlo. Con una sintaxis similar a los lenguajes C y Perl[14] (*Practical Extraction and Report Language*), que se interpreta por un servidor Web Apache y genera código HTML dinámico.

Todas estas características han hecho de este leguaje uno de los que mayor crecimiento ha experimentado en los últimos años, desde su aparición en 1944. Es de destacar especialmente la facilidad para la conectividad con sistemas gestores de bases de datos a través de un gran número de funciones especializadas. Esa facilidad de conexión ha hecho que PHP sea actualmente uno de los lenguajes más utilizados para la generación de páginas dinámicas, no solo personales sino también portales de empresas y organizaciones.

En 1994 un programador de Groenlandia, Rasmus Lerdorf, creó el lenguaje PHP con el objetivo inicial de hacer un seguimiento de los visitantes de su página personal. El sistema desarrollado originalmente por Lerdorf estaba formado por un conjunto de scripts programados en Perl que después sería remplazado por C con el objeto de obtener mayores funcionalidades.

[14]Creado por Larry Wall en 1987.

El significado original del nombre de PHP no era otro que *Personal Home Page*. Lordorf decidió hacer público el código fuente de sus programas para que cualquiera pudiera utilizarlo; de esta forma el sistema rápidamente comenzó a ser utilizado por otros usuarios de Internet y entre todos comenzó a mejorarse, de manera que el actual PHP es progresivamente construido por colaboradores desinteresados que implementan nuevas funciones en nuevas versiones del lenguaje.

La versión PHP 1 aparece en la primavera de 1995 y el PHP 2 fue desarrollado entre 1995 y 1997. En 1997 se estimaba que un 1% de los dominios de Internet hacían uso de PHP 2.

A mediados de 1997 se produce un cambio importante en el lenguaje, se reprogramó el analizador sintáctico, se incluyeron nuevas funcionalidades como el soporte a nuevos protocolos de internet y a la mayoría de los sistemas gestores de bases de datos comerciales.

Con estas nuevas funcionalidades nace el PHP 3, además se decide rebautizar el lenguaje, *Preprocesador de Hipertexto*. El PHP 3 se caracterizaba por su gran extensibilidad y por el diseño de una sintaxis mucho más potente y consistente, además del soporte de sintaxis orientado a objeto. Se estima, que en su apogeo el PHP 3 llegó a estar instalado sobre el 10% de los servidores web de Internet.

En el año 2000 surge la siguiente versión del lenguaje; el PHP 4, con una mayor independencia del servidor web y con un mayor número de funciones disponibles. Con esta versión se redefine el núcleo del programa, generando un nuevo motor que mejora la ejecución de aplicaciones complejas, este nuevo motor es bautizado como "*motor Zend"*, en honor a sus autores: Zeev Zuraski y Andi Gutmans.

La actual versión del lenguaje PHP es la 5, fue lanzada oficialmente en septiembre de 2004. Hoy en día se estima que PHP es usado por cientos de miles de programadores y que está presente en más de 20% de los servidores web en Internet. Es el sexto lenguaje de programación más utilizado en el desarrollo de software, únicamente por detrás de C, Java, C++, Visual Basic y Perl.

Inventado por Netscape en 1995, JavaScript es casi tan viejo como la Web mismas. Mientras JavaScript es bien respetado hoy en día, tiene un pasado con altibajos. Fue considerado como lenguaje de programación de hobby. Usado para agregar algunos efecto tal a los mensajes que al desplazarse con botones a través del navegador Web, o animaciones de mariposas siguiendo el mouse, movimientos alrededor de las páginas. Muy pronto, era fácil de encontrar miles de programas gratis en JavaScript (o solo llamados scripts) on-line, pero muchos de estos programas no fueron trabajados en el navegador Web.

Posteriormente, JavaScript también sufrió de incompatibilidades con los dos navegadores prominentes, Netscape e Internet Explorer. Porque Netscape y Microsoft tratando de superar a otros navegadores agregaron nuevas y ostentosas características. Los dos navegadores con frecuencia actuaron con dos diferentes caminos, marcando dificultades para crear programas con JavaScript y trabajar bien con ambos.

Afortunadamente lo peor de esos días se ha ido, los navegadores contemporáneos como Firefox, Sagari, Chrome, Opera e Internet Explorer 9 tienen estandarizado mucho del manejo de JavaScript, marcando la facilidad para programar en JavaScript que trabajan muchas personas. (Todavía hay algunas incompatibilidades entre las corrientes de los navegadores, necesitamos aprender algunos engaños para lidiar con estos problemas).

En muchos años atrás, JavaScript ha sufrido un renacimiento, alimentado por fuertes creadores de sitios Web como Google, Yahoo y Flickr, estos decidieron usar JavaScript extensivamente para crear aplicaciones interactivas. Nunca ha habido un mejor tiempo para aprender JavaScript. Con la riqueza, el conocimiento y la calidad con que han sido escritos los scripts, puede agregar sofisticadas integraciones en su sitio Web, incluso si eres principiante.

JavaScript se presenta como un lenguaje de desarrollo de aplicaciones cliente/servidor a través de Internet.

El programa en JavaScript tiene la particularidad de que esta insertado dentro mismo del documento HTML, que lo presenta al usuario y no es por ello un programa aparte. Permite crear aplicaciones similares a los CGI (Common Gateway Interface). El CGI es un mecanismo que se ha utilizado en los servidores Web para implementar las páginas Web activas.

MySQL es la base de datos elegida por la gran mayoría de programadores de PHP, además que es la forma en que Xplico lee las bases de datos que se extraen de los archivos pcap de Xplico siendo una gran ventaja que sea una base de datos gratuita.

MySQL es un sistema de administración de bases de datos relacionales rápido, sólido y flexible. Es ideal para crear bases de datos con acceso desde páginas web dinámicas, para la creación de sistemas de transacciones *on-line* o para cualquier otra solución profesional que implique almacenar datos, teniendo la posibilidad de realizar múltiples y rápidas consultas.

MySQL ofrece varias ventajas respecto a otros sistemas gestores de bases de datos:

- Tiene licencia pública, permitiendo no solo la utilización del programa sino también la consulta y modificación de su código fuente. Resulta por tanto fácil de personalizar y adaptar a las necesidades concretas.
- El programa está desarrollado en C y C++, lo que facilita su integración en otras

aplicaciones desarrolladas igualmente en esos lenguajes.

- Puede ser descargado gratuitamente de Internet (http://www.mysql.com) haciendo uso de su licencia GPL.
- Para aquellos que deseen que sus desarrollos basados en MySQL no sean "código abierto" existe también una licencia comercial.
- MySQL utiliza el lenguaje SQL (Structured Query Languaje) que es el lenguaje de consulta más usado y estandarizado para acceder a bases de datos relacionales. Soporta la sintaxis estándar del lenguaje SQL para la realización de consultas de manipulación, creación y de selección de datos.
- Es un sistema cliente / servidor, permitiendo trabajar como servidor multiusuario y de subprocesamiento múltiple, cada vez que se establece una conexión con el servidor, el programa servidor crea un subproceso para manejar la solicitud de cliente, controlando el acceso simultáneo de un gran número de usuarios de los datos y asegurando el acceso solo a usuarios autorizados.
- MySQL dispone de un sistema sencillo de ayuda en línea, y de un monitor que permite realizar todas las operaciones desde la línea de comandos del sistema, sin necesitar ningún tipo de interfaz de usuario gráfica. Esto facilita la administración remota del sistema utilizando telnet.
- Es portable, puede ser llevado a cualquier plataforma informática. MySQL está disponible en más de veinte plataformas diferentes incluyendo las distribuciones más usadas en Linux, sistemas operativos Mac X, UNIX y *Microsoft Windows*.
- Es posible encontrar gran cantidad de software desarrollado sobre MySQL o que soporte MySQL. En concreto, son de destacar diferentes aplicaciones *open Source* para la administración de las bases de datos a través de un servidor web.

Todas estas características han hecho de MySQL uno de los sistemas gestores de bases de datos más utilizados en la actualidad, no solo por pequeñas empresas sino también por algunas grandes corporaciones, como puedan ser: Yahoo! Finance, Google, CISCO, MP3.com, Motorola, NASA, Silicon Graphics, Texas Instruments, etc. A mediados del 2004 se estimaba que existían más de 5 millones de instalaciones activas del programa.

2º CAPITULO

Xplico como un todo.

Antes de entrar en materia; es necesario analizar cómo se verá la configuración del sistema una vez terminada la instalación de todos los componentes, programas y requerimientos que conforman la instalación de Xplico.

Lo primero que se requiere es tener el equipo de cómputo que funcionara como Firewall y en segundo lugar el que alojara el SO que a su vez albergara a Xplico.

Para la implementación de un Firewall en una red se necesitan ciertos requerimientos, a continuación se listan los diferentes componentes que se requieren.

1. Equipo de escritorio; puede funcionar alguno con procesador Pentium II a 400MHz.
2. Disco duro de 80 GB
3. 512MB de memoria RAM.
4. Dos tarjetas de red LAN.
5. Dos cables de red.

Las tarjetas de red deben ser instaladas en la PC, en una de ellas conectaremos el Router de donde tendremos el acceso a internet, en la otra conectaremos el Switch que será donde conectaremos la red LAN que tengamos.

Una vez que tengamos este equipo se procede a la instalación del software denominado Firewall (este proceso lo veremos más adelante con la instalación de FreeBSD no es forzoso instalar este Firewall ya que existen otros tipos de Firewalls en diferentes distribuciones).

Debemos tener en cuenta que estos requerimientos son solo si se va a instalar el puro Firewall en el equipo que se tenga disponible.

Ahora bien para nuestro SO tenemos que tener en cuanta contar con los siguientes requisitos (estos requerimientos son para la versión 12.04 LTS pero hay que tener en cuenta que funciona para las versiones subsecuentes):

- Procesador x86 a 700 MHz.
- Memoria RAM de 512 Mb.
- Disco Duro de 10 GB (swap incluida).
- Tarjeta gráfica. Teniendo en cuenta que las mejores tarjetas compatibles con el SO son de Intel. NVidia y ATI.
- Lector de DVD y puerto USB.
- Conexión a Internet.

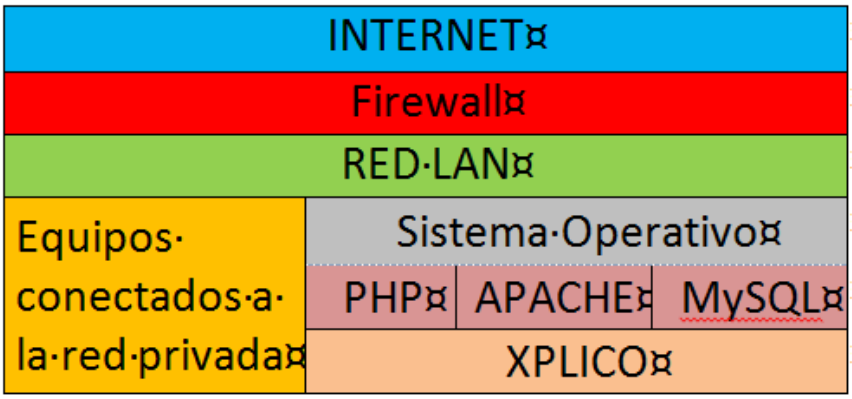
Si decides usar tú SO también como Firewall; debes agregar a la lista las dos tarjetas de red LAN que ya se mencionaron.

También se debe tener en cuenta que el disco duro en los dos casos puede variar dependiendo de cada situación que se afronte. Como recomendación se sugiere tener discos de tamaño más o menos grande ya que en el caso de que se requiera tener el Firewall y el SO en el mismo disco, se debe agregar el espacio necesario para poder almacenar los archivos *pcap* y posteriormente poder decodificarlos.

Además también se requiere el espacio necesario para la instalación de los programas adicionales necesarios para que funciones el sistema en conjunto.

Una vez que se tenga instalado el SO se procede a instalara PHP, Apache, MySQL y al final el programa Xplico (estos pasos también se mencionan más adelante).

Al terminar la instalación quedaría una configuración más o menos parecida a la siguiente:

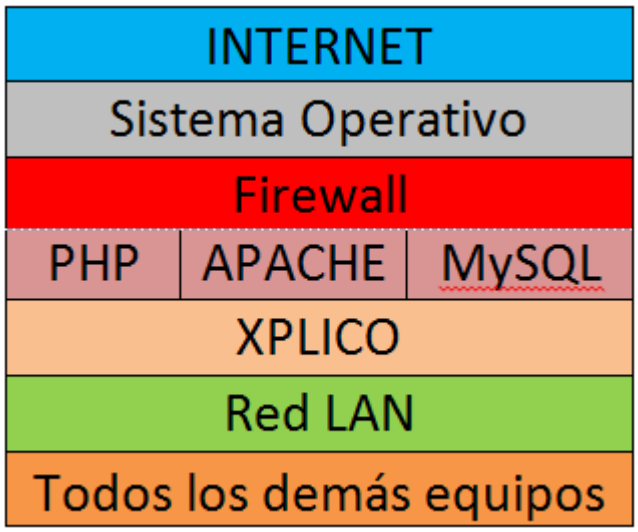


2-1 Configuración de Xplico con el Firewall y el SO por separado

Tengamos en cuenta que si escogemos tener el Firewall de manera separada del SO donde se encuentra albergado Xplico, no se tendrán los archivos PCAP en un solo equipo

así que tendremos que copiar estos archivos al equipo donde tengamos instalado Xplico.

Ahora bien, la otra configuración que podemos tener será la siguiente:



2-2 Configuración de Xplico instalado en un solo equipo.

Como se ha mencionado la ventaja de este tipo de configuración es que los archivos *pcap* ya no es necesario copiarlos a otra máquina, esto ahorra tiempo y espacio para colocar los servidores en algún espacio específico para ellos.

Nuevamente tengamos en cuenta que el disco duro tendrá que ser de un espacio mayor para poder tener instalados todos los componentes necesarios para poder hacer que funcione correctamente nuestro sistema.

Ahora bien ya tenemos una idea general como se verá nuestro sistema una vez terminadas las instalaciones correspondientes.

En los siguientes capítulos veremos las instalaciones de todos los componentes y programas que se mencionaron anteriormente.

3er CAPITULO

Políticas de seguridad Informática.

La tendencia hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computación, de las aplicaciones e incluso, de las empresas ha situado a la seguridad de los sistemas de información como un elemento central en todo el desarrollo de la sociedad.

La seguridad ha pasado de utilizarse para preservar los datos clasificados del gobierno e cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y crecientes que incluye transacciones financieras, información personal, archivos médicos, comercio y negocios por Internet. Por ellos, se hace imprescindible que las necesidades de seguridad potenciales se tengan en cuenta y se determinen para todo tipo de aplicaciones.

Este desplazamiento del enfoque de las cuestiones de seguridad, desde el nivel gubernamental al resto de la sociedad, ha elevado la importancia de la seguridad, que ha pasado a ser una disciplina cada vez más crítica, necesaria y obligatoria siendo un componente clave en todo tipo de proyectos de sistemas de información.

Para justificar el uso de herramientas de computación forense es necesario entender y analizar donde surge la necesidad de crear las llamadas Políticas de Seguridad Informática (PSI).

Las PSI son una forma de comunicarse con los usuarios y los gerentes, establecen el canal formal de acción del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

Este documento debe distribuirse a todos los empleados y usuarios del sistema. Debido a esto, la redacción utilizada para describir los procedimientos técnicos organizativos o legislativos, debería ser adecuada para permitir que todos los usuarios la entiendan adecuadamente.

No se trata de una descripción técnica de mecanismos de seguridad, no de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que deseamos proteger y el porqué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

Cada PSI debe considerar los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a casa uno de sus miembros a reconocer la información como uno de los principales archivos así como, un motor de intercambio de desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información de la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de porque deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía.

Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud que pasara cuando algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujetos a los cambios organizacionales relevantes: creciendo de la plantilla del personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

Para realizar un PSI se deben considerar algunas recomendaciones como lo son:

- Considerar efectuar un ejercicio de análisis de riesgos informáticos, a través del cual valore sus activos, el cual le permitía afinar las PSI de su organización.
- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

- Comunique a todo el personal involucrado en el desarrollo de la PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quien tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

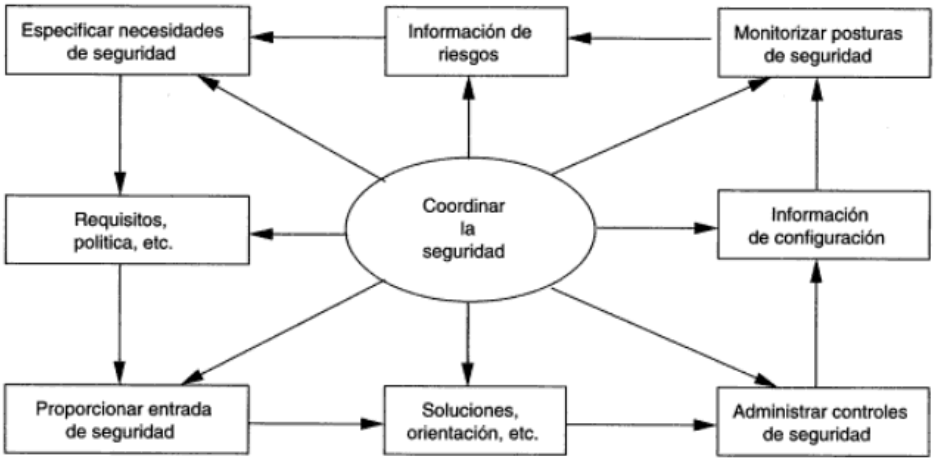
No dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan las PSI trazadas.

Una PSI se estructura y genera en diferentes pasos como son:

- Objetivo de la política.
- Ámbito de la política
- Procedimientos de seguridad a adoptar.
- Reglas, regulaciones y normas para los empleados.
- Gestión de la seguridad.
    - Implantación de la política de seguridad
    - Mantenimiento de la política de seguridad.

Objetivo de la política.

Para comenzar a realizar una política de seguridad debemos plantear un objetivo, especificar todos los detalles de a quién, cuando y donde se aplica la política de seguridad, de forma que se deben explicar los resultados esperados por el documento de la política de seguridad.



3-1 Identificación de la política de seguridad en el ciclo de vida del proceso de seguridad.

Ámbito de la política de seguridad.

Una vez planteado el objetivo de nuestra política de seguridad procederemos a definir claramente todos los aspectos cubiertos por ella, así como los sistemas utilizados, la funcionalidad del sistema, la arquitectura del sistema o el hardware y software utilizado.

Procedimientos de seguridad adoptar.

Se debe hacer una búsqueda de las vulnerabilidades del negocio y las amenazas de elevado impacto que se hayan identificado, así como las contramedidas que se han adoptado.

La intención de estipular estas cuestiones en la PSI es aumentar la concientización de todos los empleados en la seguridad. Un documento de política de seguridad de la información debe tratarse como una información sensible y bajo ninguna circunstancia debe distribuirse a personas ajenas a la organización.

Reglas, regulaciones y normas para los empleados.

Se debe definir claramente quien tiene acceso al sistema y se han de establecer los derechos de autorización para cada uno de los empleados.

Las reglas para el uso adecuado de todos los medios electrónicos deben ser claramente definidas. En caso de un incumplimiento interno de la política de seguridad, debe especificarse las acciones disciplinarias correspondientes. Asimismo debe elaborase un documento con las reglas de la política de seguridad, que debe ser firmado por todos los empleados.

Gestión de la seguridad.

Debe explicarse la forma en la que todos los empleados, pueden contribuir hacia el mantenimiento de la seguridad de la información. También debe definirse quienes son los responsables de la administración de la seguridad de la organización.

Implantación de la PSI.

Antes de implementar y distribuir la política de seguridad a todos los empleados, debe revisarse para no dejar ninguna laguna. Hay que asegurarse que la política es clara, concisa y consistente.

