Universidad Nacional Autónoma de México

Facultad de Ingeniería

Sistema avanzado de monitoreo de redes

TESIS

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

PRESENTAN:

Mauricio Enrique Arriaga Rivera

Daniel Martínez Macedo

DIRECTORA DE TESIS:

M. en C. Ma. Jaquelina López Barrientos

Ciudad Universitaria, 2015

A mi abuelita Carmen, que a pesar de ya no estar con nosotros sigue en mi corazón. Gracias por iniciar mi educación de la mejor manera posible e inculcarme la importancia del estudio. Gracias por darme el mejor regalo que cualquier persona puede tener: una madre que da todo por sus hijos, que les brinda amor incondicional y que es todo un ejemplo para nosotros, Liliana.

A mi madre, por ser el pilar de mi vida, por apoyarme y darme lo que necesitaba aunque pareciera imposible, por sacrificar su vida para que yo no tuviera carencias. Gracias mamá por sacarme adelante y darme todas las herramientas necesarias para poder construir un futuro estable a largo plazo. Esto es para ti, Lili.

A mi tío, Guillermo Carlos Hernández Corona. Que siempre ha estado al pendiente de mí, y con su amor y cariño me brindó valores fundamentales, los cuales me ayudaron a formarme como profesional.

A mi tío Etson Ramírez Hernández. Quien me enseñó que a pesar de las adversidades siempre se puede triunfar, además de ser mi mayor inspiración para la elección de esta carrera que hoy concluyo esperando llegar a ser un ejemplo para mis hermanos Bruno y Abraham que siempre han estado a mi lado y que gracias a ellos me he esforzado para ser mejor, porque no me he dejado vencer nunca por demostrarles que a pesar de ser difícil no es imposible.

A mis compañeros y amigos, quienes a lo largo de mi carrera han sido un gran apoyo. Gracias por estar conmigo en las buenas y en las malas, fue un placer enorme haber compartido las aulas de esta nuestra facultad con ustedes.

A Gabriela J. Reyes Rodríguez. Quien no solo ha sido mi compañera en esta carrera, también mi amiga y pareja. Gracias Gaby, por todo tu apoyo, por tu paciencia y comprensión, pero sobre todo gracias por estar conmigo en los buenos y en los malos momentos a lo largo de este camino.

A la maestra Jaquelina, nuestra directora de tesis. Gracias por todo el apoyo y la paciencia que nos tuvo para que este trabajo culminara exitosamente. Gracias por todo el conocimiento y los consejos brindados con el paso del tiempo, sin duda alguna fueron y son muy importantes para nosotros. ¡Lo logramos!

Arriaga Rivera Mauricio Enrique

A mi familia, fuente de apoyo constante e incondicional a lo largo de mi desarrollo personal y profesional. Como una muestra de mi cariño y agradecimiento por todo el amor y el apoyo recibido, y porque constituye la herencia más valiosa que pudiera recibir, les agradezco la orientación y el apoyo que siempre me han otorgado, tanto en los malos como en los buenos momentos.

A mis profesores de la facultad, Jaquelina López, César Govantes, por mencionar algunos nombres, quienes siempre confiaron en mí y sin dudar colaboraron apoyándome no solamente en la parte académica, sino en mi desarrollo personal y profesional.

A mis amigos, más que solo compañeros, es difícil nombrarlos, ya que todos, por poco o mucho que sea, fue todo un gusto haber trabajado juntos y disfrutado los buenos y malos momentos que vivimos durante la carrera.

A mi universidad, más que una casa de estudios, se convirtió en mi segundo hogar, donde siempre recibí la mejor formación profesional y los mejores consejos; ¡porque es imposible no sentirse orgulloso de formar parte de esta gran universidad y toda su comunidad!

¡GRACIAS!

Martínez Macedo Daniel

Sistema avanzado de monitoreo de redes

Índice general

Introducción **7**

Panorama general **8**

Objetivo general **10**

Objetivos particulares **10**

Capítulo 1. Problemática **12**

1.1 Dispositivos Apple 13
1.2 Ataques informáticos 15
1.2.1 Situación actual 15
1.2.2 Tipos de ataques informáticos 18
1.2.1.1 Malware 18
1.2.1.2 Grayware 20
1.2.3 Relación entre los ataques informáticos y las nuevas tecnologías 21

Capítulo 2. Marco teórico **24**

2.1 Redes de datos 25
2.1.1 Clasificación de las redes de datos 25
2.2 Seguridad informática 29
2.2.1 La triada de la seguridad informática 30
2.2.2 Principios básicos de la seguridad de la información .. 31
2.2.3 Herramientas de seguridad 34
a) Monitoreo 34
b) Escaneo 38
c) Firewalls 39
d) Detección de intrusos 41
e) Criptografía 42

Capítulo 3. Diseño y desarrollo del sistema de monitoreo **46**

3.1 Requerimientos del sistema 47
3.2 Plataforma de desarrollo 48
3.2.1 UNIX 48
3.2.2 PHP 50
3.2.3 MySQL 51
3.3 Herramientas de desarrollo 51
3.4 Tipo de Monitoreo 53

3.5 Diseño del sistema de monitoreo 54
3.5.1 Base de datos 56
3.5.2 Acceso y cierre de sesión 57
3.5.3 Módulo de escaneo 58
3.5.4 Generación de reportes 60
3.5.5 Generación de gráficas 61
3.5.6 Generación de listas negras 62
3.5.7 Gestión de geolocalización 63
3.5.8 Módulo de consulta 64
3.5.9 Búsqueda de registros 65
3.6 Código fuente 65
3.5.1 Conexión con la base de datos 66
3.5.2 Acceso y cierre de sesión 66
3.5.3 Escaneo de red 67
3.5.3 Escaneo de un dispositivo en específico 68
3.5.4 Generación de reportes en formato PDF 69
3.5.5 Presentación de gráficas 70
3.5.6 Generación de listas negras 71
3.5.7 Gestión de geolocalización 72
3.5.8 Consulta de registros 73
3.5.9 Búsqueda de registros 74

Capítulo 4. Auditoría y resultados 76

Conclusiones 104

Anexos 108

Glosario de términos 109
Fuentes de información 114

Índice de figuras

Capítulo 1

1.1 Ventas trimestrales internacionales del Iphone 13
1.2 Ventas trimestrales internacionales de computadoras Mac 14
1.3 Ventas totales de dispositivos Apple, 2013 14
1.4 Número de huecos de seguridad con más de 10 millones de identidades expuestas 16
1.5 Total de huecos de seguridad vs total de identidades expuestas ... 16
1.6 Total de correos Spam en porcentaje 17
1.7 Vulnerabilidades en móviles 17

Capítulo 2

2.1 Red de área personal 27
2.2 Red de área local 27
2.3 Red de área metropolitana 28
2.4 Red de área amplia 28
2.5 Triada de la seguridad informática 30
2.6 Firewall 39
2.7 Proxy 41
2.8 IDS 42
2.9 Criptografía 43

Capítulo 3

3.1 Diagrama general de usos 27
3.2 Diagrama entidad-relación de la base de datos 27
3.3 Diagrama de uso de los módulos de acceso al sistema y cierre de sesión 28
3.4 Diagrama de uso de los módulos de escaneo 28
3.5 Diagrama de usos del módulo de generación de reportes 30
3.6 Diagrama de usos del módulo de generación de gráficas 39
3.7 Diagrama de usos del módulo de generación de listas negras 41
3.8 Diagrama de usos del módulo de gestión de geolocalización ... 42
3.9 Diagrama de usos del módulo de consulta 43
3.10 Conexión con la base de datos 27
3.11 Acceso al sistema 43
3.12 Cierre de sesión 27
3.13 Escaneo de la red 28
3.14 Escaneo de un dispositivo 28
3.15 Generación de reportes en formato PDF 30
3.16 Presentación de gráficas 39
3.17 Generación de listas negras 41
3.18 Gestión de geolocalización 42
3.19 Consulta y búsqueda de registros 43

Capítulo 3

4.1 Inicio de sesión (Escritorio vs Móvil) 77
4.2 Inicio de sesión (Ingreso de credenciales no válidas) 78
4.3 Inicio de sesión (Número de intentos agotado) 78
4.4 Inicio de sesión a la base de datos (Escritorio vs Móvil) 79
4.5 Autorización para el uso de coordenadas 79
4.6 Vista principal (Escritorio) 80
4.7 Barra lateral izquierda, vista principal (Móvil) 81
4.8 Gráfica, vista principal (Móvil) 81
4.9 Estado del servidor, vista principal (Móvil) 81
4.10 Ubicación y mapa, vista principal (Móvil) 82
4.11 Análisis rápido (Escritorio) 82
4.12 Análisis rápido (Móvil) 83
4.13 Tabla de resultados para el análisis rápido (Móvil) 83
4.14 Análisis detallado (Escritorio) 84
4.15 Análisis detallado (Móvil) 85
4.16 Consulta de escaneos realizados (Escritorio) 86
4.17 Consulta de escaneos realizados (Móvil) 86
4.18 Consulta de coordenadas almacenadas (Escritorio vs móvil) 87
4.19 Mapa 88
4.20 Vista a nivel de calle 88
4.21 Registro de hosts (Escritorio) 89
4.22 Detalles registrados para cada host (Escritorio vs móvil) 90
4.23 Ajustes, preferencias de red (Escritorio vs móvil) 91
4.24 Ajustes, generación de listas negras (Escritorio vs móvil) 92
4.25 Búsqueda de registros (Escritorio vs móvil) 93
4.26 Hoja principal (estado del servidor y ubicación) 94
4.27 Resultados del análisis rápido representado en tablas 95
4.28 Resultados del análisis detallado por cada host 96
4.29 SQL injection parte 1 97
4.30 SQL injection parte 2 98
4.31 WordPress Scan sobre el sistema desarrollado 99
4.32 Fping sobre la red de prueba 100
4.33 Servidor identificable 100
4.34 Servidor en modo encubierto 101
4.35 Fping sobre la red 101
4.36 Archivo de configuración sshd_config 102

Índice de tablas

Capítulo 2

2.1 clasificación de las redes por su cobertura geográfica 26

Capítulo 3

3.1 Requerimientos vs objetivos 47

INTRODUCCIÓN

Panorama general de la seguridad informática

Hoy en día la seguridad informática juega un rol sumamente importante dentro de las diferentes organizaciones y empresas de todo el mundo, debido a que ésta es la encargada de proteger todos los activos dentro de la misma, como son: la información física y digital, los dispositivos de almacenamiento de la información, la red interna de la empresa u organización, la entrada a los edificios, entre otros. Pero con el transcurso de los años la seguridad de la información ha tenido que ir evolucionando al mismo tiempo que la tecnología, ya que así como la tecnología avanza, la forma de generar, almacenar, acceder y transmitir la información cambia, y la seguridad informática y de la información se tienen que adaptar a dichos cambios.

Cada vez son más las personas que usan la tecnología para beneficiarse de la facilidad que ésta brinda para realizar tareas diarias, como son: "socializar", realizar tareas, investigaciones, programar diversas actividades, entre muchas otras cosas. Pero también, son menos las personas conscientes del hecho de que la tecnología no se enfoca directamente a proteger la información que se maneja dentro de ella, sin embargo, existen muchas otras que están interesadas en conocer y hacerse de la información ajena, incluso hacerse de sus contraseñas para ingresar a sitios web, redes, servicios y aplicaciones a las que de otra forma no conseguirían acceder.

Y parte de toda esta evolución tecnológica ha llegado a centralizarse en los dispositivos móviles, mercado que sigue en crecimiento en todo el mundo, mismo que ha sido liderado por la empresa Apple desde el 2007.

Lamentablemente, las personas que conocen la tecnología y quieren sacar provecho de ella de forma maliciosa buscan nuevas herramientas para lograr sus objetivos, y una de ellas está en los dispositivos móviles Apple. Debido a que así como Apple libera nuevas versiones de sistema operativo y de hardware existen grupos de hackers que se encargan de romper todas las limitaciones que Apple impone sobre los mismos

dispositivos, y una de las limitaciones más importantes es la referente a la descarga de aplicaciones, ya que, al romper esa limitación impuesta por Apple, las personas que usan el método de estos grupos de hackers llamado "Jailbreak" pueden hacerse de aplicaciones que no pasaron las pruebas de Apple para ser aplicaciones oficiales.

Y si esta herramienta o método es ejecutada por esas personas maliciosas se pueden llegar a realizar ataques informáticos, ya no solo desde una computadora o laptop, sino desde un dispositivo móvil que fácilmente puede llegar a pasar desapercibido.

Por otro lado, la seguridad informática ha desarrollado muchas herramientas que le permiten a las personas y a las empresas protegerse de todo tipo de ataques informáticos: firewalls, antivirus, IDS's, monitores de seguridad, etcétera.

Lamentablemente, nunca se llegará a tener un 100% de seguridad en una red, y es necesario estar conscientes de ello, ya que los atacantes cibernéticos también se actualizan y muchas veces logran romper la seguridad de una empresa, de una organización o de una persona. Precisamente por ello es menester indispensable el correcto acoplamiento y actualización de distintas herramientas de seguridad que permitan prevenir, detectar y corregir incidentes de seguridad suscitados en una red, además de que es necesario hacerlo de manera continua ya que las personas que se dedican a realizar ciber ataques no descansan y así como día con día avanza la tecnología, éstas personas tratan de hacer uso de ella y por eso los expertos en seguridad informática necesitan estar al pendiente y actualizados todos los días.

Pero, las actualizaciones no siempre son tan efectivas como se espera, ya que la actualización de las herramientas de seguridad en comparación con el avance tecnológico llega a ser ligeramente más lenta, lo que permite que los problemas de seguridad se siguen suscitando.

Objetivo general

Desarrollar un sistema que monitoree todo tipo de red, ya sea pública o privada, y que sea capaz de detectar todos los dispositivos de los usuarios conectados a la misma, de tal forma que se pueda llevar a cabo una exploración sobre sus dispositivos con la finalidad de detectar posibles atacantes usando Jailbreak de Apple con fines de hacking.

Objetivos particulares:

a) Identificar usuarios conectados a la red
b) Identificar usuarios con Jailbreak
c) Identificar usuarios con fines de ataque

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores"

- *Kevin Mitnick*

Capítulo 1
Problemática

En los últimos años la tecnología ha avanzado a pasos agigantados, de tal forma que el uso de dispositivos móviles ha sido cada vez más común entre las personas. Y muchas de estas personas lamentablemente tienen malas intenciones, de manera que buscan hacerse de la información de los demás. Para facilitar su trabajo intentan sacarle un mayor provecho a sus dispositivos. Entonces recurren a técnicas como el conocido Jailbreak, que atenta contra el control de las empresas sobre las funciones que se le pueden dar a estos dispositivos, ampliando de esta manera las herramientas con las cuales realizar actos maliciosos.

Desde el ámbito de seguridad informática estas personas pueden llegar a penetrar los sistemas solo con la ayuda de un dispositivo con Jailbreak, y estos ataques sigilosos pueden tener repercusiones muy grandes para las empresas y organizaciones.

A lo largo de este capítulo se abordarán temas referentes a los dispositivos Apple, el Jailbreak y su juego como parte de la nueva generación de herramientas digitales para realizar todo tipo de ciber ataques.

1.1 Dispositivos Apple

Apple ha llegado a cubrir gran parte del mercado mundial. A continuación se muestran dos gráficas en las cuales se puede observar el claro crecimiento de las ventas de productos Apple; La figura 1.1, hace referencia al número de Iphone's que se han ido vendiendo con el paso de los años, empezando en 2007, mientras que la figura 1.2 muestra los números de las ventas de computadoras Mac, empezando en 2006.

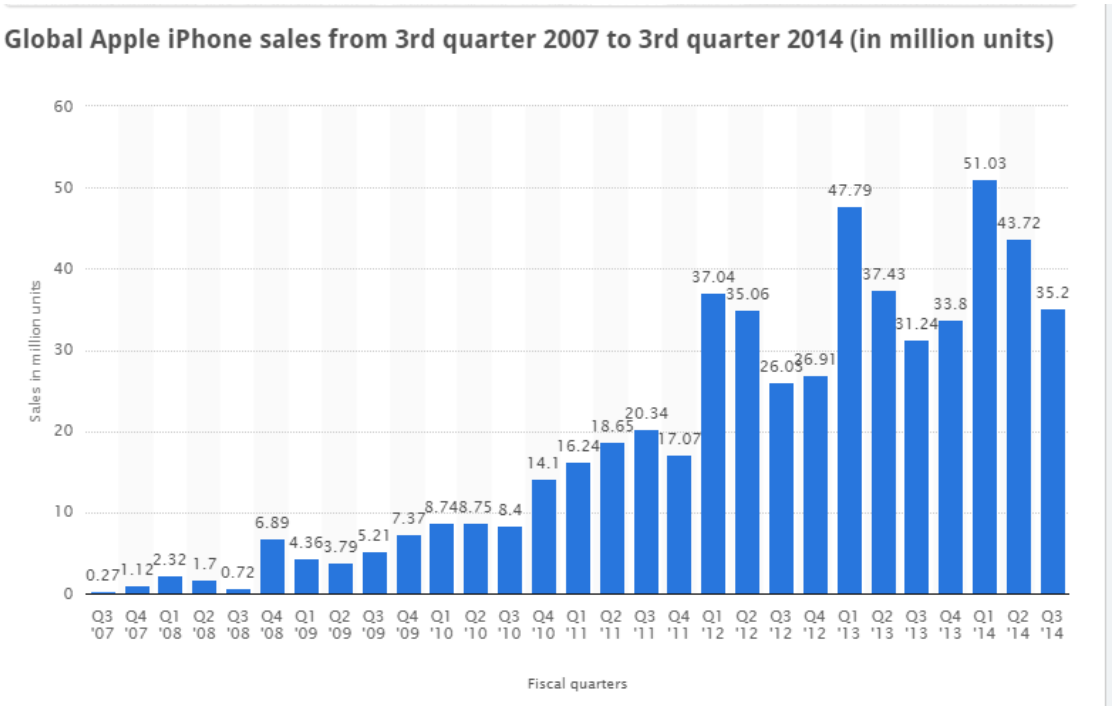


Figura 1.1 Ventas trimestrales internacionales del Iphone
Referencia: http://www.statista.com/statistics/263401/global-apple-iphone-sales-since-3rd-quarter-2007/

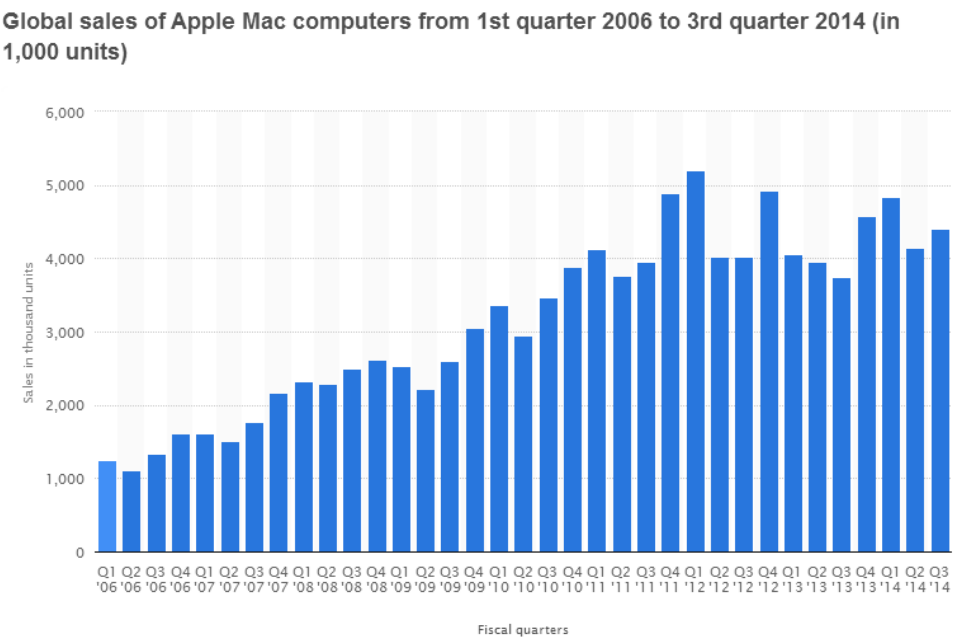


Figura 1.2 Ventas trimestrales internacionales de computadoras Mac
Referencia: http://www.statista.com/statistics/263444/sales-of-apple-mac-computers-since-first-quarter-2006/

En septiembre de 2013 Apple anunció que su venta total llegaba a 700 millones de dispositivos en todo el mundo, como se puede observar en la figura 3, por lo que se puede deducir que hoy en día, a dos años de ese anuncio, existen muchos más dispositivos Apple vendidos.

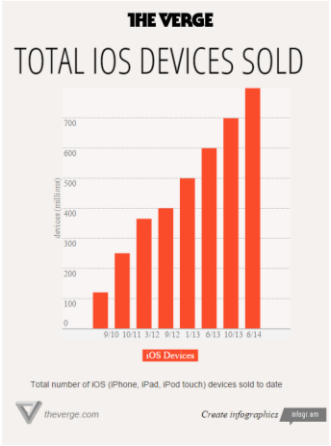


Figura 1.3 Ventas totales de dispositivos Apple, 2013
Referencia: http://www.theverge.com/2013/9/10/4715256/apple-700-million-ios-devices-sold-by-end-of-september

1.2 Ataques informáticos

Los ataques informáticos adquieren gran relevancia en la actualidad y para el desarrollo del presente proyecto es necesario conocer la situación actual y los tipos de ataques informáticos que se suscitan día con día.

1.2.1 Situación actual

Los ataques informáticos sin duda alguna han ido de la mano de los avances tecnológicos con el paso de los años, y estos mismos han puesto a prueba la seguridad de muchos sistemas. La definición de un ataque informático es la siguiente: "Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático".

De acuerdo al reporte anual de amenazas en Internet de Symantec con los datos recabados durante todo el año 2013, el número de incidentes de seguridad en algunos rubros subieron bastante en relación a años anteriores mientras que otros hicieron lo opuesto.

A continuación se muestran algunas gráficas presentadas en este documento:

La primera de ellas (figura 1.4) se refiere al número de huecos de seguridad que en 2013 dejaron más de 10 millones de identidades expuestas.

Figura 1.4 Número de huecos de seguridad con más de 10 millones de identidades expuestas.

La figura 1.5 muestra la cantidad de agujeros de seguridad y la cantidad de identidades expuestas a lo largo de todo el año 2013.

Figura 1.5 Total de huecos de seguridad vs total de identidades expuestas.

En la figura 1.6 se observa el decrecimiento de los ataques conocidos como "spam".

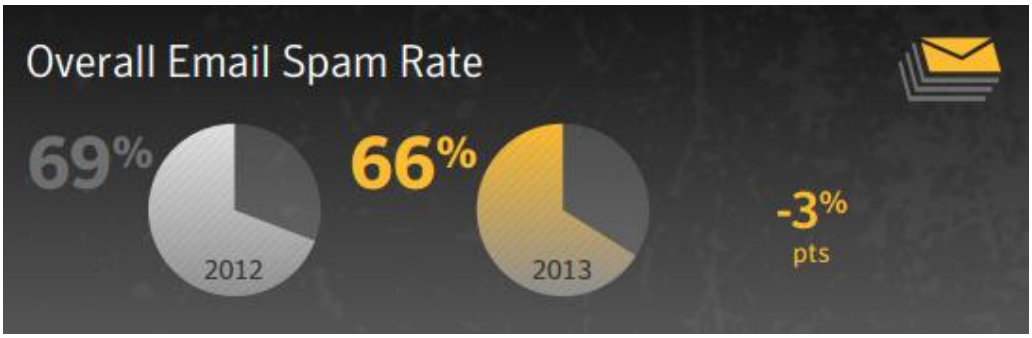


Figura 1.6 Total de correos Spam en porcentaje

En las siguientes dos gráficas se observa cómo el número de vulnerabilidades encontradas en dispositivos móviles decayó un 69% (figura 1.7), mientras que las vulnerabilidades de día cero fueron mayores en el año 2013 (figura 1.8).

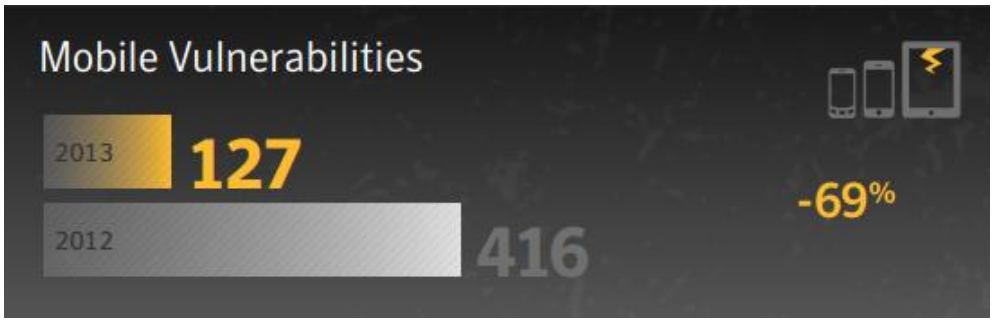


Figura 1.7 Vulnerabilidades en móviles

De las figuras vistas se puede concluir que los ataques informáticos existen y pueden llegar a dañar a terceras personas, ya sea a causa del robo de información y mal uso de la misma, fraude electrónico o mediante la denegación de algún servicio crítico dentro de una empresa. Por esa razón es indispensable contar con diferentes herramientas que ayuden a prevenir, detectar e incluso eliminar estos ataques para evitar la pérdida y el mal uso de la información almacenada en cualquier medio tecnológico.

