UNIVERSIDAD TECNOLÓGICA

ISRAEL¨

FACULTAD INGENIERIA ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

TEMA:

ESTUDIO DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA QUE PERMITA DETECTAR Y CORREGIR VULNERABILIDADES EN LA RED DE DATOS DE LA UNIDAD EJECUTORA MAGAP-PRAT PROYECTO SIGTIERRAS.

AUTOR:

OSCAR JAVIER CHIGUANO GUAYANALLA

TUTOR:

MBA.WILMER ALBARRACIN

QUITO – ECUADOR

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE TESIS

El abajo firmante, en calidad de estudiante de la Carrera de Electrónica y Telecomunicaciones, declaro que los contenidos de este Trabajo de Graduación, requisito previo a la obtención del Grado de Ingeniero en Electrónica y Telecomunicaciones, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito, noviembre del 2012

Oscar Javier Chiguano Guaynalla

CC: 171941619-8

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de Grado, aprueban la tesis de graduación de acuerdo con las disposiciones reglamentarias emitidas por la Universidad Tecnológica "ISRAEL" para títulos de pregrado.

Quito, noviembre del 2012

Para constancia firman:

TRIBUNAL DE GRADO

_____

PRESIDENTE

_____ _____

MIEMBRO 1 MIEBRO 2

AGRADECIMIENTO

El agradecimiento más grande del mundo a mis padres quienes a pesar de los quebrantos en su salud, y tantos malos momentos por los que se ha pasado han estado siempre ahí.

A mi madre, Rosa Victoria Guaynalla Escobar quien con sus consejos y apoyo incondicional me ha sabido guiar por el buen camino, siempre animándome y siendo el motor para no decaer y seguir adelante Te Amo Mami.

A mi padre, Cesar Patricio Chiguano Nasimba por ser siempre un ejemplo de trabajo duro, perseverancia y lucha constante, te agradezco por haberme enseñado a trabajar y valorar el trabajo, gracias por darnos no todo, si no lo necesario a mis hermanos y a mí. Eres el Mejor.

A mis hermanos Dani y Liliata por estar siempre ahí animándome, preocupándose por mí y por quererme tanto.

Al Ing. Wilmer Albarracín por su colaboración, consejos y ayuda para sacar adelante este proyecto, por ser no solo mi Tutor de Tesis, sino un amigo.

A mi familia, Tíos, Primos, Abuelitos a los que están, y a los que se nos adelantaron.

DEDICATORIA

A mis padres, Rosa Guaynalla y Patricio Chiguano

Gracias por haberme dado la vida, Y sobre todo por haberme dado la libertad para vivirla.

A mis amigos Ángela, Paul por estar siempre en las buenas en las malas

Se cumplió el sueño (lachi ING).

A mis panas del alma, enanos gracias por todo.

A todas las personas que colaboraron con este proyecto de grado, gracias por soportar mis preguntas y solventar mis inquietudes.

INDICE

ÌNDICE DE GRÀFICOS

ÌNDICE DE TABLAS

UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE ELECTRÒNICA Y TELECOMUNICACIONES

TEMA:

Estudio Diseño e implementación de un Sistema que permita detectar y corregir vulnerabilidades en la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS.

AUTOR

Oscar Javier Chiguano Guaynalla

TUTOR

Ing. Wilmer Albarracín, MBA

RESUMEN

El presente proyecto consiste en realizar un estudio, diseño e implementación de un sistema, el cual permita detectar y corregir vulnerabilidades en la red de datos de la Unidad Ejecutora Magap-Prat proyecto SigTierras, como objetivo principal se

realiza un PentTest el cual ayudará a verificar el estado de la red de datos, así como las vulnerabilidades que se pudiera tener.

Como sistema base y de acuerdo al decreto 10-14 el cual la presidencia de la república presidida por el Ec. Rafael Correa quien autoriza a las entidadades públicas el uso de software libre, se ha tomado como sistema base a BackTrack el cual tiene una completa variedad de herramientas para el testeo de la red así como el análisis de tráfico en la red de datos.

UNIVERSIDAD TECNOLÓGICA ISRAEL

GRAPHIC DESIGN CAREER

TOPIC:

Study Design and implementation of a system to detect and fix vulnerabilities in network data of Unidad Ejecutora Magap-Prat project Sigtierras.

AUTHOR

Oscar Javier Chiguano Guaynalla

TUTOR

Ing. Wilmer Albarracín, MBA

ABSTRACT

This project is to conduct a study, design and implementation of a system which allows to detect and correct vulnerabilities in network data-PEU Magap Prat SigTierras project, the main objective is performed PentTest which help verify the state of the data network and the vulnerabilities that could have.

As a base system and 10-14 according to the decree which the presidency of the republic led by Rafael Correa who authorizes public entidadades using free software, is taken as the basis BackTrack system which has a complete variety of tools for network testing and analysis of network traffic data. Study Design and implementation of a system to detect and fix vulnerabilities in network data-PEU MAGAP SIGTIERRAS PRAT project.

CAPÌTULO I

1. ESTRUCTURA DEL PLAN DE PROYECTO DE GRADO

1.1 Tema de investigación

Estudio Diseño e implementación de un Sistema que permita detectar y corregir vulnerabilidades en la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS.

1.2 Antecedentes

El Sistema Nacional de Información y Gestión de Tierras Rurales e Infraestructura Tecnológica "SIGTIERRAS" es un programa del Ministerio de Agricultura, Ganadería, Acuacultura y Pesca, que arrancó sus actividades en enero del 2009 y tiene como objetivo establecer un sistema de administración de la tierra rural a nivel nacional, que garantice su tenencia y proporcione información básica para la planificación del desarrollo y ordenamiento territorial, y tiene sus bases jurídicas en los siguientes lineamientos:

a) La Unidad Ejecutora MAGAP-PRAT, fue creada mediante Acuerdo Ministerial No. 076 de 19 de marzo del 2002, publicado en el Registro Oficial No 557 de 17 de abril del mismo año; instrumento que se encuentra recopilado en el Texto Unificado de la Legislación Secundaria del Ministerio de Agricultura y Ganadería, realizado mediante Decreto Ejecutivo No. 3609, publicado en el. Registro Oficial E-1, de 20 de marzo del 2003.(se encuentra concluyendo la implantación de los

sistemas y acciones previstas en la Fase Piloto del Programa de Regularización y Administración de Tierras Rurales, financiadas mediante Contrato de Préstamo No.1376/OC-EC celebrado entre la República del Ecuador y el Banco Interamericano de Desarrollo el 22 de mayo del 2002.)