También debe establecerse de forma firme la validez de la política de seguridad, que debe observar las leyes establecidas por esta, para editar complicaciones legales.

Si algún empleado despedido decide demandar a la organización, un documento PSI sería la mejor ayuda para la defensa. Se debe tener en cuenta que una PSI puede tener algunas implicaciones sociales o éticas.

Mantenimiento de la PSI.

Para que una organización mantenga un nivel suficiente de seguridad, su PSI debe evolucionar para la detección de nuevos tipos de amenazas, para lo que debe revisarse constantemente.

Esto consiste en un proceso continuo de revisión, para asegurar los que se instituyen de manera adecuada y que no tengan repercusiones negativas debidas a una política mal estructurada.

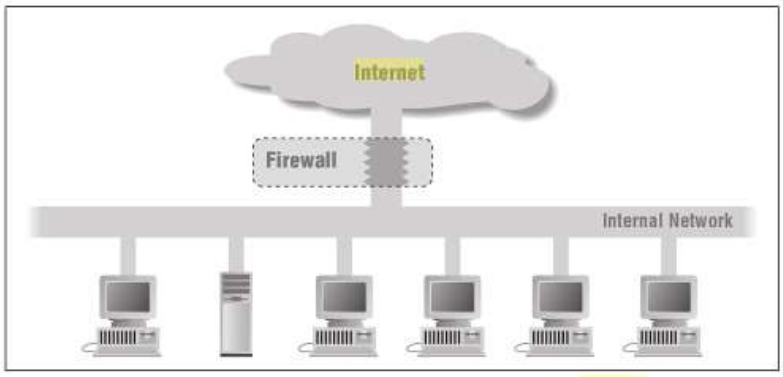
Las revisiones constantes se refieren a comprobaciones continuas para asegurar los cambios en el entorno de la organización o los avances tecnológicos.

Una vez vistos los puntos para diseñar una PSI podemos continuar con el estudio de nuestro sistema de seguridad.

4º CAPITULO

Firewall

Un Firewall es un dispositivo de seguridad de red diseñado para restringir el acceso a los recursos, tanto a la información como a los servicios, de acuerdo a una política de seguridad basada en reglas. Los Firewalls sirven para conectar dos secciones de una red y controlar el tráfico de datos ente ellas.



4-1 Colocación básica de un cortafuego entre una intranet e internet.

A menudo se instalan entre una red privada de la organización e Internet, pero también se pueden conectar entre departamentos, dentro de una intranet o bien pueden utilizarse entre socios corporativos conectados mediante una extranet. Para que pueda ser efectivo, debe ser el único camino de comunicación entre la red protegida interna y la red externa no protegida.

Un Firewall solo puede filtrar el tráfico que pasa a través de él, si el tráfico que fluye por la red corporativa procede de otro conducto, el Firewall no puede bloquearlo.

Las características principales de un Firewall son:

- Proteger parcialmente contra las amenazas de red.

- No entienden de sistemas operativos ni de vulnerabilidades de las aplicaciones.
- Los cortafuegos del tipo proxy proporcionan un control sobre el contenido de peticiones y repuestas mediante un procesamiento complejo.
- Los Firewalls corporativos perimetrales no son efectivos cuando las amenazas proceden de la red que se supone segura.
- Deben complementarse con un sistema de detección prevención de intrusiones.
- Se pueden colocar en paralelo para balancear la carga de tráfico y aumentar la disponibilidad.

Instalación del FreeBSD

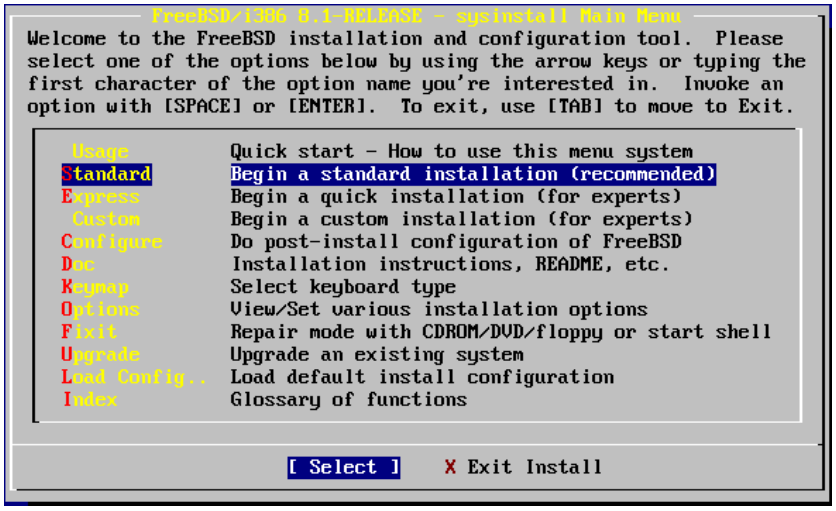
Si va a arrancar desde CD-ROM tendrá que configurar el BIOS e introducir el CD-ROM.

4-2 Pantalla de Bienvenida de FreeBSD.

Espere diez segundos o pulse Enter. Esto lanzará el menú de configuración del kernel.

4-3 Menú de selección del idioma.

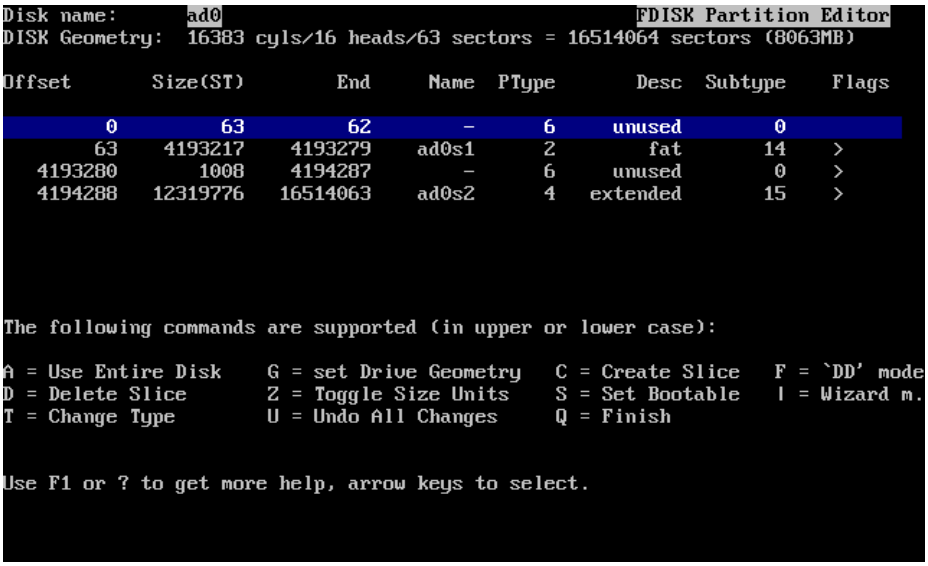
Lo siguiente que tenemos que hacer es seleccionar el idioma en el que queremos instalar FreeBSD.



4-4 Menú de selección de tipo de instalación.

Uno de los primeros pasos que tiene que hacer es asignar espacio en disco, para que sysinstall lo pueda dejar listo para su uso. Para ello debe saber cómo espera FreeBSD encontrar la información en el disco.

Seleccione el disco en el que desea instalar FreeBSD y pulse [OK]. FDisk arrancará y le mostrará una pantalla similar a la siguiente:



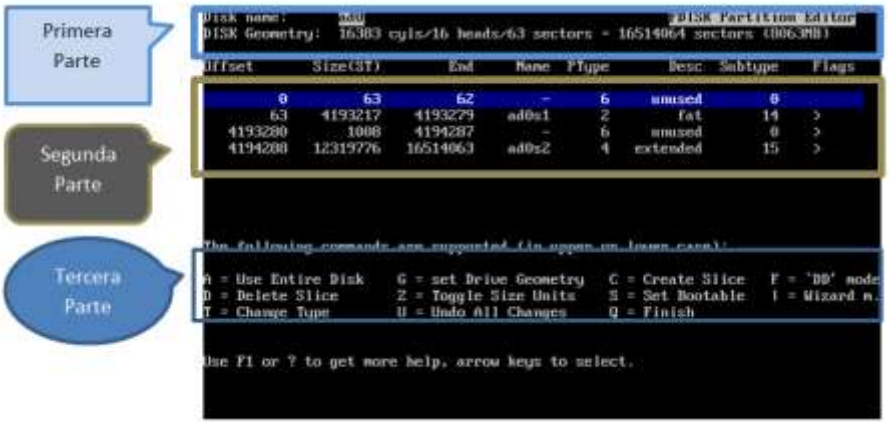
4-5 Ventana que muestra la organización de discos donde se instalara FreeBSD.

La primera parte, que ocupa las dos primeras líneas de la pantalla, muestra los detalles

del disco que seleccionemos, el nombre que FreeBSD le da, la geometría del disco y el tamaño total del disco.

La segunda parte muestra las particiones que hay en el disco, dónde comienzan y donde termina, su tamaño, el nombre que asigna FreeBSD, su descripción y el subtipo. Este ejemplo muestra dos pequeñas particiones sin usar; las particiones son un tipo de esquema estructural de los discos de PC. También muestra una gran partición FAT, que casi con total seguridad aparecerá como C: en MS-DOS / Windows, y una partición extendida, que podría contener otras letras de unidad de MS-DOS / Windows.

La tercera parte muestra las órdenes que pueden usarse en FDisk.



4-6 Estructura de la vista del disco.

Si desea usar FreeBSD en el resto del disco pulse *"A"*, que equivale a la opción Use Entire Disk. Las particiones que existieran se borrarán y serán reemplazadas por un pequeño área de disco marcado como sin usar y tras él una gran partición destinada a FreeBSD. Ahora marque la partición FreeBSD que acaba de crear como arrancable: pulse *"S"*. Observe la **A** en la columna Flags: indica que la partición es activa y se arrancará desde ella.

Si desea borrar una partición para hacer más sitio a FreeBSD selecciónela mediante las flechas y pulse *"D"*. Después pulse "*C"* y verá un mensaje en el que se le pedirá el tamaño de la partición que va a crear. Introduzca los datos apropiados y pulse Intro. El valor por defecto en ésta pantalla es el de la partición más grande que pueda crear en el disco, que debería ser la mayor parte del disco que queda sin usar o el tamaño del disco duro completo.

Si ha hecho sitio para FreeBSD puede pulsar *"C"* y crear una nueva partición. Verá de nuevo un mensaje en el que se le pedirá que escriba el tamaño de la partición que va a crear.

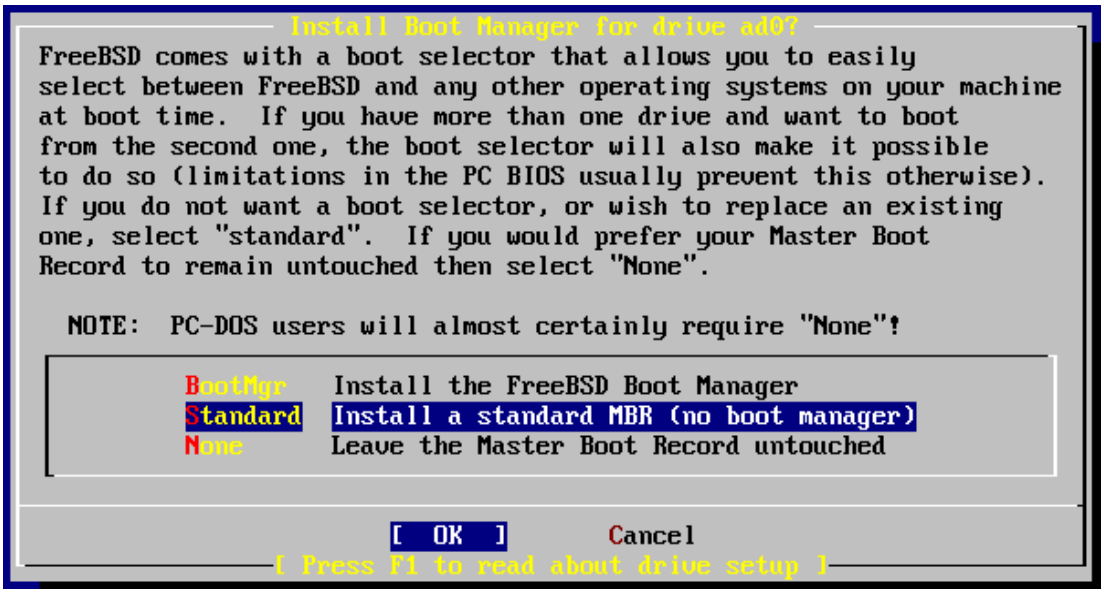
Partición con FDisk usando el disco completo

Cuando acabe pulse *"Q"*. Sus cambios se guardarán en sysinstall, pero de momento no se guardarán en disco.

Instalación de un gestor de arranque

Ha llegado el momento de instalar un gestor de arranque. Elija el gestor de arranque de FreeBSD si:

1. Tiene más de un disco y ha instalado FreeBSD en cualquiera que no sea el primero.
2. Ha instalado FreeBSD codo con codo con otro sistema operativo y quiere poder elegir si arrancar FreeBSD o ese otro sistema operativo cuando arranque su sistema.
3. Si FreeBSD va a ser el único sistema operativo en el sistema y va a instalarlo en el primer disco duro elija el gestor estándar. Elija None si va a usar algún otro gestor de arranque que sea capaz de arrancar FreeBSD.
4. Elija y pulse Intro.
5. Menú de gestores de arranque de sysinstall

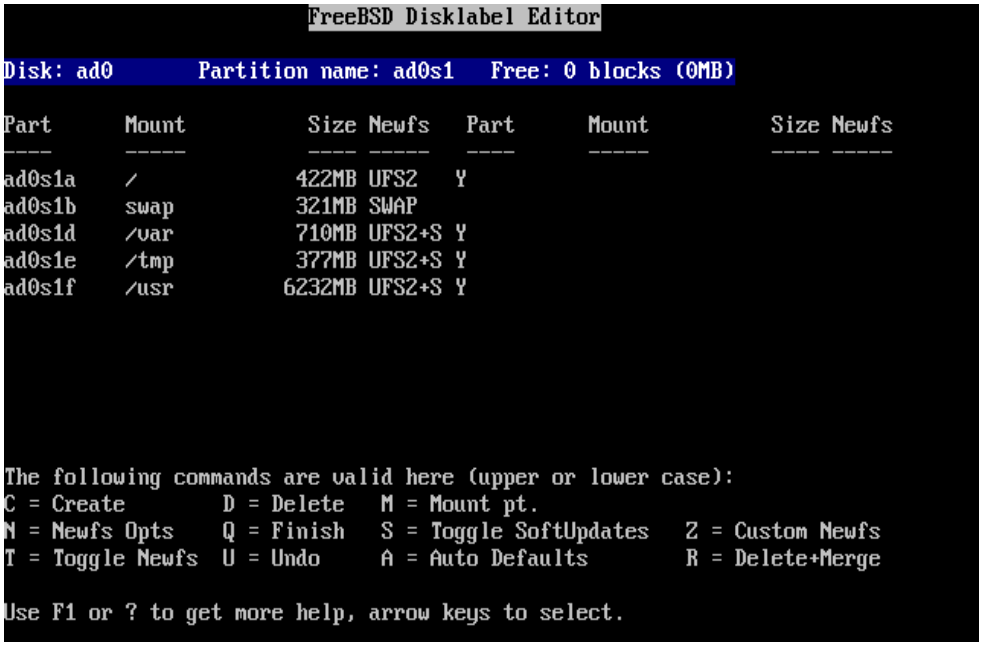


4-7 Selección del gestor de arranque.

La pantalla de ayuda, que puede consultar en cualquier momento pulsando F1, puede serle de mucha ayuda con los problemas que puede encontrarse al intentar compartir un disco duro entre varios sistemas operativos.

Disk label puede crear automáticamente particiones y asignarles tamaños por omisión. Estos tamaños se calculan con la ayuda de un algoritmo interno de dimensionamiento de

particiones que analiza el tamaño del disco. Puede probarlo pulsando *"A"*. Dependiendo del tamaño del disco que esté usando los valores por omisión pueden o no ser los apropiados. Esto no es algo de lo que deba preocuparse dado que no está obligado a aceptar esos valores por omisión.



4-8 Estructura de partición de un disco en FreeBSD.

Estructura de particiones:

A continuación se presenta la forma recomendada; para los sistemas operativos UNIX®, de cómo se debe realizar la partición del disco duro.

Partición	***Sistema de Ficheros***	***Tamaño***	***Descripción***
A	/	512 MB	Este es el sistema de ficheros raíz. El resto de sistemas de ficheros se montarán en algún punto de este sistema raíz. 100 MB es un tamaño razonable para él. No es el mejor sitio para almacenar muchos datos y la instalación de FreeBSD escribirá cerca de 40 MB de datos en ella. El resto del espacio es para datos temporales y por si futuras versiones de FreeBSD.

B	Swap	2-3 x RAM	Esta partición es el espacio de memoria de intercambio del sistema. La elección de la cantidad correcta de swap es casi un arte en sí mismo. Hay una regla básica que es asignar a la swap el doble o el triple de MB de los que haya en la memoria RAM del sistema. Si tiene más de un disco puede poner espacio swap en cada disco. FreeBSD usará ambas swap con el resultado de acelerar notablemente el intercambio de páginas de memoria.
E	/var	256 MB to 1024 MB	El directorio /var contiene ficheros que están en continuo cambio, como «logs» y otros ficheros administrativos. Muchos de esos ficheros son una consecuencia o son de gran ayuda para el correcto funcionamiento diario de FreeBSD. FreeBSD ubica dichos ficheros en ese sistema de ficheros para optimizar el acceso a los mismos sin afectar a otros ficheros ni directorios que tienen similar patrón de accesos.
f	/usr	Resto del disco(al menos 2 GB)	El resto de sus ficheros pueden almacenarse en /usr y sus subdirectorios.

Nota: En el esquema de particiones por omisión el directorio /tmp tiene su propia partición en lugar de formar parte de /. Esto ayuda a evitar el desbordamiento de / con ficheros temporales.

Elección de qué instalar

La elección de qué tipo de instalación debe hacer depende enormemente del uso que se va a dar al sistema y del espacio de disco disponible. El rango de opciones predefinidas está entre hacer la instalación más pequeña posible o instalarlo todo. Las personas con poco o ninguna experiencia en UNIX® o FreeBSD deberán elegir alguna de las opciones predefinidas que se les ofrecen, a las que llamaremos distribuciones tal y como aparecen en el menú de sysinstall. Una instalación a medida es algo más adecuado para usuarios con más experiencia.

Si tiene intención de instalar un interfaz gráfico de usuario tendrá que instalar una de las distribuciones cuyo nombre comienza con X. La configuración del servidor X y la selección de un entorno de escritorio son algunas de las tareas que tendrá una vez instalado FreeBSD.