1.2.2 Tipos de ataques informáticos

1.2.2.1 Malware

"Es un tipo de software que tiene como propósito infiltrarse y dañar una computadora o sistema de información sin el consentimiento de los propietarios."
Existen muchos tipos de malware, en seguida se definen algunos con base en el uso de los mismos para realizar ataques informáticos:

- Virus y Gusanos: Éstos, son los tipos más conocidos de software maligno que existen y se distinguen por la manera en que se propagan. El término de virus informático se usa para designar un programa que al ejecutarse se propaga infectando otro software ejecutable de la misma computadora. Pueden tener un playload que realice otras acciones maliciosas en donde se borran archivos. Los gusanos son programas que se transmiten a sí mismos, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. Su principal objetivo, es infectar a la mayor cantidad posible de usuarios y también puede contener instrucciones dañinas al igual que los virus. A diferencia que los gusanos, un virus necesita la intervención del usuario para propagarse, mientras que los gusanos se propagan automáticamente.

- Backdoor o Puerta Trasera: Es un método para eludir los procedimientos habituales de autenticación al conectarse en una computadora. Una vez que el sistema ha sido comprometido, puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro de los atacantes. Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, permaneciendo ocultos ante posibles inspecciones, utilizando troyanos, gusanos u otros métodos.

- Drive-by Downloads: Son sitios que instalan spyware o códigos que dan información de los equipos. Generalmente se presentan como descargas que de algún tipo, se efectúan sin consentimiento del usuario, lo cual ocurre

al visitar un sitio web, al revisar un mensaje de correo o al entrar a una ventana pop-up. El proceso de ataque Drive-by Downloads se realiza de manera automática mediante herramientas que buscan en los sitios web alguna vulnerabilidad e insertan un script malicioso dentro del código HTML.

- Rootkits: Es un software que modifica el sistema operativo de la computadora, para permitir que el malware permanezca oculto al usuario, evitando que el proceso malicioso sea visible en el sistema.

- Troyanos: Es un software malicioso que permite la administración remota de una computadora de forma oculta y sin el consentimiento del propietario. Generalmente están disfrazados como algo atractivo o inocuo que invitan al usuario a ejecutarlo. Pueden tener un efecto inmediato y tener consecuencias como el borrado de archivos del usuario e instalar más programas maliciosos. Son usados para empezar la propagación de un gusano, inyectándolo de forma local dentro del usuario.

- Hijackers: Son programas que realizan cambios en la configuración del navegador web, cambiando la página de inicio por páginas con publicidad, pornográficas u otros re direccionamientos con anuncios de pago o páginas de phishing bancario. Ésta es una técnica que suplanta al DNS, modificando archivos hosts, para redirigir el dominio de una o varias páginas a otras, muchas veces una web falsa que imita a la verdadera. Comúnmente es utilizada para obtener credenciales y datos personales mediante el secuestro de una sesión.

- Keyloggers y Stealers: Estos programas están encaminados al aspecto financiero, la suplantación de personalidad y el espionaje. Los Keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para realizar operaciones fraudulentas como son pagos desde cuentas de banco o tarjetas de crédito. La mayoría de estos sistemas son usados para recopilar contraseñas de

acceso, espiar conversaciones de chat u otros fines. Los Stealers también roban información privada, pero solo la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados y si tienen contraseñas recordadas, por ejemplo en los navegadores web la descifran.

- Botnets: Son redes de computadoras infectadas, también llamadas "zombies", que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de spam o para lanzar ataques contra organizaciones. En una Botnet cada computadora infectada por el malware se loguea en un canal de IRC u otro sistema de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente. Las botnets también pueden ser usadas para actualizar el malware en los sistemas infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad.

- Rogue software: Hacen creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.

- Ransomware: También llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un "rescate" para poder recibir la contraseña que permite recuperar los archivos.

1.2.2.2 Grayware

"Los Grayware o greynet son software maliciosos que no son tan peligrosos como los malwares. Suelen utilizarse para clasificar las aplicaciones o programas de cómputo y se instalan sin la autorización de los usuarios."
Los tipos de grayware son:

- Adware: Son programas que automáticamente se ejecutan y muestran publicidad web, después de instalar el programa o mientras se está utilizando la aplicación "Ad", que se refiere a "advertisement" (anuncios) en idioma inglés.

- Dialers: Son programas maliciosos que toman el control del módem, realizan una llamada a un número de teléfono de tarificación especial, muchas veces internacional, y dejan la línea abierta cargando el costo de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salva pantallas, pornografía u otro tipo de material. Actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem, lo cual hace que los Dialers ya no sean tan populares como en el pasado.

- Spyware: Son creados para recopilar información sobre las actividades realizadas por un usuario, obteniendo datos sobre los sitios web que visita, direcciones de email a las que después se envía spam. La mayoría de los programas son instalados como troyanos. Otros programas spyware recogen la información mediante cookies de terceros o barras de herramientas instaladas en navegadores web. Generalmente se presentan como programas que muestran publicidad o ventanas emergentes (pop-up) que son aceptadas de forma involuntaria, afectando los sistemas del usuario.

1.3 Relación entre los ataques informáticos y las nuevas tecnologías

Pero, ¿qué tiene que ver todo esto con la seguridad de la información?

Tiene que ver todo, ya que, así como Apple puede llegar a vender millones y millones de dispositivos anualmente, existe

una gran cantidad de personas enfocadas en ciber ataques e interesadas en realizar dichos ataques de tal forma que nadie se entere.
Así que estas personas se actualizan a tal grado que son capaces de convertir un dispositivo Apple en una computadora totalmente equipada y lista para realizar ataques de todo tipo (Spoofing, phishing, web cloning, entre muchos otros ataques que pueden llegar a comprometer la información resguardada, ya sea por una empresa o por las personas mismas).

Todo esto se puede hacer instalando alguna de las versiones de Jailbreak y posteriormente descargando aplicaciones tales como una línea de comandos, metasploit, entre muchas otras que pueden convertir un dispositivo móvil en un dispositivo de hacking con herramientas muy potentes.

Y cada vez son más las personas interesadas en el Jailbreak, el cual no es tan complicado de obtener en internet, ya sea por curiosidad o por querer tener una herramienta más con la cual obtener información de todo tipo de forma fácil.

EN Marzo del 2013, el experto en seguridad Cyril Cattiaux (alias Pod2g) y el desarrollador Jay Freeman (creador de Cydia) anunciaron que 14,051,500 dispositivos corriendo IOS 6 usaban Jailbreak, y a pesar de no haber cifras más recientes relacionadas al Jailbreak se puede deducir que en 2015 hay muchos más usuarios usando esta herramienta.

“El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados.”

-Gene Spafford

Capítulo 2
Marco teórico

En la actualidad, la importancia que tienen las redes de datos para las personas y para las organizaciones (públicas o privadas) es muy grande, debido al uso de las mismas para compartir, almacenar y resguardar el principal activo para todos: la información.

Las redes de datos, combinadas con la seguridad informática, son capaces de manipular la información de manera más eficaz haciendo uso de herramientas de seguridad que día con día van evolucionando.

A lo largo de este capítulo se ven las bases teóricas que sustentan el desarrollo de un sistema de monitoreo de red, así como aplicaciones ya existentes que permiten tener una red más controlada y segura.

2.1 Redes de datos

Las redes de datos surgen por la necesidad de distribuir la información almacenada en diferentes computadoras de forma más eficaz y eficiente. Ya que, antes de éstas, el proceso de compartir información era todo un caos, se necesitaba de medios rígidos de almacenamiento y el transportar los mismos era un trabajo para nada sencillo.
Posteriormente, las redes de datos son actualizadas según las nuevas necesidades de las personas, y llegamos a lo que se tiene hoy en día: procesamiento y compartimiento de voz, audio, video, imágenes e información.
Definición
"Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la Transmisión de información mediante el intercambio de datos…
Las redes de datos, generalmente, están basadas en la comunicación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física."

2.1.1 Clasificación de las redes de datos

Las redes de datos se pueden clasificar de diferentes maneras, según su cobertura, su utilización, y por su propiedad, así las principales 3 formas de clasificarlas son las que a continuación se presentan:

- Clasificación de las redes de datos por utilización:

1. Redes Compartidas, aquellas a las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con transmisiones de otra naturaleza.

2. *Redes exclusivas*, aquellas que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conectan dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

- Clasificación de las redes de datos por propiedad

  Redes públicas, aquellas que pertenecen a organismos estatales y se encuentran abiertas a cualquier usuario que lo solicite mediante el correspondiente contrato.
  Redes privadas, aquellas que son gestionadas por personas particulares, empresa u organizaciones de índole privado.

- Clasificación de las redes de datos por cobertura geográfica

En este sentido se puede considerar desde la red más pequeña en la cual los dispositivos están muy cercanos entre sí y son redes que se consideran efímeras dado que solamente se establecen al momento del intercambio de datos hasta redes de datos en las que se generan, transmiten y almacenan grandes cantidades de información.
En la tabla 2.1 se muestran las principales clasificaciones de las redes de datos por su cobertura geográfica:

Tabla 2.1 clasificación de las redes por su cobertura geográfica

Distancia entre ordenadores	Ubicados	Tipo de red
1 m	m^2	Red de área personal
10 m	Laboratorio - habitación	Red de área local
100 m	Edificio	Red de área local
1 km	Campus	Red de área metropolitana
10 km	Ciudad	Red de área metropolitana
100 km	País	Red de área metropolitana
1000 km	Continente	Red de área amplia
10000 km	Planeta	Red de área global

A continuación se definen los 5 tipos de redes mencionadas anteriormente:

1) PAN's

Las PAN (Personal Area Networks o redes de área personal) están destinadas para comunicaciones entre dispositivos pertenecientes a un solo propietario a través de distancias pequeñas, por lo regular de 10 metros (véase la figura 2.1).

Figura 2.1 Red de área personal

2) LAN'S

Las infraestructuras de red pueden variar en gran medida en términos de:

- el tamaño del área cubierta,
- la cantidad de usuarios conectados, y
- la cantidad y tipos de servicios disponibles

Una red LAN es aquella red que conecta dispositivos en un área relativamente pequeña (véase la tabla 2.1 para conocer la distancia geográfica que una LAN puede cubrir), esta área puede ser: una habitación, un edificio o un conjunto de edificios conectados entre sí.

Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red (véase la figura 2.2).

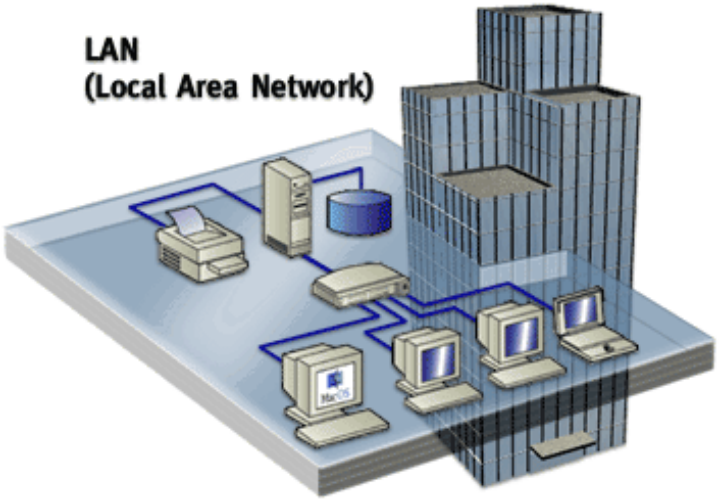


Figura 2.2 Red de área local

3) MAN's

La MAN (figura 2.3) es una red cuyo diámetro no va más allá de 100 km, y responde claramente a la necesidad de un sistema de comunicación de tamaño intermedio con beneficios que superan a los que pueden ofrecer las redes LAN o WAN. Estas redes, como se puede observar en la tabla 2.1, pueden llegar a ser países.

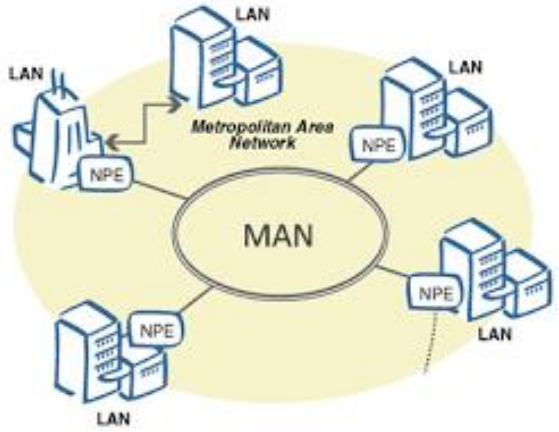


Figura 2.3 Red de área metropolitana

4) WAN's

Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, instalación y mantenimiento de éstos son aptitudes complementarias de la función de una red de la organización (véase figura 2.4).

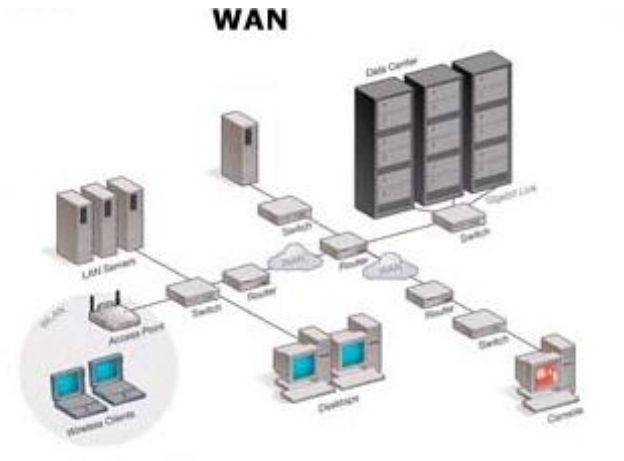


Figura 2.4 Red de área amplia

5) GAN's

La Red GAN (Red de Área Global) permite la conexión de una o varias LAN pertenecientes a diferentes países. GAN es un servicio de comunicación móvil que ofrece datos, voz y fax de alta calidad a velocidades de hasta 64 kbps. Los usuarios pueden elegir el servicio ISDN móvil de GAN (Red Digital de Servicio Integrado) para la transferencia rápida de grandes archivos de datos o el servicio móvil de datos por paquete (Mobil Packet Data Service) para aplicaciones de datos de uso variable como es el acceso a Internet y a correo electrónico. GAN también ofrece comunicaciones por voz con calidad de difusión.

2.2 Seguridad informática

Desde hace mucho tiempo, las empresas, organizaciones e incluso las personas mismas han invertido mucho esfuerzo en proteger el activo más importante para todos: la información. La seguridad informática nace como una solución derivada de la necesidad de proteger la información, ya que, en algún punto de la historia la información deja de almacenarse solamente de forma impresa y pasa a estar almacenada dentro de computadoras, servidores, y hoy en día data centers.

La seguridad informática tiene 3 objetivos básicos, los cuales son sus pilares y serán tratados más adelante: la integridad, la disponibilidad y la confidencialidad de la información.

Definición

Se pueden encontrar varias definiciones de la seguridad informática, a continuación se presentan algunas:

"La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad."

Otra definición de la seguridad informática es la siguiente:

"La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante."

Una tercera definición se presenta a continuación:

"El conjunto de normas, mecanismos, herramientas, procedimientos y recursos orientados a brindar protección a la información resguardando sus disponibilidad, integridad y confidencialidad"

Con base en lo planteado anteriormente y las definiciones vistas es que en el presente trabajo se ha construido una definición propia.

"La Seguridad Informática es el conjunto de metodologías, controles, normas, mecanismos, herramientas, procedimientos y recursos que buscan mantener en un estado de operación esperado todo aquel sistema informático, garantizando la disponibilidad, integridad y confidencialidad de la información almacenada en el mismo".

2.2.1 La triada de la seguridad informática

Sin duda alguna la triada de la seguridad informática es sumamente importante, ya que, esta es la que define los objetivos fundamentales de la seguridad informática que se definirán más adelante, la integridad, la confidencialidad y la disponibilidad de los activos de la organización.

Figura 2.5 Triada de la seguridad informática

1) Confidencialidad

   La confidencialidad de la información tiene que ver con que la información esté protegida de su revelación no autorizada.

2) Integridad

   La integridad significa que la información es confiable, completa y está protegida de modificaciones no intencionales, no anticipadas y no autorizadas por la propia organización y que mantiene la consistencia entre la información interna en la computadora y la realidad del mundo exterior.

3) Disponibilidad

   Éste último objetivo de la seguridad informática tiene que ver con que la información y los recursos informáticos estén disponibles cuando se les necesite para alcanzar los requerimientos del negocio y evitar pérdidas substanciales por su ausencia.

2.2.2 Principios básicos de la seguridad de la información

Estos principios básicos de la seguridad de la información, son indispensables para lograr tener una noción de seguridad más fuerte, ya que si se aplican más de uno de estos principios a la estructura informática en cuestión (dentro de empresas, organizaciones, dispositivos personales, etcétera) se puede proporcionar un nivel más alto de seguridad en la información que manejamos. Dentro de este apartado se tratarán conceptos tales como: Rotación de funciones, separación de tareas, menos privilegio, no repudio, rastreabilidad, control de accesos y audit trails o logs.

a) Rotación de funciones

- Rotar al personal en las diferentes funciones de la organización.

- No dejar a una persona demasiado tiempo en un solo rol.
- Obligar al personal con funciones clave a tomar vacaciones al menos una vez al año.

El no rotar funciones representa un problema para la organización, ya que una sola persona puede llegar a adquirir un gran conocimiento dentro de un área en específico, con el cual podría atacar a la organización sin que nadie lo note.

b) Separación de tareas

- Dos mecanismos o personas que se deben coordinar para "abrir", "desplegar" o "completar" un proceso sensitivo, información o un componente del sistema.
- Debe haber un acuerdo explícito entre dos entidades para ganar acceso o permiso al recurso solicitado.

Aplicar este principio dentro de una organización ayuda a mitigar ataques internos, debido a que los movimientos críticos de una organización (económicos, de información, etcétera.) no los lleva a cabo una sola persona.

c) Menor privilegio

- Asignación mínima de permisos de acceso en base a la necesidad para poder cumplir con sus tareas ("*Least privilege / nee to know*")

Este privilegio asegura que los activos de las organizaciones cumplan con los 3 objetivos de la seguridad informática, ya que limita el uso de los recursos informáticos dentro de la misma con la finalidad de mitigar ataques internos de cualquier índole.

d) Control de accesos

- Identificación: El usuario se identifica al querer acceder a algún dispositivo dentro del sistema.
- Autenticación: Es el proceso mediante el cual las credenciales proporcionadas por el usuario se validan.

- Algo que sé: Por lo general, tiene que ver con las contraseñas de los usuarios.
- Algo que tengo: Este método se basa en que el usuario tenga algo físico, como un token, para poder acceder a los sistemas.
- Algo que soy: Este último, está relacionado directamente con los diferentes métodos de acceso en los cuales se pide al usuario identificarse haciendo uso de diferentes extremidades de su cuerpo: ojos, manos, dedos, etcétera.

- Autorización: Se autoriza al usuario para hacer uso del sistema.

El control de accesos es una herramienta de seguridad que permite controlar el acceso a los recursos informáticos de una organización, con lo que se puede prevenir que una persona acceda a áreas restringidas si ésta no tiene el permiso de hacerlo.

e) Rastreabilidad

Es la propiedad que permite detectar al usuario responsable de las actividades en el sistema.

Este principio permite conocer quién está haciendo qué en el sistema, sin importar que tipo de perfil esté usando. Con lo que se puede evitar que un usuario realice actos ilícitos que atenten contra la organización o contra terceras personas.

f) No repudio

Es la propiedad de detectar que usuario hace qué en el sistema y que éste no pueda negar el haber hecho algo. Ayuda a detectar ataques internos como la fuga de información, así como encontrar al responsable del ataque.

g) Logs

Registro de las actividades tanto del sistema como los usuarios.

2.2.3 Herramientas de seguridad

Actualmente existen diferentes aplicaciones de seguridad que ayudan a prevenir, detectar y mitigar los ataques informáticos a los que están expuestos diariamente los sistemas de información. Y a pesar de que dichas aplicaciones no pueden garantizar al 100% la seguridad de la información resguardada en sistemas informáticos, se intentan mantener al margen de las necesidades del mercado y se actualizan periódicamente para ofrecer un nivel de seguridad mayor a la versión anterior. Algunas de estas herramientas se ven a continuación.

a) Monitoreo

Esta técnica, sin duda alguna es una herramienta sumamente importante dentro de cualquier infraestructura o sistema de información. Su definición formal es la siguiente:

"El término *Monitoreo de red* describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico u otras alarmas."

Y ¿qué se debería monitorear?

Esta técnica o herramienta de seguridad puede ser utilizada para monitorear los recursos informáticos que se encuentran en la red, como son:

- Utilización de ancho de banda
- Servicios en ejecución
- Tipo de tráfico
- Estado físico de las conexiones

- Consumo de memoria
- Consumo de CPU

Con base en los resultados obtenidos mediante el monitoreo de red, los altos mandos dentro de las empresas con el apoyo de los administradores de la red pueden llegar a tomar decisiones más certeras en cuanto al uso de los recursos informáticos dentro de la misma.

Existen dos tipos de monitoreo de red, los cuales se presentan a continuación:

- Monitoreo activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red en la que se está trabajando, o simplemente enviando paquetes a algunas aplicaciones para medir el tiempo de respuesta de las mismas. El resultado arrojado por este tipo de monitoreo está directamente relacionado con el rendimiento de la red, y su problema principal es el cargar tráfico a la misma.
Algunas de las técnicas más usadas para realizar un monitoreo de este tipo son:

- Basadas en ICMP: Ayudan a dimensionar la disponibilidad de una red y de los hosts dentro de la misma. También se puede medir el retardo, la pérdida de paquetes e identificar diversos problemas en la red.
- Basadas en TCP: Se usan para tener una idea más clara de la tasa de transferencia y para diagnosticar problemas a nivel de la capa de aplicación.
- Basadas en UDP: Pueden identificar la pérdida de paquetes en un solo sentido, además de algunos problemas en la red.

- Monitoreo pasivo

El monitoreo pasivo se basa en obtener y analizar el tráfico generado en la red, y al contrario del monitoreo activo, este tipo de monitoreo no genera más carga a la red. Usa

diferentes aplicaciones para lograr su objetivo, herramientas como los sniffers.

- Aplicaciones

En la actualidad existen diversas herramientas que permiten realizar un monitoreo de red exitoso, algunas de ellas son más usadas que otras, pero todas nacieron de la necesidad de tener un conocimiento más extenso acerca de la red en la que se trabaja. A continuación, se presenta una lista de aplicaciones y una breve descripción de las mismas:

Netcat: Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP.

TCPDump / WinDump: El sniffer clásico para monitoreo de redes y adquisición de información. Tcpdump es un conocido y querido analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red {"network interface"} que concuerden con cierta expresión de búsqueda. Es posible utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma.

Ethereal: Ethereal es un analizador de protocolos de red para Unix y Windows, y es libre. Permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que se desee ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Hping2: Una utilidad de observación {probe} para redes similar a ping pero con esteroides. Hping2 ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. Esta herramienta es particularmente útil al tratar de utilizar funciones como las

de traceroute/ping o analizar de otra manera hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.

GFI LANguard: Un escáner de red no-libre para Windows. LANguard escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches {patches} de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro {"key registy entries"}, passwords débiles, usuarios y grupos; y más. Los resultados del escaneo se muestran en un reporte en formato HTML, que puede ser modificado a gusto propio o consultado.

Whisker/Libwhisker: Whisker es un escáner que nos permite poner a prueba servidores de HTTP con respecto a varios agujeros de seguridad conocidos, particularmente, la presencia de scripts/programas peligrosos que utilicen CGI.

Nessus: Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

Nikto: Nikto es un escáner de servidores de web que busca más de 2000 archivos/CGIs potencialmente peligrosos y problemas en más de

200 servidores. Utiliza la biblioteca LibWhisker pero generalmente es actualizado más frecuentemente que el propio Whisker.

Kismet: Kismet es un sniffer y disecador de redes 802.11b. Es capaz de "sniffear" utilizando la mayoría de las placas inalámbricas; de detectar bloques de IP automáticamente por medio de paquetes de UDP, ARP, y DHCP; listar equipos de Cisco por medio del "Cisco Discovery Protocol"; registrar paquetes criptográficamente débiles y de generar archivos de registro compatibles con los de ethereal y tcpdump. También

incluye la habilidad de graficar redes detectadas y rangos de red estimados sobre mapas o imágenes.

XProbe2: XProbe es una herramienta que sirve para determinar el sistema operativo de un host remoto. Logran esto utilizando algunas de las mismas técnicas que Nmap al igual que muchas ideas diferentes. Xprobe siempre ha enfatizado el protocolo ICMP en su enfoque de identificación {fingerprinting}.

Para mayor información acerca de estas herramientas y muchas otras más, se puede consultar el siguiente link:
http://insecure.org/tools/tools-es.html

b) Escaneo

Las herramientas de escaneo actuales se encargan de analizar, detectar, procesar e incluso monitorear los hosts dentro de una red para verificar el nivel de protección de los mismos contra ataques, incluso también verificar el nivel de vulnerabilidad de uno o más hosts. También pueden llegar a escanear todo un segmento de red.

Muchas de las aplicaciones utilizadas para realizar el monitoreo de la red también se utilizan al realizar el escaneo. A continuación se mencionan algunas de estas aplicaciones:

Nessus: Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

Nmap: Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

GFI LANguard: Un escáner de red no-libre para Windows. LANguard escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches {patches} de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro {"key registy entries"}, passwords débiles, usuarios y grupos; y más. Los resultados del escaneo se muestran en un reporte en formato HTML, que puede ser modificado a gusto propio o consultado.

c) Firewalls

Un firewall es un sistema que protege una computadora o a una red de computadoras contra intrusiones provenientes de redes de terceros u otros segmentos dentro de la misma red organizacional. Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet (véase figura 2.6).

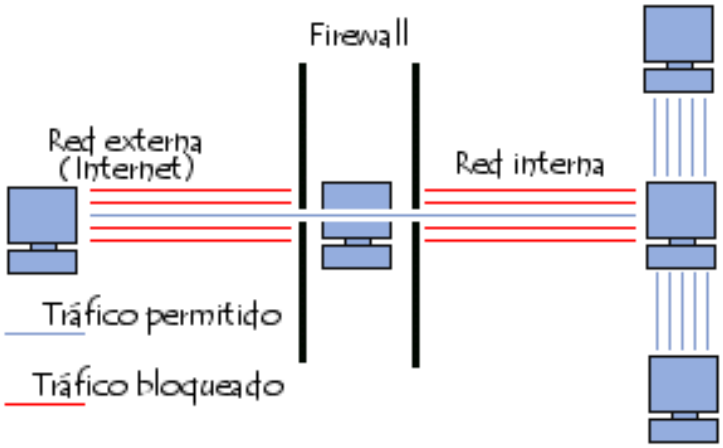


Figura 2.6 Firewall

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local y una o más redes externas.