b) La Ley Reformatoria para la Equidad Tributaria, publicada en el Suplemento del Registro Oficial No. 242 de 12 de diciembre del 2007, en los artículos 173, 174; y en sus Disposiciones Transitorias Décimo Segunda; Tercera; y, Cuarta.

c) El Presidente Constitucional de la República, mediante Decreto No. 1092 de 18 de mayo del 2008, publicado en el Registro Oficial No. 351 del 3 de junio del 2008, que contiene el Reglamento para la aplicación del impuesto a la tierras rurales, dispone que el Ministerio de Agricultura, Ganadería, Acuacultura y Pesca, definirá la metodología a seguir a nivel nacional para establecer la identificación de los predios rústicos que deben registrarse en el catastro municipal correspondiente.

d) El Ministro de Agricultura, Ganadería y Pesca, mediante Acuerdo No. 160 de 23 de septiembre del 2008, publicado en el Registro Oficial No. 448 de 17 de octubre del 2008, en cumplimiento a la disposición del mencionado Decreto Ejecutivo; y, en base a la calificación prioritaria realizada por la Secretaria Nacional de Planificación y Desarrollo, SENPLADES, encarga a la Unidad

Ejecutora MAGAP – PRAT la ejecución “Programa Sistema Nacional de Gestión e Información de Tierras Rurales – SIGTIERRAS” en los ámbitos técnico, administrativo, financiero, de gestión y control.

1.3 Diagnóstico o planteamiento de la problemática general

Actualmente no existen mecanismos ni métodos eficaces que permitan determinar la seguridad de la red de datos cableada e inalámbrica, esto debido a que cualquier usuario tanto interno como externo, es decir, personas invitadas a las instalaciones de la Unidad Ejecutora MAGAP-PRAT proyecto Sigtierras, podría infiltrar ataques contra la red, ya que, la red no cuenta con normas de uso ni limites de acceso, o un plan de defensa para la red de datos.

A pesar de que la conexión a internet para la red inalámbrica y cableada cuenta con una velocidad de transmisión de 54 y 100 Mbps respectivamente, esta capacidad no es aprovechada al 100%, debido a que los usuarios al contar con ingreso simultaneo a la red, hacen mal uso de la misma y malgastan recursos utilizando la conexión a internet para navegar en redes sociales y paginas de ocio.

La conexión inalámbrica se la realiza mediante un Acces Point, de marca CISCO, que permite la conexión de los PC’s inalámbricos y de las estaciones de trabajo, las cuales pierden la conexión reiteradamente causando molestias a los usuarios,

Además no se cuenta con un monitoreo y el análisis del tráfico en la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto Sigtierras.

Además la red inalámbrica de la Unidad Ejecutora MAGAP-PRAT proyecto Sigtierras no cuenta con un estudio de vulnerabilidades que permita determinar los posibles ataques que se pueden perpetrar contra la red, los cuales pueden ser tan simples como un análisis del tráfico de paquetes hasta el robo de información de las estaciones de trabajo y servidores de la red. Estos posibles ataques se los pueden realizar mediante el uso de protocolos como:

ARP Poison Routing: es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en switch y no en hubs), que puede permitir al atacante husmear paquetes de datos en la LAN (red de área local), modificar el tráfico, o incluso detener el tráfico (conocido como DoS: Denegación de Servicio). Wardriving: es la actividad de encontrar puntos de acceso a redes inalámbricas, mientras uno se desplaza por la ciudad haciendo uso de una notebook con una placa de red Wireless para detectar señales.

Las imágenes georeferenciales (Orto fotos), utilizadas en la Unidad Ejecutora MAGAP-PRAT proyecto Sigtierras para la realización del catastro, requieren un mayor ancho de banda de por lo menos 256 Kbps para su respectiva manipulación, debido a que estas imágenes tienen un peso aproximado de 3Gb.

Actualmente existen dispositivos de comunicación como el Packet Shaper el cual permite una configuración óptima, brindando seguridad además, se puede limitar el ancho de banda y priorizar páginas, permite el bloqueo de puertos, y la detección de intrusos.

1.4 Formulación de la problemática

1.4.1 Problema principal

La Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS no cuenta con un sistema que detecte vulnerabilidades en su red, y que podrían afectar el correcto desempeño y funcionamiento de la misma.

1.4 2 Problemas secundarios

- No existe un sistema que permita determinar ataques y detecte vulnerabilidades en la red de datos cableada e inalámbrica la Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS.

- No se ha implementado un sistema que permita validar el grado de confiabilidad de la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS.

- La Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS no cuenta con un monitoreo y análisis de tráfico en su red de datos.

1.5 Objetivos

1.5.1 Objetivo General

Estudiar, Diseñar e implementar un (“PENTEST”) Test de Penetración o Intrusión para detectar vulnerabilidades en la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS.

1.6 Objetivos Específicos

- Implementar un sistema que permita determinar ataques y detecte vulnerabilidades en la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto Sigtierras.

- Implementar el sistema y realizar pruebas que permitan validar el sistema y determinar el verdadero estado de la red y sus posibles vulnerabilidades.

- Monitorear y Analizar el tráfico en la red de datos de la Unidad Ejecutora MAGAP-PRAT proyecto Sigtierras.

1.6 Justificación

1.6.1 Justificación Teórica

El presente proyecto que se basa en implementar un sistema que permita detectar vulnerabilidades en la red de datos de la UNIDAD EJECUTORA MAGAP-PRAT proyecto Sigtierras, contribuirá a mejorar el desempeño y eficiencia aprovechando la infraestructura tecnológica con la que cuenta la unidad, ya que al implementar un sistema que permita establecer las posibles falencias, se podrá realizar las correcciones adecuadas y así brindar un mejor uso tanto a los usuarios como a las personas encargadas de administrar la red, se podrá hacer recomendaciones en el uso de las páginas de internet que realmente se necesita y maneja la Unidad, debidamente con el estudió se evitará posibles ataques a la red de datos, servidores y estaciones de trabajo en fin de precautelar y evitar el robo de información. Se podrá recomendar el uso de diferente tipo de tecnología que puede mejorar aun más la eficiencia y calidad de servicio en la red de datos, Tecnología inalámbrica como Access Point switch´s administrables, estaqueables, apilables.

1.6.2 Justificación Metodológica

De acuerdo a las cuatro etapas que se van a desarrollar en el proyecto:

En la primera etapa se empleará los métodos de observación, análisis y síntesis los cuales ayudarán a dar un concepto claro y un mejor entendimiento de los temas y conceptos que se van tratando en el transcurso del proyecto.