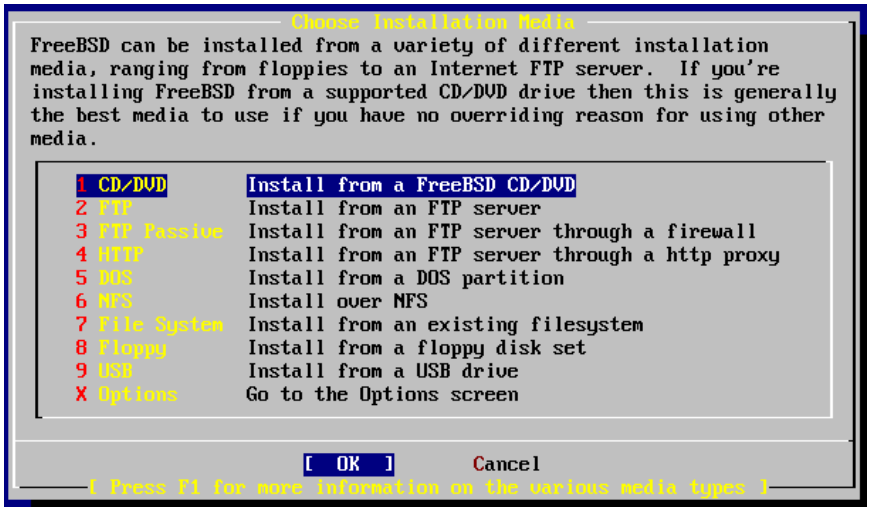
Evidentemente el sistema más versátil es aquél que lo tiene todo. Si dispone de espacio de disco suficiente seleccione All, usando las flechas y pulsando Intro. Si el espacio en disco es limitado piense en usar alguna de las otras opciones. No pierda con ello demasiado tiempo puesto que el resto de distribuciones pueden añadirse en cualquier momento tras la instalación.

Elección del medio de instalación

Si va a instalar FreeBSD desde CD-ROM o DVD seleccione Install from a FreeBSD CD/DVD con las flechas direccionales del teclado. Una vez que [OK] está seleccionado pulse Intro y siga adelante con la instalación.

Si quiere usar otro método de instalación seleccione la opción correspondiente y siga las instrucciones.

Pulse F1 si necesita acceder a la ayuda del medio de instalación elegido. Pulse Intro para regresar al menú de selección de medios.



4-9 Menú de selección de donde se copian los archivos de instalación.

El punto sin retorno

A partir de aquí entramos en la instalación propiamente dicha. Esta es la última oportunidad antes de empezar a escribir datos en el disco duro.

User Confirmation Requested
Last Chance! Are you SURE you want to continue the installation?
If you're running this on a disk with data you wish to save then WE
STRONGLY ENCOURAGE YOU TO MAKE PROPER BACKUPS before proceeding!
We can take no responsibility for lost disk contents!

[Yes] No

Seleccione [Yes] y pulse Intro.

La instalación tardará más o menos tiempo según la distribución que haya elegido, el

medio de instalación y la velocidad del sistema. Se le irán mostrando mensajes durante el proceso para irle informando de cómo van las cosas.

Cuando acabe la instalación verá un mensaje como este:

Message

Congratulations! You now have FreeBSD installed on your system.
We will now move on to the final configuration questions.
For any option you do not wish to configure, simply select No.
If you wish to re-enter this utility after the system is up, you may
do so by typing: sysinstall.

[OK]

[Press enter to continue]

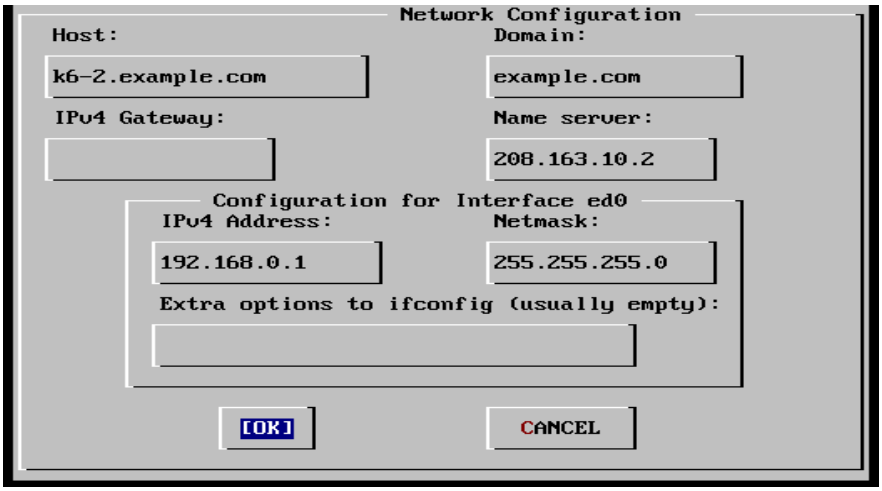
Pulse Intro; pasaremos a acometer ciertas tareas posteriores a la instalación.

Si selecciona [No] y pulsa Intro la instalación se detendrá para evitar hacer más modificaciones en su sistema. Vera el siguiente mensaje.

Message
Installation complete with some errors. You may wish to scroll
through the debugging messages on VTY1 with the scroll-lock feature.
You can also choose "No" at the next prompt and go back into the
Installation menus to retry whichever operations have failed.

[OK]

Configuración de ed0



4-10 Ventana de configuración de red.

Use el tabulador para ir pasando de un campo al siguiente una vez que los vaya rellenando:

Host

El nombre de la máquina; por ejemplo, k6-2.ejemplo.com.

Dominio

El nombre del dominio al que pertenece la máquina; en este caso ejemplo.com.

Gateway IPv4

La dirección IP del sistema que reenvía paquetes a destinos fuera de la red local. Debe rellenar este campo si esta función la realiza una máquina que forme parte de la red. Déjelo en blanco si el sistema es el enlace de su red con Internet. El Gateway recibe también los nombres de puerta de enlace o ruta por omisión.

Servidor de nombres

Dirección IP de su servidor local de DNS. En la red del ejemplo no hay servidor DNS local así que se ha introducido la dirección IP del servidor DNS del proveedor de Internet: 208.163.10.2.

Dirección IPv4

En este interfaz se usará la dirección IP 192.168.0.1. O bien la que desee usar según su red privada.

Máscara de red

En esta red local se usa un bloque de redes de Clase C 192.168.0.0 -192.168.0.255. La máscara de red es, por tanto, 255.255.255.0.

Opciones adicionales de ifconfig

Cualquiera de las opciones que quiera agregar a su interfaz mediante ifconfig. En nuestro caso no había ninguna.

Utilice el tabulador para seleccionar [OK] cuando haya acabado y pulse Intro.

User Confirmation Requested

Would you like to Bring Up the ed0 interface right now?

[Yes] No

Seleccione [Yes] y pulse Enter si quiere conectar inmediatamente su sistema a la red mediante el o los interfaces que acaba de configurar, pero recuerde que aún tendrá que reiniciar la máquina.

Configuración del Gateway

User Confirmation Requested

Do you want this machine to function as a network gateway?

[Yes] No

Si el sistema hará de enlace de la red local y reenviará paquetes entre otras máquinas elija [Yes] y pulse Intro. Si la máquina es un nodo de una red elija [No] y pulse Intro.

Configuración de servicios de internet

User Confirmation Requested
Do you want to configure inetd and the network services that it provides?

Yes [No]

Si selecciona [No] varios servicios de la máquina, como telnet y otros, no se activarán. Eso significa que los usuarios remotos no podrán acceder al sistema mediante telnet. Los usuarios locales, en cambio, podrán acceder a sistemas remotos mediante telnet.

Dichos servicios pueden activarse en cualquier momento editando /etc/inetd.conf con el editor de texto que prefiera.

Seleccione [Yes] si desea configurar estos servicios durante la instalación. Se le mostrará el siguiente mensaje:

User Confirmation Requested
The Internet Super Server (inetd) allows a number of simple Internet services to be enabled, including finger, ftp and telnet. Enabling these services may increase risk of security problems by increasing the exposure of your system.

With this in mind, do you wish to enable inetd?

[Yes] No

Select [Yes] to continue.

User Confirmation Requested

inetd (8) relies on its configuration file, /etc/inetd.conf, to determine which of its Internet services will be available. The default FreeBSD inetd.conf(5) leaves all services disabled by default, so they must be specifically enabled in the configuration file before they will function, even once inetd(8) is enabled. Note that services for

IPv6 must be separately enabled from IPv4 services.
Select [Yes] now to invoke an editor on /etc/inetd.conf, or [No] to use the current settings.

[Yes] No

Si selecciona [Yes] podrá añadir servicios borrando caracteres # al comienzo de las líneas correspondientes.

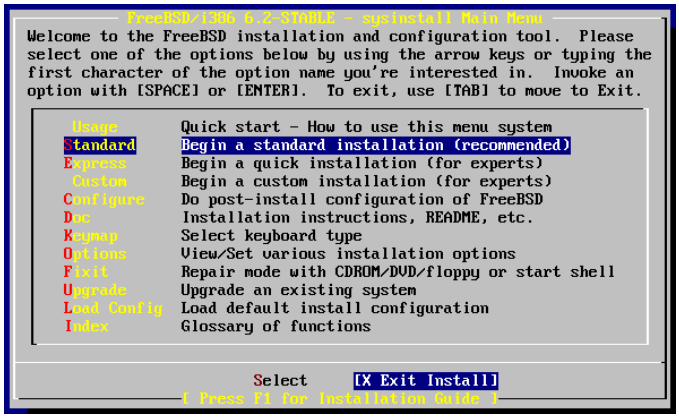
Salir de la instalación

Si tiene que configurar servicios de red o cualquier otra cosa, puede hacerlo ahora mismo o tras terminar la instalación ejecutando sysinstall.

User Confirmation Requested
Visit the general configuration menu for a chance to set any last options?

Yes [No]

Seleccione [No] con las flechas y pulse Intro para volver al menú principal de la instalación.



4-11 Ventana de inicio y salida.

Seleccione [X Exit Install] con las flechas y pulse Intro. Se le pedirá que confirme que quiere salir de la instalación:

User Confirmation Requested
Are you sure you wish to exit? The system will reboot (be sure to remove any floppies/CDs/DVDs from the drives).

[Yes] No

Seleccione [Yes] y extraiga la unidad CD-ROM está bloqueada hasta que la máquina comience a reiniciarse. La unidad CD-ROM se desbloquea y puede extraerse el CD-ROM.

El sistema reiniciará. Esté atento por si aparece algún mensaje de error.

5º CAPITULO

Ubuntu

Ubuntu es un sistema operativo basado en UNIX®.

Ubuntu es una palabra Africana que significa "*Humanidad hacia otros*" o "*Yo soy porque nosotros somos*". La distribución Ubuntu lleva el espíritu de Ubuntu al mundo del software.

Con el sistema operativo Ubuntu no pagas por una licencia de uso. Puedes descargar, usar y compartir Ubuntu con tus amigos, familiares, escuela o negocios libremente.

Se publica un nuevo lanzamiento de la versión de escritorio y servidor cada seis meses. Esto significa que siempre tendrás las más recientes aplicaciones que el mundo del Open Source te puede ofrecer.

Ubuntu está diseñado pensando en la seguridad. Con la versión con Long Term Support (LTS) tienes soporte por tres años en la versión de escritorio, y cinco años en la versión de servidor. No se requiere de pagos extra por la versión LTS,

Todo lo que necesitas está en un CD, que proporciona un entorno de trabajo completo. Software adicional se puede encontrar online.

Hay muchos sistemas operativos distintos basados en GNU/Linux: Debian, Gentoo, RedHat o Mandriva son algunos ejemplos. ¿Qué hace a Ubuntu diferente?

Basado en Debian que es una de las distribuciones más respetadas, tecnológicamente avanzadas y mejor soportadas; Ubuntu pretende crear una distribución que proporcione un sistema GNU/Linux actualizado y coherente para la informática de escritorio y servidores.

Con la mirada puesta en la calidad, Ubuntu proporciona un entorno robusto y funcional, adecuado tanto para uso doméstico como profesional y se publica una nueva versión

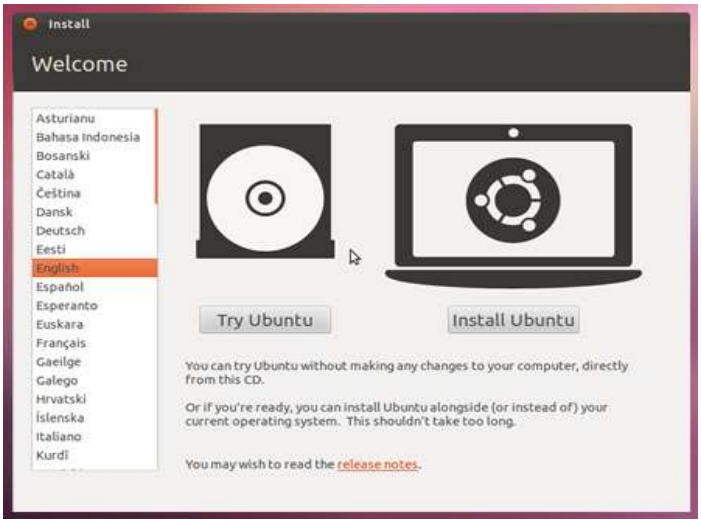
cada seis meses, una en Abril y otra en Octubre, esto se refleja en la numeración de las versiones.

Lo que debemos saber antes de comenzar.

Descarga el ISO accediendo al sitio web oficial que es http://www.ubuntu.com/download. Quemar el ISO en CD, DVD con algún programa de grabación o en su defecto crear un USB live. Ya sé que se haya quemado el CD, DVD o creado un Live-USB; ajustamos el BIOS del equipo para que inicie con el lector de CD o USB

Instalar Ubuntu paso a paso

Lo primero que vemos al correr el DVD o el Live USB son las opciones de Probar Ubuntu (Try Ubuntu) o de instalarlo (Install Ubuntu) directamente en el equipo. También tenemos la opción para seleccionar el idioma con el que nos guiaremos para el proceso de instalación, que será el mismo con el que se instalara el sistema operativo.

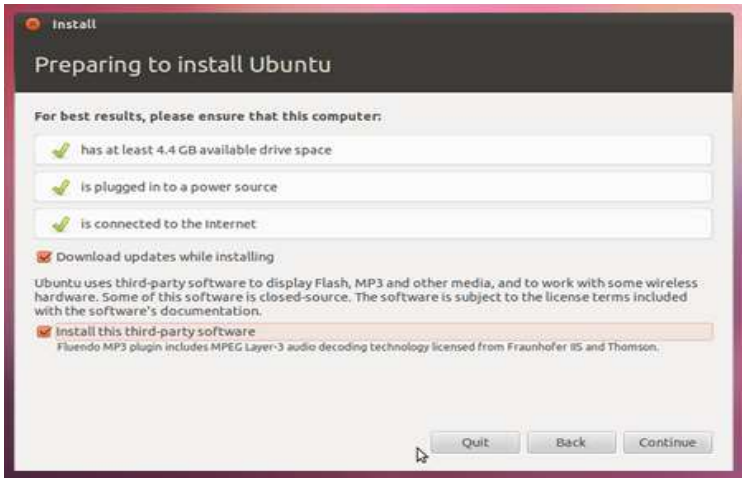


5-1 Ventana de bienvenida de la instalación de UBUNTU.

En esta primera pantalla se elige el idioma que quieras utilizar para el resto del proceso de instalación; pulsa sobre el botón “Instalar Ubuntu”.

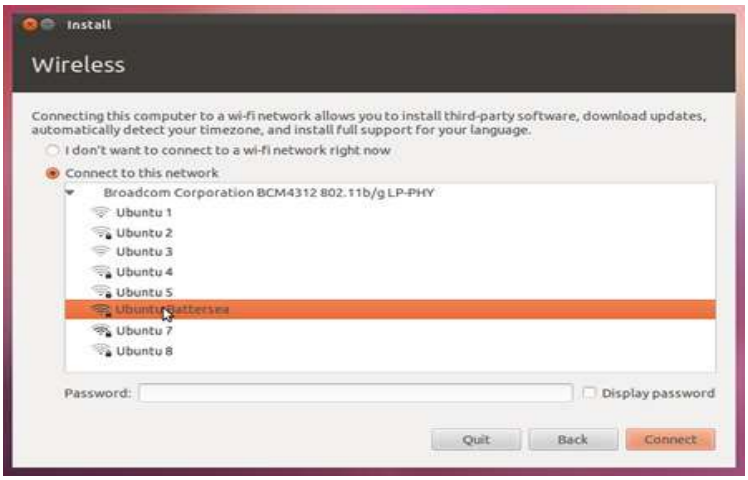
La siguiente pantalla es de información; donde te recomienda conectar el equipo a internet, verificar si hay suficiente espacio en disco y conectar el equipo a una fuente de alimentación (esto es para evitar la interrupción de energía y evitar que se pueda cometer errores de instalación, este mensaje se presenta más frecuentemente en las instalaciones de las laptops).

En la parte inferior de la pantalla aparecen dos check boxes que se pueden activar; uno de ellos es para descargar actualizaciones mientras se está realizando la instalación (Download up dates while installing) y la otra es para que instale software de terceros (Install this third-party software) que permitirá descargar e instalar el software que por tema de licencias no está incluido en el CD pero que se puede instalar.



5-2 Requerimientos antes de la instalación.

El siguiente paso es configurar el acceso a internet mediante conexión wireless (si se encuentra alguna red disponible y si se tiene una tarjeta de red inalámbrica).



5-3 Selección de redes para conectarse a internet.

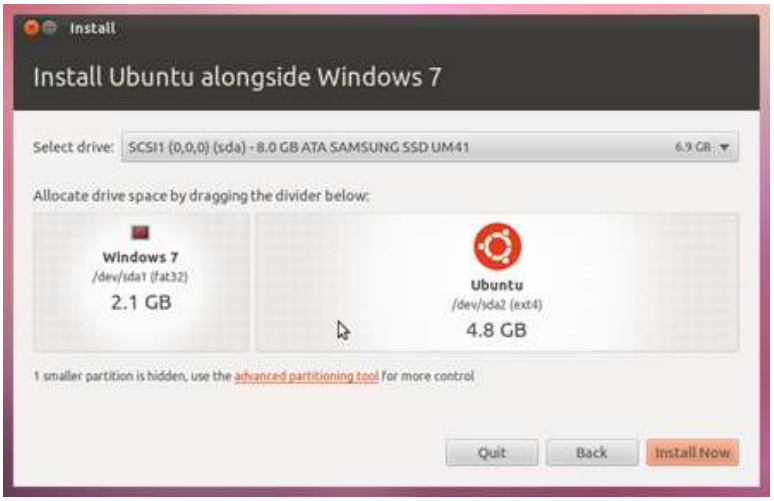
Asignaremos el espacio donde se instalara Ubuntu. Podemos utilizar cualquier opción de los check boxes:

- Instalar Ubuntu junto a otro sistema operativo que ya tengas instalado
- Suprimir el sistema operativo actual para reemplazarlo por Ubuntu

- Si eres un usuario más experimentado configurar a medida el particionado del disco duro para la instalación.

5-4 Menú para seleccionar el tipo de instalacion.

Al comienza la instalación, se podrá verificar la manera que se ha elegido para instalar Ubuntu. Pudiendo volver atrás en el caso de que quieras modificar algo o aceptando las opciones indicadas.



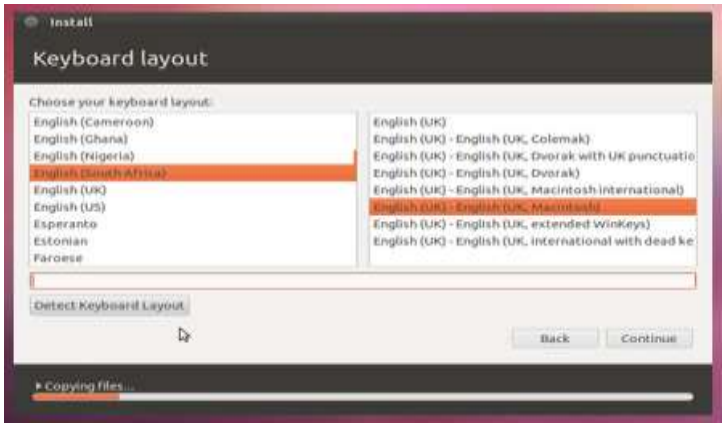
5-5 Instalación con un sistema operativo adyacente.

Ubuntu necesita un mínimo de 4.5 GB de espacio aunque es recomendable usar un tamaño mayor para el futuro almacenamiento de nuestros archivos personales o aplicaciones adicionales.