La función del firewall dentro de una red la determina el administrador de la misma, ya que, para que éste funcione correctamente se tienen que establecer ciertas reglas, ya sean de denegación de conexión o de autorización de conexión. Estas reglas están directamente relacionadas con las

políticas de seguridad de cada empresa, organización o persona.

Existen diferentes tipos de firewalls, los cuales se mencionan a continuación:

Filtrado de paquetes: Un sistema de firewall opera según el principio del filtrado simple de paquetes, o filtrado de paquetes stateless. Analiza el encabezado de cada paquete de datos (datagrama) que se ha intercambiado entre un dispositivo de la red interna y el exterior.
Así, los paquetes de datos que se han intercambiado entre un dispositivo de la red externa y uno con la red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP origen
- La dirección IP destino
- El tipo de paquete (TCP o UDP)
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Filtrado Dinámico: El filtrado dinámico de paquetes se basa en la inspección de las capas 3 y 4 del modelo OSI, lo que permite controlar la totalidad de las transacciones entre el cliente y el servidor. El término que se usa para denominar este proceso es "inspección stateful" o "filtrado de paquetes stateful".
Un dispositivo de firewall con "inspección stateful" puede asegurar el control de los intercambios. Esto significa que toma en cuenta el estado de paquetes previos cuando se definen reglas de filtrado. De esta manera, desde el momento en que una máquina autorizada inicia una conexión con una máquina ubicada al otro lado del firewall, todos los paquetes que pasen por esta conexión serán aceptados implícitamente por el firewall.

Filtrado de aplicaciones: El filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones opera en la capa 7 del modelo OSI (capa de aplicación), a diferencia del filtrado simple de paquetes (capa 4). El filtrado de aplicaciones implica el conocimiento de los protocolos utilizados por cada aplicación.

Un firewall que ejecuta un filtrado de aplicaciones se denomina generalmente "pasarela de aplicaciones" o "proxy" (véase figura 2.7), ya que actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido en los paquetes intercambiados. Por lo tanto, el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Además, el filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad.

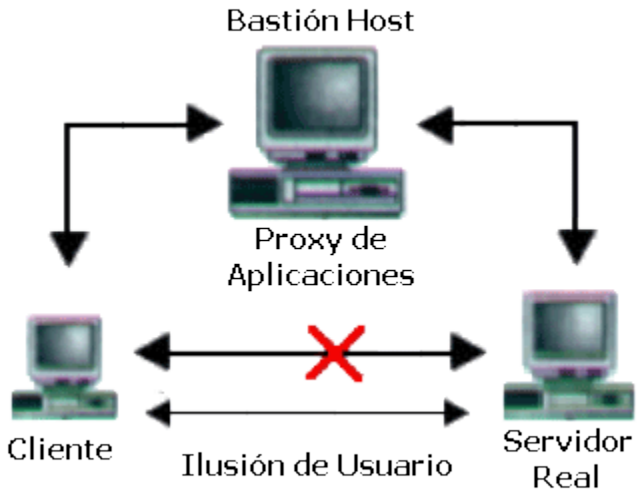


Figura 2.7 Proxy

d) Detección de intrusos

Un sistema de detección de intrusos (IDS) es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. La forma en que un IDS detecta las anomalías pueden variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a sus recursos.

Un IDS, figura 2.8, protege a un sistema contra ataques, malos usos y compromisos. Puede también monitorear la actividad de la red, auditar las configuraciones de la red y sistemas por vulnerabilidades, analizar la integridad de los datos y más.

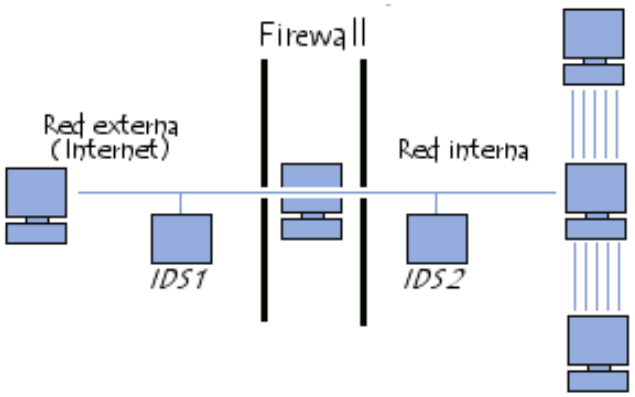


Figura 2.8 IDS

Dentro de los sistemas de detección de intrusos se tienen dos grandes vertientes:

- HIDS: Son los sistemas de detección de intrusos en el host, y su función principal es garantizar la seguridad en el host.
- NIDS: Sistemas de detección de intrusos en la red, garantizan la seguridad en la red.

e) Criptografía

Esta puede ser definida como una rama de las matemáticas y en la actualidad también de la informática, que hace uso de métodos y técnicas con el objeto principal de transformar la información a fin de que sea ininteligible, esto es, cifrar, y por tanto proteger un mensaje o archivo por medio de un algoritmo usando una o más claves, como se puede observar en la figura 2.9.
Esto da lugar a diferentes tipos de sistemas de cifrado, denominados criptosistemas, que permiten resguardar aspectos básicos de la seguridad informática: la confidencialidad o secreto del mensaje, la integridad del mensaje y autenticidad del emisor, así como el no repudio mutuo entre cliente y servidor.

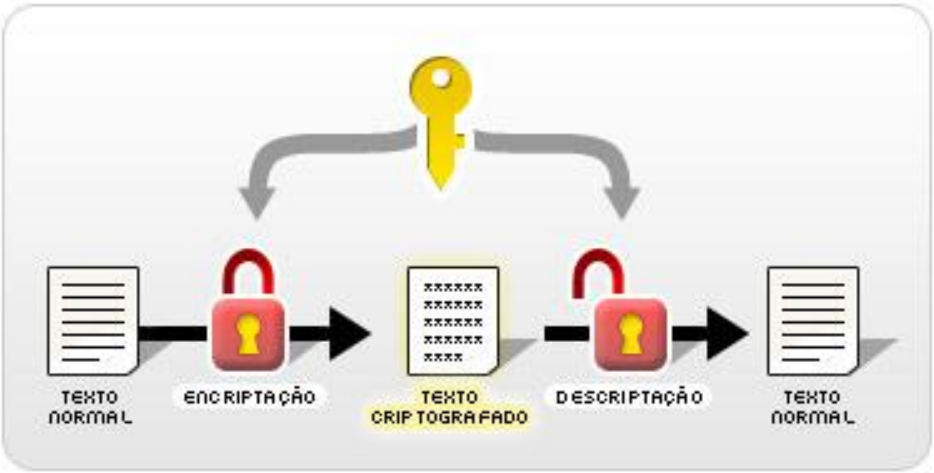


Figura 2.9 Criptografía

Algunas aplicaciones utilizadas para cifrar información son las siguientes:

- *GnuPG / PGP*: PGP es el famoso programa de cifrado diseñado por Phil Zimmerman que ayuda a proteger nuestra información de curiosos y otros riesgos.

- *AES Crypt*: es un software avanzado de cifrado de archivos que utiliza el estándar *Advanced Encryption Standard* también conocido como *Rijndael*, para cifrar de forma fácil y segura tus archivos. Esta herramienta se ejecuta desde la línea de comandos en Linux y integra con la *shell* Windows. Todos los archivos y directorios cifrados con AES Crypt son accesibles mediante una contraseña que solo debería manejar el autor, eliminando así los accesos no autorizados. También dispone de una biblioteca para los desarrolladores que utilizan Java para leer y escribir archivos con formato AES.

- *Axcrypt*: es un software de cifrado de archivos de código abierto que hace uso del algoritmo AES-128 y SHA-1 para estos fines. Se integra perfectamente con Windows para comprimir, cifrar, descifrar, almacenar, enviar y trabajar con archivos individuales. Protege con contraseña cualquier número de archivos a través de un fuerte cifrado y viene listo para usar ya que no requiere configuración.

- *EncFS*: es un sistema de archivos cifrado basado en FUSE, el sistema de archivos en el espacio de usuario. Cifra los archivos utilizando un directorio arbitrario como almacenamiento de los mismos, quedando esto transparente al usuario.

Para concluir el presente capítulo, es necesario reflexionar acerca del beneficio que brindan las herramientas de seguridad ya que se vuelven sumamente importantes cuando se habla de proteger los activos de una empresa y los sistemas informáticos que la componen. Es por ello, que con base en el panorama mostrado a lo largo de este capítulo se realiza un sistema de monitoreo con la finalidad de prevenir y detectar posibles incidentes de seguridad en una red de cualquier tipo, tomando en cuenta los nuevos recursos tecnológicos que los ciber atacantes utilizan.

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

- Bruce Schneier

Capítulo 3
Diseño y desarrollo del sistema de monitoreo de red

A lo largo de este capítulo se explican el diseño y el desarrollo de la aplicación de monitoreo, tomando en cuenta lo visto en los dos capítulos anteriores con la finalidad de cumplir con los objetivos planteados al inicio del presente documento.

Al llevar a cabo el desarrollo de la aplicación, es necesario establecer claramente las funciones que va a realizar la misma. Por lo que al inicio de este capítulo quedan establecidos los requerimientos del sistema con lo que se da lugar al diseño de cada uno de los módulos o subsistemas que hacen posible el correcto funcionamiento del mismo.

3.1 Requerimientos del sistema

Los requerimientos del sistema son parte sustancial en el diseño de cualquier aplicación, ya que con base en estos se implementa el sistema solicitado. A continuación se presenta la lista de requerimientos sobre los cuales se basa el desarrollo del sistema de monitoreo que cumple con los objetivos que se plantearon al inicio de este documento.

- Escaneo rápido de la red
- Escaneo detallado sobre un dispositivo
- Analizar el tráfico de red

El sistema no cuenta directamente con un analizador de tráfico, pero es capaz de tener relación con cualquier sniffer de uso libre o de licencia, por lo que se ha utilizado WireShark como la herramienta que usará el administrador de red para tales fines.

En la tabla 3.1 se puede observar la relación entre los requerimientos del sistema y los objetivos planteados.

Tabla 3.1 Requerimientos vs objetivos

Requerimientos Objetivos	Escaneo rápido de la red	Escaneo detallado sobre un dispositivo	Analizar el tráfico de red
Identificar usuarios conectados a la red	✓		
Identificar usuarios con Jailbreak	✓	✓	
Identificar usuarios con fines de ataque		✓	✓

Con la finalidad de crear un ambiente con mayor control y seguridad por parte del administrador de la red y los altos mandos de las organizaciones, el sistema cuenta con requerimientos adicionales:

- Login del administrador de la red
- Base de datos para las credenciales
- Consulta de registros
- Búsqueda de registros
- Base de datos para almacenar la información del escaneo
- Generación de reportes en formato PDF
- Generación de gráficas
- Geolocalización
- Generación de listas negras
- Cierre de sesión
- Persistencia en la base de datos
- Persistencia sobre los archivos
- Software intuitivo
- Alta compatibilidad

3.2 Plataforma de desarrollo

Para llevar a cabo el desarrollo de este sistema de monitoreo, es menester definir claramente la plataforma en la cual se implementará y sobre la cual podrá ser ejecutado sin problema alguno.
Para ello, se presenta una comparativa entre los sistemas operativos con mayor demanda hoy en día, a partir de la cual se identifica un sistema operativo basado en UNIX como plataforma de desarrollo, así como el lenguaje de programación PHP y el manejador de bases de datos MySQL.
A lo largo de este subtema se explica el porqué de esta elección, empezando por el sistema operativo y concluyendo con el manejador de bases de datos.

3.2.1 UNIX

Se elige un sistema operativo basado en UNIX debido a que hoy en día, estos sistemas operativos son los más usados en

ambientes de seguridad informática y de desarrollo web debido a la seguridad que estos tienen a nivel de servidor.

A continuación se dan a conocer las razones por las cuales se lleva a cabo esta elección.

- Precio: Es posible descargar el sistema operativo gratuitamente, y en una enorme variedad de versiones (Kali Linux, Mint, Fedora, etcétera) las cuales incluyen distintas herramientas y enfoques tecnológicos distintos.

- Requisitos de hardware: Debido a que UNIX se puede usar exclusivamente en modo texto, no existe la necesidad de cargar un entorno gráfico, lo que permite que se ejecute en cualquier máquina, por lo que no es necesario contar con una gran cantidad de recursos computacionales.

- Estabilidad: Al tener su núcleo basado en UNIX, hereda las características de estabilidad que siempre han distinguido a un sistema operativo UNIX. Con lo que se puede asegurar que el seleccionar este tipo de sistemas operativos hace que el sistema de monitoreo implementado funcione de manera óptima.

- Seguridad: Algunos de los sistemas operativos basados en UNIX cuentan con el aval de seguridad por parte de la NSA (Agencia Nacional de Seguridad de los Estados Unidos de América), por ejemplo Trusted Xenix. Y a pesar de que no todos estos sistemas operativos pueden costear una evaluación de la NSA, no se consideran totalmente inseguros, a tal punto que incluso Yahoo cuenta con sistemas operativos Linux o FreeBSD dentro de su red.

- Compatibilidad: Reconoce otros sistemas operativos en una red, lo cual para fines prácticos y de desarrollo es fundamental para el sistema de monitoreo.

- Velocidad: En cuestiones de velocidad, el entorno gráfico de cualquier sistema operativo basado en UNIX es más rápido que algunos otros sistemas comerciales.

3.2.2 PHP

PHP es un lenguaje de programación de uso general, por lo que es posible realizar consultas a bases de datos, desarrollo web y comunicación entre dispositivos fácilmente. También, es un lenguaje cuyo código es ejecutado del lado del servidor, lo que hace que el usuario final no requiera de recursos computacionales precipitados. Es por ello que se ha elegido PHP como el lenguaje de programación, y a continuación se explican algunos puntos relacionados a esta selección.

- Velocidad: PHP es un lenguaje de programación que no requiere de muchos recursos computacionales para ser ejecutado, ya que este se ejecuta a nivel de servidor, lo que lo hace más rápido que otros lenguajes.

- Estabilidad: PHP utiliza su propio sistema de administración de recursos y dispone de un buen manejo de variables, conformando un sistema robusto y estable. Ya que, en comparación con otros lenguajes de programación, PHP no utiliza muchos recursos computacionales por parte del usuario, debido a que se ejecuta a nivel de servidor. Mientras que otros lenguajes, hacen uso de los recursos de la máquina en donde son ejecutados para funcionar correctamente.

- Seguridad: El código fuente escrito en PHP es invisible al navegador y al cliente, ya que es el servidor el que se encarga de ejecutar el código y enviar su resultado HTML al navegador. Y es por ello que el programar en PHP hace que se cumpla la confidencialidad a nivel de código.

- Simplicidad: Se les debe permitir a los programadores generar código productivamente en el menor tiempo posible con un mayor alcance en cuanto a funcionalidad. PHP dispone de una amplia gama de bibliotecas por lo que agregar extensiones es más práctico.

- Accesibilidad: PHP es un lenguaje de programación de código abierto y gratuito, mantenido por toda una comunidad de desarrolladores con gran facilidad para acceder a documentación, ejemplos y contenido para desarrolladores.

3.2.3 MySQL

MySQL es un sistema de gestión de bases de datos relacionales de código abierto, de la misma manera en que lo es PHP y las distribuciones de GNU/Linux, lo que permite que el sistema se desarrolle sin necesidad de pagar licencias de uso. También, cabe mencionar el uso de este manejador de bases de datos en ambientes web, el cual ha ido incrementando por las bondades del mismo.
A continuación se presentan los puntos clave para la elección de este manejador de bases de datos.

- Alta velocidad al realizar las operaciones de consulta. Esta característica de Mysql ayuda a que el rendimiento de las bases de datos desarrolladas para el sistema de monitoreo sea óptimo.

- Elaboración de bases de datos con lo mínimo de recursos computacionales.

- Soporta gran variedad de sistemas operativos, siendo principalmente utilizado en aquellos basados en UNIX.

3.3 Herramientas de desarrollo

En este apartado se muestran y explican las diferentes herramientas de desarrollo que se usan para la implementación del sistema de monitoreo de red, de tal forma que este sistema cumpla con los requerimientos establecidos anteriormente.

A continuación, se listan las herramientas utilizadas:

- **Kali Linux**

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd.

Este sistema operativo basado en UNIX trae preinstalados numerosos programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usada desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

- **XAMPP (PHPMyAdmin y Apache)**

XAMPP es el entorno más popular de desarrollo con PHP. A su vez, es una distribución de Apache completamente gratuita y fácil de instalar que contiene MySQL, PHP y Perl.

- **Fping**

Fping es un programa que permite enviar paquetes ICMP, similar a un ping, pero con un mejor rendimiento al momento de enviar pings a múltiples hosts.

- **Nmap**

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

- **SSH**

SSH es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH cifra la sesión de conexión, haciendo

imposible que alguien pueda obtener información en texto claro.

- **Curl**

Curl es una herramienta software para transferencia de archivos con sintaxis URL mediante intérprete de comandos, soportando FTP, FTPS, HTTP, HTTPS, TFTP, SCP, SFTP, Telnet, DICT, FILE y LDAP.

- **WireShark**

WireShark es un analizador de protocolos de red para Unix y Windows, y es libre. Permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Este sniffer cuenta con varias características poderosas, incluyendo un completo lenguaje para filtrar lo que se desee ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Y haciendo uso de cada una de estas herramientas es como se desarrolla el sistema de monitoreo de red, así como se vuelve sustancial el uso de un analizador de tráfico externo para cumplir con los objetivos planteados al inicio, así como con los requerimientos planteados en este capítulo.

3.4 Tipo de monitoreo

Como se vio en el capítulo 2, existen dos maneras de llevar a cabo un monitoreo de red: pasivo y activo.
Para comenzar el diseño y el desarrollo del sistema de monitoreo es menester realizar un comparativo entre ambos tipos de monitoreo para finalmente poder elegir uno en el que el sistema estará basado.

Un monitoreo pasivo es aquél en el que se basa en la obtención de datos a partir de la recolección y el análisis del tráfico de red, por lo que para realizar dicho monitoreo se necesitan herramientas tales como sniffers. Este tipo de

monitoreo no añade tráfico a la red, como lo hace el monitoreo activo.

Un monitoreo activo se realiza inyectando paquetes a la red, midiendo el tiempo de respuesta de los dispositivos y aplicaciones conectados a la misma. Este monitoreo hace uso de tres protocolos básicos (ICMP, TCP y UDP) para recabar la información necesaria de los dispositivos y aplicaciones de la red.

Con la explicación anterior de cada uno de los tipos de monitoreo se puede llegar a la conclusión de que el sistema que se desarrolla a lo largo de este capítulo, es un sistema que se basa en el monitoreo activo, ya que dentro de los objetivos del sistema se destaca principalmente el de detectar dispositivos que se encuentren en la red y que estén utilizando el Jailbreak de Apple.

Sin embargo, una de las cualidades del sistema es que también se pueden incorporar herramientas de monitoreo pasivo para llevar a cabo un seguimiento a los datos arrojados por el sistema desarrollado, como análisis del tráfico de red y generación de listas negras.

3.5 Diseño del sistema de monitoreo

Con base en los requerimientos proporcionados del sistema, se llega a una lista de módulos que en conjunto realizan todo lo que el usuario pide. A continuación se presenta la lista con 8 módulos o subsistemas:

1. Base de datos
2. Acceso al sistema y cierre de sesión
3. Escaneo
4. Generación de reportes en PDF
5. Presentación de gráficas
6. Generación de listas negras
7. Gestión de geolocalización
8. Consulta
9. Búsqueda de registros

El subsistema número 2 tiene que ver con el acceso al sistema, este módulo hace uso de una base de datos para validar las credenciales de los usuarios. Mientras que el módulo de cierre de sesión termina la sesión activa del usuario.

El siguiente subsistema (número 3) se hace cargo de los diferentes tipos de escaneos que tiene posibilidad de ejecutar con el sistema de monitoreo. Posteriormente se pueden visualizar los datos obtenidos con el módulo de presentación de gráficas, o si el usuario lo requiere se genere un reporte en formato PDF.

También es posible, haciendo uso de una herramienta que analice el tráfico de red, identificar dispositivos que estén haciendo mal uso de la misma y generar listas negras para bloquear dichos dispositivos de la red. Con el módulo de geolocalización se obtienen las coordenadas del servidor en el que se esté utilizando la herramienta.

El módulo de consulta realiza búsquedas de dispositivos ya conocidos por el mismo, así como antiguos escaneos para mitigar o facilitar la detección de ataques, de no ser suficiente la consulta de registros anteriores, se puede utilizar el módulo de búsqueda de registros para aumentar la precisión y facilidad para consultar registros en específico.

En la figura 3.1 se observan las tareas que el administrador puede llevar a cabo (color azul), y la salida del sistema (color rojo).

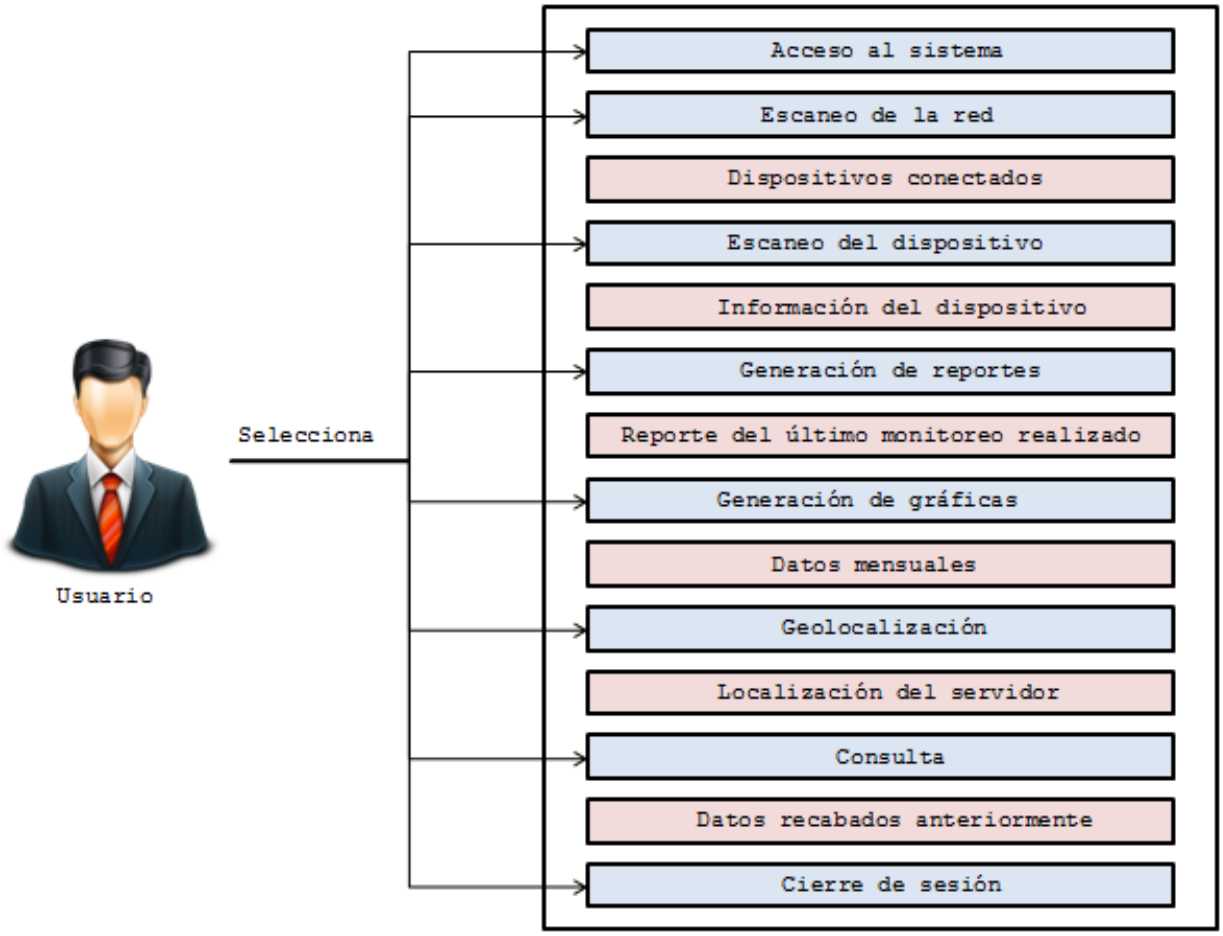


Figura 3.1 Diagrama general de usos

a) Diseño de la base de datos

Dentro de esta sección se tiene el diseño de la base de datos que se usa para almacenar la información obtenida de los escaneos realizados a la red, la información de la localización del servidor en el que se esté corriendo el sistema, credenciales de los usuarios autorizados y la información básica de los dispositivos que se encuentran conectados a la red (hostname, dirección ip, dirección mac, etcétera) Véase la figura 3.2.