En la segunda etapa se aplicará los métodos inductivo y deductivo, el cual reunirá un conjunto de hipótesis con las que se validarán y formularán alternativas para el diseño del estudio para el proyecto.

En la tercera etapa del proyecto a través del método experimental se buscará la mejor tecnología que pudiera aplicarse y recomendarse en lo que se refiere a software y hardware.

En la cuarta etapa del presente proyecto se empleará metodología experimental, la cual nos permitirá elaborar y realizar pruebas que permitan validar el proyecto.

1.6.3 Justificación Práctica

El presente proyecto está orientado a mejorar la eficiencia y el desempeño en la red de datos, con el fin de aprovechar al cien por ciento toda la infraestructura tecnológica con la que cuenta la Unidad Ejecutora MAGAP-PRAT proyecto SIGTIERRAS.

El proyecto advertirá y prevendrá a los administradores de red de los ataques que pueden afectar y dañar la red, así como también se brindará soluciones y técnicas de defensa que puedan prevenir estos hechos.

Además el proyecto presentará un informe detallando cuales han sido los riegos a los que se ve expuesta la red en mención, así, como los planes de defensa que se debe implementar con el fin de precautelar el ataque hacia la red y los métodos de defensa que se debe aplicar.

CAPÌTULO II

2. Introducción

Es muy importante ser consciente, que por más que una empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la seguridad física consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”.

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.1 Marco Teórico

2.2 Amenazas humanas

2.2.1 Personal (insiders)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70% son causados por el propio personal de la organización propietaria de dichos sistemas (“Inside Factor”).

Hablando de los Insiders Julio C. Ardita explica que desde mitad de 1996 hasta 1999 la empresa tuvo dos casos de intrusiones pero en el 2000 registramos siete, de las cuales 5 eran intrusos internos o ex–empleados.

2.2.2 Personal interno

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema. Al evaluar la situación, se verá que aquí el daño no es intencionado pero ello no está en discusión; el daño existió y esto es lo que compete a la seguridad informática.

2.2.3 Ex – empleado

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia.

Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex–empleado deja Bombas Lógicas que “explotan” tiempo después de marcharse.

2.2.4 Intrusos remunerados

Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar “secretos” (código

fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera la imagen de la entidad atacada.

Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

2.2.5 Hackers

La palabra hackers tiene una variedad de significados. Para muchos, significa programadores de Internet que intentan ganar acceso no autorizado a dispositivos en Internet. También se usa para referirse a individuos que corren programas para prevenir o reducir la velocidad del acceso a las redes por parte de un gran número de usuarios, o corromper o eliminar los datos de los servidores.

Pero para otros, el término hacker tiene una interpretación positiva como un profesional de redes que utiliza habilidades de programación de Internet sofisticadas para asegurarse de que las redes no sean vulnerables a ataques. Bueno o malo, el hacking es una fuerza impulsora de la seguridad en redes.

El trabajo del profesional de seguridad en redes es el de estar siempre un paso más adelante que los hackers tomando capacitaciones, participando en organizaciones de seguridad, suscribiéndose a canales web (feeds) en tiempo real sobre amenazas y visitando sitios web de seguridad diariamente.El profesional de seguridad en redes también debe tener acceso a herramientas de seguridad, protocolos, técnicas y tecnologías de última generación.

Los profesionales de la seguridad en redes deben tener muchas de las cualidades que se buscan en el personal de policía: deben mantenerse al tanto de actividades maliciosas y tener las habilidades y herramientas para minimizar o eliminar las amenazas asociadas con esas actividades.

2.2.6 Crackers

Los Crackers, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la manera equivocada o simplemente personas que hacen daño solo por diversión.

Los hackers opinan de ellos que son “. Hackers mediocres, no demasiados brillantes, que buscan violar (literalmente “break”) un sistema”.

2.3 Seguridad

2.3.1 Seguridad física

Ubicar el router y los dispositivos físicos que se conectan a él en un cuarto bajo llave que sea accesible solo para personal autorizado, esté libre de interferencia magnética o electrostática y tenga un sistema contra incendios y controles de temperatura y humedad. Instalar un sistema de alimentación ininterrumpida (uninterruptible power supply - UPS) y mantener los componentes de repuesto disponibles.

2.3.2 Seguridad de los sistemas operativos

Seguridad de las funciones y rendimiento de los sistemas operativos del router: Configurar el router con la máxima cantidad de memoria posible.La disponibilidad de la memoria puede ayudar a proteger la red de ataques de DoS, mientras que soporta el máximo rango de dispositivos de seguridad.

Usar la última versión estable del sistema operativo que cumpla los requerimientos de la red. Las funciones de seguridad de un sistema operativo evolucionan con el tiempo. Tenga en cuenta que la última versión de un sistema operativo puede no ser la versión más estable disponible.

Mantenga una copia segura de resguardo de la imagen del sistema operativo y el archivo de configuración del router.

2.3.3 Hardening del router[1]

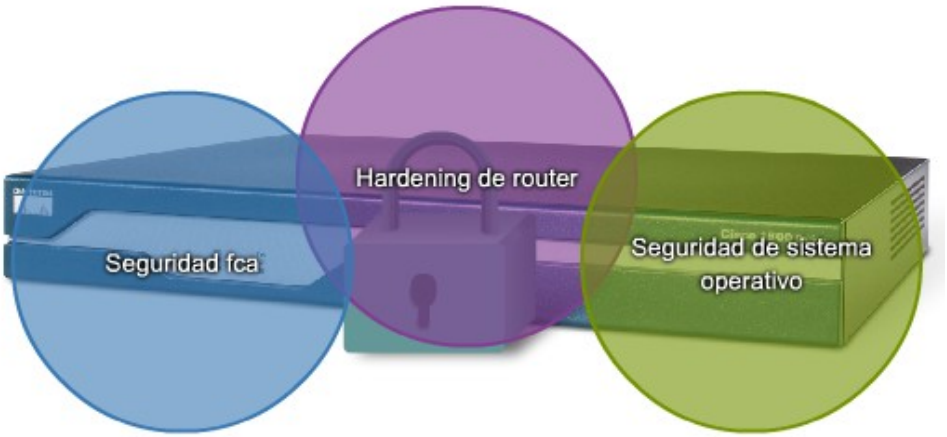
Elimine potenciales abusos de puertos y servicios no utilizados:

- Asegure el control administrativo. Asegúrese de que solo personal autorizado tenga acceso y su nivel de acceso sea controlado.

- Deshabilite puertos e interfaces no utilizadas. Reduzca la cantidad de maneras por las que puede accederse a un dispositivo.