Elegirla zona horaria. En este punto; simplemente seleccionamos en el mapa, la zona horaria donde nos encontramos.

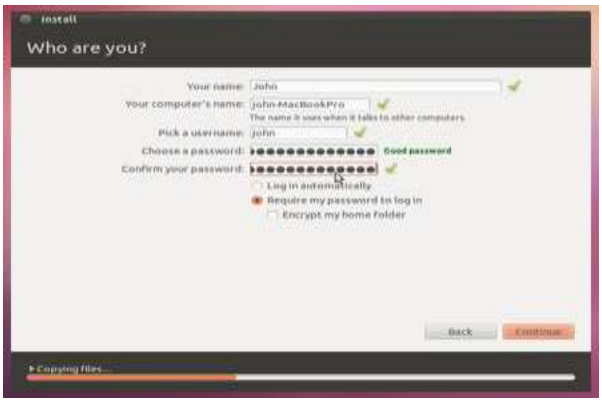
5-6 Selección del país donde está el usuario.

Selecciona la configuración de tu teclado. Se puedes escribir un texto en la caja de texto que se muestra para asegurarte que la selección es la correcta.



5-7 Selección del teclado y el idioma del teclado.

Añade información de la cuenta: El nombre de usuario principal, el nombre de la máquina y la contraseña de acceso que se quiere utilizar.

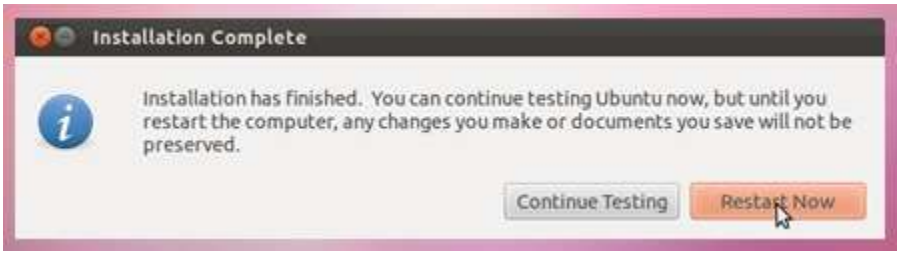


5-8 Configuración del usuario, nombre del equipo y contraseña.

Solo queda esperar a que la instalación termine. Y esa es toda la información requerida. Mientras continúa la copia de archivos se te van mostrando una serie de diapositivas que te van informando de las características de Ubuntu.

5-9 Comienzo de la instalación.

Tras unos breves minutos, termina la instalación y la instalación solicitara el reinicio del equipo.



5-10 Termino de la instalación y reinicio del equipo.

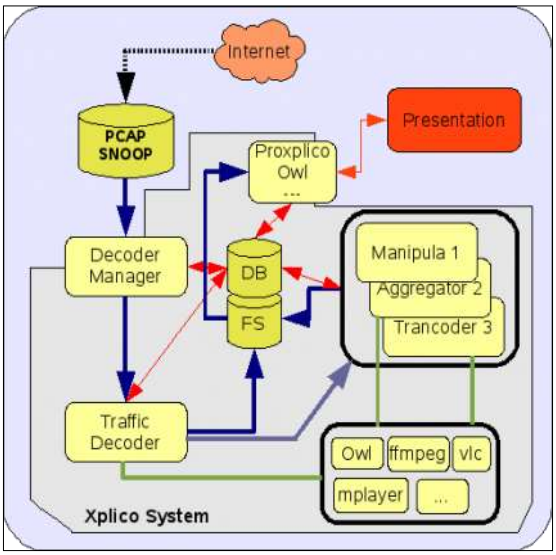
6º CAPITULO

Arquitectura del sistema Xplico.

Aunque ya se ha mencionado la configuración de Xplico y como está conformado, no está de más recordar esto. El sistema Xplico está compuesto por los siguientes componentes:

- Un decodificador maestro llamado DeMa.
- Un decodificador de red/IP llamado Xplico.
- Un conjunto de aplicaciones llamadas Manipuladores para la manipulación y decodificación de datos.
- Un sistema visualizador para ver los datos extraídos.

La relación entre estos componentes se muestra en esta figura.



6-1 Estructura del sistema Xplico.

También hay otras aplicaciones y códigos que son usadas indistintamente por cuatro componentes.

Explicación de la ilustración y su flujo.

Podría ser útil para ver lo que pasa en Xplico, para comprender cómo funciona. Para demostrarlo, vamos a ver qué pasa cuando Xplico procesa el archivo PCAP.

Desde la función main(), CapInit() se llama para inicializar el módulo de captura que se va a utilizar que es la función CapMain(). Cuando CapInit() es llamada, se establece una función puntero a un módulo de captura adecuado. En este caso, el puntero de la función se carga desde un archivo llamado cap_pcap.so, así desde el interior CapMain(); la función CaptMain() puntero se llama, que en realidad se está llamando al archivo capt_dissectors/pcap/pcap.c de la función CaptDisMain().

Una vez que se alcanza el módulo de captura PCAP; pcap_loop se llama, y cada paquete será procesado por PcapDissector(). ProtDissec() tiene un bucle while, que encuentra y ejecuta un disector apropiado para cada paquete en la jerarquía de protocolo.

Una vez terminado el proceso de captura con los disectores PcapDissector(), se lanza a él despachador adecuado para ser presentado al usuario, ya con los datos decodificados y listos para ser vistos en pantalla.

Todos estas funciones están bien especificadas en el código fuente, aquí solo se mencionan para ver el funcionamiento global de Xplico, ya que ver el código fuente como tal llevaría un capítulo entero; lo que nos interesa realmente es ver su funcionamiento; si se quisiera realizar alguna modificación, o agregarle alguna función que se crea necesaria para el funcionamiento, si sería necesario comprender como está estructurado dicho código; si alguna persona esta interesada en estudiar y ver la composición y estructura del código fuentes visiten la página oficial; http://www.xplico.org/.

DeMa: Decodificador maestro.

DeMa tiene las siguientes características:

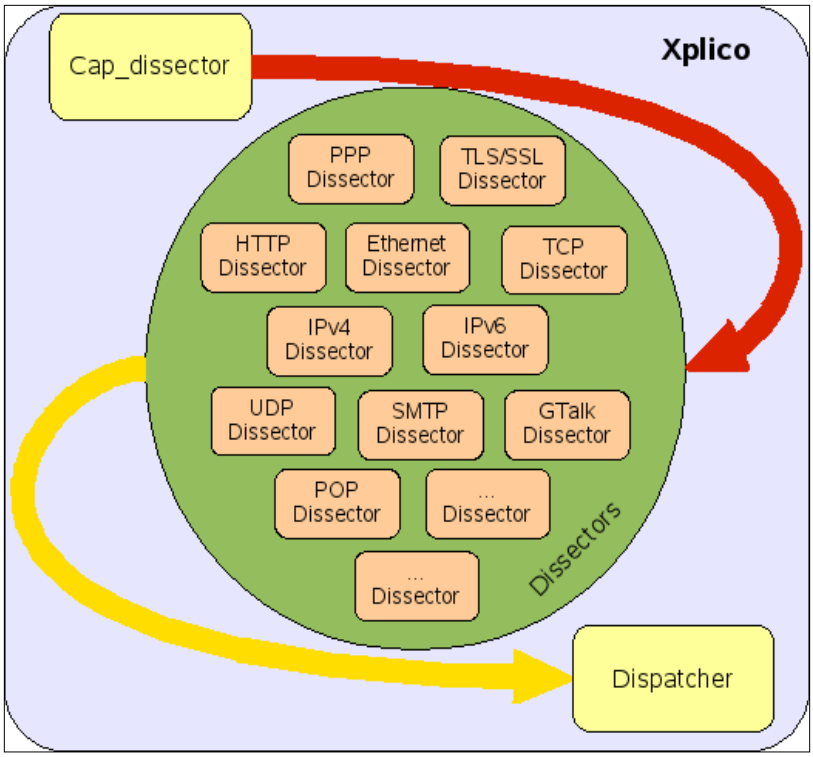
- Organizar las salidas de los datos.
- Establecer la configuración, archivos de historial de decodificación y manipularlos.
- Iniciar la decodificación y la manipulación.
- Control y ejecución del decodificador y la manipulación.

El decodificador de tráfico; Xplico.

Xplico es un decodificador de tráfico, esta diseñado para usar cualquier arquitectura estándar. La característica principal son las decodificaciones, su alta modalidad, escalabilidad y capacidad de configuración.

El decodificador esta designado solo para la decodificación del protocolo según el formato (en crudo) de salida y también el formato usado por los datos de salida (reconstrucción).

El flujo de datos e información en Xplico está representado en la siguiente figura.



6-2 Funcionamiento de Xplico en forma gráfica.

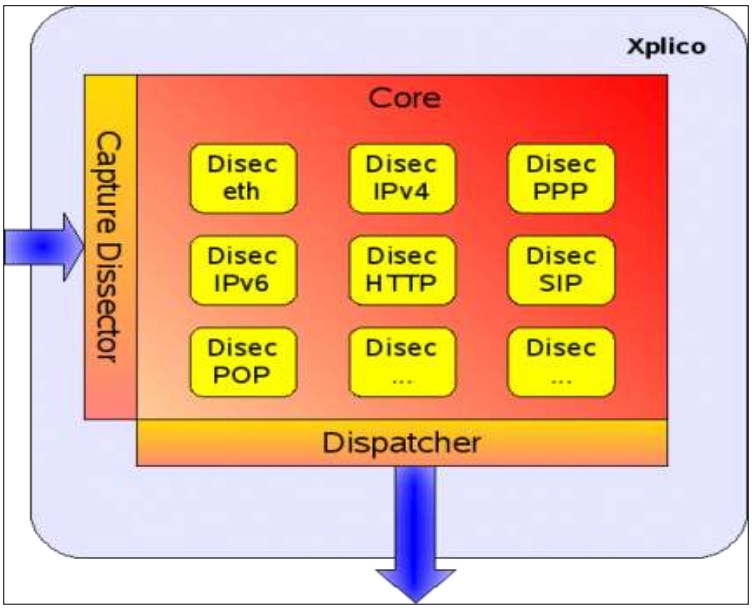
Los datos se leen en crudo del bloque de disectores de captura, después de ser enviados en bloques por el protocolo y finalmente los datos se reconstruyen y normalizan; previsto del bloque distribuidor.

El distribuidor reorganiza los datos o los envía a un manipulador si es necesario.

Por lo tanto Xplico está compuesto por tres tipos de módulos:

- Módulos de captura
- Módulos disectores
- Módulos despachadores

La siguiente figura representa la estructura modular de Xplico, donde el núcleo es el substrato donde los módulos están interconectados.



6-3 Otra forma de ver el sistema Xplico en forma gráfica.

Módulos disectores de captura, módulos disectores y el despachador de módulos.

Xplico lee el tráfico de datos disecciona la información de los datos de acuerdo al protocolo y despacha la información a una salida deseada.

Cada parte del decodificador es un conector y un módulo. En Xplico, distinguimos entre tres tipos de módulos:

- Módulos de captura: estos módulos permiten la interfaz entre todo tipo de datos adquiridos por el sistema.
- Módulos de disección: estos módulos son decodificadores de protocolos y son divididos en varias categorías.
- Módulos despachadores: estos módulos permiten la interfaz de todo tipo de datos almacenados en el sistema (disectores/archivos, SQLite, Oracle, MySQL, PostgreSQL, sistemas almacenados en el conector,… y lo que puedas imaginar). Todo se puede hacer fácilmente y sin modificar los protocolos disectores (Módulos Disectores).

Módulos de captura.

Los módulos de captura están localizados en el directorio capt_dissectors en niveles superiores del árbol. La interfaz pcap son módulos de captura del tráfico en archivos

PCAP. El ritm (el acrónimo de 'real time') captura el tráfico de datos en tiempo real de la interfaz de red. (eth0, wlan0, en1, etc.)

Módulos disectores

Estos módulos disectores extraen información del protocolo específico del tráfico de red y puede estar funcionando en el disector en niveles superiores del directorio. Están divididos en subdirectorios por cada protocolo soportado (eth, ip, tcp,…).

Dissector FTP

En la actualidad, los puntos de FTP *PEI.cmd* se componen de un nombre de archivo donde el texto de la sesión de FTP se almacena. Si desea extraer comandos de FTP y respuestas de una conversación (desde el interior de un despachador), tiene dos opciones sugeridas. La primera (y la más fácil) seria para analizar el nombre del archivo dato y obtener la información deseada. La segunda opción es para modificar el disector que incluye la información del componente *PEI*.

Dissector TCP

Para evitar mayores problemas de sincronización entre los flujos (por ejemplo, comandos FTP´s y canal de datos) se sugiere el uso de disectores TCP llamado *tcp_soft*. Tenemos desarrollado dos disectores separados de TCP para dos diferentes necesidades. Ambos proporcionan los mismos datos de mayores disectores (FTP, POP y SMTP), pero con limitaciones de tiempo diferentes. Nuestra "aplicación" disector (los disectores a través de TCP) puede designar el trabajo correcto con ambos disectores de TCP.

Módulos despachadores

Los módulos despachadores exportan los datos de un destino, está en una base de datos (SQLite, Postgres,…), para establecer un disector y archivo, en la conexión de red, o cualquier otro lugar que desee. Estos pueden estar funcionando en el dispatch en los directorios de alto nivel.

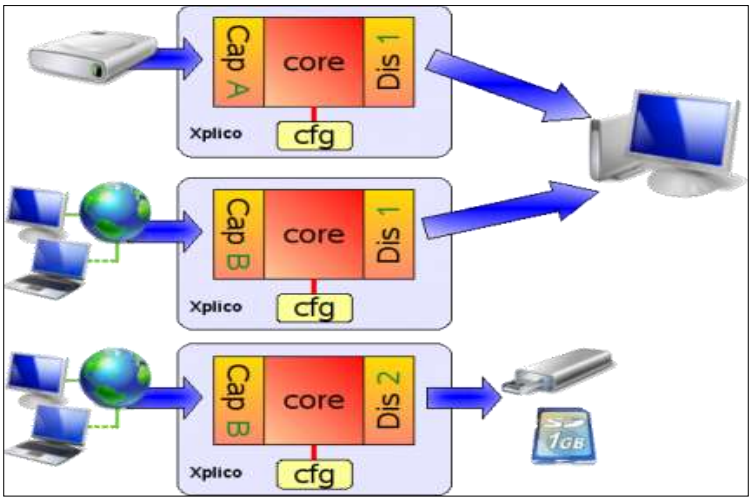
Para crear su propio despachador, tendrá que ponerlo en la interfaz localizada en *xplico-src/dispatch/dispatch.h*. Específicamente, tendrá que implementar tres funciones: **Dispinit()**, **DispEnd()**, **Dispinspei()**. **Dispinit()** se usa típicamente para establecer nombres de ID específicamente para los protocolos que tiene la intención de usar y también para establecer cualquier otra necesidad. Crea que esta función es solo para llamar un par de despachadores. **DisplnsPei()** es llamado algunas veces y cada vez es

pasado a un puntero objeto Protocol Element Information (PEI). **DispEnd()** es llamado para limpiar todo lo que necesite.

Si crea su propio despachador y descubre de que protocolo desea información no puede derivar de los protocolos compuestos *PEI*, para esto es necesario modificar los correspondientes disectores para obtener la información incluida/obtenida.

Tips: *para otras salidas de datos de captura/decodificada, observar su pei.time y pei.time_cap.*

Los despachadores de Xplico se pueden usar en varios contextos dependiendo de las necesidades de cada usuario.



6-4 Diferentes casos de cómo obtener un archivo .pcap

Como se muestra en la figura, los despachadores se pueden usar de un disco duro para presentarlos en el equipo, de la misma red LAN para presentarlos en el equipo y de la red LAN para almacenarlos en un dispositivo de almacenamiento para luego decodificarlos.

Protocol Element Information

La definición de la estructura de los datos PEI puede ser encontrado en *xplico-src/dispatch/include/pei.h*. Cada protocolo soportado por las herramientas que tienen los disectores pueden decodificar el tráfico de red y pueden decodificar la información dentro de un protocolo específico de formato PEI. El formato PEI para un protocolo dado es definido por los correspondientes módulos disectores en la función **DissecRegist ()**. Puede ser observado con el comando adecuado con la opción *–i*.

Por ejemplo, el FTP PEI es definido en *xplico-src/dissectors/ftp/ftp.c*; **DissecRegist()**. Por el momento, el valor de un componente de PEI puede ser una cadena o un archivo. Los

módulos disectores son responsables de construir PEIs de paquetes puros de datos. Y en estos PEIs están dados de módulos despachadores por salida.

No todos los disectores generan un PEI.

Alguna información importante acerca de la captura en vivo, tráfico de red en GB (TB).

Desde la versión 0.6.2 hay un nuevo código llamado sesión_mng.pyc que facilita la administración.

Si tiene GB o TB de datos para decodificar los pasos son los siguientes (obviamente después de a ver instalado Xplico y XI).

sudo su
cd /opt/xplico
rm –rf pol_*
rm xplico.db
cd /opt/xplico/script/db/sqlite2
./create_xplcio.db.sh

Con XI se crea solo un caso y dentro del caso puede a ver una cesión. Al correr DeMa (decodificador maestro);

/opt/xplico/script/sqlite_demo.sh

Copia todos los archivos pcap (en cualquier momento, incluso sobre una base diaria) en este directorio (los nombres de los archivos deben estar en orden alfabético en el momento de la captura).

/opt/xplico/pol_1/new/

Con la base de datos en SQLite la decodificación es lenta. En CLI tiene una mayor velocidad, pero los datos extraídos son más difíciles de leer y ver.

INSTALACIÓN DE XPLICO EN UBUNTU.

Antes de continuar con la instalación de Xplico es necesario instalar algunos otros programas que son necesarios para la configuración y el manejo del programa.

Apache es uno de estos programas ya que es indispensable para el buen funcionamiento del sistema Xplico.

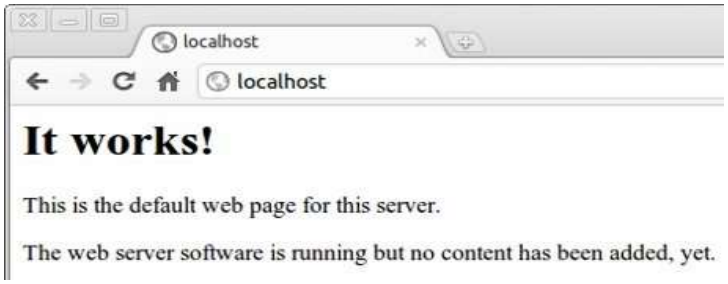
Instalación de Apache 2.

Para instalar **Apache2** en **Ubuntu11.10** tenemos que abrir una terminal tecleando la combinación de teclas *CTRL + ALT + T* o en el buscador del **SO** escribimos "terminal", para la instalación de **Apache2** tenemos que estar registrados o bien tener permisos de **ROOT**.

Una vez abierta la terminal tecleamos el siguiente comando:

sudo apt-get install apache2

Con este comando instalaremos **Apache2** junto con los módulos y librerías básicos. Una vez finalizada la instalación puedes comprobar su funcionamiento colocando en el navegador (cualquiera que tenga instalado en su equipo) la siguiente dirección http://localhost/ *o* http://127.0.1.1.



6-5 Página para mostrar que está funcionando Apache.

Los parámetros más importantes que se tienen que tener en cuenta para el funcionamiento de Apche2 son los siguientes.