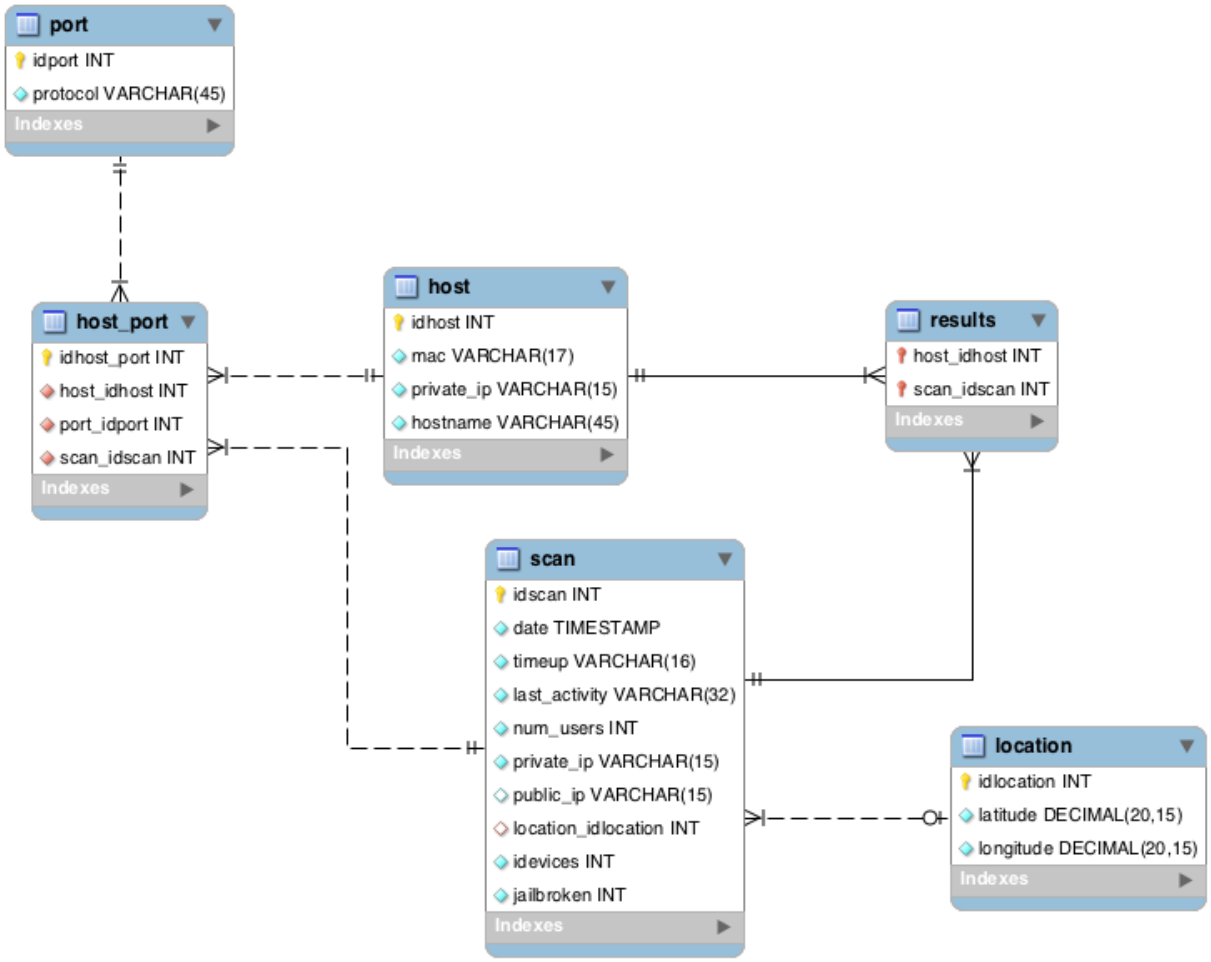


Figura 3.2. Diagrama entidad-relación de la base de datos

b) Diseño de los módulos de acceso al sistema y cierre de sesión

Para el diseño de estos módulos se toman en cuenta las políticas de seguridad correspondientes a la creación de contraseñas, ya que se crean credenciales para que los usuarios autorizados estén en condiciones de utilizar el sistema, así como salir del mismo.

El siguiente diagrama (figura 3.3) explica el uso de los dos módulos de acceso al sistema que se tienen, el módulo de acceso y el módulo de cierre de sesión.

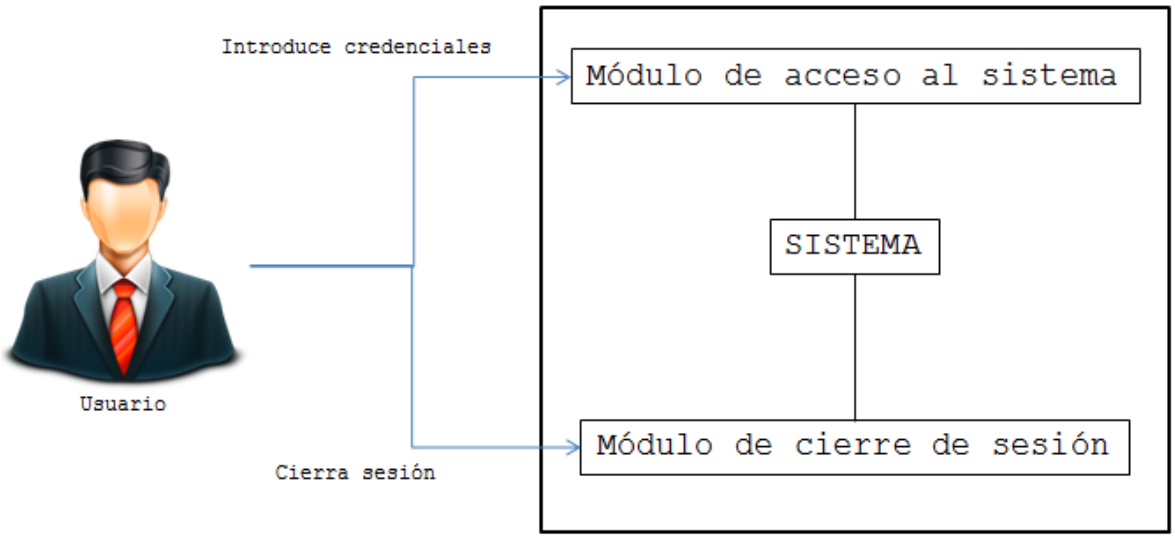


Figura 3.3. Diagrama de uso de los módulos de acceso al sistema y cierre de sesión

Como se puede observar en el diagrama de la figura 3.3, el usuario hace uso de ambos módulos. Para acceder al sistema y utilizar el mismo, es necesario que el usuario proporcione sus credenciales. Estas credenciales son validadas por el módulo de acceso al sistema, usando una base de datos, y de ser correctas dichas credenciales el usuario está en condiciones de utilizar el sistema, de lo contrario se manda un mensaje de error.

El módulo de cierre de sesión, saca al usuario del sistema, pero lo hace solo cuando el usuario realiza la petición.

c) Diseño de los módulos de escaneo

Al ser un sistema de monitoreo de red es imprescindible que este sistema sea capaz de llevar a cabo escaneos de la red y escaneos profundos sobre los dispositivos conectados a la misma, es por ello que se han incorporado al sistema dos módulos de escaneo. El primer escaneo que puede realizar el usuario se da sobre la red, con la finalidad de detectar a todos los dispositivos de la red y los servicios básicos que estén utilizando (Jailbreak, SSH, HTML, entre otros).

Mientras que el segundo escaneo tiene lugar sobre un dispositivo en específico, esto se hace con el fin de conocer a fondo un dispositivo que podría o no estar realizando ataques hacia o desde la red en cuestión o simplemente conocer más de su actividad dentro de la red para que dentro de la organización los recursos de esta sean usados como está establecido. Véase la figura 3.4.

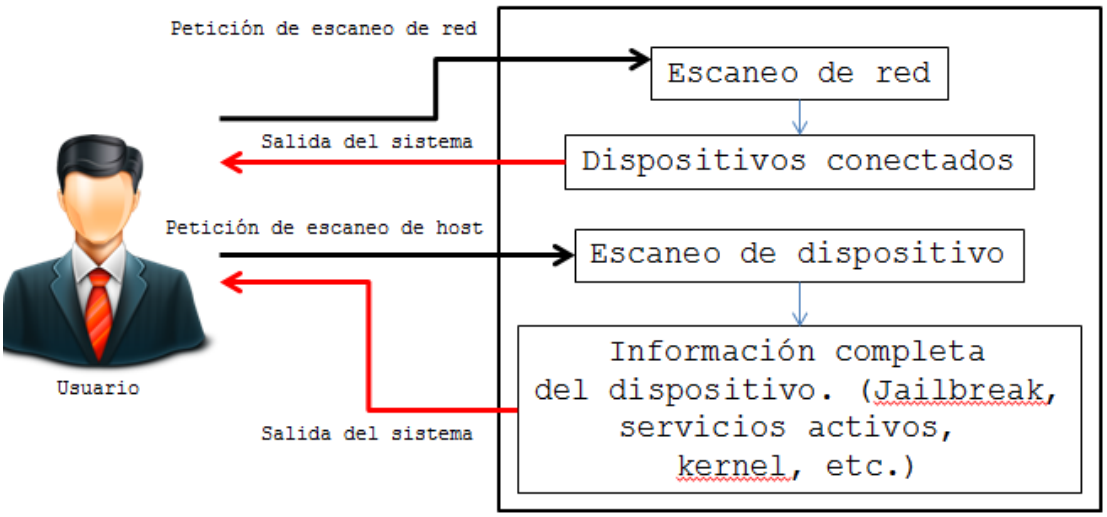


Figura 3.4. Diagrama de uso de los módulos de escaneo

Como se menciona anteriormente, el sistema hace uso de una herramienta de análisis de tráfico (cualquiera de las vistas en el capítulo dos), pero con la finalidad de hacer más sencilla la tarea del administrador de red se ha elegido Wireshark como el sniffer con el cual el sistema de monitoreo complementa la tarea de detección de intrusos por todas las bondades de este software (véase el capítulo 3.3 "Herramientas de desarrollo").

Empleando Wireshark como herramienta de análisis de tráfico de red se pueden identificar las acciones específicas de un dispositivo dentro o fuera de la red, con la finalidad de prevenir, detectar e inclusive eliminar ataques provenientes de dispositivos conectados en la red con el uso de listas negras.

d) Diseño del módulo de generación de reportes

La capacidad para generar reportes, los cuales puedan posteriormente ser impresos es uno de los requerimientos primordiales para el sistema, es por esto que para generar la impresión de un reporte, previamente el usuario debió ejecutar un análisis rápido en el sistema, y de igual manera si se desea obtener información sobre algún host en específico se deberá realizar dicho análisis para que de manera posterior pueda ser integrado en el documento generado.

Uno de los aspectos más relevantes para el sistema es la movilidad de los dispositivos, es por ello, que una vez que es generado el reporte, en este se incluye información importante respecto al servidor, datos como la fecha y hora, nombre del host, direcciones IP, segmentos de red, tiempo de encendido, última actividad registrada, versión y nombre del sistema operativo, coordenadas para la geolocalización, entre algunos otros.

Dentro del reporte se incluye una fotografía de la ubicación en donde se ejecutó el análisis, puesto que la movilidad es una característica de la cual se debe llevar un control de ubicaciones registradas. Véase la figura 3.5

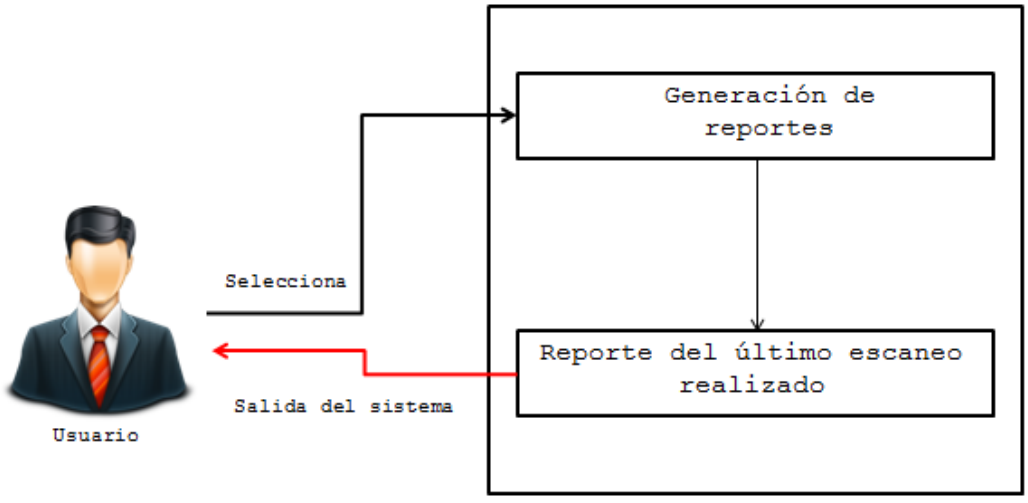


Figura 3.5 Diagrama de usos del módulo de generación de reportes

e) Diseño del módulo de generación de gráficas

Una pieza fundamental del sistema son las gráficas, las cuales tienen la finalidad de que el usuario de una manera sencilla tenga un panorama más amplia respecto a la cantidad de hosts que han sido analizados, así como realizar una distinción entre aquellos que ejecutan el sistema operativo iOS, y de esta manera identificar de manera visual, cuántos de estos dispositivos representan una amenaza para los dispositivos en red.

Se presenta información almacenada en la base de datos, ejecutando una serie de conteos y consultas que servían como referencia para el usuario final. Como se puede observar en la figura 3.6 el uso de este módulo es sencillo para el administrador de red.

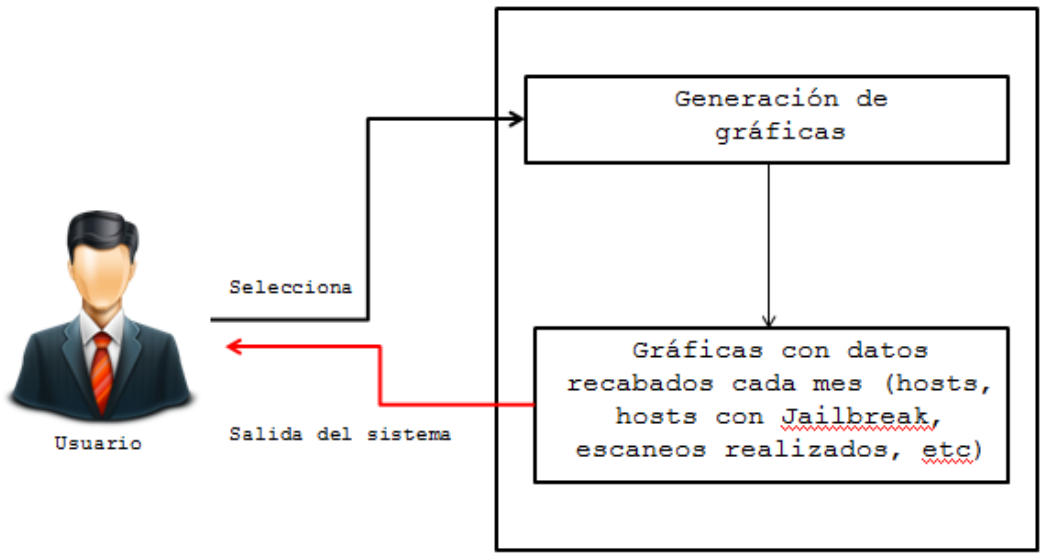


Figura 3.6 Diagrama de usos del módulo de generación de gráficas

f) Diseño del módulo de generación de listas negras

La generación de listas negras, como la persistencia de las mismas juega un papel importante para el administrador de la red, desde servir de referencia para identificar aquellos hosts que tienen una actividad sospechosa que inclusive fue corroborada, hasta tener la utilidad como logs del sistema basándose en fechas y dispositivos relacionados a ellas.

Dentro del sistema este módulo se encarga de generar en un archivo de texto plano un listado de todos aquellos hosts seleccionados por el usuario, donde sin identificados a partir de su nombre de host, dirección física y dirección lógica, con lo cual se obtiene una mayor precisión al identificar un dispositivo en específico, el archivo en texto plano generado tiene por nombre las palabras "black_list" junto con la fecha y hora en la que fue generado dicho archivo, esto evita que se sobrescriba el archivo si se generan varias listas negras por día. Véase figura 3.7

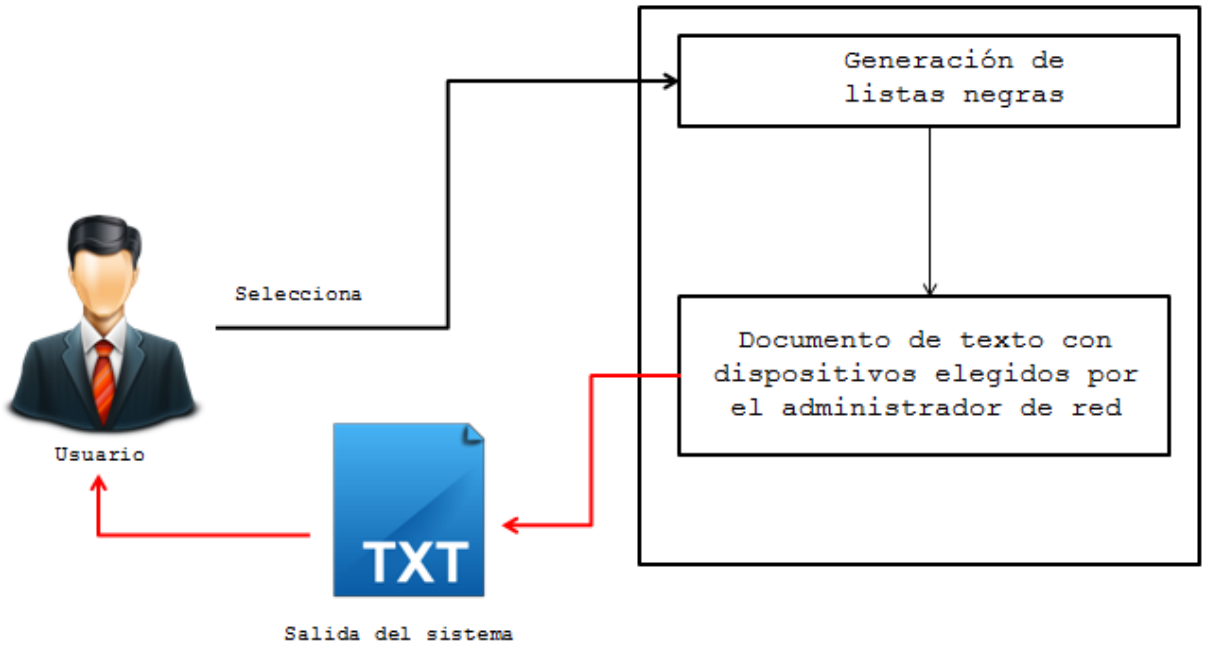


Figura 3.7 Diagrama de usos del módulo de generación de listas negras

g) Diseño del módulo de gestión de geolocalización

Para este módulo deberán cumplirse un conjunto de condiciones, tales como que el usuario final otorgue autorización al servidor para utilizar la geolocalización de esta manera se muestra la ubicación dentro del sistema y será almacenada en la base de datos, para su uso y consulta posterior.

Dentro de la sección de registros se despliega la información en cuanto a las coordenadas registradas de todas las ubicaciones almacenadas dentro de la base de datos, así como dos ligas que hacen referencia a la consulta directa en un mapa online, y una imagen de tal ubicación.

Este módulo también es utilizado para la generación de reportes PDF, por lo cual se incluyen las coordenadas y una fotografía de la ubicación dentro del documento. Véase la figura 3.8

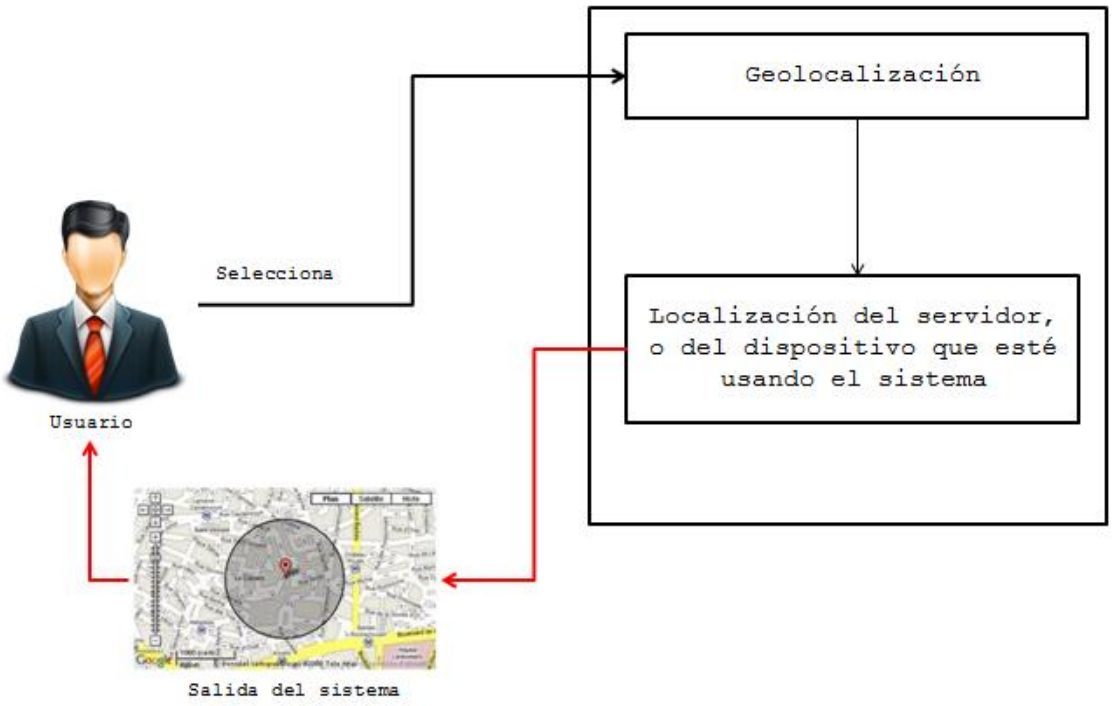


Figura 3.8 Diagrama de usos del módulo de gestión de geolocalización

h) Diseño del módulo de consulta

El módulo de consulta posee un diseño sencillo que permite consultar la información necesaria de una manera automatizada y con una complejidad nula. Dentro de este módulo se ejecuta la consulta directamente a la base de datos quien responde con el contenido almacenado, para ser presentado de manera posterior mediante la interfaz web y otorgar una presentación al usuario final, más agradable.

Se puede realizar la consulta respecto a los análisis realizados, obteniendo información respecto al servidor, y así como fechas de ejecución, mientras que también es posible consultar todas aquellas ubicaciones donde se han ejecutados los análisis, con la posibilidad de visualizar en el mapa la ubicación de donde se realizó dicho análisis, y por último, la parte medular es la consulta de toda aquella información almacenada respecto a los hosts que han sido escaneados, puertos abiertos, fechas de análisis, direcciones lógicas y físicas, nombres de host y la posibilidad de consultar informes específicos respecto a cierto host. Véase la figura 3.9.

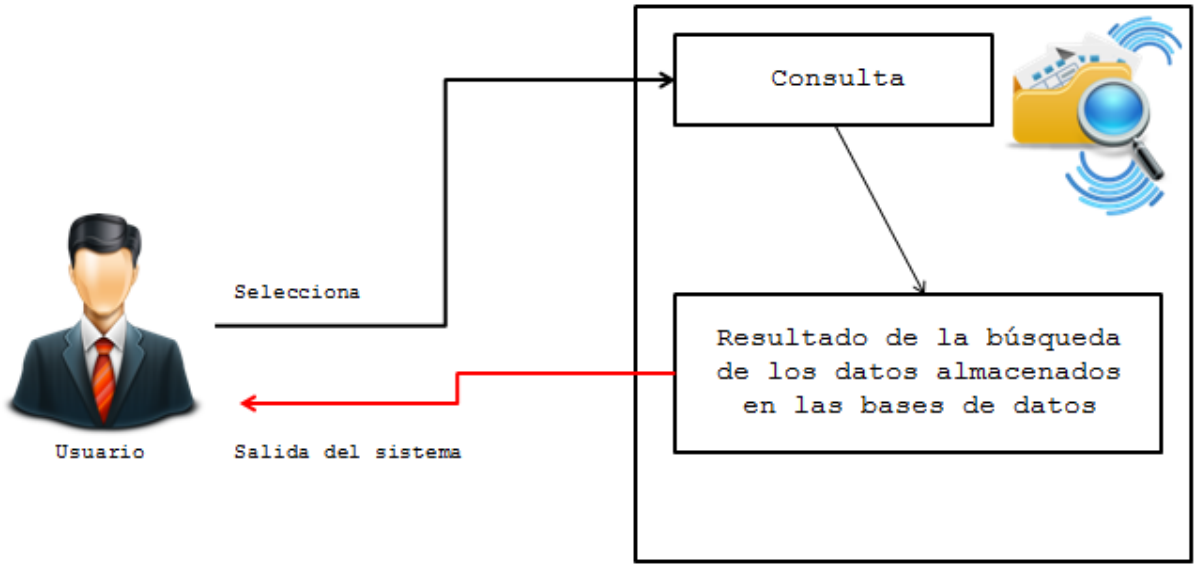


Figura 3.9 Diagrama de usos del módulo de consulta

i) Diseño del módulo de búsqueda de registros

La búsqueda de registros es una característica necesaria debido a la facilidad que le provee al administrador de red para detectar y mitigar ataques realizados a través de la red.

Se pueden realizar búsquedas a partir de fechas para un análisis proporcionado por el usuario, dando como resultado todos aquellos dispositivos involucrados en el análisis para la fecha solicitada. También es posible realizar una búsqueda mediante direcciones MAC, IP o nombres de host correspondientes a algún dispositivo, obteniendo por resultados todos los registros y fechas relacionadas a la información proporcionada.