- Deshabilitar servicios innecesarios. Como muchas computadoras, el router tiene servicios habilitados por defecto. Algunos de estos servicios son innecesarios y pueden ser utilizados por un atacante para reunir información o para efectuar explotaciones.

[1] http://www.cisco.com/web/learning/netacad/index.html



Gràfico2. 1 Hardening

2.3.4 Dmz

Una variante del enfoque de defensa profunda es ofrecer un área intermedia llamada zona desmilitarizada (demilitarized zone - DMZ).

La DMZ puede ser utilizada para los servidores que tienen que ser accesibles desde Internet o alguna otra red externa. La DMZ puede ser establecida entre dos routers, con un router interno conectado a la red protegida y un router externo conectado a la red no protegida, o ser simplemente un puerto adicional de un solo router.

El firewall, ubicado entre las redes protegida y no protegida, se instala para permitir las conexiones requeridas (por ejemplo, HTTP) de las redes externas (no confiables) a los servidores públicos en la DMZ. EL firewall sirve como protección primaria para todos los dispositivos en la DMZ. En el enfoque DMZ, el router

provee protección filtrando algún tráfico, pero deja la mayoría de la protección a cargo del firewall.

Gràfico2. 2 Enfoque DMZ

2.4 Dominios de la seguridad en redes

Es vital que los profesionales de la seguridad en redes entiendan los motivos de la misma y se familiaricen con las organizaciones dedicadas a ésta. También es importante entender los varios dominios de la seguridad en redes. Los dominios proveen un marco organizado para facilitar el aprendizaje sobre la seguridad en redes.

Existen 12 dominios de seguridad en redes especificados por la International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC).

Descriptos por ISO/IEC 27002, estos 12 dominios sirven para organizar a alto nivel el vasto reino de la información bajo el paraguas de la seguridad en

redes.Los 12 dominios están diseñados para servir como base común para desarrollar los estándares de seguridad en las organizaciones.

Evaluación de riesgos
Política de seguridad
Organización de la seguridad de la información
Administración de los bienes
Seguridad de los recursos humanos
Seguridad física y ambiente
Administración de las comunidades y las operaciones
Control de acceso
Adquisición, desarrollo y mantenimiento de los sistemas de Información
Administración de incidentes de seguridad de la información
Administración de la continuidad de los negocios

Tabla 1 Dominios de Elaborado por Oscar Chiguano

2.5 Políticas de seguridad en redes

La política de seguridad en redes es un documento amplio diseñado para ser claramente aplicable a las operaciones de una organización. La política se utiliza para asistir en el diseño de la red, transmitir principios de seguridad y facilitar el despliegue de la red.

La política de seguridad en redes traza las reglas de acceso a la red, determina cómo se harán cumplir las políticas y describe la arquitectura básica del ambiente básico de seguridad de la información de la empresa. El documento generalmente consta de varias páginas. Por su amplitud de cobertura e impacto, generalmente es un comité el que lo compila. Es un documento complejo que está diseñado para gobernar temas como acceso a los datos, navegación en la web, uso de las contraseñas, criptografía y adjuntos de correo electrónico.

Una política de seguridad deberá mantener a los usuarios malintencionados lejos y tener control sobre usuarios potencialmente peligrosos. Antes de crear una política debe entenderse qué servicios están disponibles a cuáles usuarios. La política de seguridad de red establece una jerarquía de permisos de acceso y da a los empleados solo el acceso mínimo necesario para realizar sus tareas.

La política de seguridad de la red establece cuáles bienes deben ser protegidos y da pautas sobre cómo deben ser protegidos. Esto será luego usado para determinar los dispositivos de seguridad y las estrategias y procedimientos de mitigación que deberán ser implementados en la red.

2.6 Virus

Un virus es código malicioso que se adjunta a archivos ejecutables o programas legítimos. La mayoría de los virus requiere una activación de parte del usuario final y puede permanecer inactivo por largos períodos de tiempo y luego activarse en una fecha u hora específica. Un virus simple puede instalarse en la primera línea de código en un archivo ejecutable. Una vez activado, el virus puede buscar en el disco otros ejecutables para infectar todos los archivos que aún no hayan sido infectados. Los virus pueden ser inofensivos, como aquellos que muestran una imagen en la pantalla, pero también.

Las principales vulnerabilidades de las computadoras de los usuarios finales son los ataques de virus, gusanos y troyanos:

- Un virus es un software malicioso que se adjunta a otro programa para ejecutar una función indeseada específica en una computadora.

- Un gusano ejecuta código arbitrario e instala copias de sí mismo en la memoria de la computadora infectada, que luego infecta a otros hosts.

- Un troyano es una aplicación escrita para parecerse a otra cosa. Cuando se descarga y ejecuta un troyano, ataca a la computadora del usuario final desde dentro.

2.7 Gusanos

Es un tipo de código hostil particularmente peligroso. Se multiplican explotando vulnerabilidades en las redes independientemente. Los gusanos generalmente hacen que las redes operen más lentamente.

Mientras que los virus requieren un programa huésped para ejecutarse, los gusanos pueden ejecutarse solos. No requieren la participación del usuario y pueden diseminarse muy rápidamente en la red.

Los gusanos son responsables de algunos de los ataques más devastadores de Internet. Por ejemplo, el SQL Slammer Worm de enero de 2003 hizo que el tráfico global de Internet fuera más lento como resultado de un ataque de Denegación de Servicio. Más de 250,000 hosts fueron afectados en los primeros 30 minutos. El gusano explotó una vulnerabilidad de desbordamiento de buffer

en el servidor SQL de Microsoft. Se había lanzado un parche para esta vulnerabilidad a mediados de 2002, por lo que los servidores que fueron afectados eran aquellos que no habían descargado la actualización que contenía el parche. Este es un buen ejemplo de por qué es tan importante que la política de seguridad de la organización exija actualizaciones y parches oportunos para los sistemas operativos y aplicaciones.

2.8 Caballos de troya

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocía, y que tenía una función muy diferente a la que ellos podían imaginar; un Caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped. Si bien este tipo de programas NO cumplen con la condición de auto–reproducción de los virus, encuadran perfectamente en las características de programa dañino.

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

Los ejemplos más conocidos de troyanos son el Back Oriffice y el Net Bus que, si bien no fueron desarrollados con ese fin, son una poderosa arma para tomar el control de la computadora infectada. Estos programas pueden ser utilizados para la administración total del sistema atacado por parte de un tercero, con los mismos permisos y restricciones que el usuario de la misma.