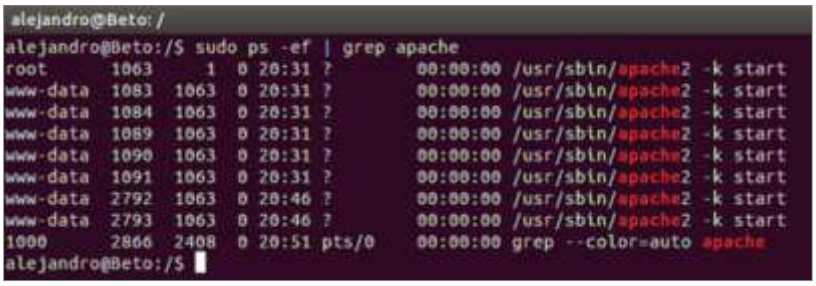
Para iniciar el servidor Apache tecleamos el comando:

sudo /etc/init.d/apache2 start

Para detener el servidor Apache tecleamos el comando:

sudo /etc/init.d/apache2 stop

Para comprobar que el servidor apache esta iniciado, comprobamos los procesos que se están ejecutando, para ello usamos el comando "*ps –ef*", pero para especificar los procesos activos de apache tecleamos: *ps –ef* | *grep apache*.



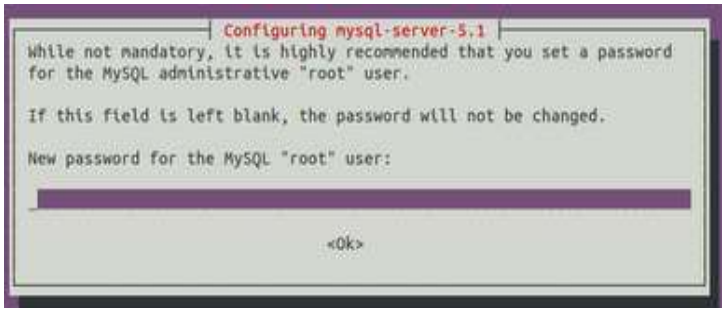
6-6 Procesos activos de apache.

Si queremos colocar una página web en nuestro servidor, tenemos que ir a la carpeta raíz del servidor que es */var/www/*, y allí colocaremos la página que queremos.

Para ver las bases de datos también requerimos la instalación de **MySQL**, para la instalación tecleamos los siguientes coma24ndos en una terminal.

sudo apt-get install mysql-server

Preguntará en el proceso por la contraseña que queremos asignar al acceso a las bases de datos.



6-7 Crear un password para poder acceder a MySQL.

Instalando PHP5

Por último y no por eso menos importante, se va a instalar PHP. Tecleamos en una terminal el siguiente comando:

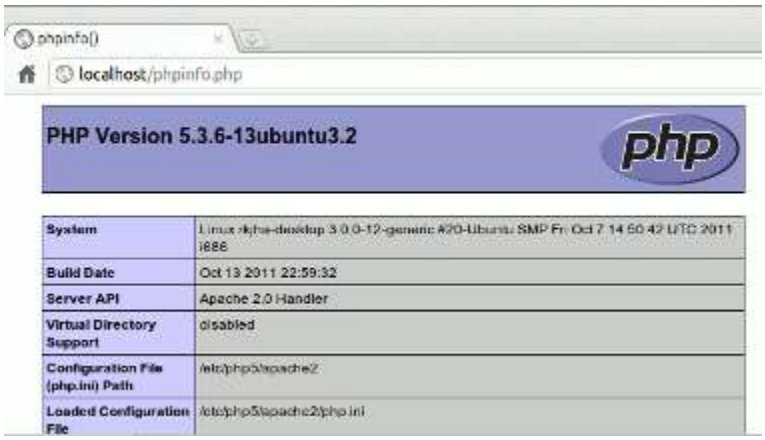
sudo apt-get install php5 libapache2-mod-php5 php5-mysql

Para comprobar el correcto funcionamiento del PHP, crea un archivo de prueba que lo guardaremos en la dirección /var/www llamándolo test.php escribiendo lo siguiente:

<?phpprint_r (phpinfo()); ?>

Tras ello, reinicia Apache2; no sin antes compilar el archivo y comprobar que está correctamente escrito:

Finalmente para comprobar que se visualiza correctamente el archivo ponemos en el navegador http://localhost/test.php, aparecerá una ventana como la siguiente:



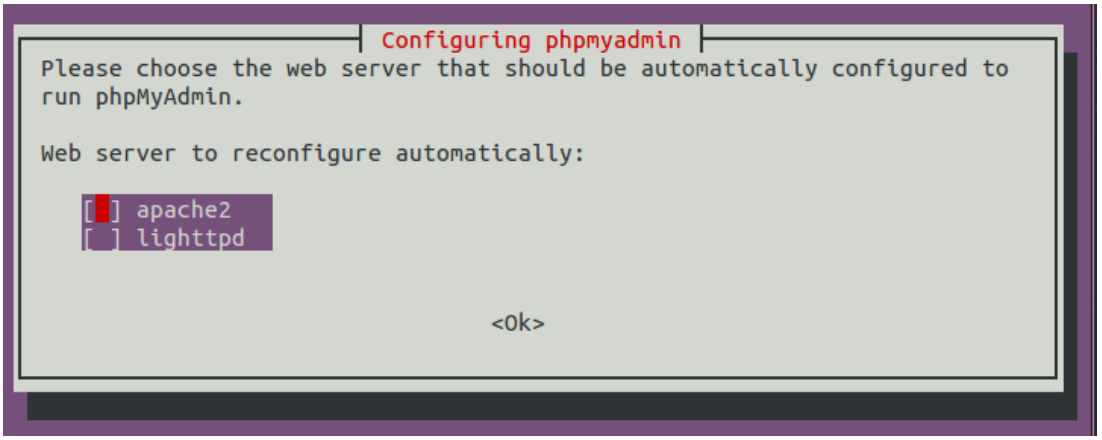
6-8 Resultado de ejecutar el mini programa <?phpprint_r(phpinfo()); ?>.

Instalando phpmyadmin

Para instalar el servidor de PHP tecleamos en la consola.

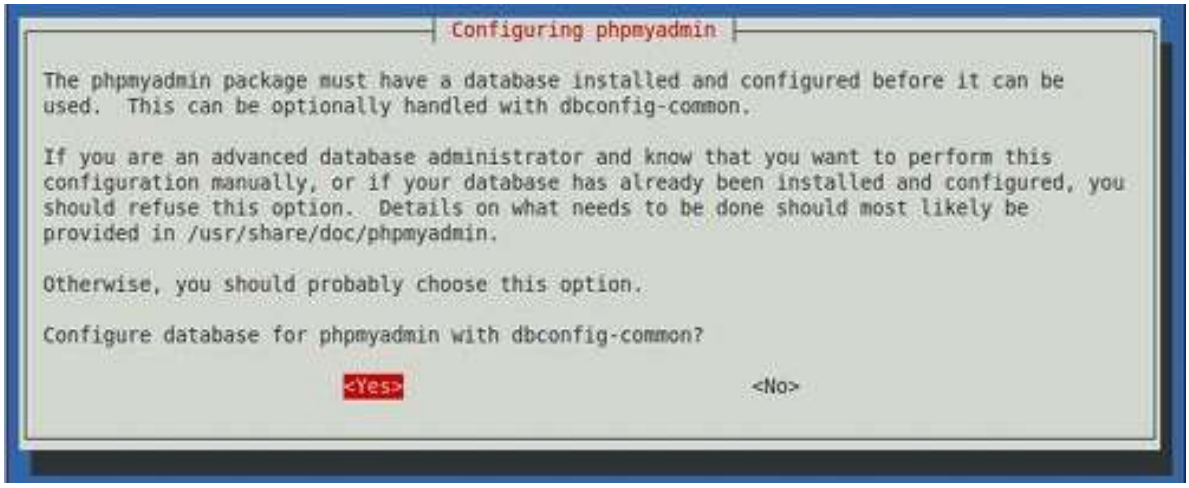
sudo apt-get install phpmyadmin

En el transcurso de la instalación veremos una ventana parecida a la siguiente:



6-9 Tipo de servidor que queremos instalar.

Esta nos dirá que elijamos el servicio web que debería ser automáticamente configurado para comenzar phpMyAdmin.



6-10 Mensaje para confirmar si tenemos instalada una base de datos.

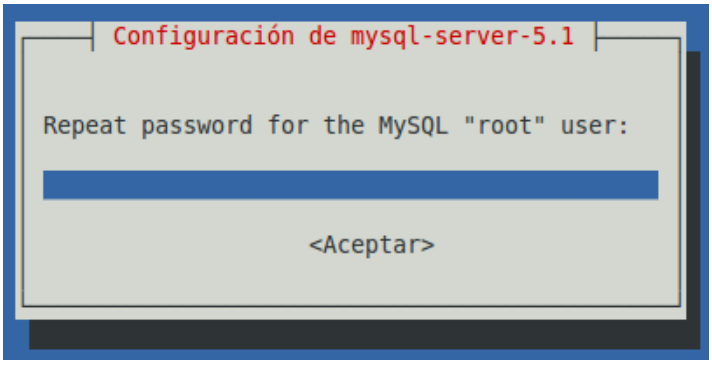
En el siguiente cuadro de dialogo nos pedirá confirmar que; *el paquete phpmyadmin necesita tener una base de datos instalada y configurada para poder usada.*

Si es un administrador avanzado de bases de daos y si quiere realizar esta configuración manual, o si su base de datos esta ya estaba configurada e instalada, debería rechazar esta opción. Los detalles sobre lo que hay que hacer probablemente está en el link /usr/share/doc/phpmyadmin.

De otra manera, deberías probablemente cambiar esta opción.

Al final nos pedirá confirmar lo que queremos realizar.

¿Configurara la base de datos para phpmyadmin con dbconfig-common?



6-11 Petición de contraseña.

Por ultimo nos pedirá una contraseña para la base de datos y su confirmación.

Una vez terminada la instalación podrás comprobar que esta correcto accediendo a http://localhost/phpmyadmin con los datos que introdujiste durante la instalación.

6-12 Ventana de registro de phpmyadmin

Instalación de Xplico

Hay que tomar en cuenta que la instalación de Xplico se lleva de la misma manera en sistemas UBUNTU de 32 y 64 bits así como en las versiones del servidor de 32 y 64 bits.

Si usas **UBUNTU** 11.10 o superior; entonces puede usar los repositorios. Con el siguiente comando agregamos a él SO los repositorios de Xplico.

sudo bash –c 'echo "deb http://repo.Xplico.org/ $(lsb_release –s -c) main" >> /etc/apt/sources.list'

Para confirmar que se agregó correctamente a los repositorios de **UBUNTU** tecleamos el comando (claro pueden usar otro editor como el *nano, en este caso usamos el editor gedit*):

sudo gedit /etc/apt/sources.list

Para continuar con la instalación colocamos los siguientes comandos:

sudo apt-key adv –keyserver keyserver.ubuntu.com --recv-keys 791C25CE

sudo apt-get update

sudo apt-get install xplico

Después de esto tenemos que cambiar los puertos de acceso de **Apache**, en el archivo /etc/apache2/ports:

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default

# xplico Host ports
NameVirtualHost *:9876
Listen 9876

Listen 80
<IfModule ssl_module>
        Listen 443
</ifModule>
<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
```

Para ello tenemos que editar el archivo con la siguiente instrucción:

sudo gedit /etc/apache2/ports.conf

Si hemos realizado bien todos los pasos anteriores podremos colocar en el explorador la dirección IP de nuestra maquina (ejemplo: http://192.168.1.73:9876 esta dirección se puede conseguir viendo las propiedades del dispositivo de red) y aparecerá la ventana de inicio de **Xplico**. Con esto sabemos que hemos realizado bien nuestra instalación.

Instalar la interfaz de Xplico

La interfaz de Xplico está desarrollada en **PHP** y está basada en el marco de **Cake PHP**. Esta interfaz puede usar la base de datos **SQLite** o **MySQL**, por el momento solo usaremos SQL terminado y probado en el decodificador de **Xplico**. La base de datos de **MySQL** se puede obtener de **iSerm**.

Navegando.

Habilita el proxy en **Firefox**. El proxy IP para maquinas donde tiene instalado **Xplico** y los puertos son 80 o 9876 (el puerto **Apache** se define en el archivo de configuración). El **URL** para ver la interfaz de **Xplico** es: http://IP:port. Si usa el nombre de la maquina es posible que no pueda entrar a la interfaz Web.

***NOTA**: Cuanto reinicies tu equipo y no se pueda iniciar Xplico correctamente y no se presente la página de*

bienvenida comprueba que APACHE este iniciado correctamente y en una terminal teclea el comando **sudo /etc/init.d/xplico start** *esto iniciara la aplicación de Xplico en el equipo.*

Usuarios predeterminados.

Para poder registrarse en el sistema tenemos la opción de registrarnos como User o Administrador.

El user name y el password son:

- user name: ***xplico***
- password: ***xplico***

El administrador es:

- user name: ***admin***
- password: ***xplico***

Usando la interfaz Web

En esta interfaz es posible crear nuevos casos, introducir nuevos archivos capturados, ver todos los datos extraídos para decodificar.

Primero tenemos que registrarnos:

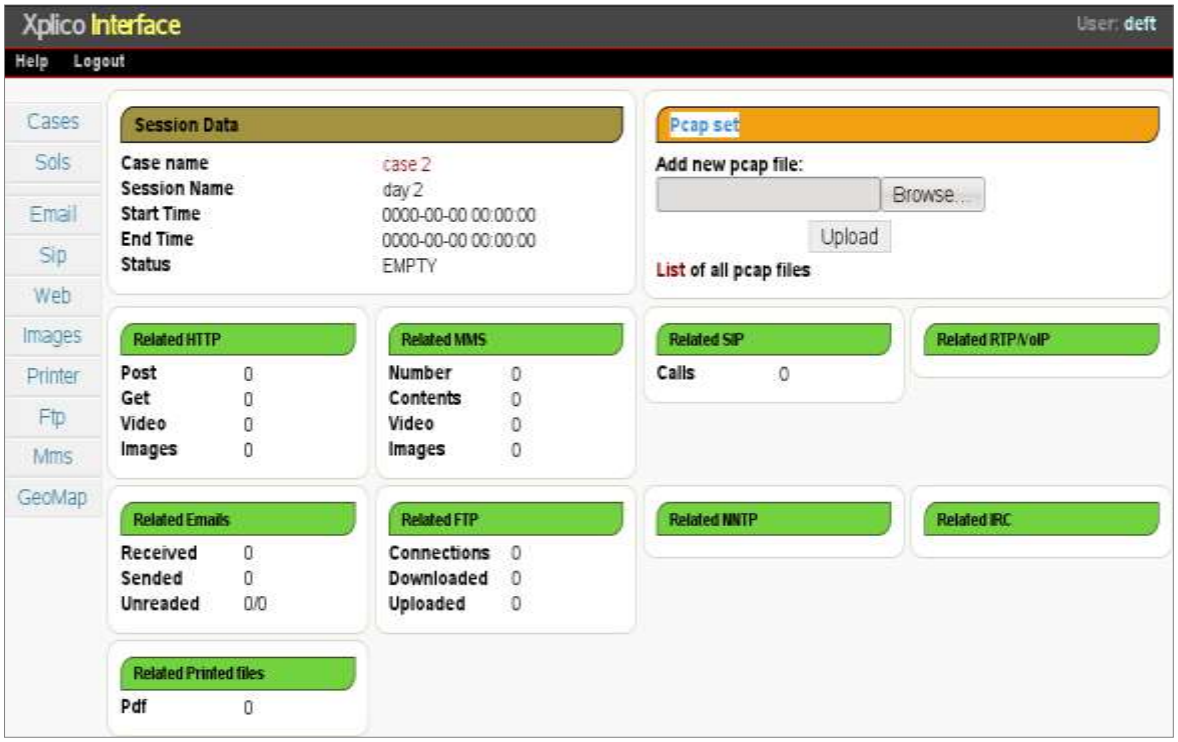
6-13 Pantalla de bienvenida de Xplico.

Los usuarios para registrarse ya se mencionaron en la parte superior.

Capturando archivos

Selecciona la sesión dentro del sumario de la página de los datos decodificados en dicha

sesión.



6-14 Listado de los archivos decodificados en el archivo .pcap

En cada sesión podemos introducir uno o más archivos capturados. Esto puede ser realizado del "conjunto **pcap**".

6-15 Ventana para agregar un archivo .pcap

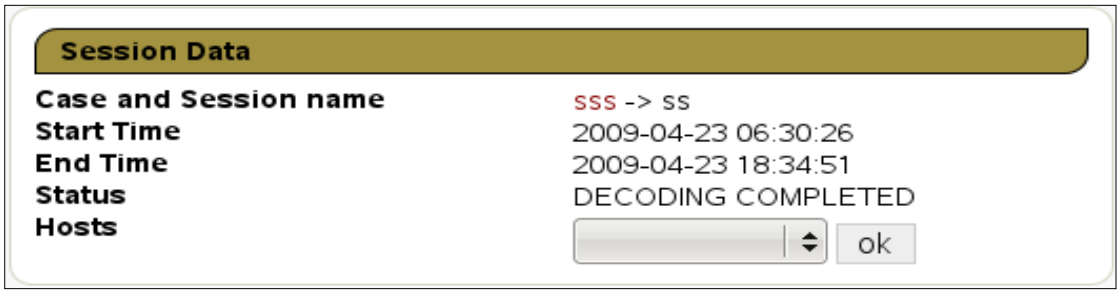
Una vez que encontramos el archivo que buscamos le damos click en el botón Upload para cargar el archivo que hemos seleccionado.

Da click en la lista para obtener una lista entera de los datos.

In "*Session Data*" podemos reportar el nombre del caso y la sesión, el tiempo de

comienzo y de fin.

La “Session Data” podemos solo seleccionar el host correcto y ver los datos de dicho host.



6-16 Informe del tiempo que tarda en decodificar el archivo.

Casos

6-17 Crear nuevos casos.

En **Xplico** los casos coinciden con el punto de escucha (los puntos capturados en la red) esto se debe a que el sistema **Xplico** trata de correlacionar los datos extraídos, a:

- Emular la cache del navegador
- Reconstruye archivos P2P (descargados en los diferentes días)
- Reconstruye archivos descargados con herramientas similares a ***Down Them All***
- Y así sucesivamente

En todos los casos se puede definir;

- Un nombre (sin repetirlo)
- La fuente de los datos, si los archivos provienen de la red.
- Una referencia externa es opcional. Esta referencia puede ayudar para localizar los repositorios del nuevo caso.
- En este punto podemos listar todos los casos creados.

6-18 Ventana de listado de casos.

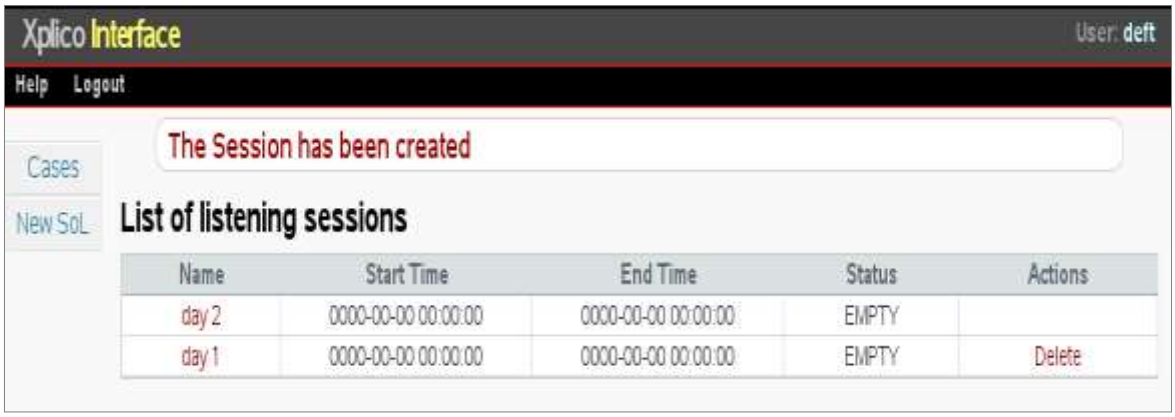
Las sesiones

Un caso se compone por una o más sesiones, para seleccionar un caso podemos entrar en la página de sesiones. En **Xplico** cada sesión contiene la arquitectura de los datos especificados en un intervalo de tiempo, los intervalos de tiempo en cada sesión **deben ser disjuntos** y cada comienzo de tiempo de una sesión debe ser mayor o igual a la hora de finalizar la sesión anterior.

Para crear una nueva sesión dentro de un caso podemos dar click en el botón "*Newsol*". La sesión se define solo con el nombre: *sesión name.*

6-19 Crear una nueva sesión dentro de un caso.

Como se ha mencionado, todos los casos pueden tener más de una sesión.

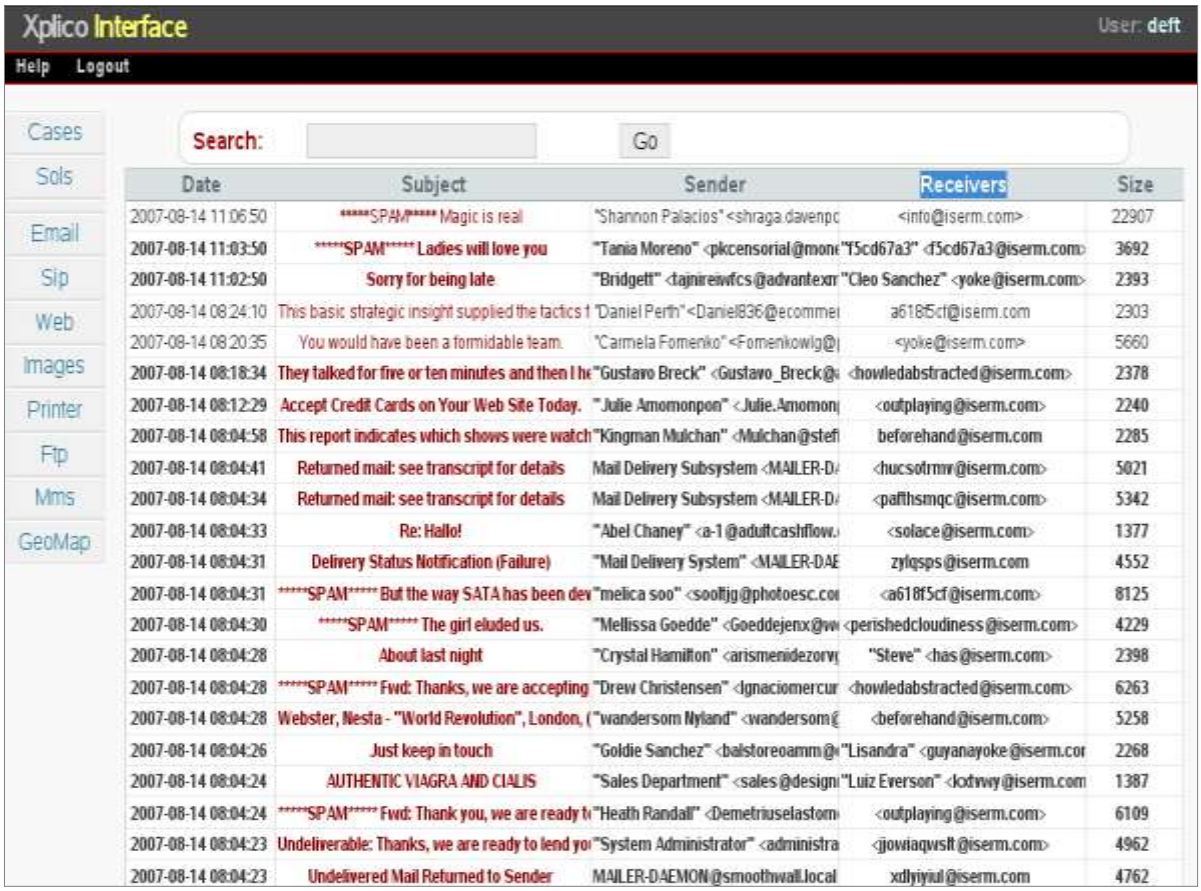


6-20 Listado de las sesiones que se encuentran en el sistema.

Captura en tiempo real.

Si necesita crear un caso de captura en vivo puede seleccionar la interfaz de red y comenzar/para la adquisición, en la página se *Session* de XI.

Email



6-21 Lista de archivos dentro del archivo .pcap

La página de correos presenta una lista de todos los emails enviados y recibidos.

Con:

- El tiempo de envió
- El asunto
- El remitente
- Los reportes enviados en *bcc*
- El tamaño del correo electrónico (con lo adjunto incluido)

La búsqueda le permite encontrar emails con asunto, reportes y remitente. Seleccionando uno de los correos puede observar dicho evento si es en *HTML* y contiene archivos adjuntos.

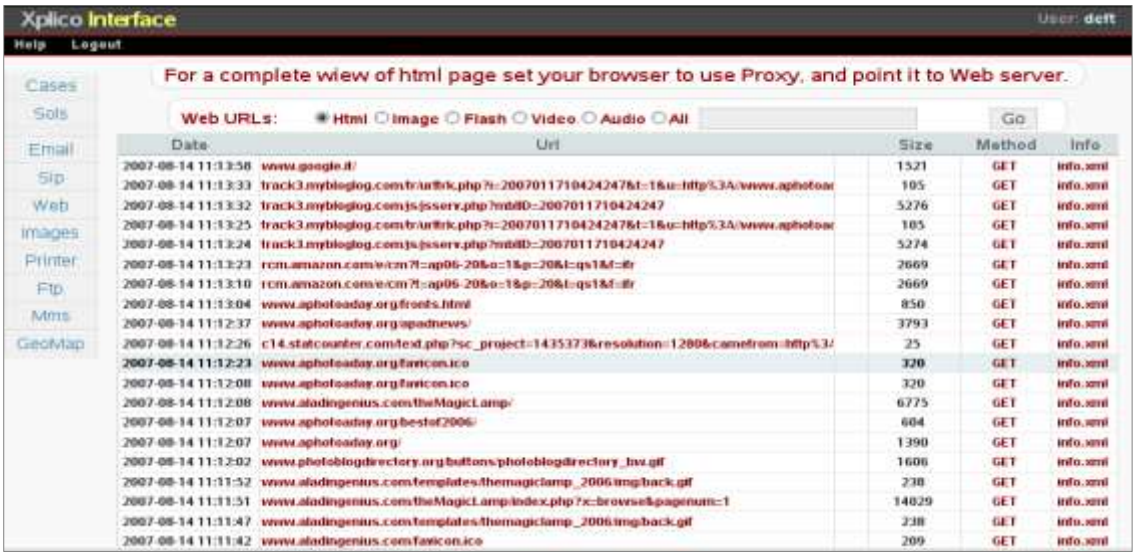
6-22 Muestra de un E-mail decodificado.

En cada email puede obtener el **PCAP** con solo seguir los contenidos. Para hacer eso tenemos que apuntar con el ratón en la línea de información y haga click en el enlace pcap.

6-23 Enlace del pcap

Web

Las entradas en el menú Web pueden ver todos los HTTP contenidos en las sesiones. Puede seleccionar el remitente y contenido.



6-24 Selección de páginas HTML

Da click en el link para abrir la página, que en cada sistema Xplico, puede reconstruir todas las paginas URL. Contenidos en decodificaciones pcap. El sistema Xplico simula una cache original del navegador, por supuesto si el archivo pcap contiene los datos para simular la cache. Todo funciona si, y solo si el proxy es deshabilitado en **Firefox** y en este punto el servidor debe estar corriendo en **Xplico** System.

Además, en cada contenido se puede examinar el remitente en el encabezado, del encabezado de respuesta y el cuerpo al hacer click en el enlace. Es posible archivar los pcap en el interior del flujo que transporta el contenido.

6-25 Muestra del remitente y el destinatario.

Si el contenido es un video (en formato flv) puede verlo directamente, dando click en el URL.

6-26 Reproducción de videos en Xplico.

Imágenes

Para obtener una visión general de todas las imágenes transportadas en protocolo HTTP puede entrar al menú de imágenes.

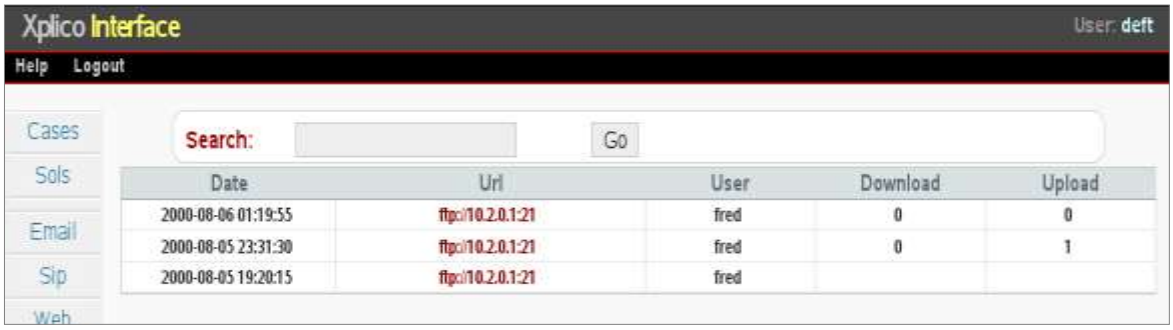
6-27 Menú para seleccionar el tipo de peso de la imagen.

Impresiones

En esta parte podemos ver una lista de todos los documentos en la impresora de red, este usa el “Printer Command Language”. Todos los documentos son convertidos en formato pdf.

FTP y TFTP

Las paginas FTP y TFTP son similares.



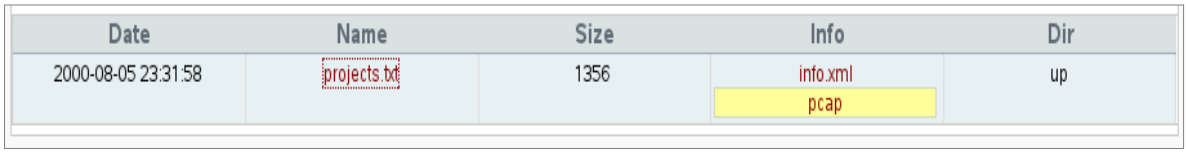
6-28 Lista de archivos descargados.

En el inicio de la página se puede ver la lista del contenido en un servidor ftp / tftp, cada uno corresponde al número de archivos descargados y subidos.

6-29 Muestra de un FTP y la fecha y tipo de archivo que se descargó.

Para todos los servidores, dando click en el link, puede ver la información del servidor, nombre de usuario, password, comandos, archivos descargados y subidos.

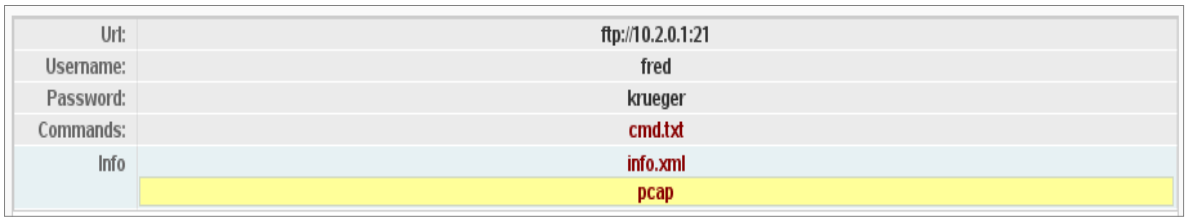
Para cada archivo puede tener el correspondiente archivo pcap que contiene solo los paquetes del archivo.



Date	Name	Size	Info	Dir
2000-08-05 23:31:58	projects.txt	1356	info.xml pcap	up

6-30 Selección del archivo .pcap de cada archivo.

También puede examinar todos los comandos intercambiados con el servidor.

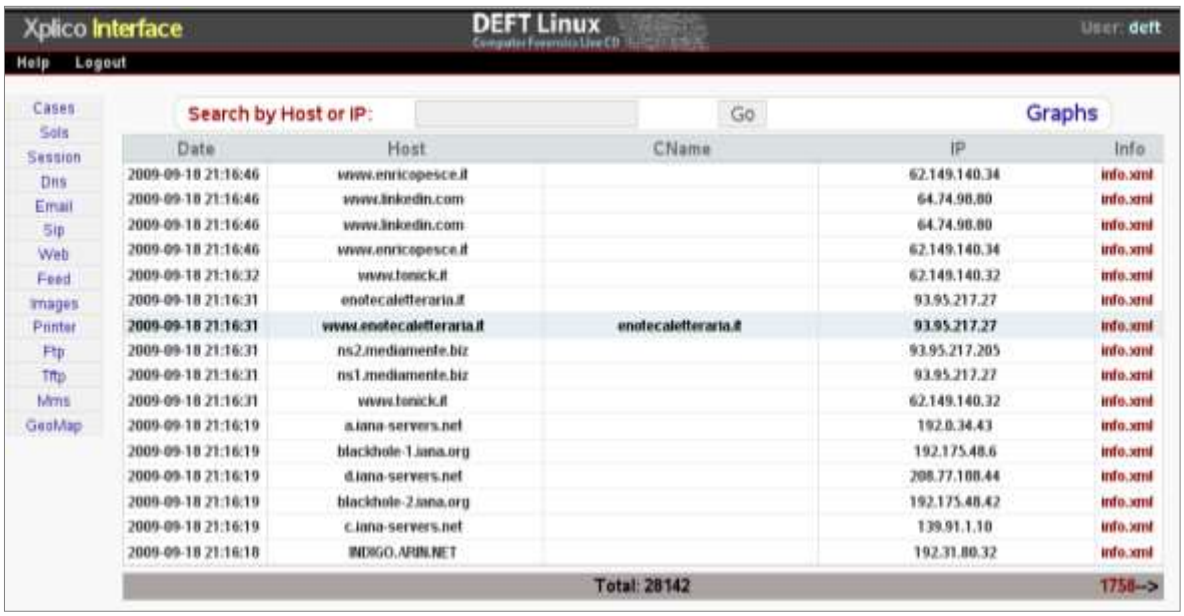


Url:	ftp://10.2.0.1:21
Username:	fred
Password:	krueger
Commands:	cmd.txt
Info	info.xml
	pcap

6-31 Selección del archivo .pcap de un FTP.

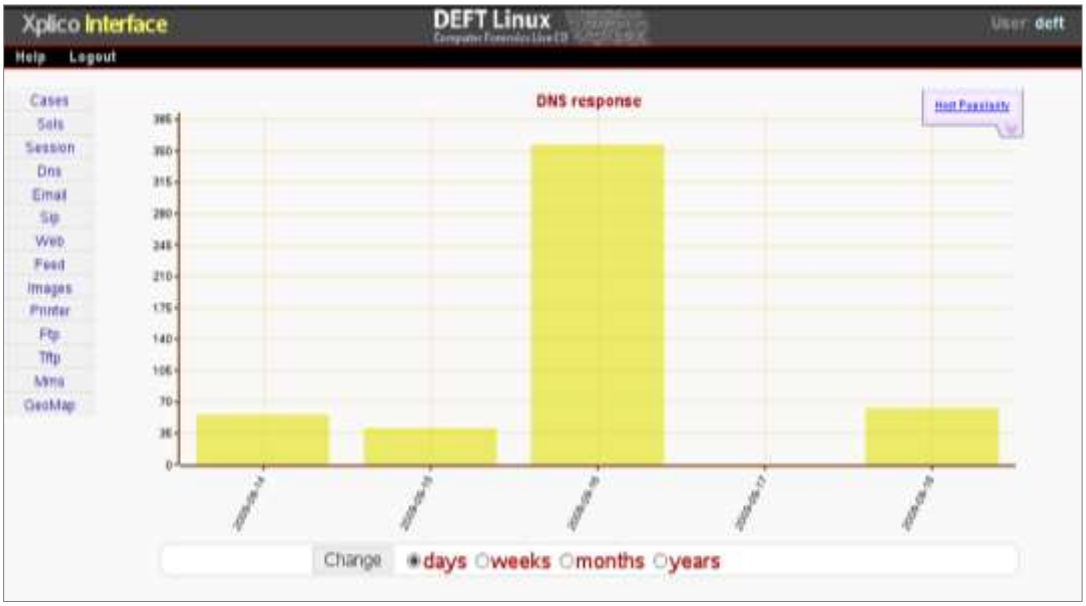
DNS

Las paginas DNS despliegan todos los DNS contestadas sin errores, listando el Canonical name si este existe y la primera IP que responde. Otra vez puede investigar el host o la IP.

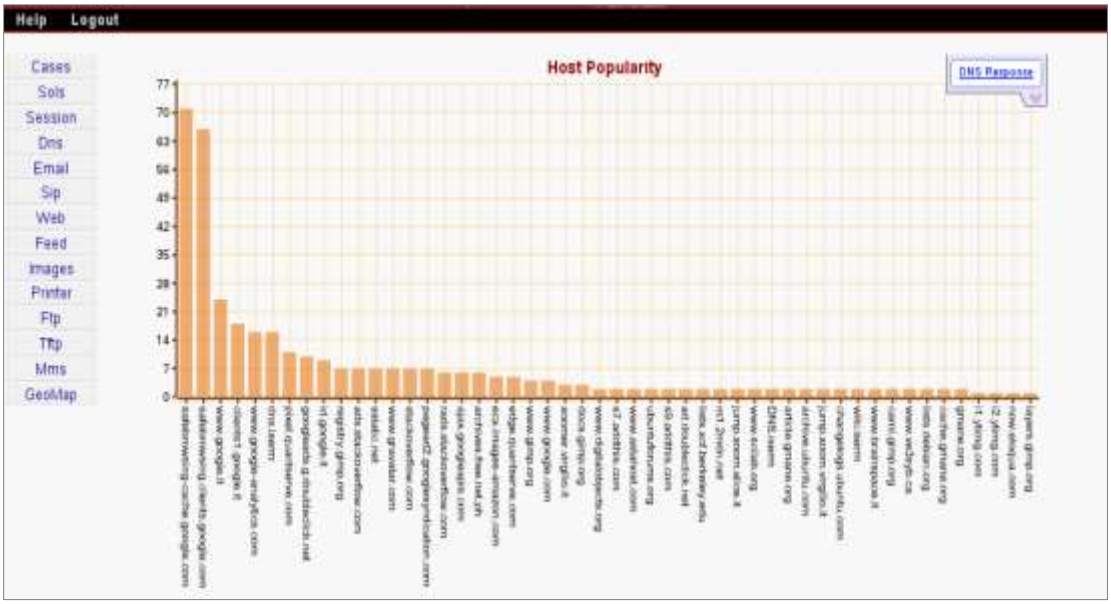


6-32 Estadísticas de los DNS más usados.

A partir de los gráficos de enlace en la página principal de DNS es posible representar con el gráfico de las estadísticas de las respuestas DNS, o ver el gráfico de la serie de los 50 más populares. Host más popular.



6-33 Muestra grafica de del uso de los DNS.



6-34 Grafico del HOST más popular.

MMS

Si los mensajes MMS (Servicio Multimedia de Mensajes) son transportados por protocolo

HTTP la decodificación en Xplico puede descomponer los mensajes MMS dentro del contenido, en texto, video e imágenes.

Al inicio de la página de reportes MMS muestra los MMS decodificados.

6-35 Lista de mensajes decodificados.

Da click en el link para poder ver el contenido de los mensajes.

6-36 Mensajes decodificados.

Si tiene mensajes MMS en binario (raw), puede decodificar los con la herramienta mmsdec.

Conclusiones.

Se logró comprender, estudiar y ver el funcionamiento de sistema Xplico, manipularlo y usarlo en un sistema instalado en un equipo.

Se instaló el sistema operativo en un equipo y se puso en marcha Xplico. Se instalaron todos los componentes y programas para que funcionara y se logró hacerlo funcionar en el equipo instalado.

En la investigación se menciona cuáles son las principales características para realizar una política de seguridad, no se profundiza en ello porque no es el objetivo de la tesis. Pero se da una idea general de los puntos más importantes a trata.

Se mencionó la instalación de un Firewall que es FreeBSD y su homónimo en Ubuntu, este está integrado en el sistema operativo así que no tiene un nombre específico.

Se completó con la traducción de la documentación que se encuentra en la página oficial de Xplico y de ahí se menciona el funcionamiento de Xplico y la forma de instalarlo.

Por su distribución libre, es económico para implementarlo en empresas pequeñas y con una infra estructura poco robusta.

La ventaja más importante de Xplico es su facilidad de instalación, al menos para personas que tengan un poco de conocimiento de cómo se instalan programas en UBUNTU, pero independientemente de ese conocimiento, la documentación encontrada en la página oficial, es muy buena y ayuda mucho para comprender como podemos instalar nuestra herramienta.

Una vez instalado el programa tiene un ambiente bastante amigable; fácil de utilizar y de comprender, su manejo requiere de un poco de estudio pero realmente se puede usar perfectamente bien. Aunque tiene un ambiente en línea de comandos, es más fácil usarlo directamente en el entorno grafico; vía web, ya que es más intuitivo y más fácil de usar.

Aunque en un principio se pensó que sería conveniente tener un equipo dedicado para el

Firewall, he encontrado que UBUNTU tiene un Firewall propio. Este es realmente potente y no deja nada que desear ante FreeBSD ya que también está basado en lo que se llama IPTables; así que si se escoge uno u otro no se tendrá mayor problema en comprobar su efectividad. La ventaja es que no se tiene que administrar dos diferentes servidores, si no que todo se tendría ya en un solo equipo.

Esto es más conveniente si hablamos de personas con pocos recursos (por ejemplo en mi caso que solo tengo un equipo portátil) para poder usar dos equipos, donde; uno estará dedicado al Firewall y otro a UBUNTU donde estará instalado Xplico; con el Firewall ya integrado en UBUNTU se tiene la comodidad de poder tener un solo equipo dedicado a las dos tareas.

Esto también se puede realizar con virtualización de los sistemas ya que en la página oficial se puede descargar una máquina virtual que ya tiene todo lo necesario instalado; pero en muchos casos se tiene que tener equipos con las características necesarias para poder realizar dichas operación; en muchos casos los equipos no están adaptados para la virtualización.

Por eso se tiene que hacer un estudio de que marcas de computadoras permiten la instalación de máquinas virtuales.

En la página oficial de Xplico ya se encuentran disponibles para descargar las máquinas virtuales. Esto es más práctico; ya que si no se sabe cómo hacer una máquina virtual se ahorra el tiempo de investigación para la implementación.

Esto también es conveniente si no se tiene el conocimiento para usar sistemas operativos basados en UNIX®; o bien, no se quiere cambiar de sistema operativo, ya que VMWare da la facilidad de tener la máquina virtual instalada en Windows.

En cualquier caso si se necesita un equipo dedicado a este tipo de tareas. Ya que no se puede tener cualquier equipo de uso diario para esta función, si es necesario que el equipo al que se le asigne este sistema, sea únicamente para este uso; y que ningún otra aplicación interfiera con su funcionamiento y rendimiento.

Con lo escrito aquí es suficiente para poder implementar todo un sistema de sniffer para cualquier red. Solo depende de la persona que utilice esta información, el cómo administre su red y que tipo de firewall use para administrarla.

El análisis en la computación forense aún tiene poco uso en nuestro país pero con un poco más de estudio y capacitación de diferentes personas se puede lograr generar un buen desarrollo en este tipo de programas y aplicarlos correctamente en empresas. La mayor parte del uso de programas orientados a la recopilación de datos computacionales, ha sido en un sentido mal orientado, ya que en su mayoría se utilizan para obtener

beneficios para las personas; con esto me refiero a obtener claves WAB para acceder a las redes inalámbricas de algún lugar, obtener las claves de las cuentas de las personas entre otras tantas formas de obtener información.

El software libre también puede ser un buen aliado ya que el código que está disponible en las diferentes paginas oficiales de los diferentes proyectos puede tenerse una base para lograr mejores programas o incluso crear nuevos y probarlos en dichos sistemas operativos.

En la india se ha tenido un gran avance en cuestión de Software ya que la licencia libre se maneja para crear más proyectos y generar mejor conocimiento entre los ingenieros de sistemas. También da la oportunidad de generar sus propios programas sin tener que pagar grandes licencias como sucede en el Software de licencia.

Entre más popular sea el uso de sistemas operativos y programas de licencia libre entre los estudiantes de ingeniería en sistemas o computación mejor será la auto-enseñanza y el impulso de los estudiantes para crear proyectos nuevos y generar programas eficaces robustos y bien diseñados.

Existen muchos estudiantes que gustan de la programación y el estudio autodidacta, es ahí donde se tiene que aprovechar el potencial de dichas personas para generar proyectos bien intencionados y no dirigidos a diferentes fines mal intencionados.

BIBLIOGRAFIA

1. **Jacobo Pavón Puertas.** (2001). *Creación de un portal con PHP y MySQL*. 4ªEdición. México, ALFAOMEGA
2. **Perpiña Días, Antonio.** (2009) *GNU Fácil, UBUNTU.* 3ª Edición. República Dominicana. Impresos GAMMA.
3. **Víctor Van Reijswoud y Arjan de Jager.** (2008) *Free and open sources of tware for development.* Milan Italy Volumen 5 Polimétrica
4. **Elizabeth D. Zwicky; Simon Cooper y D. Brent Chapman.** (2000)**.** *Building internet firewalls, Internet and web security;* 2nd Edition. U.S.A. O´reilly.
5. **William R. Cheswick; Steven M, Bellovin y Aviel D. Rubin.** (2003) *Firewall and internet security, repelling the Wily Hacker.U.S.A.* 2nd Edition. Rubin.
6. **Brian Komar; Ronald Beekelaar y Joern Wettern.** (2003) *Firewalls for dummies. 2nd Edition*, Nueva York. Wiley Publishing, Ing.