3.6 Código fuente

En el presente apartado se muestran fragmentos de código fuente indispensables para que el desarrollo del sistema de monitoreo de red implementado cumpla con las funciones requeridas.
Con base en los módulos diseñados en el capítulo anterior, las funciones que se toman en cuenta en este apartado y es menester explicar son:

- Conexión con la base de datos
- Acceso al sistema y cierre de sesión
- Escaneo de red
- Escaneo de un dispositivo en particular
- Generación de reportes en formato PDF
- Presentación de gráficas
- Generación de listas negras
- Gestión de geolocalización
- Consulta

a) Conexión con la base de datos

El código necesario para establecer una conexión a la base de datos está determinado por las líneas de la figura 3.10, donde se intenta establecer una conexión al servidor "localhost"; para establecer tal conexión es necesario agregar otros parámetros como el nombre de usuario y la contraseña definidos para el servicio en ejecución de MySQL, teniendo como resultado una conexión exitosa o fallida, si el resultado de la conexión fuese fallido se responderá de tal manera de que el usuario identifique que existe algún problema con el servicio de la base de datos.

```php
<?php
    // Intenta la conexión con MySQL
    // Se utiliza el usuario "root" para poder insertar en la base de datos
    if($conexion = mysql_connect ("localhost",$_POST['user'],$_POST['password'])){

        // Selecciona la BD
        mysql_select_db ("tesis",$conexion) or header('Location:index.php?mensaje=No+existe+BD');

        mysql_close($conexion);

?>
```

Figura 3.10 Conexión con la base de datos

b) Acceso al sistema y cierre de sesión

El acceso al sistema se define en dos etapas, ambas se basan en el mismo principio, identificar y autenticar a un usuario a partir de un identificador de usuario (user) y una contraseña (password).

En la primera etapa, una vez que el usuario es autenticado comparando el nombre de usuario y su contraseña con una cadena de texto cifrada almacenada en la sesión actual, siendo que si este punto se corrobora satisfactoriamente se redirige al usuario en cuestión a un nuevo portal donde se establece la conexión directamente a la BD de la cual el sistema hace uso. En la figura 3.11 se muestran las líneas de código correspondientes a este módulo.

```php
<?php
session_start();

if(isset($_POST['user']) && isset($_POST['password'])){
    if($_POST['user']!="" && $_POST['password']!=""){

        // Intenta la conexión con MySQL
        // Se utiliza el usuario "root" para poder insertar en la base de datos
        if($conexion = mysql_connect ("localhost",$_POST['user'],$_POST['password'])){

            // Selecciona la BD
            mysql_select_db ("tesis",$conexion) or header('Location:index.php?mensaje=No+existe+BD');

                mysql_close($conexion);

                header('Location:home.php');

        }else{
            header('Location:index.php?mensaje=Error+al+conectar+con+el+servidor+verifique+usuario+y/o+contraseña');
        }

    }else{
        header('Location:index.php?mensaje=No+se+aceptan+espacios+en+blanco');
    }

}else{
    header('Location:index.php?mensaje=Debes+llenar+todos+los+campos');
}

?>
```

Figura 3.11 Acceso al sistema

El código correspondiente al cierre de sesión (figura 3.12), consta de unas cuantas líneas que solo tienen como finalidad cerrar la sesión del usuario, así como todo el contenido e información almacenada en ella, terminar conexiones con la base de datos y por último, redirigir al usuario al portal de inicio.

```php
<?php
    session_start();
    session_destroy();
    mysql_close($conexion);
    header('Location:index.php');
?>
```

Figura 3.12 Cierre de sesión

c) Escaneo de red

El análisis de red consiste básicamente en tres pasos:

1. Identificar las direcciones IP asignadas dentro de la red.

2. Obtener la dirección física relacionada a cada dirección IP encontrada.
3. Realizar la identificación y verificación de los puertos definidos para el análisis rápido, comprobando el estado de cada puerto en las distintas direcciones IP.

El código fuente mostrado en la figura 3.13 retorna un valor booleano como salida, señalando si se realizó un análisis exitosamente o no fue posible realizarlo.

```php
<?php
  function scan() { //Descubrimiento de red

    $ping = shell_exec($_SESSION['fpingcmd']." ".$_SESSION['network']." 2>&1");

    $direcciones = explode("\n", $ping);//Separamos la cadena por salto de línea
    array_pop($direcciones);//Eliminamos el último elemento

    foreach ( $direcciones as $ip) { //Almacenamos en un arreglo
        $_SESSION['direcciones'][$ip] =
        shell_exec($_SESSION['arpcmd']." | grep '".$ip.(
        ($_SESSION['system'] == "Linux\n") ? " ' | awk '{print $3}' 2>&1" : " ' | awk '{print $2}' 2>&1" )
        ); //Cada indice de alguna IP tiene por contenido su dirección MAC
    }

    if( isset($_SESSION['direcciones']) ){
        return 0; //Análisis exitoso
    }else{
        return -1; //Error, no hay direcciones identificadas en la red definida
    }

  }
?>
```

Figura 3.13 Escaneo de la red

d) Escaneo de un dispositivo

Nmap, una herramienta completamente versátil y ya mencionada anteriormente es un complemento esencial para el sistema. Su función principal es la ejecución de OS fingerprinting y banner grabing, devolviendo la salida al sistema para ser posteriormente mostrada al usuario y si éste lo desea, también será almacenada directamente en la base de datos.

Uno de los puntos importantes en esta función, se refiere a la capacidad de realizar la ejecución exitosa de Nmap y obtener la información requerida, para lo cual es necesario ejecutarlo a nivel usuario "root" por lo que se establece una conexión loopback al mismo servidor autenticado como usuario root, puesto que si el mismo servidor web ejecutara tal

acción, el comando sería lanzado bajo los privilegios del usuario "daemon". Véase la figura 3.14

```php
<?php

session_start();
    if(isset($_SESSION['network'])){
        include('Net/SSH2.php');

        function scan($ip) {

        $ssh = new Net_SSH2('127.0.0.1');//Conexión SSH loopback

        if (!$ssh->login($_SESSION['ssh_user'], $_SESSION['password']) ){
            exit('SSH Fingerprinting fallido y/o no coincide el password');
        }

        $stream = $ssh->exec($_SESSION['nmapcmd']." ".$ip." 2>&1");//ejecutamos nmap
        $stream = strstr($stream, 'Host is');//Quitamos todo texto no necesario

        $_SESSION['info'][$ip] = $stream; //Almacenamos la información obtenida para esta IP

        }
    }
?>
```

Figura 3.14 Escaneo de un dispositivo

e) Generación de reportes en formato PDF

La documentación generada a partir de la información recopilada por el sistema se redirige como datos a una función que básicamente mediante el uso de coordenadas y páginas, identifica en qué parte colocar la información correspondiente para cada reporte, asegurando de esta manera el mismo formato del documento al ser generado por el sistema, el cual lleva un conteo de las páginas generadas en cada reporte.

Es importante mencionar que exactamente la misma información adquirida en un análisis rápido y aquellos análisis detallados por dispositivo serán agregados a tal reporte incluyendo la fecha, estado del servidor en ejecución, una fotografía de la ubicación donde se realizó el análisis, si es que se encuentra disponible y algunas cabeceras con imágenes para el documento.
El código fuente de esta función se muestra en la figura 3.15.

```php
<?php
session_start();

if (isset($_SESSION['direcciones'])) {

        $_SESSION['public_ip'] = shell_exec("curl http://myip.dnsomatic.com");//Corroboramos la conexión a internet

        //Recibimos dentro de una cadena la fecha
        $fecha=utf8_decode(shell_exec("date '+%A %d %B %Y %H:%M:%S' 2>&1"));

        //Se crea un objeto de PDF
        //Para hacer uso de los métodos
        $pdf = new PDF();
        $pdf->AddPage('P', 'Letter');


        $pdf->SetFont('Arial','',9);
        $pdf->Cell(0,5,$fecha,0,1,'R');


        $pdf->SetFont('Arial','B',14);
        $pdf->Cell(0,5,utf8_decode('Estado del servidor:'),0, 1 , ' L ');
        $pdf->Ln();


        //Array de cadenas para la cabecera
        $pdf->SetFont('Arial','B',12);
        $pdf->tabla($cabecera,$datosServer,31,55,70,7,12,' L '); //Método que integra a cabecera y datos, así como (X,Y)

        $pdf->SetXY(10,135);
        $pdf->SetFont('Arial','B',14);
        $pdf->Cell(0,10,utf8_decode('Foto de la ubicación:'),0, 1 , ' L ');
        $pdf->Ln();

        $pdf->SetXY(0,0);

        $pdf->SetXY(20,247);
        $pdf->Cell(170,8,utf8_decode('Se han encontrado X dispositivos ejecutando iOS y Y tienen JailBreak'),1, 2 , 'C' );
}
?>
```

Figura 3.15 Generación de reportes en formato PDF

f) Presentación de gráficas

Utilizando tecnología y desarrollo web basado en Javascript, son generadas las gráficas para el sistema, la información proyectada en ellas es obtenida a partir de consultas a la base de datos, realizando conteos en 4 distintas categorías respecto a los registros almacenados en la base de datos.

- Número de escaneos realizados por mes.
- Cantidad de dispositivos identificados por mes.
- Cantidad de dispositivos identificados por mes que ejecutan iOS.
- Número de dispositivos identificados con Jailbreak por mes.

Posteriormente estos datos serán desplegados como parte de una representación gráfica, la cual será interpretada por el usuario de una manera más sencilla, visualizando el aumento o decremento de conexiones por dispositivos de manera mensual,

facilitando la identificación de comportamientos en la cantidad de conexiones de manera mensual. Véase figura 3.16

```php
<?php
    if(!isset($_SESSION['month_scans'])){
        statistics_query();//Generamos las estadisticas
    }

    $flag = 0;//Bandera para utilizarse en generar el script

    echo "
        <script id='isbin-javascript'>
            Morris.Line({
            element: 'morris-line-chart',
            data: [";

            for ($i=0; $i < (count($_SESSION['month_scans'])); $i++) {
                foreach ($_SESSION['month_scans'][$i] as $index => $content) {
                    if($flag==0){
                        echo "{".$index.": '".$content."',";
                        $flag=1;
                    }else{
                        echo "escaneos: ".$content.
                        ", dispositivos: ".$_SESSION['devices_number'][$i]['cantidad'].
                        ", ios: ".$_SESSION['ios_jailbreak_number'][$i]['ios'].
                        ", jailbreak: ".$_SESSION['ios_jailbreak_number'][$i]['jailbreak']."},";
                        $flag=0;
                    }
                }
            }
            echo "],
            xkey: 'mes',
            ykeys: ['escaneos', 'dispositivos', 'ios', 'jailbreak'],
            labels: ['Análisis realizados', 'Dispositivos análizados', 'Ejecutan iOS', 'Tienen JailBreak']
            });
        </script>
        ";
    ?>
```

Figura 3.16 Presentación de gráficas

g) Generación de listas negras

Para la generación de listas negras se trabaja mediante el uso de identificadores basados en la fecha y hora, persistiendo estas listas en una ruta fija, donde por si no es suficiente realizar la descarga de cada lista negra generada, se mantienen copias fieles para su consulta posterior dentro de la ruta "./blacklist/black_list_[ID].txt", esto como logs de sistema como se puede observar en la figura 3.17.

```php
<?php
session_start();

    if(isset($_SESSION['id_black_list'])){
        header("Content-disposition: attachment; filename=black_list_".$_SESSION['id_black_list'].".txt");
        header("Content-type: application/octet-stream");
        readfile("blacklist/black_list_".$_SESSION['id_black_list'].".txt");
    }else{
        header("Location:settings.php");
    }

?>
```

Figura 3.17 Generación de listas negras

h) Gestión de geolocalización

La geolocalización es gestionada directamente a partir de trabajar el API desarrollada por Google y la implementación de tecnología Javascript, siendo un conjunto adecuado para realizar la obtención de coordenadas a partir de triangulación mediante el punto de acceso Wi-Fi o coordenadas GPS obtenidas a partir de un dispositivo móvil.

Es posible que las coordenadas en algunos casos no sean accesibles, por las siguientes razones:

- El usuario no concedió los permisos para hacer uso de su ubicación.
- No existe una calidad de señal adecuada para realizar la triangulación y ubicación mediante el dispositivo GPS.
- El navegador web no soporta esta tecnología.

Por ello, de no ser posible la obtención de tales coordenadas simplemente no serán mostradas, almacenadas o tomadas en cuenta para la generación de reportes en PDF, como se puede observar en la figura 3.18

```
function success(position) {
    var s = document.querySelector('#status');
    var mapcanvas = document.createElement('div');
    mapcanvas.id = 'mapcanvas';
    mapcanvas.style.height = '300px';
    mapcanvas.style.width = '320px';

    document.querySelector('article').appendChild(mapcanvas);
    //Variables de ubicación
    var latitude = position.coords.latitude;
    var longitude = position.coords.longitude;
    //Almacenando las variables de ubicación para ser utilizadas con PHP
    document.cookie ='latitude='+latitude+'; expires=Thu, 2 Aug 2025 20:47:11 UTC; path=/';
    document.cookie ='longitude='+longitude+'; expires=Thu, 2 Aug 2025 20:47:11 UTC; path=/';

    var latlng = new google.maps.LatLng(latitude,longitude);
    var myOptions = {
      zoom: 15,
      center: latlng,
      mapTypeControl: false,
      navigationControlOptions: {style: google.maps.NavigationControlStyle.SMALL},
      mapTypeId: google.maps.MapTypeId.ROADMAP
    };
    var map = new google.maps.Map(document.getElementById("mapcanvas"), myOptions);

    var marker = new google.maps.Marker({
        position: latlng,
        map: map
    });

    var img_url = "http://maps.googleapis.com/maps/api/staticmap?center="+latlng+"&zoom=14&size=300x300&sensor=false";
    document.getElementById("mapholder").style.visibility="hidden";
    document.getElementById("mapholder").innerHTML = "<img id='map' src='"+img_url+"'>";

  }

  if (navigator.geolocation) {
    navigator.geolocation.getCurrentPosition(success, error);
  } else {
    error('Ubicación no disponible');
  }
```

Figura 3.18 Gestión de geolocalización

i) Consulta

El código fuente mostrado en la figura 3.19 es de carácter parcial, siendo la estructura base para la consulta de los análisis registrados en la BD. Se compone de tres segmentos esencialmente:

- Conexión a la BD y ejecución de la consulta respectiva.
- Generación de tablas en HTML con la información obtenida para su posterior presentación en el sistema.
- Impresión y visualización del resultado.

El mismo principio es utilizado para las diferentes consultas que son posibles realizar dentro del sistema.

j) Búsqueda de registros

La búsqueda de resultados dentro de la primera versión del sistema consiste únicamente en la ejecución de una consulta directamente a la base de datos utilizando un conjunto de operadores OR, con los cuales se compara la información solicitada con los posibles campos que puedan contener la información solicitada dentro de la base de datos, siendo estos la fecha, dirección IP, dirección MAC y el nombre del dispositivo. Una vez ejecutada la consulta serán generadas las tablas mediante HTML para su posterior despliegue y visualización por el usuario.

```php
<?php
    //Consultar datos en BD
    $query="SELECT scan.date,host.hostname,host.mac,host.private_ip FROM scan
    JOIN results
    ON scan.idscan=results.scan_idscan
    JOIN host
    ON results.host_idhost=host.idhost
    WHERE host.hostname='".$_POST['search']."'
    OR host.mac='".$_POST['search']."'
    OR host.private_ip='".$_POST['search']."'
    OR scan.date='".$_POST['search']."'
    ORDER BY scan.date";

    $resultados=mysql_query($query,$conexion) or die (mysql_error());

    if(mysql_num_rows($resultados)!==0){//Se encontró uno o más registros en BD
        $output = "";
        $output = $output."<div class='table-responsive'>";
            $output = $output."<thead>";
            $output = $output."  <tr>";
                $output = $output."  <th><center>Fecha</center></th>";
                $output = $output."  <th><center>Nombre del host</center></th>";
                $output = $output."  <th><center>MAC</center></th>";
                $output = $output."  <th><center>IP</center></th>";
            $output = $output."  </tr>";
            $output = $output."</thead>";

        $output = $output."<tbody>";
            while ($resultado = mysql_fetch_assoc($resultados)){//Realizamos un recorrido por los resultados obtenidos
                $output = $output."  <tr>";
                foreach ($resultado as $key => $value) {
                    $output = $output."  <td><center>".$value."</center></td>";
                }
                $output = $output."  </tr>";
            }
        $output = $output."</tbody>";
        $output = $output."</div>";

        $_SESSION['search_query'] = $output;
        unset($output);
    }else{
        $_SESSION['search_query'] = "<div class='alert alert-info'>No hay información.</div>";
    }
}
?>
```

Figura 3.19 Consulta y búsqueda de registros

"El testing de componentes puede ser muy efectivo para mostrar la presencia de errores, pero absolutamente inadecuado para demostrar su ausencia"

-Edsger Dijkstra

Capítulo 4
Auditoría y resultados

Parte fundamental del desarrollo de un sistema cualquiera es la sección de pruebas o auditoría, en donde se determina si el sistema desarrollado es o no lo que el usuario final espera.

Al tratarse de un sistema de monitoreo de red es menester que se realicen pruebas en busca de vulnerabilidades y estas, de encontrarse, se mitiguen. De esta manera se asegura que el sistema no es blanco fácil para los ciber atacantes.

Es por ello que a lo largo de este capítulo se documentan las pruebas, se corrigen fallas en el código fuente del sistema y se presentan los resultados obtenidos.

En este capítulo se realizan 4 pruebas:

1. Prueba general del sistema: En esta prueba se buscan bugs de programación que logren romper las medidas de seguridad del sistema o que logren que el sistema falle de una manera u otra mientras está siendo ejecutado por el administrador del sistema.
   Esta prueba se realiza tanto en un dispositivo fijo (computadora de escritorio o laptop), como en un dispositivo móvil (smartphone o tablet) con la finalidad de verificar que el sistema puede ser ejecutado en cualquier ambiente.

Se presentan las capturas de pantalla para las diferentes vistas del sistema: la vista de escritorio y la vista desde un móvil.

El módulo de inicio de sesión se divide en dos partes, en el primero se corroboran las credenciales para al acceso a la sesión de usuario que ejecuta el servicio del sistema de monitoreo, mientras que en la segunda parte de la autenticación se proporciona acceso a la base de datos en caso de ser válidas las credenciales para la misma.

Login

Primer módulo de inicio de sesión, en donde se autentica la sesión del usuario que ejecuta el servicio del sistema de monitoreo dentro del servidor (figura 4.1).

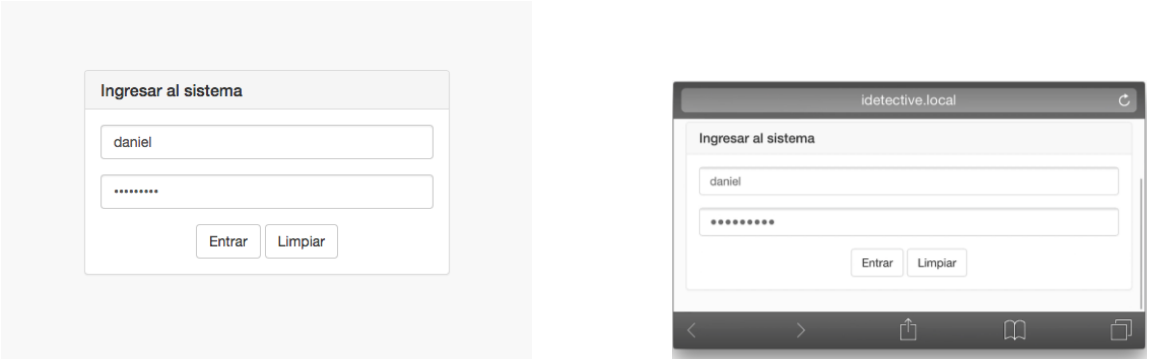


Figura 4.1 Inicio de sesión (Escritorio vs Móvil)

Si el usuario ingresa credenciales no válidas, el sistema inmediatamente le muestra un mensaje de error para que éste verifique su nombre de usuario y contraseña (figura 4.2).

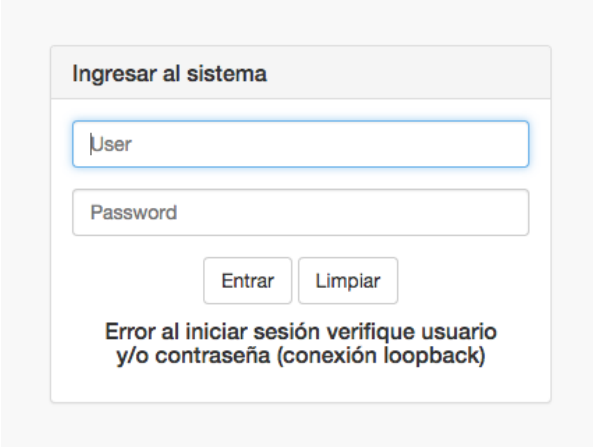


Figura 4.2 Inicio de sesión (Ingreso de credenciales no válidas)

Las credenciales deben ser correctas, de lo contrario el sistema bloquea el acceso de manera indefinida forzando al usuario (en caso de saberlo) a cerrar completamente el navegador que esté ejecutando (figura 4.3).

Figura 4.3 Inicio de sesión (Número de intentos agotado)

Acceso a la BD

Respecto a la parte correspondiente a la autenticación del sistema, se proporciona acceso a la base de datos configurada por el administrador del servidor, las credenciales pueden ser las mismas que las de inicio de sesión o pueden ser

completamente diferentes, brindando una mayor flexibilidad y seguridad para el sistema.

La autenticación para el acceso a la base de datos tiene el siguiente portal, posee las mismas características que el portal anterior, además de validar que no sean ingresados campos vacíos. Véase figura 4.4

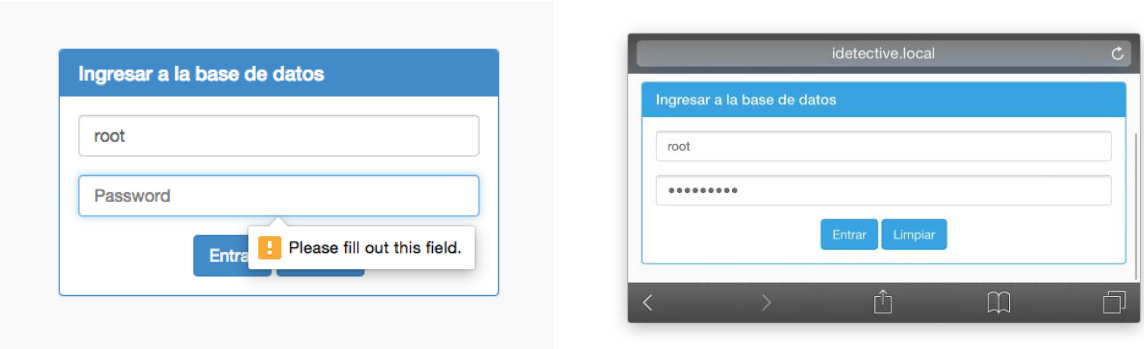


Figura 4.4 Inicio de sesión a la base de datos (Escritorio vs Móvil)

Acceso a coordenadas y geolocalización

Durante la ejecución del sistema, este pregunta al usuario si desea proporcionar acceso para utilizar coordenadas satelitales para geolocalización (figura 4.5), las cuales serán utilizadas dentro de los reportes generados y también puedan almacenarse en la base de datos con relación a la ubicación de cada análisis realizado.

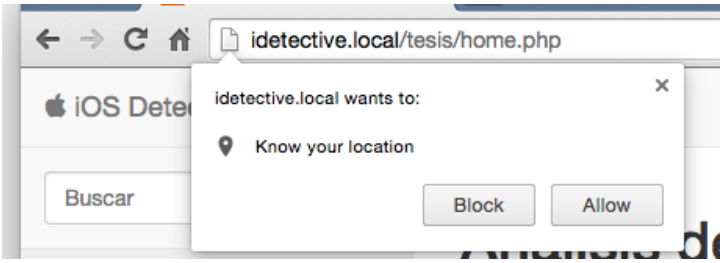


Figura 4.5 Autorización para el uso de coordenadas

Vista principal

En la vista principal (figura 4.6 para la versión de escritorio, y las figuras 4.7, 4.8, 4.9 y 4.10 para la versión móvil) se encuentran la gran parte de los componentes y módulos desarrollados, teniendo acceso a todos y cada uno de ellos a partir de esta vista.

El reporte generado y presentado a partir de una gráfica, el estado del servidor, la ubicación geográfica así como un mapa, búsqueda de información, ejecución de análisis rápidos, consulta de registros, modificación de ajustes y generación de reportes en PDF son componentes de fácil acceso a partir de esta vista.