2.9 Tipos de ataque

Hay diferentes formas de ataques de red que no son virus, gusanos o troyanos. Para mitigar los ataques, es útil tener a los varios tipos de ataques categorizados. Al categorizar los ataques de red es posible abordar tipos de ataques en lugar de ataques individuales. No hay un estándar sobre cómo categorizar los ataques de red. El método utilizado en este curso clasifica los ataques en tres categorías principales.

2.9.1 Ataques de reconocimiento

Los ataques de reconocimiento consisten en el descubrimiento y mapeo de sistemas, servicios o vulnerabilidades sin autorización. Los ataques de reconocimiento muchas veces emplean el uso de sniffers de paquetes y escáners de puertos, los cuales están ampliamente disponibles para su descarga gratuita en Internet.

El reconocimiento es análogo a un ladrón vigilando un vecindario en busca de casas vulnerables para robar, como una residencia sin ocupantes o una casa con puertas o ventanas fáciles de abrir.

2.9.2 Ataques de acceso

Los ataques de acceso explotan vulnerabilidades conocidas en servicios de autenticación, FTP y web para ganar acceso a cuentas web, bases de datos confidenciales y otra información sensible. Un ataque de acceso puede efectuarse de varias maneras. Un ataque de acceso generalmente emplea un ataque de diccionario para adivinar las contraseñas del sistema. También hay diccionarios especializados para diferentes idiomas.

2.9.3 Ataques de denegación de servicio

Los ataques de Denegación de Servicio envían un número extremadamente grande de solicitudes en una red o Internet. Estas solicitudes excesivas hacen que la calidad de funcionamiento del dispositivo víctima sea inferior. Como consecuencia, el dispositivo atacado no está disponible para acceso y uso legítimo. Al ejecutar explotaciones o combinaciones de explotaciones, los ataques de DoS desaceleran o colapsan aplicaciones y procesos.

2.9.4 Ataques de reconocimiento

El reconocimiento también se conoce como recolección de información y, en la mayoría de los casos, precede un ataque de acceso o de DoS. En un ataque de reconocimiento, el intruso malicioso típicamente comienza por llevar a cabo un barrido de ping en la red objetivo para determinar qué direcciones IP están siendo utilizadas. El intruso entonces determina qué servicios o puertos están disponibles en las direcciones IP activas. Nmap es la aplicación más popular para escanear puertos. A partir de la información de puertos obtenida, el intruso interroga al puerto para determinar el tipo y la versión de la aplicación y el sistema operativo que está corriendo sobre el host objetivo. En muchos casos, los intrusos buscan servicios vulnerables que puedan ser explotados luego, cuando hay menos probabilidad de ser atrapados.

Los ataques de reconocimiento utilizan varias herramientas para ganar acceso a una red:

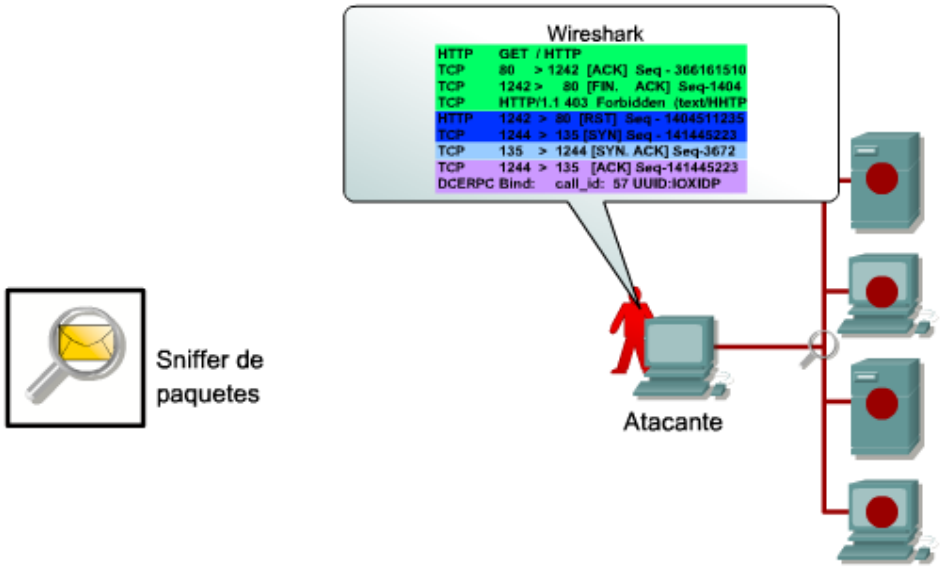
- Sniffers de paquetes
- Barridos de ping
- Escaneo de puertos
- Búsquedas de información en Internet

Un sniffer de paquetes es una aplicación de software que utiliza una tarjeta de red en modo promiscuo para capturar todos los paquetes de red que se transmitan a través de una LAN.

El modo promiscuo es un modo mediante el cual la tarjeta de red envía todos los paquetes que se reciben a una aplicación para procesarlos. Algunas aplicaciones de red distribuyen paquetes de red en texto plano sin cifrar. Como los paquetes de red no están cifrados, pueden ser entendidos por cualquier aplicación que pueda levantarlos de la red y procesarlos.

- Los sniffers de paquetes solo funcionan en el mismo dominio de colosión que la red bajo ataque, salvo que el atacante tenga acceso a los switches intermedios.

- Hay numerosos sniffers de paquetes disponibles, tanto freeware como shareware. Estos no requieren que el usuario tenga entendimiento de los protocolos que operan detrás.



Gràfico2. 3 Sniffer

Cuando se usan como herramientas legítimas, las aplicaciones de barrido de ping y escaneo de puertos efectúan una serie de pruebas en los hosts y dispositivos para identificar servicios vulnerables. La información se recolecta examinando el direccionamiento IP y datos de puerto o banner de los puertos TCP y UDP. Un atacante usa barridos de ping y escaneos de puerto para adquirir información para comprometer el sistema.

El barrido de ping es una técnica de escaneo de redes básica que determina qué rango de direcciones IP corresponde a los hosts activos. Un solo ping indica si un host específico existe en la red. El barrido de ping consiste en solicitudes de eco ICMP enviadas a varios hosts. Si una dirección dada está activa, la dirección devuelve una respuesta de eco ICMP.

Los barridos de ping están entre los métodos más viejos y lentos utilizados para escanear una red. Cada servicio de un host está asociado con un número de puerto bien conocido. El escaneo de puertos es un escaneo de un rango de números de puerto TCP o UDP en un host para detectar servicios abiertos. Consiste en el envío de un mensaje a cada puerto de un host. La respuesta recibida indica si el puerto es utilizado.