7. **Enzo augusto Marchionni.** (2011) *Administración de servidores, herramientas, consejos y procedimientos para el profesional.* 1ª Edicion. Buenos Aires. Manuales USERS.
8. **ArCER Coordinación de emergencia en Redes Teleinformáticas.** *Manual de Seguridad en Redes*. Argentina. Secretaria de la Fundación Pública.
9. **Javier Areitio.** (2008) *Seguridad de la información, redes, informática y sistemas de información*, España. Paraninfo.
10. **Luis Duran.** (2000) *Sistemas Operativos*, Barcelona. marcombo.
11. **P. Martínez Cobo; M. Cabello Requena y J.C. Díaz Martín.** (1997) *Sistemas Operativos teoría y práctica.* España. Díaz de Santos.
12. **David Martínez Perales.** (2001) *UNIX® a base de ejemplos. 3ª Edición. España. Lulu.com*
13. **Peter J. Arroyo.** (2008)*Introducción a la PC.* España. Lulu.com
14. **M. Merino Egea; D. Corbella Ribes; R. Ocaña López; et al.** (1998)*Diseño asistido por ordenador con Imagineer*; España. Díaz de Santos.
15. **Pedro Muños Rodríguez.** (2010) *Mantenimiento de portales de información.* España. Visión Libros.
16. **José M. Barceló; Jordi Íñigo Griega; Silvia Llorente Viejo; et al.** (2008)*Protocolos y aplicaciones Internet.* Barcelona. UOC.
17. **Jordi Íñigo Griega; José María Barceló; LlorenÇ Cerda Alabern; et al.** (2008)*Estructura de redes de computadores.* Barcelona. UOC.
18. **Ramón Machado Suárez.** (2010) *Guía de linux edu para secundaria.* Madrid. Liber Factory.
19. **Jhon Mullins; Randy Komisar.** (2010) *Mejorando el modelo de negocio, como transformar su modelo de negocio en un Plan B viable.* Barcelona. PROFIT.
20. **México, en "Top 5" de ataques cibernéticos al AL.** *El economista.* 7 Mayo, 2012 – 17:06. Tecno ciencia, seguridad e informática.
21. **México, uno de los países con mayor número de ataques cibernéticos.** *Publimetro.*28 Enero 2014.

22. **Ángel Cobo; Patricia Gómez; Daniel Pérez; et al;** (2005) *PHP y MySQL Tecnologías para el desarrollo de aplicaciones web. España.* Ediciones Días de Santos.
23. **Deitel, Harvey M. y Deitel, Paul J;** (2004) *Como programar en C/C++ y java. México.* Ediciones Prentice Hall.
24. **Franklin, Beedle y associates;** (2004) *Python programming: an introduction to computer science. U.S.A.* Franklin, Beedls & associates, Incorporated.
25. **Innovacion y cualificación;** (2001) *Internet JavaScript. España.* Innovacion y cualificación, S.L.
26. **Brian W. Kernigan Dennis y M. Ritchie;** *(1991) El lenguaje de programación C. México;* Pearson Education.
27. **A. P. Godse y D. A. Godse;** (2008) *C programming y data structures. Primera edicion. India.* Technical Publications Pune.
28. **David Sawyer McFarland.** (2008). *JavaScript & jQuery the missing manual, The book that should have been in the box*. Second Edition. U.S.A, O´REILLY.Media.
29. **Mark Lutz.** (2013). *Learning Python*.5th Edition. U.S.A, O´REILLY Media.
30. **Benjamín Ramos Álvarez, Arturo Ribagorda Garnacho.** (2004). *Avances en criptología y seguridad de la información*. España, Diaz de Santos.

REFERENCIAS DE INTERNET

1. **Open Source Network Forensic Analysis Tool (NFAT).** (2007 – 2014) Documentation: Xplico Wiki. Disponible en http://www.xplico.org/docs
2. **Gerhard Eschelbeck.** (2012) Informe de amenazas de seguridad; 2012; En *SOPHOS*. Consultado el 15 de Agosto de 2013. Disponible en http://www.sophos.com/es-es/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf
3. **MAX MIND;** (2013) GeoIP database and web service; En *MAX MIND*. Consultado el 20 de Mayo de 2013. Disponible en http://www.maxmind.com/en/geolocation_landing
4. **FreeBSD.** (2013)Pagina de descarga de FreeBSD. En *FreeBSD*. Consultado el 23 de Abril de 2013. Disponible en http://www.freebsd.org/doc/
5. **The FreeBSD Documentation proyect;** (1995 – 2010); Manual de FreeBSD. En Manual de FreeBSD. Consultado el 6 de Marzo de 2013.http://www.freebsd.org/doc/es_ES.ISO8859-1/books/handbook/
6. **UBUNTU LIVE;** (2011); Instalar Ubuntu 11.10 Oneiric Ocelot paso a paso. En Ubuntu Life #WoldRevolution. Consultado el 18 Abril de 2013http://ubuntulife.wordpress.com/2011/10/14/instalar-ubuntu-11-10-oneiric-ocelot-paso-a-paso/
7. **TCPDump where information is found;** 2007; Welcome to TCPDump. Consultado el 6 de Abril de 2013.http://www.tcpdump.com/
8. **ADSL FAQS;**(2012); Como usar el comando tcpdump en Linux Ubuntu, Debian, Fedora. En ADSL FAQS. Consultado el 25 de Mayo de 2013http://www.adslfaqs.com.ar/como-usar-el-comando-tcpdump-en-linux/
9. **FreeBSD ;**(1995 – 2014). TCPDump. Disponible en FreeBSD The power to Server. Consultado el 29 de Septiembre de 2013. http://www.freebsd.org/cgi/man.cgi?query=tcpdump&sektion=1
10. **UBUNTU es**. (2013) Sobre Ubuntu. Disponible en Ubuntu.es. Consultado el 13 de Abril de 2013.http://www.ubuntu-es.org/
11. **MIT;** Education. Disponible en la página official del MIT. Consultado el 25 de Noviembre de 2013.http://web.mit.edu/education/
12. **Ammateos;** (2009). Intel 386. Disponible en Enprende Wiki. Consultado el 3 de Junio de 2013. http://www.emprendewiki.com/tiki-index.php?page=Intel+386
13. **Ubuntu Documentation;** Firewall. Disponible en Ubuntu Documentation. Consultado el 20 de Diciembre de 2013.https://help.ubuntu.com/lts/serverguide/firewall.html#other-firewall-toolsl

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

Termino	Definición
DNS	Es el encargado de traducir el nombre de dominio a una dirección IP.
FTP	Es un protocolo de transferencia de ficheros, se basa en un modelo cliente/servidor, y permite la transferencia tanto del servidor al cliente como del cliente al servidor. Uno de los objetivos principales de este protocolo consiste en permitir la interoperabilidad entre sistemas muy distintos, escondiendo los detalles de la estructura interna de los sistemas de ficheros locales y de la organización de los contenidos de los ficheros.
GNU/LINUX	GNU más conocido como Linux, es un sistema operativo, compatible UNIX®. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado: la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.
HTML	(Hyper Text Markup Language) Sistema de escritura que comprende etiquetas, siendo una etiqueta una instrucción contenida entre corchetes angulares.
Kernel	Programa que constituye el núcleo del sistema operativo. Tiene control de todo lo que ocurre en la computadora. En Linux está escrito mayormente en C y código de máquina y debe ser compilado por otro programa antes de ser utilizado.
MIT	Massachusetts Institute of Technology. La misión del MIT es crear estudiantes con conocimiento avanzado en la ciencia, tecnología y otras áreas con becas para una mejor nación. Alberga cinco escuelas: arquitectura y planificación, ingeniería, humanidades, arte y ciencia sociales. Más de 30 departamentos y programas, en educación el MIT cubren más de lo justo en ciencia y tecnología.
P2P	Forma de compartir archivos entre usuarios uno a uno directamente de internet.

PCAP Archivo comprimido que se obtiene de la captura del tráfico de la red por medio de un firewall.

PROMISCUO En informática se refiere a tarjetas (alámbricas e inalámbricas) que conectadas a una red permiten capturar todo el tráfico que circula por ellas.

ROOT En todos los sistemas UNIX® y derivados (lo mismo que Windows 200 o XP) existe un usuario privilegiado que tiene acceso a todos los recursos del ordenador y a todos los datos de los demás usuarios. A este usuario especial se le conoce con el nombre de súper usuario, administrador o simplemente root.

SNIFFER Un sniffer es un programa que capturar todos los datos que pasan a través de una tarjeta de red. Para ello se basa en un defecto del protocolo Ethernet. Ethernet normalmente manda los paquetes de datos a todas las estaciones de la red, entonces lo que hace el sniffer es poner la tarjeta en modo promiscuo (promiscuo usmode). El modo promiscuo significa que la tarjeta capturara todos los paquetes ethernet, aunque no vayan dirigidos a ella.

TFTP Para satisfacer las necesidades de transacciones simplificadas, se ha definido el TFTP, cuya última versión esta especificada en el estándar RFC 1350. Este protocolo está basado en datagramas, sólo proporcionan dos operaciones (leer y escribir ficheros) y no hay ningún tipo de identificación de usuario.

UBUNTU Sistema operativo de licencia Open Source. El más famoso y el más usado en el mundo por su estabilidad y su gran cantidad de seguidores.

UNIX® Sistema operativo multiusuario, multitarea, portable, con distintos intérpretes de comandos, multiprocesador, multicore, con compiladores propios, con entorno gráfico, etc. La institución está formada por un grupo de empresas punteras en tecnología, como HP IBM o SUN entre otras, que se encargan de otorgar estándares en distintas ramas de la informática.

URL (Universal Resource Locator) es una dirección específica de una página web. Las direcciones URL sirven para enviarse la información de la Web de forma compacta y nada ambigua: describen exactamente donde se encuentra la información. La URL es una dirección postal o un número de teléfono. Hay diferencias por el tipo de encabezamiento. Para describir recursos de hipermedia (http://), FTP Y Gopher (gopher:// y ftp://), grupos de debate (news://), etc.

x386 El Intel 80386 es un Microprocesador CISC con arquitectura x86. Durante su diseño se le llamó 'P3', debido a que era el prototipo de la tercera generación x86. Fue empleado como la unidad central de proceso de muchos ordenadores personales desde mediados de los años 80 hasta principios de los 90.

XPLICO Herramienta de análisis forense de red, cuyo objetivo es extraer del tráfico de red los datos. Fue realizado dentro de GNU y con scripts de licencia CC BY-NC-CA 3.0.

1 Er ANEXO

TCPDUM

TCPdump es una herramienta en línea de comandos de dominio público, cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado. Es posible ejecutarlo en modo promiscuo con lo que tendremos las cabeceras de los paquetes que viajan por la red.

Tanto en la captura como en la visualización de la información, es posible aplicar filtros por protocolos, puertos, direcciones fuente, direcciones destino, direcciones de red, así como realizar filtros con operadores (=, <, >, ≠).

TCPdump funciona en la mayoría de los sistemas operativos UNIX®: Linux, Solaris, BSD, Mac OS X, HP -UX y AIX entre otros.

En esos sistemas, TCPdump hace uso de la biblioteca ***libpcap*** para capturar los paquetes que circulan por la red. Tcpdump está instalado por default en FreeBSD. Pero para sistemas operativos que no lo tengan instalado a continuación se presentan los pasos a seguir para la instalación.

INSTALACIÓN DE TCPDUMP

Para descargar TCPdump tecleamos el siguiente comando en la consola:

apt-get install tcpdump

Para ver las dependencias de TCPdump tecleamos el siguiente comando en la consola:

apt-cache depends tcpdump

Esto nos mostrara todas las dependencias del comando como se muestra a continuación.

tcpdump

Depends: libc6
Depends: libpcap0.8
Depends: libssl1.0.0
Suggests: apparmor

Para ver la versión que se tiene instalada de TCPdump en el equipo tecleamos el siguiente comando.

apt-cache policy tcpdump

Nos mostrara una información parecida a la siguiente:

tcpdump:

Installed: 4.4.0-1ubuntu1
Candidate: 4.4.0-1ubuntu1
Version table:
*** 4.4.0-1ubuntu1 0
500 http://mx.archive.ubuntu.com/ubuntu/ saucy/main i386 Pakages
100 /var/liob/dpkg/status

Sintaxis

tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [-C file_size]
[-E algo:secret] [-F file] [-i interface] [-M secret]
[-r file] [-s snaplen] [-T type] [-w file]
[-W filecount] [-y datalinktype] [-Z user]
[expression]

Opciones

- -A: Imprime cada paquete en código ASCII
- -D: Imprime la lista de interfaces disponibles
- -n: No convierte las direcciones de salida
- -p: No utiliza el interfaz especificado en modo promiscuo
- -t: No imprime la hora de captura de cada trama
- -x: Imprime cada paquete en hexadecimal
- -X: Imprime cada paquete en hexadecimal y código ASCII
- -c count: Cierra el programa tras recibir ‘count’ paquetes
- -C después de escribir la captura de paquetes lo salva en un archivo, comprueba si el archivo está correctamente grande en file_size y, solo si, se cierra el archivo y se abre otro nuevo.
- -E algo: secret
- -F usa archivos de salida para filtrar las expresiones. Cualquier

expresión dada en la línea de comando es ignorada.

- -i interface: Escucha en el interfaz especificado
- -M secret
- -r lee los archivos de file. La salida estándar que se usa es "-".
- -s snaplen organice los bytes de cada paquete de la mejor manera, por default se organiza en 65535 bytes.
- -T forzar los paquetes seleccionados con expresión para ser interpretados especificado con type
- -w file: Guarda la salida en el archivo 'file'. Puede usarse después de la opción –r.
- -W se usa en conjunto con la opción –C. limita el número de archivos creados con un numero especifico.
- -y establece el tipo de enlace de datos para utilizar durante la captura de paquetes a data link type
- -Z dota de privilegios de administrador y cambia el ID de usuario.

Modificadores

Los modificadores también forman parte importante de en la elaboración de comandos para la captura de datos. Estos modificadores son:

! or **Not**

&& or **And**

|| or **Or**

Ejemplos

A continuación se presentan algunos ejemplos de cómo usar estos modificadores.

udp dst port not 53	UDP sin brincar el Puerto 53.
Host 10.0.0.1 && host 10.0.0.2	Trafico entre estos hosts.
tcp dst port 80 or 8080	Paquetes entre estos puertos TCP.

Aquí se presenta otros ejemplos de cómo se usar este comando.

[src|dst] host <host>	Comparar un host para la IP fuente, destino, o entre ellos.
ether [src|dst] host <ehost>	Comparar un host para la Ethernet fuente, destino, o entre ellos.
gateway host <host>	Comparar paquetes que usa el host para un Gateway
[src|dst] net <network>/<len>	Comparar por paquetes o de un lugar específico que está en la red.
[tcp|udp] [src|dst] port <port>	Comparar paquetes TCP o UDP enviados para/de él puerto.
[tcp|udp] [src|dst] portrange<p1>-<p2>	Comparar paquetes TCP o UDP para/de a un Puerto en el rango proporcionado
less <length>	Comparar paquetes menores que o igual a la longitud.
greater <length>	Comparar paquetes mayores que o iguales a la longitud.
(ether|IP|IP6) proto <protocol>	Comparar un protocolo Ethernet, IPv4, o IPv6
(ether|IP) broadcast	Comparar un broadcasts Ethernet or IPv4.
(ether|IP|IP6) multicast	Comparar multicasts Ethernet, IPv4, o IPv6.
type (mgt|ctl|data) [subtype <subtype>]	Comparar el protocolo 802.11 basándose en el tipo and opcionalmente el subtipo
vlan [<vlan>]	Comparar el protocolo 802.1Q, opcionalmente con un ID VLAN de la vlan
mpls [<label>]	Comparar paquetes MPLS, opcionalmente con un nivel a nivel.
<expr> <relop> <expr>	Comparar paquetes aparte en una expresión arbitraria.
tcpdump host sundown	Para imprimir todos los paquetes de llegada o salida después de la puesta de sol
tcpdump host helios and \(hot or ace\)	Para imprimir el tráfico entre helios y entre caliente o frio.
tcpdump IP host ace and not helios	Para imprimir todos los paquetes entre frio y cualquier caliente excepto helios.
tcpdump net ucb-ether	Para imprimir todo el tráfico entre el hosts locales y hosts a Berkeley
tcpdump 'gateway snup and (port ftp or ftp-date)'	Para imprimir todo el tráfico ftp a través del Gateway de internet snup: (nota que la expresión es citada para prevenir el Shell de (mis-) interpretando lo del paréntesis).
tcpdump IP and not net localnet	Para imprimir el tráfico de la Fuente no destinado a hosts locales (si su Gateway de otra red, esta cosa muestra nunca hacer esto sobre su red local).
Tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-fin) !=0 and not src and dst net localnet'	Para imprimir los paquetes de principio y fin (los paquetes SYN y FIN) de cada conversación TCP que envuelve a ningún host local.