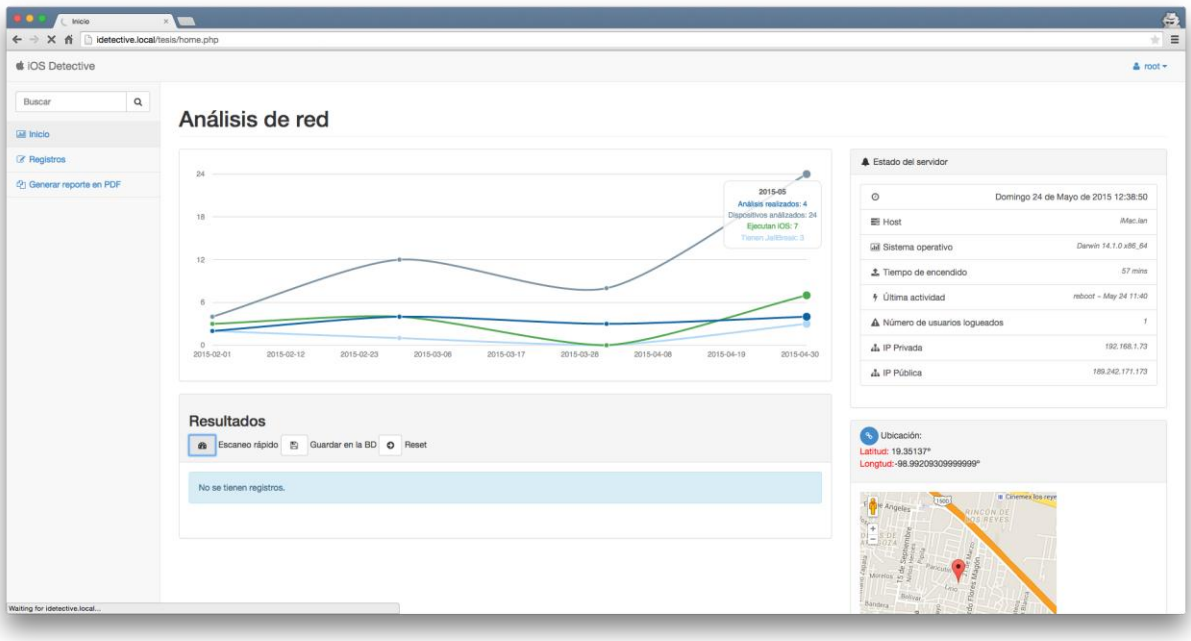


Figura 4.6 Vista principal (Escritorio)

Figura 4.7 Barra lateral izquierda, vista principal (Móvil)

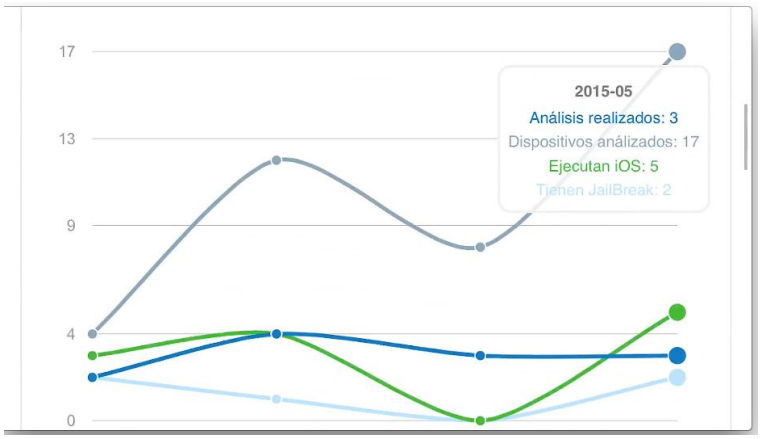


Figura 4.8 Gráfica, vista principal (Móvil)

Figura 4.9 Estado del servidor, vista principal (Móvil)

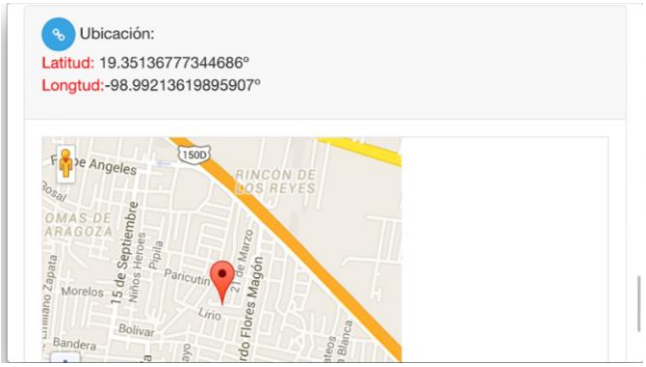


Figura 4.10 Ubicación y mapa, vista principal (Móvil)

Análisis rápido

El análisis rápido es el módulo vertebral, a partir de este se identifican los dispositivos que se encuentran conectados a la red, se ejecuta una verificación para un grupo de servicios definidos, corroborando el estado de los mismos e identificando aquellos dispositivos que ejecutan alguna versión de iOS, así como aquellos que tienen JailBreak. Véase figura 4.11 para la versión de escritorio, y las figuras 4.12 y 4.13 para la versión móvil.
Los resultados obtenidos a partir de un análisis rápido pueden ser almacenados en la base de datos o simplemente ignorados o reemplazados por un nuevo análisis.

Figura 4.11 Análisis rápido (Escritorio)

Figura 4.12 Análisis rápido (Móvil)

IP	Hostname	FTP	SSH	Telnet	HTTP	HTT
192.168.1.73	imac.lan	✗	✓	✗	✓	✓
192.168.1.254	dsldevice.lan	✓	✗	✓	✓	✓
192.168.1.253	192.168.1.253	✗	✗	✗	✗	✗
192.168.1.65	iphonededaniel.lan	✗	✓	✗	✓	✗
192.168.1.79	hp-elitepad.lan	✗	✗	✗	✗	✗
192.168.1.69	daniels-iphone.lan	✗	✗	✗	✗	✗

Figura 4.13 Tabla de resultados para el análisis rápido (Móvil)

Análisis detallado

La obtención de una mayor cantidad de información respecto a un dispositivo en específico es algo que se obtiene a partir de la ejecución de un análisis detallado, la idea principal se centra en la identificación de dispositivos (análisis

rápido), para posteriormente detallar toda aquella información que pueda ser obtenida del dispositivo como el sistema operativo, la versión que ejecuta del mismo, nombre y versión de servicios en ejecución, dirección física (MAC), servicios no identificados en un análisis rápido. Véase figura 4.14 para la versión de escritorio, y la figura 4.15 para la versión móvil.

Para la ejecución de un análisis detallado, basta con dar click sobre la dirección IP del dispositivo en cuestión, suministrado a partir de la tabla de resultados del análisis rápido.

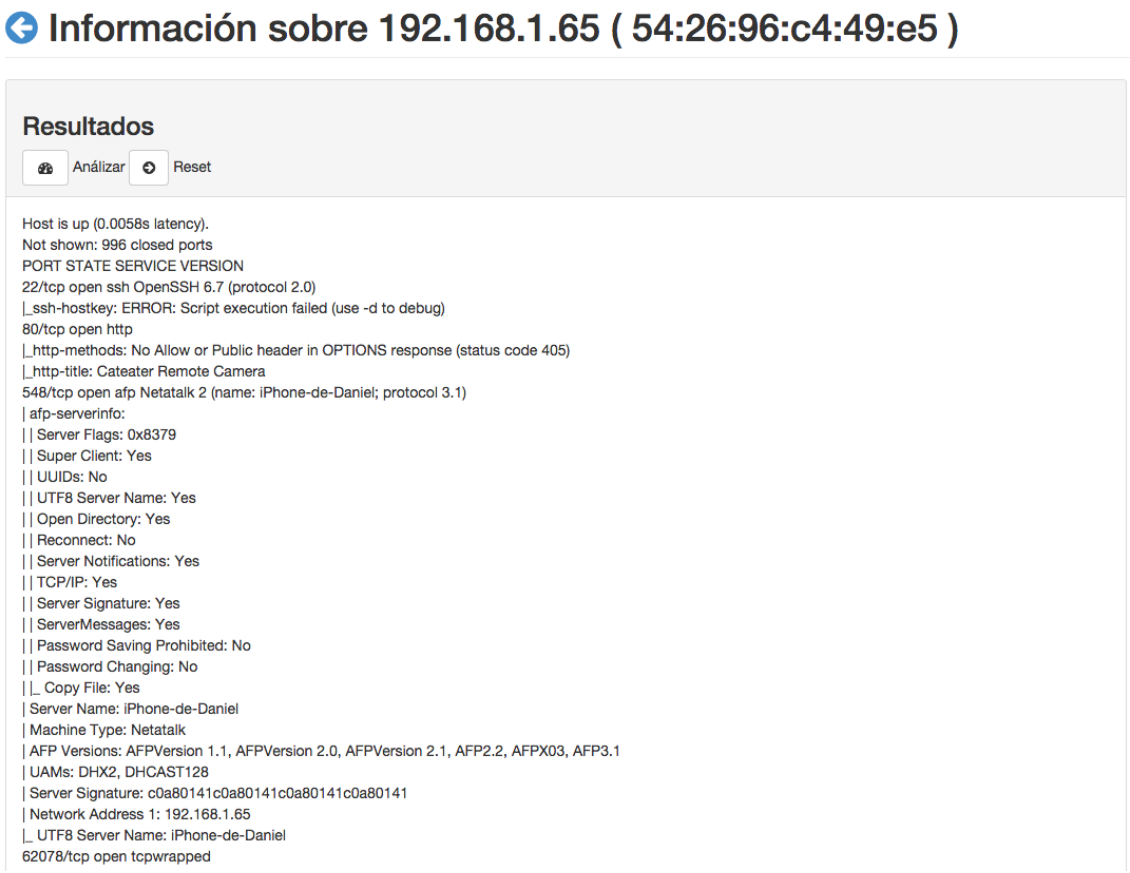


Figura 4.14 Análisis detallado (Escritorio)

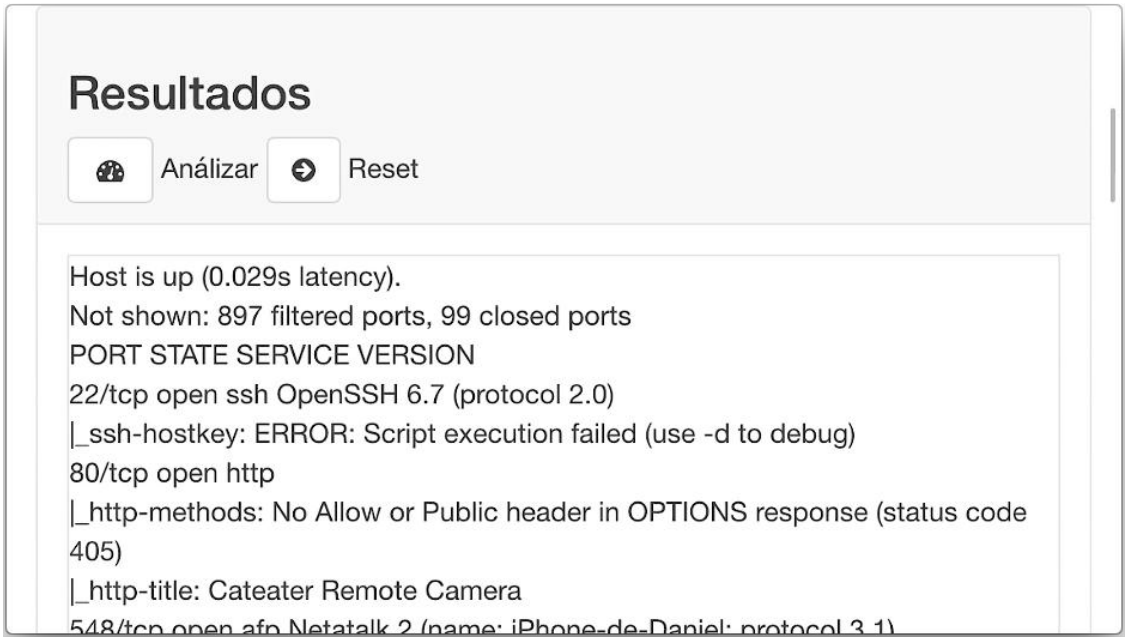


Figura 4.15 Análisis detallado (Móvil)

Consulta de registros

Los registros almacenados en la base de datos son una parte importante para dar seguimiento a actividades sospechosas, el sistema desarrollado proporciona acceso y ejecución de consultas para tres distintos resultados.

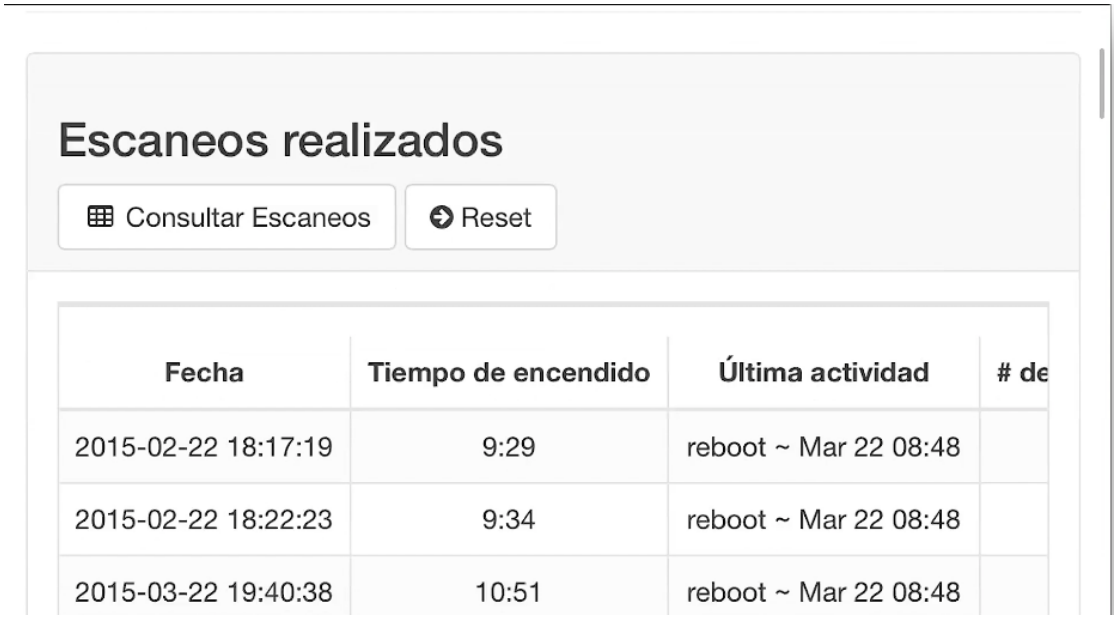
Es posible consultar los escaneos realizados, donde se obtiene toda la información relevante del estado del servidor, estado de conexiones y el número de dispositivos que ejecutan iOS y aquellos que tienen Jailbreak, como se puede observar en las figuras 4.16 (prueba de escritorio) y 4.17 (prueba en un móvil).

Escaneos realizados

Consultar Escaneos | Reset

Fecha	Tiempo de encendido	Última actividad	# de Usuarios	IP Privada	IP Pública	iDevices	Jailbroken
2015-02-22 18:17:19	9:29	reboot ~ Mar 22 08:48	1	192.168.1.76	189.137.207.98	2	2
2015-02-22 18:22:23	9:34	reboot ~ Mar 22 08:48	1	192.168.1.76	189.137.207.98	1	0
2015-03-22 19:40:38	10:51	reboot ~ Mar 22 08:48	1	192.168.1.76	189.137.207.98	1	0
2015-03-22 19:48:26	11 hrs	reboot ~ Mar 22 08:48	1	192.168.1.76	189.137.207.98	1	1
2015-03-24 17:32:53	8:45	reboot ~ Mar 24 08:47	1	192.168.1.76	189.179.191.252	0	0
2015-04-26 15:01:40	2:11	reboot ~ Mar 26 12:49	1	192.168.1.69	189.137.205.84	0	0
2015-03-26 18:45:25	5:55	reboot ~ Mar 26 12:49	1	192.168.1.69	189.137.205.84	2	0
2015-04-03 16:47:06	7:27	reboot ~ Apr 3 09:19	2	192.168.1.77	189.242.169.93	0	0
2015-04-03 16:47:56	7:28	reboot ~ Apr 3 09:19	2	192.168.1.77	189.242.169.93	0	0
2015-05-23 13:18:25	5 hrs	reboot ~ May 23 08:18	1	192.168.1.73	189.242.176.246	1	0
2015-05-24 08:31:36	40 mins	reboot ~ May 24 07:51	1	192.168.1.73	189.242.171.173	2	1
2015-05-24 09:04:16	1:13	reboot ~ May 24 07:51	1	192.168.1.73	189.242.171.173	2	1
2015-05-24 12:04:05	23 mins	reboot ~ May 24 11:40	1	192.168.1.73	189.242.171.173	2	1

Figura 4.16 Consulta de escaneos realizados (Escritorio)



Escaneos realizados

Consultar Escaneos | Reset

Fecha	Tiempo de encendido	Última actividad	# de
2015-02-22 18:17:19	9:29	reboot ~ Mar 22 08:48	
2015-02-22 18:22:23	9:34	reboot ~ Mar 22 08:48	
2015-03-22 19:40:38	10:51	reboot ~ Mar 22 08:48	

Figura 4.17 Consulta de escaneos realizados (Móvil)

Consulta de coordenadas

La consulta de coordenadas se vuelve importante al momento de identificar físicamente al dispositivo que ejecuta el sistema de monitoreo de red implementado.
Debido al uso que se le puede dar al sistema desde un dispositivo móvil o de escritorio, es necesario almacenar un registro de aquellas ubicaciones donde fueron identificados (figura 4.18), facilitando el acceso e interpretación de las mismas, el sistema genera ligas para mostrar la ubicación a partir de un mapa (figura 4.19), o simplemente la presentación de una fotografía a nivel de calle (figura 4.20) de dichas coordenadas geográficas.

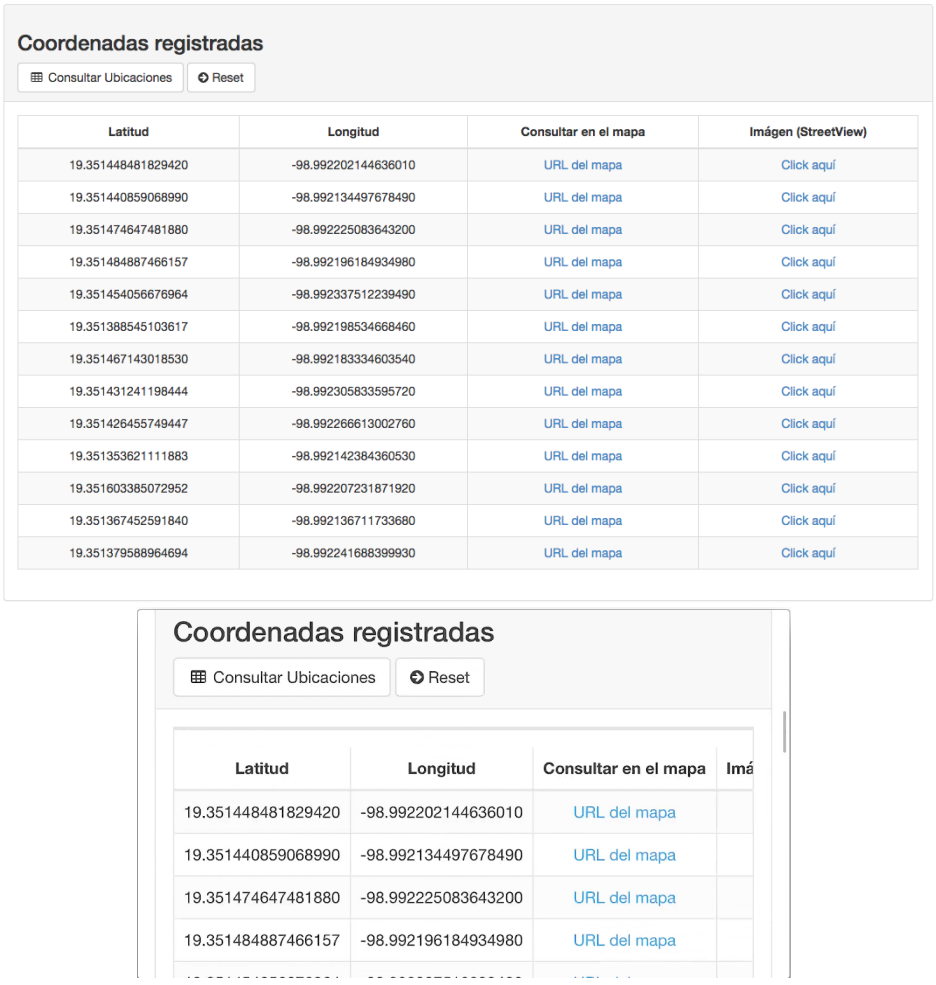


Figura 4.18 Consulta de coordenadas almacenadas (Escritorio vs móvil))

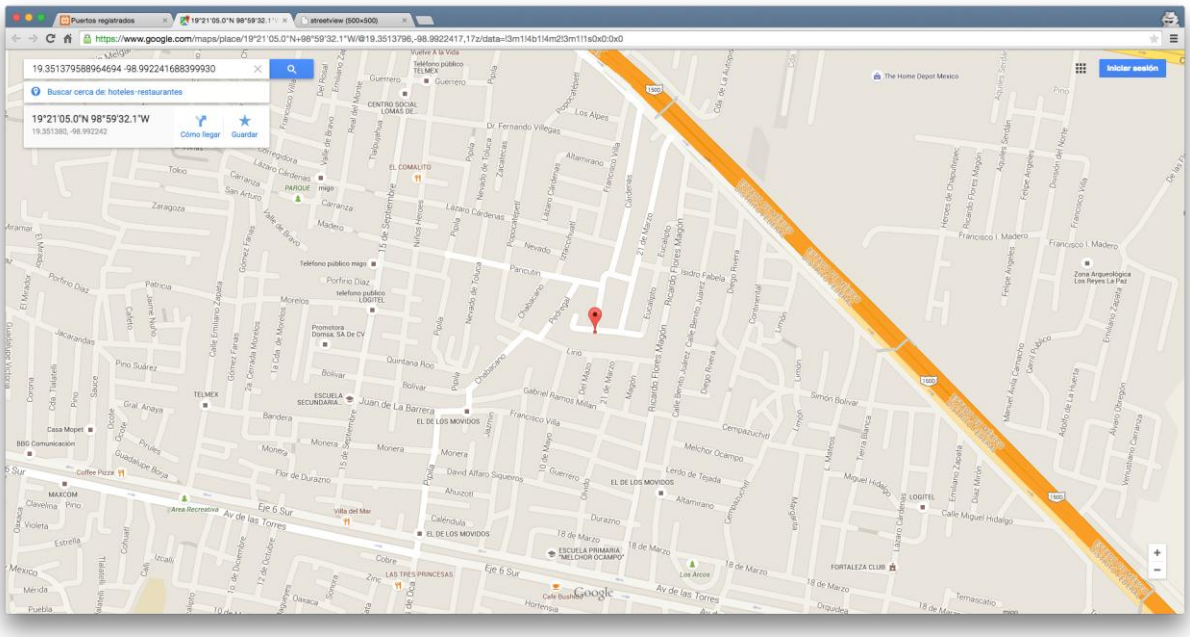


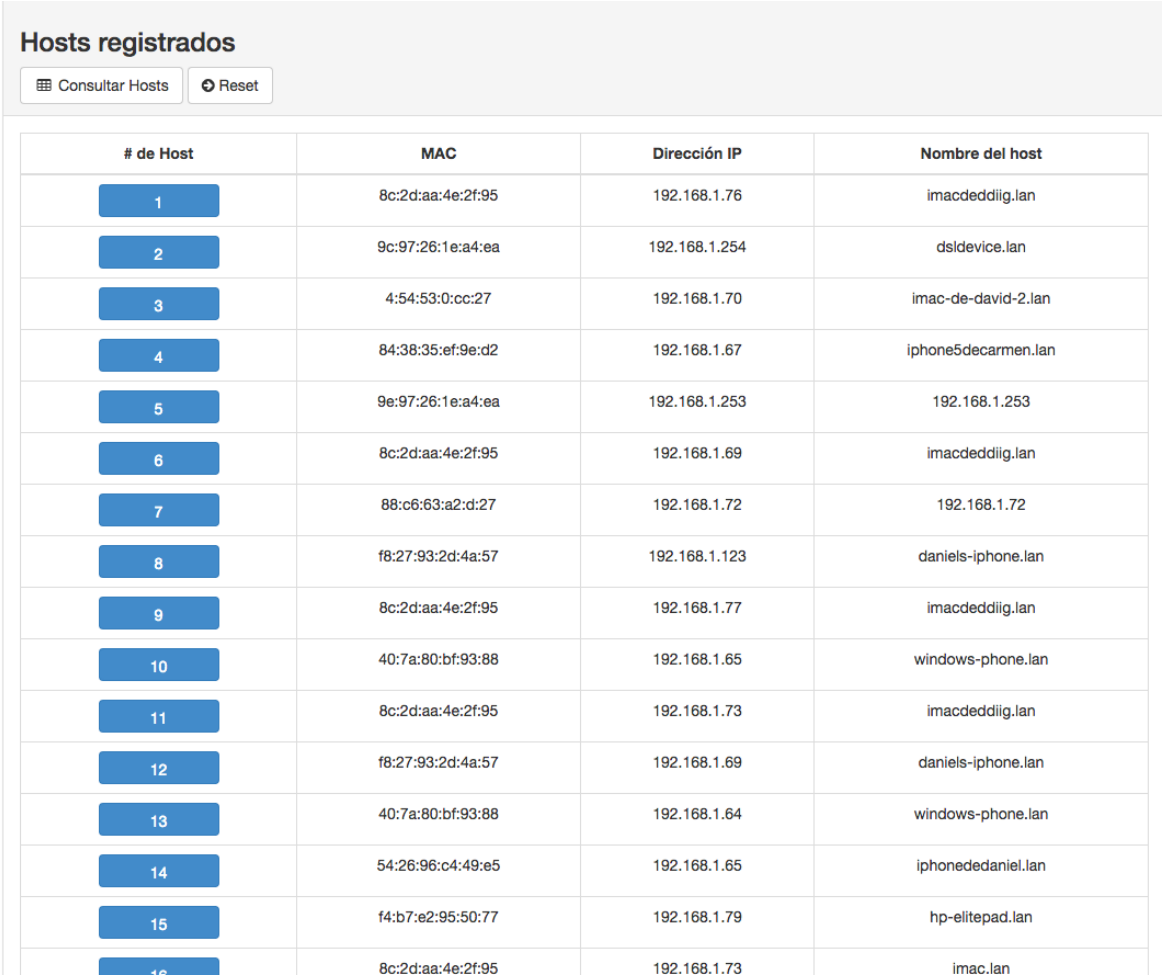
Figura 4.19 Mapa

Figura 4.20 Vista a nivel de calle

Los hosts posteriormente identificados y registrados, son almacenados y presentados a partir de la tabla de hosts, en donde se despliega un identificador (número entero bajo la

columna "# de host") para cada host, dirección IP, dirección MAC y su respectivo nombre del host. Véase figura 4.21

El sistema registra un nuevo host siempre y cuando la dirección IP, MAC o el nombre del host sean diferentes a los previamente almacenados, permitiendo un seguimiento de cada cambio respecto a algún host, esta condición es muy útil puesto que si para un ejemplo dado se realiza el cambio de dirección física o lógica esto se verá reflejado en la tabla de registros.