Las búsquedas de información en Internet pueden revelar información sobre quién es el dueño de un dominio particular y qué direcciones han sido asignadas a ese dominio. También pueden revelar quién es el dueño de una dirección de IP particular y qué dominio está asociado con la dirección.

Los barridos de ping sobre direcciones reveladas por búsquedas de información en Internet pueden dar una imagen de los hosts activos en un ambiente en particular. Luego de que se ha generado esa lista, las herramientas de escaneo de puertos pueden pasar por todos los puertos bien conocidos para proporcionar una lista completa de todos los servicios que están corriendo en los hosts que el barrido de ping descubrió.

Los hackers pueden entonces examinar las características de las aplicaciones activas, de donde pueden extraer información específica útil para un hacker cuya intención es comprometer ese servicio pueden ser destructivas, como aquellos

que modifican o eliminan los archivos del disco rígido. Los virus también pueden ser programados para mutar con el propósito de evitar su detección.

2.9.5 Ataques de contraseña

El atacante intenta adivinar las contraseñas del sistema. Un ejemplo común es un ataque de diccionario.

2.9.6 Explotación de la confianza

El atacante usa privilegios otorgados a un sistema en una forma no autorizada, posiblemente causando que el objetivo se vea comprometido. Redirección de puerto - Se usa un sistema ya comprometido como punto de partida para ataques contra otros objetivos. Se instala una herramienta de intrusión en el sistema comprometido para redirección de sesiones.

2.9.7 Ataqué Man in the middle

El atacante se ubica en el medio de una comunicación entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes. Un ataque Man in the Middle popular involucra a una laptop actuando como un punto de acceso no autorizado (rogue access point) para capturar y copiar todo el tráfico de red de un usuario objetivo.

Frecuentemente el usuario está en un lugar público conectado a un punto de acceso inalámbrico.

2.9.8 El ping de la muerte

En un ataque de ping de la muerte, un hacker envía una solicitud de eco en un paquete IP más grande que el tamaño de paquete máximo de 65535 bytes. Enviar un ping de este tamaño puede colapsar la computadora objetivo. Una variante de este ataque es colapsar el sistema enviando fragmentos ICMP, que llenen los buffers de reensamblado de paquetes en el objetivo.

2.9.9 Ataque smurf

En un ataque smurf, el atacante envía un gran número de solicitudes ICMP a direcciones broadcast, todos con direcciones de origen falsificadas de la misma red que la víctima. Si el dispositivo de ruteo que envía el tráfico a esas direcciones de broadcast reenvía los broadcast, todos los host de la red destino enviarán respuestas ICMP, multiplicando el tráfico por el número de hosts en las redes.

En una red broadcast multiacceso, cientos de máquinas podrían responder a cada paquete.

2.9.10 Inundación TCP/SYN

En un ataque de inundación TCP/SYN, se envía una inundación de paquetes SYN TCP, generalmente con una dirección de origen falsa. Cada paquete se maneja como una solicitud de conexión, causando que el servidor genere una conexión a medio abrir devolviendo un paquete SYN-ACK TCP y esperando un paquete de respuesta de la dirección del remitente. Sin embargo, como la dirección del remitente es falsa, la respuesta nunca llega. Estas conexiones a medio abrir saturan el número de conexiones disponibles que el servidor puede atender, haciendo que no pueda responder a solicitudes legítimas hasta luego de que el ataque haya finalizado.

2.9.11 Ataques de Monitorización

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

2.10 Seguridad del router de borde

La seguridad la infraestructura de la red es crítica para la seguridad de toda la red. La infraestructura de la red incluye routers, switches, servidores, estaciones de trabajo y otros dispositivos. Considere un empleado descontento mirando casualmente por sobre el hombro del administrador de la red mientras el

administrador se está identificando en el router de borde. Esto se conoce como shoulder surfing y es una manera sorprendentemente fácil para un atacante de ganar acceso no autorizado.

Si un atacante obtiene acceso a un router, la seguridad y la administración de toda la red pueden ser comprometidas, dejando a los servidores y las estaciones de trabajo bajo riesgo. Es crítico que las políticas y controles de seguridad apropiados puedan ser implementados para prevenir el acceso no autorizado a todos los dispositivos de la infraestructura. Aunque todos los dispositivos de una infraestructura están en riesgo, los routers generalmente son el objetivo principal para los atacantes de redes. Esto ocurre porque los routers actúan como la policía del tránsito, dirigiendo el tráfico hacia, desde y entre redes.

El router de borde es el último router entre la red interna y una red de confianza como Internet. Todo el tráfico a Internet de una organización pasa por este router de borde; por lo tanto, generalmente funciona como la primera y última línea de defensa de una red. A través del filtrado inicial y final, el router de borde ayuda a asegurar el perímetro de una red protegida. También es responsable de implementar las acciones de seguridad que están basadas en las políticas de seguridad de la organización. Por estas razones, es imperativo asegurar los routers de la red.

2.11 El modelo OSI

El modelo conceptual OSI (Open System Interconection) es utilizado por, prácticamente, la totalidad de las redes del mundo. Este modelo fue creado por el ISO (International Standard Organization), y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas.

Esta clasificación permite que cada protocolo fuera desarrollado con una finalidad determinada, lo cual simplifica el proceso de implementación. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores.

Los siete niveles del modelo OSI son los siguientes:

2.11.1 Capa física:

Esta capa tiene que ver con el envío de bits en un medio físico de transmisión y asegura que si de un extremo del medio se envía un 1 (carga eléctrica) del otro lado se reciba ese 1. Brinda los medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace físico entre los sistemas.

2.11.2 Capa de enlace:

En esta capa se toman los bits que entrega la Capa Física y se agrupan para formar marcos de bits (Frames). Se realiza un chequeo de errores sobre cada frame. Si un marco se pierde o se daña en el medio físico este capa se encarga de retransmitirlo, aunque en ocasiones dicha operación provoca que un mismo marco se duplique en el destino. Dado el caso es obligación detectar tal anomalía y corregirla. También en esta capa se decide cómo acceder al medio físico.

2.11.3 Capa de red:

Se encarga de controlar la operación de la subred (medios físicos y dispositivos de enrutado). Una tarea primordial es decidir cómo hacer que los paquetes lleguen a su destino desde su origen en el formato predefinido por un protocolo. Otra función importante en este nivel es la resolución de cuellos de botella. En estos casos se pueden tener varias rutas para dar salida a los paquetes y a base de algunos parámetros de eficiencia o disponibilidad se eligen rutas dinámicas de salida. A los efectos de la obtención de estadísticas, se registra el tipo y cantidad de paquetes que circulan.