Tcpdump 'tcp port 80 and (((IP[2:2] – ((IP[0]&0xf)<<2)) – ((tcp[tcp[12]&0xf0)>>2)) !=0)'	Para imprimir todos los paquetes IPv4 HTTP y del Puerto 80, es decir, imprimir solo paquetes que contengan datos, por ejemplo, paquetes SYN y FIN y solo paquetes ACK. (IPv6 es bueno para el ejercicio de lectura).
tcpdupm 'gateway snup an IP[2:2] > 576'	Para imprimir paquetes IP largos que 576 bytes enviados a través del Gateway snup.
Tcpdump 'ether[0] & 1 = 0 and IP [16] >= 224'	Para imprimir paquetes broadcast IP o multicast que no eran enviados vía broadcast o multicast Ethernet.
tcpdupm 'icmp[icmptype] !=icmp-echo and icmp [icmptype] != icmp-echoreply'	Para imprimir paquetes ICMP que no son eco respuesta / replica (es decir, paquetes que no sean ping):

2º ANEXO

Sistema Operativo

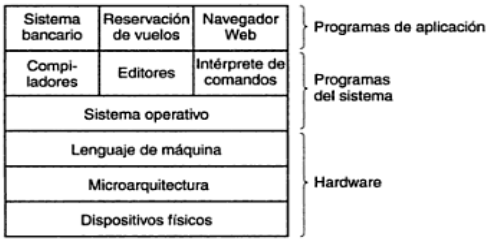
El sistema operativo es el soporte lógico imprescindible para convertir el soporte físico de un computador en una máquina utilizable por el usuario. Se encarga de comunicar la parte física del PC para que esta cumpla las órdenes que le llegan y adaptarlo a la configuración deseada por el usuario, sin que éste deba preocuparse por ello.

También se encarga de supervisar la ejecución de los demás programas, ya sea estableciendo el orden de prioridades en el proceso de datos por parte del procesador o dirigiendo el tránsito en modo de prioridades, de los datos a través de los circuitos internos del PC.

Debe ser capaz de detectar errores que se produzcan en la ejecución de algún programa o en algún componente de la PC. El mismo sistema operativo debe ser capaz de solucionar y avisar al usuario el error y de su solución o no.

Debe disponer de una estructura que permita la creación de archivos, el borrado y la organización de los mismos dentro de los sistemas de almacenamiento de PC.

Se compone de diferentes partes, pero solo dos son las más importantes: el núcleo y el entorno. Las funciones centrales de un sistema operativo están controladas por el núcleo del sistema también conocido como KERNEL, Mientras que las funciones que controlan la interfaz del sistema operativo son el entorno, también conocido como SHELL.



2-1 Componentes de un Sistema Operativo.

3 Er ANEXO

¡Un firewall en UBUNTU!

Dado a las dificultades con que es conseguir el Firewall de FreeBSD, existe un Firewall nativo de UBUNTU que contiene prácticamente todas las características de uno tan potente como lo es el FreeBSD. Este se puede manipular y configurar a las necesidades del usuario, sea administrador o simplemente una persona que quiere tener mayor seguridad en su red privada.

Además, tener un Firewall integrado directamente en el equipo donde tendremos el sistema Xplico es de gran utilidad, ya que nos ahorra espacio en nuestro lugar de trabajo; pudiendo eliminar un equipo más o un disco duro más en nuestro servidor.

E aquí la importancia de simplificar nuestras necesidades en un solo equipo que nos funciones para diferentes actividades.

El kernel de Linux incluye Netfilter como subsistema, si desea puede manipularlo o, si lo decide; destinarlo para manejar el tráfico de la red como su servidor personal. Todos los Firewalls modernos basados en Linux usan este sistema para filtrado de paquetes.

Los kernel´s para sistemas de filtrado de paquetes hacen poco uso de espacios dedicados para la manipulación de estos sistemas. Este es el propósito de IPtables. Cuando un paquete alcanza su servidor, y quiere ser entregado fuera del sistema Netfilter, este manipula, acepta o rechaza basándose en las reglas suministradas por el usuario en las IPtables. Así, IPtables son toda una necesidad para gestionar su firewall, si está familiarizado con él hay muchas interfaces disponibles para simplificar la tarea.

UFW un firewall sin complicaciones.

La herramienta para configurar por defecto el firewall de Ubuntu es *ufw.* Desarrollado para simplificar la configuración de firewall con IPtables. *Ufw* proporciona una forma amigable para crear firewalls basadas en host de IPv4 o IPv6. Inicialmente *ufw* esta deshabilitado. Desde una ventana de comandos:

“ufw no está destinado a proporcionar por completo todas las funcionalidades vía comandos, pero en su lugar proporciona una interfaz simple para agregar reglas. Esto actualmente es usado; principalmente, por host firewalls.

El siguiente es un ejemplo de cómo se usa *ufw*:

1. Primero, *ufw* necesita ser activado. Desde una terminal tecleamos:
2. ***sudo ufw enable***
3. Para abrir un puerto (ssh en este ejemplo):
4. ***sudo ufw allow 22***
5. Algunas reglas son agregadas usando formato numeral.
6. ***sudo ufw insert 1 allow 80***
7. Algo similar, para para cerrar un puerto abierto:
8. ***sudo ufw deny 22***
9. Para remover una regla, usamos delete seguido por la regla:
10. ***sudo ufw deleted eny 22***
11. También es posible permitir el acceso de host específicos o puertos de una red. El siguiente ejemplo permite el acceso ssh del host 192.168.0.2 para cualquier dirección IP en este host.
12. ***sudo ufw allow proto tcp from 192.168.0.2 to any port 22***
    Reemplace 192.168.0.2/24 para permitir el acceso ssh en toda la subred.
13. Agregando la opción --dry-run en el comando ufw sería como resultado una regla, pero no aplica para esto. Por ejemplo, el siguiente comando abre el puerto HTTP
14. ***sudo ufw --dry-run allow http***
15. ****filter***
16. ***:ufw-user-input - [0:0]***
17. ***:ufw-user-output - [0:0]***
18. ***:ufw-user-forward - [0:0]***
19. ***:ufw-user-limit - [0:0]***
20. ***:ufw-user-input -accept - [0:0]***
21. ***## RULES ##***

22. ***### tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0***
23. ***-A ufw-user-input -p tcp --dport 80 -j ACCEPT***

24. ***### END RULES ###***
25. ***-A ufw-user-input -j RETURN***
26. ***-A ufw-user-output -j RETURN***
27. ***-A ufw-user-forward -j RETURN***
28. ***-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT]: "***
29. ***-A ufw-user-limit -j REJECT***
30. ***-A ufw-user-limit-accept -j ACCEPT***
31. ***COMMIT***
32. ***Rules updated***

33. ufw puede ser deshabilitado con
34. sudo ufw disable
35. Para seguir el estado del firewall, tecleamos:
36. sudo ufw status
37. Y para más estados verbose usamos
38. sudo ufw status verbose
39. para ver el formato numeral usamos;
40. sudo ufw status numberad

Si quiere abrir un puerto o cerrarlo, se debe definir en */ets/services*, puede usar el nombre del puerto en lugar del número. En el ejemplo de arriba reemplace 22 por ssh.

Esta es una rápida introducción del uso de *ufw*. Por favor para mayor información diríjase a la página oficial de *ufw*.

Integrando la aplicación ufw.

Aplicaciones que abren puertos pueden incluir perfiles *ufw*, cada puerto necesitar detallarse para que la aplicación funcione apropiadamente. Los perfiles están integrados en */etc/ufw/applications.d* y pueden ser editados si los puertos por defecto han sido cambiados.

1. Para ver que aplicaciones tiene instaladas un perfil, tecleamos lo siguiente en una terminal:
2. ***sudo ufw app list***
3. Algo similar para permitir el tráfico en un puerto, usando una aplicación del perfil realizado para acceder.
4. ***sudo ufw allow Samba***
5. una ampliación de la sintaxis es posible también como:
6. ufw allow from 192.168.0.0/24 to any app samba
   Reemplace *Samba* y 192.168.0.0/24 con la aplicación del perfil que use y el rango IP de su red.
   No es necesario especificar el *protocolo* de la aplicación, porque esa información es detallada en el perfil. También note que el nombre de la app remplaza el número del puerto.
7. Para ver los detalles acerca de cada puerto, protocolos, etc. Definimos la aplicación:
8. ***sudo ufw app info Samba***

No todas las aplicaciones que requieren abrir un puerto en la red vienen con perfiles en ufw, pero si tiene un perfil la aplicación y requiere que el archivo sea incluido en el paquete, debería enviar un mensaje de error en el paquete Launchpad.

Ubuntu-bug name of package

Enmascarando la red

El propósito del enmascaramiento es para mantener las maquinas en privacidad, sin en rutar las direcciones IP en su red para acceder a Internet a través de la máquina que realiza en enmascaramiento. El tráfico de su red privada destinada para Internet necesita ser manipulada para tener una contestación de retorno.

Para eso el kernel necesita modificar la dirección IP fuente para cada paquete, así que la respuesta será ruteada cuando retorne, más bien la dirección IP privada que hace la solicitud, haciendo posible llegar a internet. Linux usa rastreo de conexiones (pistas) para mantener pistas para cada conexión para ver a quien pertenece la petición y desvía cada paquete retornado en consecuencia. Dejando el tráfico de la red privada enmascarado desde la máquina que contiene UBUNTU. Este proceso es referido en la documentación de Microsoft como conexión compartida de Internet.

Enmascaramiento ufw.

El enmascaramiento puede ser archivado usando reglas tradicionales de *ufw*. Esto es posible porque en la parte final de ufw se restauran las IPtables con las reglas del archivo /etc/ufw/*.rules. Este archivo es un gran lugar para agregar reglas de IPtables usadas fuera de ufw y reglas más enfocadas a redes Gateway o conexión puente. Las reglas son divididas en dos diferentes archivos, reglas que son ejecutadas después de las reglas de *ufw*, y reglas son ejecutadas después de las líneas de comandos *ufw*.

1. Primero, paquetes enviados que necesitan ser enviados en *ufw*. Dos, configurar archivos que necesitan ser adjuntados, en /etc/default/ufw cambiando el DEFAULT_FORWARD_POLICY por “ACCEPT”:
2. ***DEFAULT_FORWARD_POLICY=“ACCEPT”***
   Entonces editamos /etc/ufw/sysctl.conf y comentamos:
   Del mismo modo, para IPv6 enviados sin comentarios:
   net/IPv6/conf/default/forwarding/1
3. Ahora agregaremos reglas al archivo /etc/ufw/before.rules. Las reglas por defecto solo configuran la tabla de filtro, y habilitar el enmascaramiento de la tabla *nat* necesitaran ser configuradas. Agregando lo siguiente en lo más alto después de la cabecera de comentarios:
4. ***# natTable rules***
5. ****nat***
6. ***:POSTROUTING ACCEPT [0:0]***

7. ***# Forward traffic from eth1 through eth0.***
8. ***-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE***

9. ***# don't delete the 'COMMIT' line or these nat table rules won't be processed***

10. COMMIT

Los comentarios no son estrictamente necesarios, pero son considerados buena práctica para documentar la configuración de la red. También, cuando modificamos cualquiera de las reglas en el archivo /etc/ufw, hace seguro que las líneas que modificamos sean las correctas:

 # don't delete the 'COMMIT' line or these rules won't be processed

COMMIT

Para cada tabla es requerida una corresponde COMMIT, en este ejemplo solo las tablas *nat* y *fiter* son mostradas

En el ejemplo de arriba reemplace eth0, eth1 y 192.168.0.0/24 con la interfaz apropiada y el rango de IP de su red.

11. Finalmente, deshabilite y restablezca la aplicación ufw para aplicar los cambios:

12. sudo ufw disable&& sudo ufw enable

El enmascaramiento muestra ahora estar habilitado. Puede ser también agregado adicionalmente cualquier regla FORWARD al archivo /etc/ufw/before.rules. Es recomendado que esas reglas adicionales sean agregadas en la cadena ufw-before-forward.

En mascarando con IPtables.

Las IPtables pueden ser usadas para habilitar el enmascaramiento.

1. Como en ufw, el primer paso es habilitar él envió de paquetes IPv4 editando en /etc/sysctl.conf y sin comentarios en la siguiente línea.
2. ***net.IPv4.IP_forward=1***

   Si desea habilitar él envió de IPv6 haga lo siguiente sin comentarios:

   net.IPv6.conf.default.forwarding=1
3. Lo siguiente, ejecuta el comandos y ctl habilitando los nuevos ajustes en la configuración del archivo:
4. **sudo sysctl –p**
5. Ahora el enmascaramiento puede ser cumplido con las reglas de la IPtables, que es posible definir basado ligeramente con la configuración de su red:
6. ***sudo IPtables –t nat –A POSTROUTING –s 192.168.0.0/16 –o pp0 –j MASQUERADE***

El comando de arriba asume que la dirección privada de la red está en el espacio 192.168.0.0/16 y que la fuente de Internet es el dispositivo ppp0. La sintaxis se describe a continuación.

1. –t nat – la regla va dentro de la tabla nat.
2. –A POSTROUTING – Agrega –A a la cadena POSTROUTING.
3. –s 192.168.0.0/16 – aplica el tráfico de origen especificando de donde es.

4. –o ppp0 – aplica el trafico programado para ser ruteado a través de la red especificada.
5. –j MASQUERADE – Coincide el tráfico con la regla, “jump” (-j) con la etiqueta MASQUERADE para ser manipulada como se describe arriba.

7. También, cada cadena en la tabla de filtrado (en la tabla por defecto, y donde ocurre la mayoría o todo el filtrado de los paquetes) tiene por defecto la política de ACCEPT, pero si crea un firewall adicionando un dispositivo Gateway, puede tener un conjunto de políticas DROP o REJECT, en cada caso el enmascaramiento del trafico necesita ser permitido a través de la cadena FORWARD para las reglas de arriba a trabajar:

8. sudo IPtables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT

***9. sudo IPtables -A FORWARD -d 192.168.0.0/16 -m state ***

10. --state ESTABLISHED,RELATED -i ppp0 -j ACCEPT

El comando de arriba permitirá toda conexión de la red local a Internet y todo el tráfico relacionado a aquellas conexiones que regresan a la máquina que realice la solicitud.

11. Si quiere enmascarar lo más probable es que necesite reiniciar. Edite /etc/rc.local y agregué cualquier comando usado arriba. Por ejemplo agregar el primer comando para no filtrar.

12. IPtables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE

Registros.

El registro en el firewall es esencial para reconocer ataques, soluciona el problema de las reglas en los firewalls y nota cualquier actividad inusual en la red. Necesita incluir una regla de registro en el firewall para que ello sea generado, sin embargo, la regla de registro necesita venir después de cualquier terminación de la regla a aplicar (una regla con un objetivo que decide el destino del paquete, tal como ACDEPT, DROP o REJECT).

Si ésta usando ***ufw***, puede girar un registro tecleando lo siguiente en la terminal:

sudo ufw loggingon

Para girar el registro a off en **ufw**, simplemente reemplazamos on con off en el comando de arriba.

Si usa IPtables en lugar de ufw, teclee:

***sudo IPtables -A INPUT -m state --state NEW -p tcp --dport 80 ***

-j LOG --log-prefix "NEW_HTTP_CONN: "

Una solicitud en el Puerto 80 de una maquina local, hará generar el registro en dmesg que mira bien esto (la siguiente línea se ha dividido en 3 para ajustarlo al documento):

[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00

SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP

SPT=53981 DPT=80 WINDOW=32767 RES=0x00 SYN URGP=0

El registro de arriba debería también aparecer en /var/log/massages, /var/log/syslog, y /var/log/kern.log. Este comportamiento puede ser modificado editando /etc/sysog.conf adecuadamente o instalando y configurando *ulogd* y usando el ULOG con el objetivo de usarlo en lugar de LOG.

El daemonulogd es para servidores dedicados que listan los registros; instrucciones que son del kernel, específicamente del firewall, y pueden registrarlos en cualquier archivo que gusten, o incluso en bases de datos como aPostgreSQL o MySQL.

Marcando el sentido de los registros en el firewall, puede simplificarse usando un analizador de registros tal como son las herramientas logwatch, fwanalog, fwlogwatch o lire.

Otras herramientas.

Existen muchas herramientas disponibles para ayudar a la construcción de un firewall sin tener muchos conocimientos de IPtables. Para GUI incluye el:

1. fwbuilder es muy potente y se verá familiarizado con los administradores que tienen firewall comercial, tales como Checkpoint FireWall-1.

Sí prefiere una herramienta en línea de comandos con configuraciones en texto plano. Es recomendable:

2. shorewall es una muy potente solución.