# de Host	MAC	Dirección IP	Nombre del host
1	8c:2d:aa:4e:2f:95	192.168.1.76	imacdeddiig.lan
2	9c:97:26:1e:a4:ea	192.168.1.254	dsldevice.lan
3	4:54:53:0:cc:27	192.168.1.70	imac-de-david-2.lan
4	84:38:35:ef:9e:d2	192.168.1.67	iphone5decarmen.lan
5	9e:97:26:1e:a4:ea	192.168.1.253	192.168.1.253
6	8c:2d:aa:4e:2f:95	192.168.1.69	imacdeddiig.lan
7	88:c6:63:a2:d:27	192.168.1.72	192.168.1.72
8	f8:27:93:2d:4a:57	192.168.1.123	daniels-iphone.lan
9	8c:2d:aa:4e:2f:95	192.168.1.77	imacdeddiig.lan
10	40:7a:80:bf:93:88	192.168.1.65	windows-phone.lan
11	8c:2d:aa:4e:2f:95	192.168.1.73	imacdeddiig.lan
12	f8:27:93:2d:4a:57	192.168.1.69	daniels-iphone.lan
13	40:7a:80:bf:93:88	192.168.1.64	windows-phone.lan
14	54:26:96:c4:49:e5	192.168.1.65	iphonededaniel.lan
15	f4:b7:e2:95:50:77	192.168.1.79	hp-elitepad.lan
16	8c:2d:aa:4e:2f:95	192.168.1.73	imac.lan

Figura 4.21 Registro de hosts (Escritorio)

Un aspecto fundamental para los registros relacionados a los hosts es poder consultar los análisis detallados que fueron realizados en su momento para cada uno de ellos, por lo cual solo basta seleccionar el host a partir de su identificador y dar click sobre el botón azul para ingresar a los detalles de dicho host.

A partir de una representación en tablas se despliegan resultados mostrando la fecha en la que se registró dicha información y cuáles eran los puertos reportados a partir del análisis rápido realizado (figura 4.22). Para realizar la consulta de los resultados de un análisis detallado se generan indicadores a partir de botones color gris ubicados en la fecha registrada, siendo un botón que redirecciona a una página donde será presentada la información registrada respecto al análisis detallado.

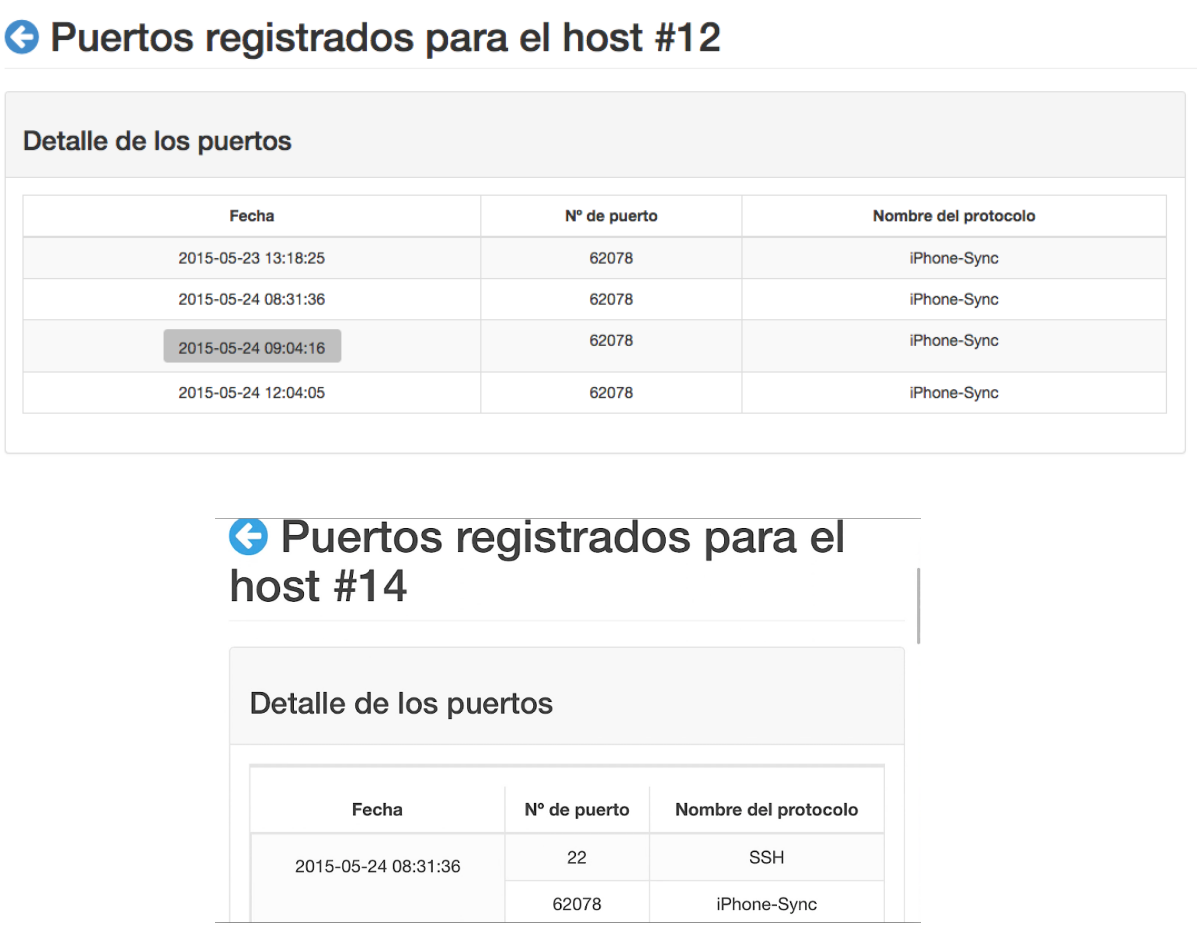


Figura 4.22 Detalles registrados para cada host (Escritorio vs móvil)

Ajustes para la sesión

La identificación y configuración adecuada del segmento de red sobre el cual se trabaja es un componente localizado dentro de la sección de ajustes (figura 4.23). Es posible definir el ID de la red y la representación de su máscara de red sobre los cuales trabajará el sistema.

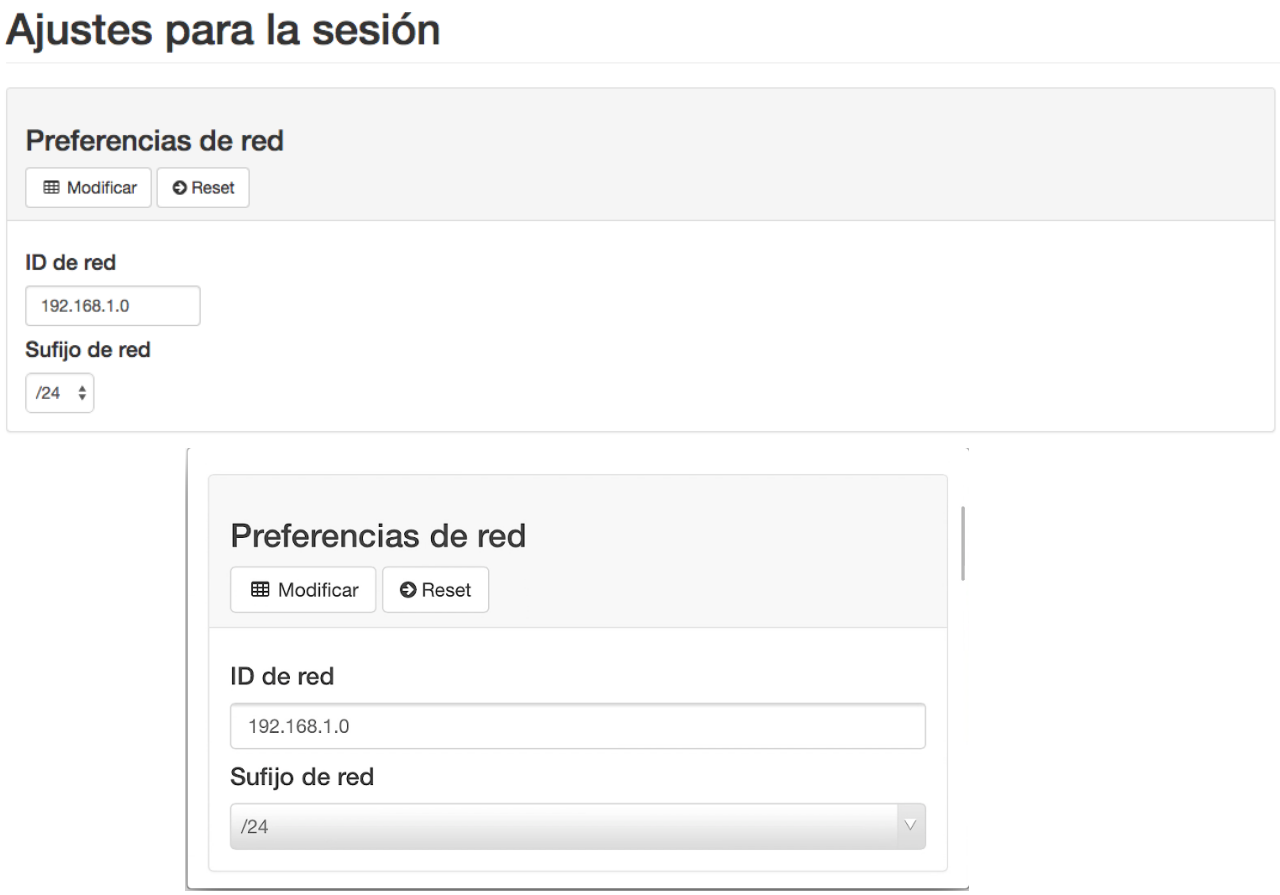


Figura 4.23 Ajustes, preferencias de red (Escritorio vs móvil)

Así mismo la generación de listas negras se encuentra ubicada dentro del módulo de ajustes, permitiendo al usuario a partir de la sección de ajustes generar un listado con aquellos dispositivos que presentan una actividad sospechosa o previamente identificados por el administrador de red y poder tomar las medidas necesarias.

Sólo es posible generar una lista negra una vez ejecutado un análisis rápido, puesto que es necesario previamente realizar una identificación de los dispositivos conectados a la red.

Las listas negras son generadas a partir de un documento de texto plano (.txt) donde se encuentran sus correspondientes nombres de host, direcciones IP y MAC, de todos aquellos dispositivos seleccionados. La gestión de direcciones se muestra en la figura 4.24.

Figura 4.24 Ajustes, generación de listas negras (Escritorio vs móvil)

Búsqueda de registros

La ejecución de una búsqueda de registros (figura 4.25) facilita al administrador la obtención o indagación de información a partir de cierto dato, el sistema es capaz de realizar búsquedas partiendo de fechas (en el formato manejado por los registros), nombre de host, direcciones lógicas o físicas.

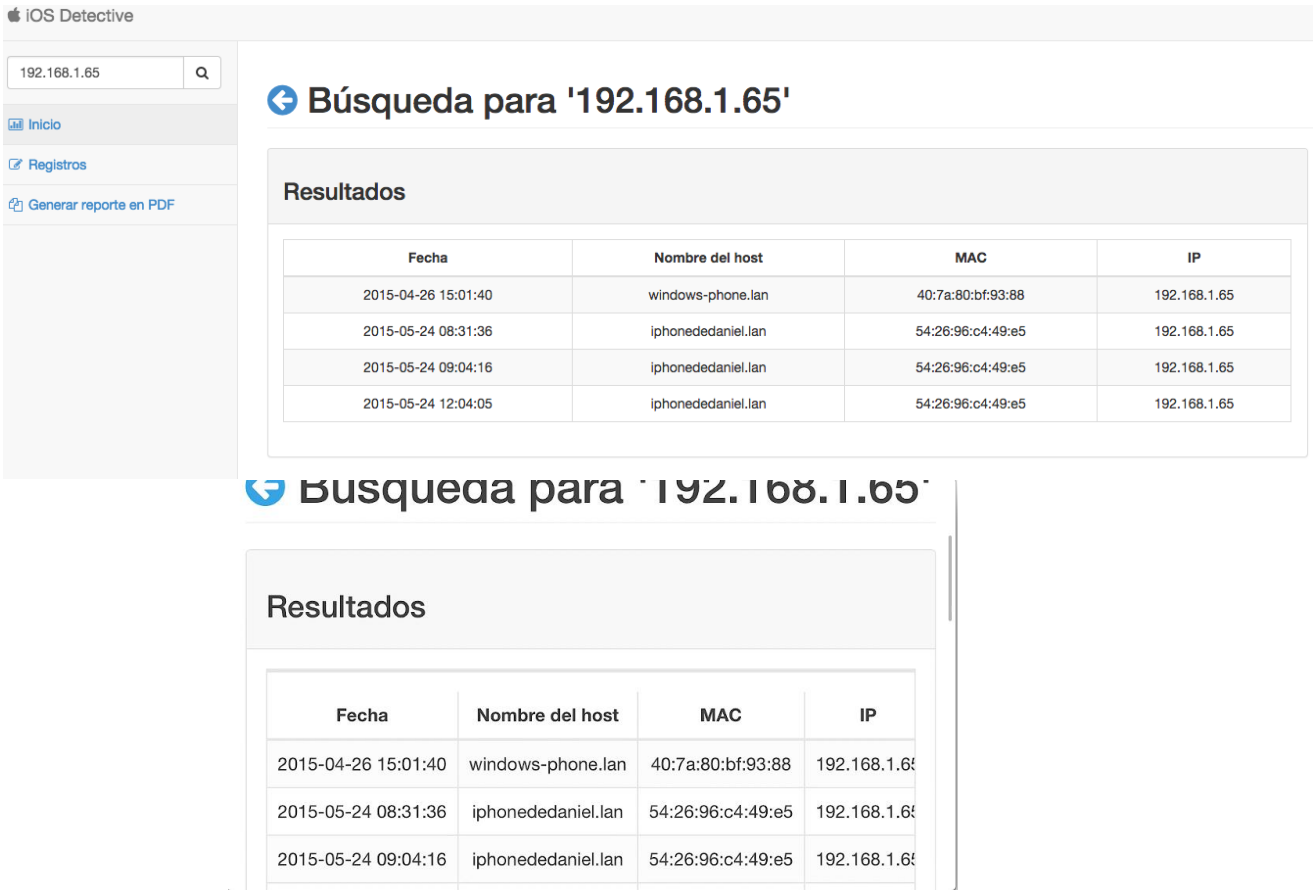


Figura 4.25 Búsqueda de registros (Escritorio vs móvil)

Generación de reportes PDF

Los reportes PDF ayudan a proporcionar una gestión mucho más completa, puesto que el documento generado, bien puede ser impreso posteriormente o solo almacenado de manera digital.

Las características del reporte generado por el sistema desarrollado se centran en hacer uso de la información obtenida a partir de la sesión del usuario, estado del servidor, coordenadas geográficas, fotografías de la ubicación (si están disponibles), resultado para el número de dispositivos que ejecutan iOS y/o tienen Jailbreak.

La estructura del documento generado contempla la generación de pequeñas tablas para cada uno de los hosts reportados a partir de un análisis rápido, y si bien sobre estos se

realizó un análisis detallado, de igual manera es información presentada en el correspondiente reporte dentro del documento en formato PDF.

El reporte generado es posible visualizarlo desde cualquier equipo de escritorio o dispositivo móvil, por lo cual la vista del mismo no se altera ni cambia independientemente de la plataforma sobre la que se visualiza. En las figuras 4.26, 4.27 y 4.28 se muestra un reporte generado por el sistema.

iOSDetective

Sunday 24 May 2015 12:55:11

Estado del servidor:

Hostname	iMac.lan
Sistema operativo	Darwin 14.1.0 x86_64
Tiempo de encendido	1:14
Última actividad	reboot ~ May 24 11:40
Número de usuarios logueados	1
Segmento de red	192.168.1.0/24
IP privada	192.168.1.73
IP pública	189.242.171.173
Latitud	19.351377199999998
Longitud	-98.9921966

Foto de la ubicación:

Se han encontrado 2 dispositivos ejecutando iOS y 1 tiene JailBreak

Figura 4.26 Hoja principal (estado del servidor y ubicación)

iOS Detective

Sunday 24 May 2015 12:55:11

Resultados del análisis rápido (Página 1 de resultados).

imac.lan (192.168.1.73) [8c:2d:aa:4e:2f:95]

FTP	-
SSH	X
Telnet	-
HTTP	X
HTTPS	X
Oracle	-
MySQL	X
iPhone-Sync	-

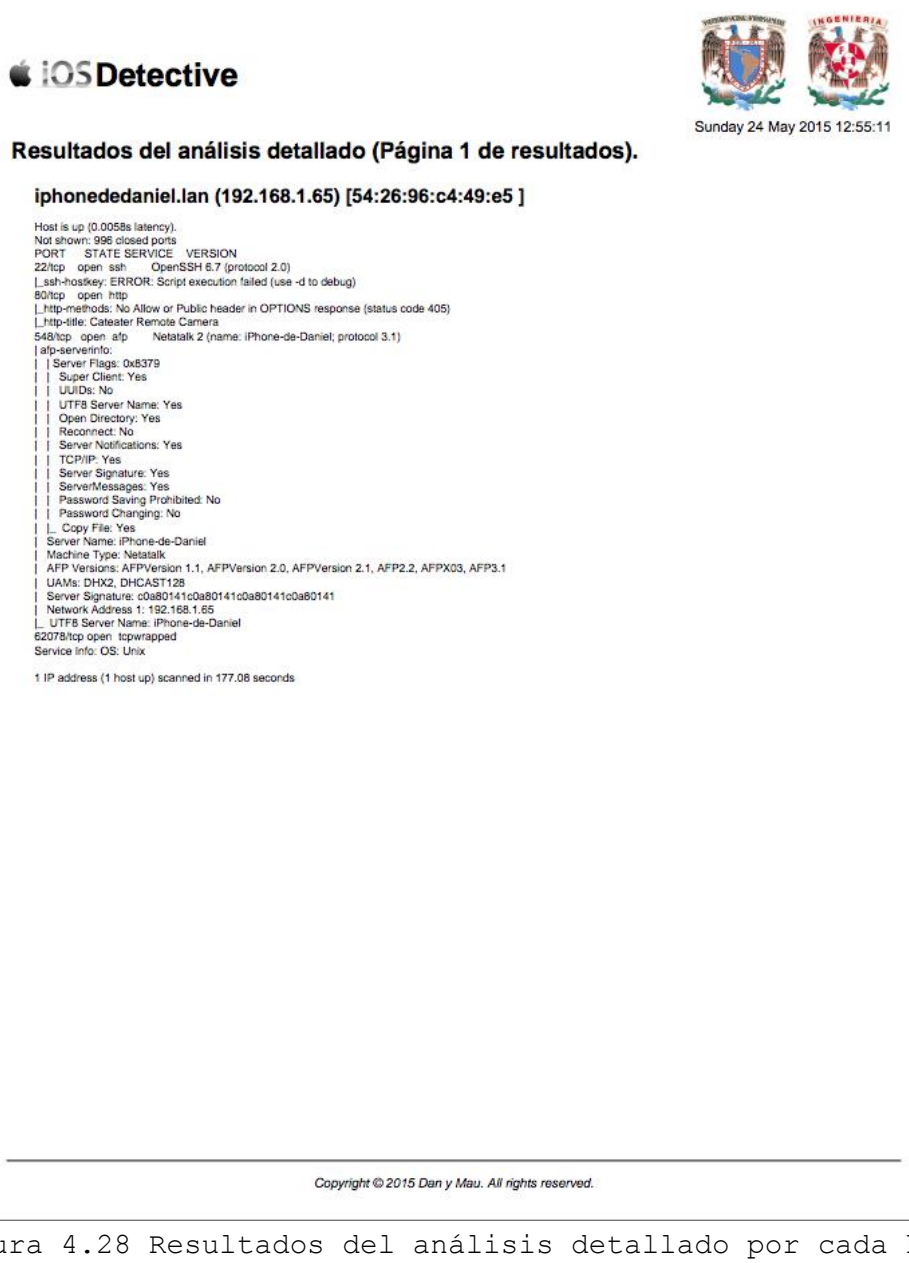
dsldevice.lan (192.168.1.254) [9c:97:26:1e:a4:ea]

FTP	X
SSH	-
Telnet	X
HTTP	X
HTTPS	X
Oracle	-
MySQL	-
iPhone-Sync	-

192.168.1.253 (192.168.1.253) [9e:97:26:1e:a4:ea]

FTP	-
SSH	-
Telnet	-
HTTP	-
HTTPS	-
Oracle	-
MySQL	-
iPhone-Sync	-

Figura 4.27 Resultados del análisis rápido representado en tablas



iOS Detective

Sunday 24 May 2015 12:55:11

Resultados del análisis detallado (Página 1 de resultados).

iphonededaniel.lan (192.168.1.65) [54:26:96:c4:49:e5]

```
Host is up (0.0058s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 6.7 (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
|_http-title: Cateater Remote Camera
548/tcp  open  afp        Netatalk 2 (name: iPhone-de-Daniel; protocol 3.1)
| afp-serverinfo:
|   | Server Flags: 0x8379
|   |   Super Client: Yes
|   |   UUIDs: No
|   |   UTF8 Server Name: Yes
|   |   Open Directory: Yes
|   |   Reconnect: No
|   |   Server Notifications: Yes
|   |   TCP/IP: Yes
|   |   Server Signature: Yes
|   |   ServerMessages: Yes
|   |   Password Saving Prohibited: No
|   |   Password Changing: No
|   |_  Copy File: Yes
|   Server Name: iPhone-de-Daniel
|   Machine Type: Netatalk
|   AFP Versions: AFPVersion 1.1, AFPVersion 2.0, AFPVersion 2.1, AFP2.2, AFPX03, AFP3.1
|   UAMs: DHX2, DHCAST128
|   Server Signature: c0a80141c0a80141c0a80141c0a80141
|   Network Address 1: 192.168.1.65
|_  UTF8 Server Name: iPhone-de-Daniel
62078/tcp open  tcpwrapped
Service Info: OS: Unix

1 IP address (1 host up) scanned in 177.08 seconds
```


Figura 4.28 Resultados del análisis detallado por cada host

2. Ataque a la base de datos (SQL injection): Se ha elegido este ataque debido a que el sistema fue desarrollado en un ambiente web, y esto lo hace susceptible a una inyección de sentencias SQL.
   Este ataque consiste en insertar sentencias SQL sobre el sistema de tal forma que se logre tomar control de la o las bases de datos utilizadas, poniendo en riesgo los activos de las organizaciones.
   A continuación se muestra el ataque hacia el sistema y los resultados obtenidos:

Se utiliza el sistema operativo Kali Linux para realizar la prueba de SQL injection debido a que este sistema operativo contiene una herramienta (sqlmap) para efectuar este tipo de ataques.

En la figura 4.29 observa la forma en la que se realiza dicho ataque y como este va arrojando información del mismo.

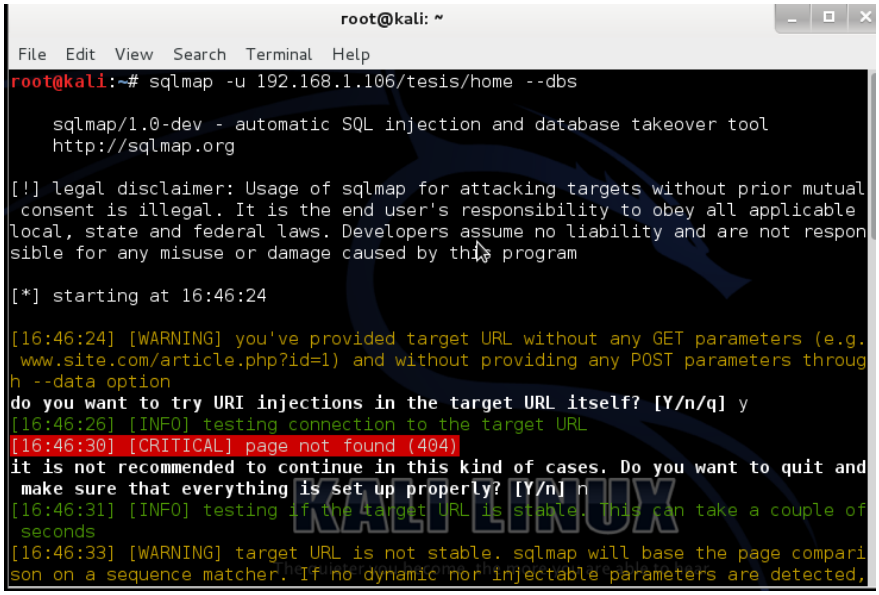


Figura 4.29 SQL injection parte 1

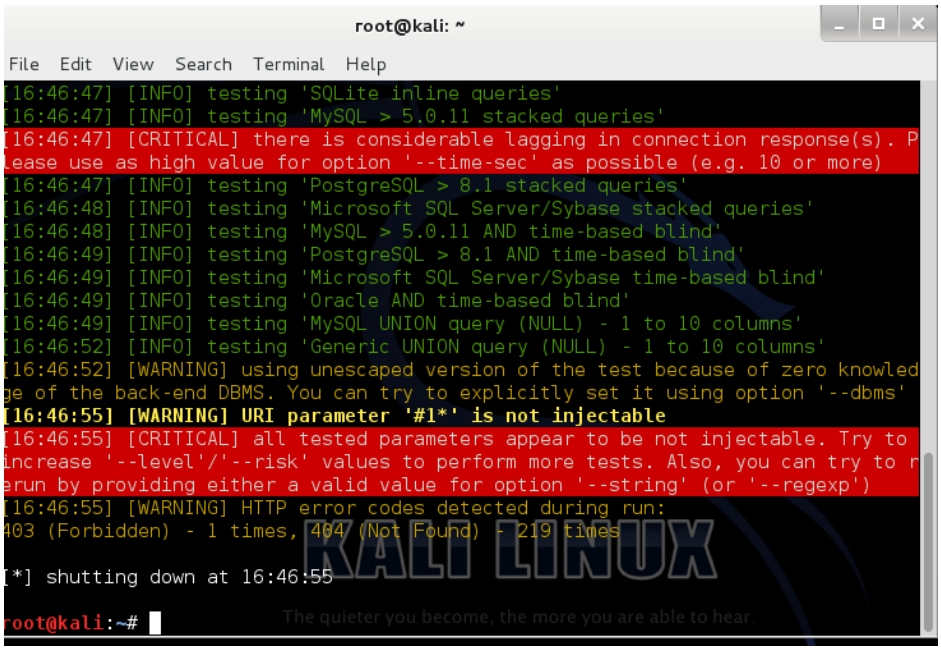


Figura 4.30 SQL injection parte 2

Como se observa en la figura 4.30, el ataque de sql injection no logró su cometido. Debido a que desde las páginas de autenticación no se hacen consultas a bases de datos con la finalidad de autenticar al usuario. Se usa la sesión del usuario a nivel de sistema operativo para guardar las credenciales de acceso al sistema.