2.11.4 Capa de transporte:

El objetivo de esta capa es el de tomar datos de la Capa de Sesión y asegurarse que dichos datos llegan a su destino. En ocasiones los datos que vienen de la Capa de Sesión exceden el tamaño máximo de transmisión (MTU Maximum Transmission Unit) de la interfaz de red, por lo cual es necesario particionarlos y enviarlos en unidades más pequeñas, lo cual da origen a la fragmentación y ensamblado de paquetes cuyo control se realiza en esta capa. La última labor importante de la Capa de Transporte es ofrecer un mecanismo de nombrado que sirva para identificar y diferenciar las múltiples conexiones existentes, así como determinar en qué momento se inician y se terminan las “conversaciones”; es decir, en esta capa hay un mecanismo de control de flujo. Por ejemplo, si el usuario "a" en el nodo (A) quiere iniciar una sesión de trabajo remoto en un nodo (B), existirá una conexión que debe ser diferenciada de la conexión que el usuario "b" necesita para transferir un archivo del nodo (B) al nodo (A).

2.11.5 Capa de sesión:

Esta capa ofrece el servicio de establecer sesiones de trabajo entre nodos diferentes de una red, sincroniza y establece puntos de chequeo. Por ejemplo, si se hace necesario transferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que

una transmisión ordinaria nunca terminaría porque algún interlocutor perderá la conexión. La solución es que se establezcan puntos de chequeo cada pocos minutos de manera que, si la conexión se rompe, más tarde se pueda reiniciar a partir del punto de chequeo, lo cual ahorra tiempo y permite la finalización de la transferencia.

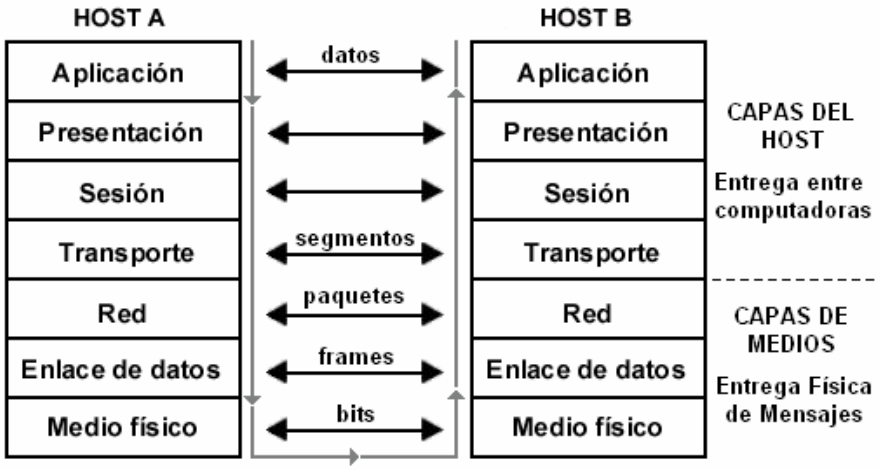
2.11.6 Capa de presentación:

Esta provee las facilidades para transmitir datos con la sintaxis propia de las aplicaciones o el nodo. En esta capa es posible convertir los datos a un formato independiente de los nodos que intervienen en la transmisión.

2.11.7 Capa de aplicación:

En esta capa se encuentran las aplicaciones de red que permiten explotar los recursos de otros nodos. Dicha explotación se hace, por ejemplo, a través de una emulación de una terminal que trabaja en un nodo remoto, interpretando una gran variedad de secuencias de caracteres de control que permiten desplegar en la terminal local los resultados, aún cuando éstos sean gráficos. Otra forma de explotación se da cuando se transmite desde una computadora origen que almacena sus archivos en un formato distinto al del destino.

Es posible que el programa de transferencia realice las conversiones necesarias de manera que el archivo puede usarse inmediatamente bajo alguna aplicación.



Gràfico2. 4 Modelo OSI

2.12 Dns

Ya que para el ser humano se hace difícil recordar direcciones IP como 209.89.67.156 se creó lo que dio en llamar DNS (Domain Name Server), el cual es el encargado de convertir la dirección IP en un nombre de dominio generalmente fácil de recordar y viceversa. Así www.clarin.com será entendida, merced al servicio de DNS como 110.56.12.106 o \\Carlos se convertirá en 10.0.0.33.

2.13 Puertos

Para acceder desde el nivel de red al nivel de aplicaciones no sirve simplemente indicar la dirección IP; se necesitarán mas especificaciones para que el Host de destino pueda escoger la aplicación correcta.

Estas especificaciones harán necesario la definición de Puerto. Un puerto se representa por un valor de 16 bits y hace la diferencia entre los posibles receptores de un mensaje.

La combinación Dirección IP + Puerto identifican una región de memoria única denominada Socket. Al indicar este Socket, se puede trasladar el paquete a la aplicación correcta (FTP, Telnet, WWW, etc.) y, si además recibe el puerto desde donde fue enviado el mensaje, se podrá suministrar una respuesta.

Actualmente existe miles de puertos ocupados de los 2^{16} = 65535 posibles, de los cuales apenas unos cuantos son los más utilizados y se encuentran divididos en tres rangos:

- Desde el puerto 0 hasta el 1023: son los puertos conocidos y usados por aplicaciones de servidor.

- Desde el 1024 hasta el 49151: son los registrados y asignados dinámicamente.

- Desde el 49152 hasta 65535: son los puertos privados.

Puerto	Aplicación	Protocolo	Descripción
20	FTP–Data	TCP/UDP	Transferencia archivos
21	FTP	TCP	Control Transferencia Archivos
23	TELNET	TCP/UDP	Servicio Remoto
25	SMTP	TCP/UDP	Envío de mails
43	Whois	TCP/UDP	
53	DNS	TCP/UDP	Servicio de Nombre de Dominios
70	Gopher	TCP/UDP	
79	Finger	TCP/UDP	
80	WWW–HTTP	TCP/UDP	World Wide Web
110	POP3 (PostOffice)	TCP/UDP	Recepción de mail
119	UseNet	TCP	Newsgropus de usuarios
137	NetBIOS	UDP	
194	IRC (Internet Relay Chat)	TCP/UDP	Chat
443	HTTPS	TCP	HTTP Seguro vía SSL
750	Kerberos	TCP/UDP	
6667	IRC (Internet Relay Chat)	TCP	Chat

Tabla 2. Puertos más relevantes. Elaborado por Oscar Chiguano

2.14 Ingeniería social

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente (generalmente es así), puede engañar fácilmente a un usuario (que desconoce

las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords. Por ejemplo, suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente.

O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

2.15 Ingeniería social inversa

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social. En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

- Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruso tenga un mínimo contacto con el sistema.