3. Ataque a las vulnerabilidades de las platillas (WordPress Scan): Este ataque encuentra las vulnerabilidades del sistema a nivel de las plantillas utilizadas para mejorar la apariencia del mismo.
   A continuación se muestra el intento de atacar el sistema por esta vía y el resultado del mismo.

Para lograr identificar las vulnerabilidades de las platillas utilizadas en el sistema también se usa una herramienta de Kali Linux (WPScan). Y como se puede observar en la figura 4.31 no se utiliza WordPress en el sistema, por lo que el ataque fue fallido.

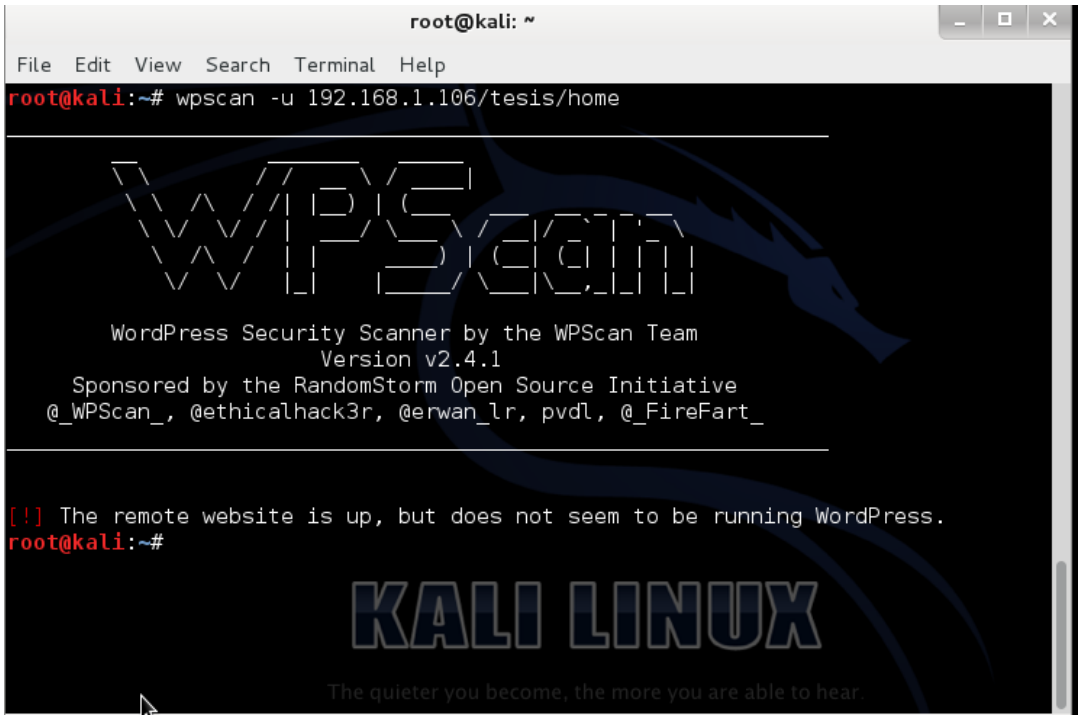


Figura 4.31 WordPress Scan sobre el sistema desarrollado

4. Fuerza bruta vía SSH: Con este ataque se intenta tomar control del sistema de monitoreo de forma remota. Se hace uso de diccionarios y de fuerza bruta para conseguir acceso al mismo. Está demás decir que este sistema es susceptible a ataques de fuerza bruta, por lo que a continuación se muestra de qué manera se puede mitigar este ataque.

Lo primero que se hace es verificar que es posible identificar el servidor en donde se encuentra el sistema de monitoreo (IP: 192.168.1.106), para ello se usa fping. El resultado se muestra en la figura 4.32.
Como se puede observar es posible identificar fácilmente la IP del servidor.

Figura 4.32 Fping sobre la red de prueba

Evitar que un atacante identifique la dirección IP del servidor en donde se encuentra alojado el sistema, es posible realizando un Hardening sobre el mismo.
El servidor responde a mensajes ICMP (figura 4.33), por lo que es necesario poner en modo encubierto la máquina (figura 4.34).

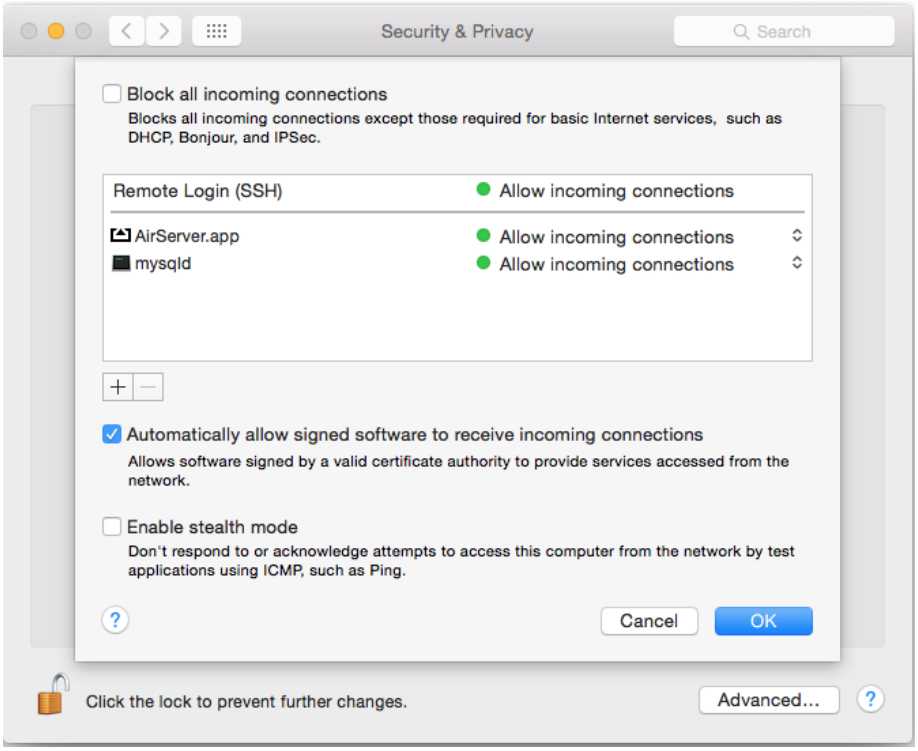


Figura 4.33 Servidor identificable

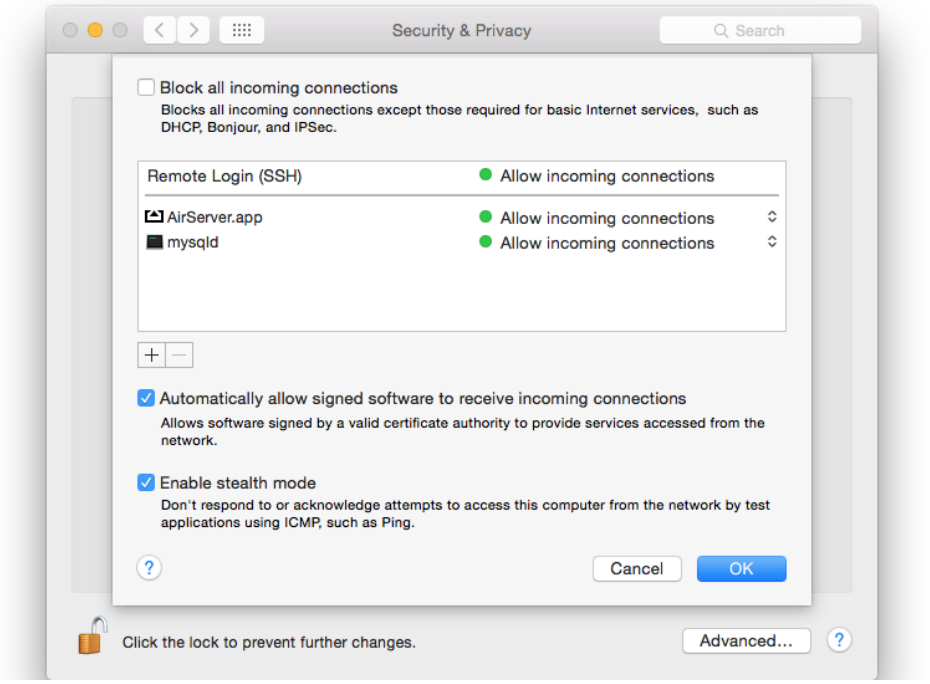


Figura 4.34 Servidor en modo encubierto

Para corroborar que este cambio re realizó correctamente, se realiza de nuevo un fping sobre la red de prueba. Figura 4.35.

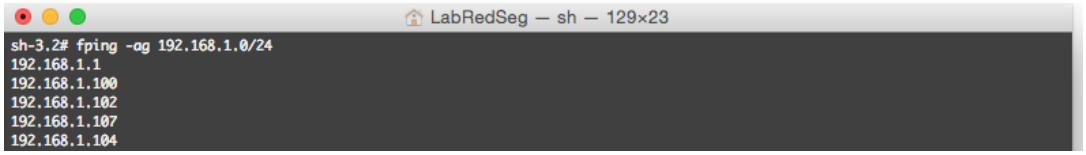


Figura 4.35. Fping sobre la red

Como puede observarse, el servidor ya no respondió al mensaje ICMP, por lo que ahora es difícil para el atacante identificarlo.

El segundo hardening que se puede realizar para evitar ataques de fuerza bruta vía SSH es cambiar el archivo de configuración del deamon SSH. En la figura 4.36 se pueden observar los parámetros que el administrador de red puede cambiar para fortalecer la seguridad del sistema y su entorno.

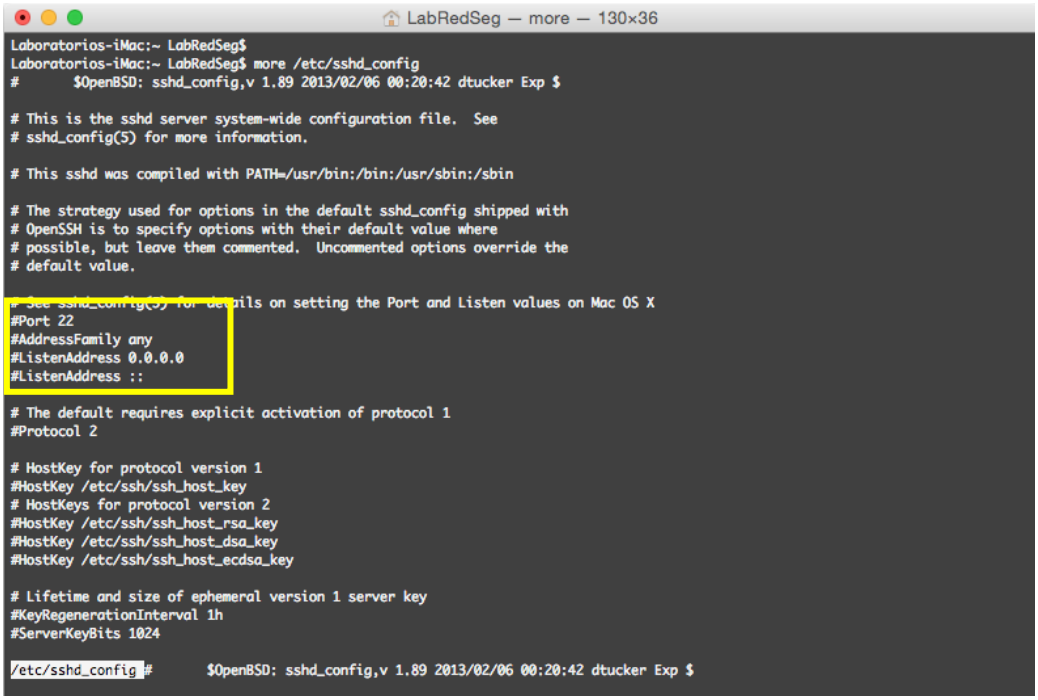


Figura 4.36 Archivo de configuración sshd_config

Como se puede observar en las 4 pruebas anteriores, el sistema cuenta con la seguridad necesaria para empezar a hacer uso del mismo. Por medio del Hardening sobre algunos parámetros del sistema operativo, el ambiente en el cual el sistema de monitoreo de red es ejecutado se convierte en un ambiente más seguro y puede llegar a evitar ataques de fuerza bruta de manera remota.

"La imaginación es más importante que el conocimiento. El conocimiento es limitado, mientras que la imaginación no"

-Albert Einstein

Conclusiones

Sin lugar a dudas, la seguridad informática y de la información es o debe ser una prioridad para la protección de los activos no solo de las organizaciones sino de las personas. Esto se debe al constante crecimiento y avance de la tecnología en estos días, así como a la demanda de la misma para resguardar información importante.

Si bien, la seguridad informática no puede ir a la par de la tecnología, esta debe aplicarse de tal manera que se puedan proteger los activos de terceras personas sin necesidad de contar con las herramientas más recientes. Esto gracias al conjunto de metodologías, normas, mecanismos, procedimientos, recursos y herramientas de seguridad que pueden implementarse para lograr resguardar la información.

El desarrollo de cualquier herramienta de seguridad, llámese antivirus, escáner o monitor de red es indiscutiblemente una tarea ardua y llena de altibajos, debido al nivel de conocimiento necesario para cubrir o intentar cubrir todas las características de estos y desarrollarlas de tal manera que funcionen plenamente.
Se torna complicado el estar completamente actualizado en todos los ámbitos que giran en torno a las tecnologías de la información (tecnología, herramientas tecnológicas, ataques informáticos, mitigación de ataques, etcétera) debido a la alta demanda que está teniendo la tecnología hoy en día.

La implementación de un sistema de monitoreo de red es una tarea que conlleva toda una línea de investigación en ataques informáticos, ya que esta herramienta es una de las armas principales que tiene un administrador de red para prevenir, detectar y eliminar o mitigar ataques informáticos que estén tomando lugar en la red con la que se trabaja. Un sistema de monitoreo de red debe ser capaz de detectar los dispositivos conectados a la red, para que en conjunto con el conocimiento que el administrador de red tiene de la misma se logren descubrir posibles atacantes.

No se pone en duda el impacto que hoy en día tienen los teléfonos inteligentes (Smartphones), así como tampoco el impacto que los ataques cibernéticos tienen sobre las empresas u organizaciones, por lo que el sistema de monitoreo de red desarrollado logra detectar ataques realizados desde dispositivos fijos, pero al existir una enorme relación entre los ataques y la nueva tecnología móvil, también detecta posibles ataques realizados a través dispositivos móviles con sistema operativo iOS.

Todo esto se logra a través de escaneos de una red completa, y específicamente sobre cada uno de los dispositivos detectados/encontrados en ella. Obteniendo datos tales como direcciones IP's, direcciones MAC, servicios ejecutados (establecidos por defecto), uso de tecnologías y herramientas alternas, entre otras cosas.

Ahora bien, es importante tener en cuenta que la seguridad informática no es el uso de una sola herramienta, de esta forma se logra un mayor control sobre el acceso al sistema y a los recursos informáticos que lo contengan, mediante la aplicación y aseguramiento del cumplimiento de normas o políticas de seguridad destinadas a reducir y minimizar los ataques internos y/o externos hacia el sistema. Estas políticas pueden ir desde la extracción de información vía USB, dispositivos de almacenamiento externo hasta el acceso a los recursos informáticos.

Con base en las pruebas realizadas al sistema es posible concluir que de contarse con un buen ambiente de seguridad informática dentro y fuera del ente que lo utilice, es posible prevenir ataques cuyo objetivo sea el controlar o robar información del sistema, detectar ataques que estén teniendo lugar en la red, y mitigar los mismos.

Como beneficios adicionales al sistema avanzado de monitoreo de red desarrollado en el presente trabajo, se tienen los siguientes:

- Generación de listas negras, con lo que se facilita la tarea del administrador de red al bloquear dispositivos dentro de la misma.
- Generación de reportes en formato PDF, para un mejor manejo de la información entregada por el sistema.
- Generación de gráficas, cuyo objetivo es el visualizar gráficamente los resultados obtenidos con esta herramienta.
- Geolocalización, la cual facilita la localización del dispositivo (fijo o móvil) que ejecuta el sistema de monitoreo de red.
- Consulta y búsqueda de registros, con lo que el administrador de red puede llevar a cabo un seguimiento de las actividades que toman lugar en la red en cuestión.

El usuario final de este sistema puede utilizar herramientas externas como analizadores de tráfico y firewalls para mejorar la seguridad de la información almacenada en la red en cuestión, detectando y mitigando ataques provenientes desde o hacia la misma.
El tiempo de vida del sistema va a depender de la utilización del mismo, así como de las actualizaciones y el mantenimiento que se le den para que éste sea capaz de seguir cumpliendo los objetivos principales y particulares establecidos al inicio de este documento, así como la demanda y el uso de nuevas tecnologías que se vayan suscitando en un futuro.

A posteriori, se podría llegar a añadir un analizador de tráfico e inclusive un firewall al sistema para que las tareas del administrador de red sean más efectivas que si éste usa las herramientas por separado.

Anexos

Glosario de términos

A

Apple: Empresa multinacional estadounidense que diseña y produce equipos electrónicos y software.

Agujero de seguridad: Es una vulnerabilidad de un sistema de información que permite mediante su explotación violar la seguridad del sistema.

Ancho de banda: Es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él.

Ataques informáticos: Todo aquél ataque destinado a quebrantar la seguridad de la información resguardada en sistemas informáticos, para poder hacer uso de la misma sin autorización.

B

Base de datos: Es una entidad en la cual se pueden almacenar datos de manera estructurada, con la menor redundancia posible.

C

Cliente: Cualquier dispositivo que realiza peticiones a un servidor.

Cydia: Un gestor de paquetes dpkg para iOS que utiliza una interfaz gráfica.

D

Data center: Un centro de datos es un espacio exclusivo donde las empresas mantienen y operan las infraestructuras TIC que utilizan para gestionar su actividad empresarial. Es el espacio donde alojar los servidores y sistemas de almacenamiento donde se ejecutan las aplicaciones y se procesan y almacenan los datos y el contenido.

Datagrama: Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes.

Dirección IP: Es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

Dirección MAC: Es la dirección de la tarjeta de red.

Dispositivo: Un dispositivo es un aparato o mecanismo que desarrolla determinadas acciones.

H

Hardening: El hardening de sistemas computacionales es el proceso de asegurar un Sistema computacional, con la finalidad de eliminar tantos riesgos como sea posible.

I

ICMP: El Protocolo de control de Mensajes de Internet (ICMP), su utilidad no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc.

Intrusión: Es un conjunto de actividades que conllevan la violación de la seguridad de un sistema informático.

J

Jailbreak: Se denomina Jailbreak al proceso de suprimir algunas de las limitaciones impuestas por Apple en dispositivos que utilicen el sistema operativo iOS mediante el uso de kernels modificados.

M

Metasploit: Es un framework desarrollado para facilitar el pentest en sistemas informáticos.

MySQL: MySQL es un sistema de gestión de base de datos relacional (RDBMS) de código abierto, basado en lenguaje de consulta estructurado (SQL).

P

Paquete: Conjunto limitado de datos

Phishing: El "phishing" es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.

PHP: Lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Proceso: Es un conjunto de actividades mutuamente relacionadas o que al interactuar juntas en los elementos de entrada y los convierten en resultados.

Proxy: Un servidor proxy es un equipo que actúa de intermediario entre un explorador web e Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas. Cuando un explorador solicita una página web almacenada en la colección (su caché) del servidor proxy, el servidor proxy la proporciona, lo que resulta más rápido que consultar la Web. Los servidores proxy también ayudan a mejorar la seguridad, ya que filtran algunos contenidos web y software malintencionado.

Puerto: Interfaz (física o lógica) a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

S

Seguridad informática: La Seguridad Informática es el conjunto de metodologías, controles, normas, mecanismos, herramientas, procedimientos y recursos que buscan mantener en un estado de operación esperado todo aquel sistema informático, garantizando la disponibilidad, integridad y confidencialidad de la información almacenada en el mismo.

Servidor: Es una computadora o pieza de software que está al "servicio" de otras dispositivos o personas llamadas clientes y que le suministran a estos, todo tipo de información.

Sistema: Un sistema es módulo ordenado de elementos que se encuentran interrelacionados y que interactúan entre sí.

Sistema operativo: Es el conjunto de programas informáticos que permiten una satisfactoria administración de los recursos que ostenta una computadora.

Sniffer: Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado dispositivo.

Spam: Se define SPAM a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva.

Spoofing: Se refiere al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación

SSH: Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.

Symantec: Es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática.

T

TCP: Protocolo de control de transmisión. Se utiliza cuando es necesario llevar un control en los paquetes enviados a través de la red.

Tecnologías de la información (TIC's): Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro.

U

UDP: Protocolo de servicios de internet orientado a la no conexión. Se utiliza cuando es necesario transmitir voz o vídeo, y resulta más importante transmitir con velocidades que garanticen la correcta recepción.

Unix: Sistema operativo multitarea y multiusuario de gran importancia en el desarrollo y la evolución de la tecnología.

V

Vulnerabilidad: Capacidad de sufrir daño.

W

Web cloning: Clonación de páginas web.

Fuentes de información

- Comandos Avanzados de Nmap (2012). En [In]Seguridad Informática. Consultado el 20 de septiembre de 2014, de http://calebbucker.blogspot.mx/2012/08/comandos-avanzados-de-nmap.html

- Intrusion Detection FAQ: How can passive techniques be used to audit and discover network vulnerability? (2013). En SANS. Consultado el 20 de septiembre de 2014, de http://www.sans.org/security-resources/idfaq/passive_vuln.php

- OS detection 100% success (2013). En e-solution. Consultado el 20 de septiembre de 2014, de http://esoln.net/blog/2013/12/27/os-detection-100-success/

- Funciones de strings (2005). En PHP manual. Consultado el 14 de noviembre de 2014, de http:// php.net/manual/es/ref.strings.php

- Operadores (2005). En PHP manual. Consultado el 14 de noviembre de 2014, de http://php.net/manual/es/language.operators.php

- Ssh2_shell (2005). En PHP manual. Consultado el 14 de noviembre de 2014, de http://php.net/manual/es/function.ssh2-shell.php

- Tips: Pasar variables de JavaScript a PHP (año). En Jodacame. Consultado el 6 de febrero de 2015, de http://blog.jodacame.com/tips-pasar-variables-de-javascript-a-php.html

- Nmap in the Enterprise: Your Guide to Network Scanning (2008). En Google Books. Consultado el 17 de febrero de 2015, de https://books.google.com.mx/books?id=VjgezB784XIC&printsec=frontcover&hl=es

- Definición de Seguridad Informática (2012). En Gestión de riesgo en la seguridad informática. Consultado el 13 de marzo de 2015, de https://protejete.wordpress.com/gdr_principal/definicion_si/

- Las 75 Herramientas de Seguridad Más Usadas (2003). En Insecure. Consultado el 16 de marzo de 2015, de http://insecure.org/tools/tools-es.html

- Seguridad perimetral "Monitoreo de recursos de red" (2005). En Julio Restrepo Wordpress. Consultado el 16 de marzo de 2015, de http://juliorestrepo.files.wordpress.com/2011/04/monitoreo.pdf

- How firewalls work. En How Stuff Works. Consultado el 16 de marzo de 2015, de http://computer.howstuffworks.com/firewall.htm

- Firewall / Cortafuegos (2000). En Segu Info. Consultado el 16 de marzo de 2015, de http://www.segu-info.com.ar/firewall/firewall.htm

- Firewall (2014). En CCM. Consultado el 16 de marzo de 2015, de http://es.ccm.net/contents/590-firewall

- Sistemas de detección de intrusos (2005). En Instituto tecnológico de informática. Consultado el 16 de marzo de 2015, de http://web.iti.upv.es/actualidadtic/2005/02/2005-02-intrusos.pdf

- Red Hat Enterprise Linux 4: Manual de seguridad. En Massachusetts Institue of Technology. Consultado el 17 de marzo de 2015, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

- Sistema de detección de intrusiones (IDS) (2014). En CCM. Consultado el 17 de marzo de 2015, de http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

- 5 herramientas de cifrado como alternativas a TrueCrypt (2014). En Hipertextual. Consultado el 17 de Marzo de 2015, de http://bitelia.com/2014/07/alternativas-truecrypt

- Redes de datos. En Redesdedatosinfo. Consultado el 17 de marzo de 2015, de http://redesdedatosinfo.galeon.com/enlaces2128619.html

- Apuntes de las asignaturas de redes de datos I y redes de datos II (2009). En Profesores FI-B UNAM. Consultado el 20 de marzo de 2015, de http://profesores.fi-b.unam.mx/victor/CCNA/Productos/Notas%20de%20Curso/Manual%20de%20la%20Asignatura%20de%20Redes%20de%20Datos%20I%20y%20II%20%20%28avance%2050%25%29.pdf

- Redes de datos. En Ecured. Consultado el 20 de Marzo de 2015, de http://www.ecured.cu/index.php/Redes_de_datos

- Ataques informáticos (2013). En Sykrayo y las F.C.S. Consultado el 20 de marzo de 2015, de https://sites.google.com/site/sykrayolab/ataques-informaticos

- Internet Security Threat Report (2014). En Symantec. Consultado el 21 de marzo de 2015, de http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

- Tipos de ataques informáticos. En Core One IT. Consultado el 21 de marzo de 2015, de http://www.coreoneit.com/tipos-de-ataques-informaticos/