- Comunicación a los usuarios de que la solución es brindada por el intruso(publicidad).

- Provisión de ayuda por parte del intruso encubierto como servicio técnico.

2.16 Trashing (cartoneo)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema..."nada se destruye, todo se transforma".

- El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

- El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

2.17 Shoulder surfing

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post–it adheridos al monitos o teclado). Cualquier intruso puede pasar por ahí,

verlos y memorizarlos para su posterior uso. Otra técnica relacionada al Surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

2.18 Decoy (señuelos)

Los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras “visitas”.

Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

2.19 Scanning (búsqueda)

El Escaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma.

El Escaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número.

2.20 Utilización de backdoors

“Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo.

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

2.21 Utilización de exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos “agujeros” reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

2.22 Obtención de passwords

Este método comprende la obtención por “Fuerza Bruta” de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia.

En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

2.23 BackTrack

Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. Fue incluida en el puesto 32 de la famosa lista *"Top 100 Network Security Tools"* de 2006.

Gràfico2. 5 Pantalla BackTrack Elaborado por Oscar Chiguano

2.24 Herramientas

BackTrack le ofrece al usuario una extensa colección de herramientas completamente usables desde un Live CD o un Live USB por lo que no requiere una instalación para poder usarse. O bien, se ofrece la opción de instalar en un disco duro. Entre las herramientas ofrecidas se encuentran:

- Aircrack-ng, Herramientas para auditoría inalámbrica
- Kismet, Sniffer inalámbrico
- Ettercap, Interceptor/Sniffer/Registrador para LAN
- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta

- Nmap, rastreador de puertos

Y una larga lista de otras herramientas, que se agrupan en 11 familias:

- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de aplicaciones Web
- Análisis de redes de radio (WiFi, Bluetooth, RFID)
- Penetración (Exploits y Kit de herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de Acceso
- Forenses
- Ingeniería inversa
- Voz sobre IP

CAPÌTULO III

3. Introducción

Las herramientas de seguridad son una parte fundamental y esencial en la administración, protección y cuidado de los diferentes componentes que integran la red de datos de la Unidad Ejecutora Magap-Prat.

En este capítulo se hace énfasis al estudio de algunas de las herramientas más utilizadas en el Test de Penetración, así como sus características, usos y utilidades.

Dadas las descripciones de cada una de estas herramientas, hay que tomar en cuenta que también pueden ser utilizadas para realizar diferentes tipos de ataques dependiendo de la información que se requiere descubrir, y dependiendo de la ética de cada una de las personas.

Las herramientas descritas en el presente capitulo son solo algunas de la gran variedad que existen actualmente en el mercado de la seguridad.

3.1 Estudio del Sistema

3.2 Identificación de amenazas y análisis de riesgos

Uno de los primeros pasos para establecer las necesidades de seguridad de una empresa es la identificación de posibles vulnerabilidades. La identificación de estas proporciona a la empresa una lista de amenazas a las que el sistema puede estar sujeto en un ambiente particular. Para identificar las amenazas, es importante hacerse preguntas:

¿Cuáles son las posibles vulnerabilidades del sistema?
¿Cuáles pueden ser las consecuencias si se explotan las vulnerabilidades del sistema?

Por ejemplo, la identificación de amenazas en la conexión de un sistema de servidores podría incluir:

Robo de datos de los clientes: El atacante roba los datos personales y financieros de los clientes del banco de la base de datos de clientes.

Transacciones falsas de un servidor externo: El atacante altera el código de una aplicación y ejecuta transacciones arbitrarias haciéndose pasar por un usuario legítimo.
Ataque interno al sistema: Un empleado del banco encuentra una falla en el

sistema y monta un ataque.

Errores de ingreso de datos: El usuario ingresa datos incorrectos o efectúa solicitudes de transacción incorrectas.

El análisis de riesgos es el estudio sistemático de las incertidumbres y los riesgos. Estima la probabilidad y severidad de las amenazas a un sistema y proporciona a la organización una lista de prioridades. Los analistas de riesgos identifican el riesgo, determinan cómo y cuándo puede aparecer y estiman el impacto (financiero u otros) de un resultado adverso.

Compromiso interno del sistema: Extremadamente severo y probable si se usa software no confiable para pasar datos a la red interna. Información se utiliza en el análisis de riesgos. Hay dos tipos de análisis de riesgos en la seguridad de la información: cuantitativo y cualitativo.

Análisis de riesgos cuantitativo: El análisis de riesgos cuantitativo usa un modelo matemático para asignar una representación monetaria al valor de los activos, el costo de las amenazas realizadas y el costo de las implementaciones de seguridad. Las representaciones monetarias generalmente se basan en costo anual.

Análisis de riesgo cualitativo: Hay muchas maneras de llevar a cabo un análisis de riesgo cualitativo. Un método utiliza un modelo basado en la situación.

Este enfoque es conveniente para grandes ciudades, estados o provincias y países ya que en estos casos no es práctico hacer listas de los activos, lo cual constituye el primer paso en cualquier análisis de riesgo cuantitativo. Si un gobierno nacional decidiera confeccionar una lista de todos sus activos, estos habrían cambiado cientos o miles de veces mientras la lista se llenaba y nunca llegaría a ser correcta.

Con un análisis de riesgo cualitativo, la investigación es exploratoria y no siempre se puede graficar o probar matemáticamente. Se concentra mayormente en entender por qué hay riesgos y cómo se pueden resolver de diferentes maneras.

El análisis de riesgos cuantitativo es más preciso matemáticamente y es utilizado por las empresas como justificación de los costos de las contramedidas. Por esta razón, el siguiente tema es una profundización en la construcción del análisis de riesgo cuantitativo.

3.3 Código de Ética IAB

Según la página http://www.iab.org.br, el IAB emitió su código de ética Internet que es un complejo nacional cuya utilidad es mayormente consecuencia de su gran disponibilidad y accesibilidad. El uso irresponsable de este recurso crítico representa una amenaza enorme a la continuidad de su disponibilidad a la comunidad técnica. El gobierno de los Estados Unidos de América, patrocinador de este sistema, sufre cuando ocurren abusos que producen interrupciones significativas. El acceso a y uso de Internet es un privilegio que debe ser tratado como tal por todos los usuarios del sistema.

- Ganar acceso no autorizado a los recursos de Internet.
- Interrumpir el uso de Internet.
- Desperdiciar recursos, como personas, capacidad y computadoras, a través de tales acciones.
- Destruir la integridad de la información basada en computadoras
- Comprometer la privacidad de los usuarios.

3.4 Whois.net

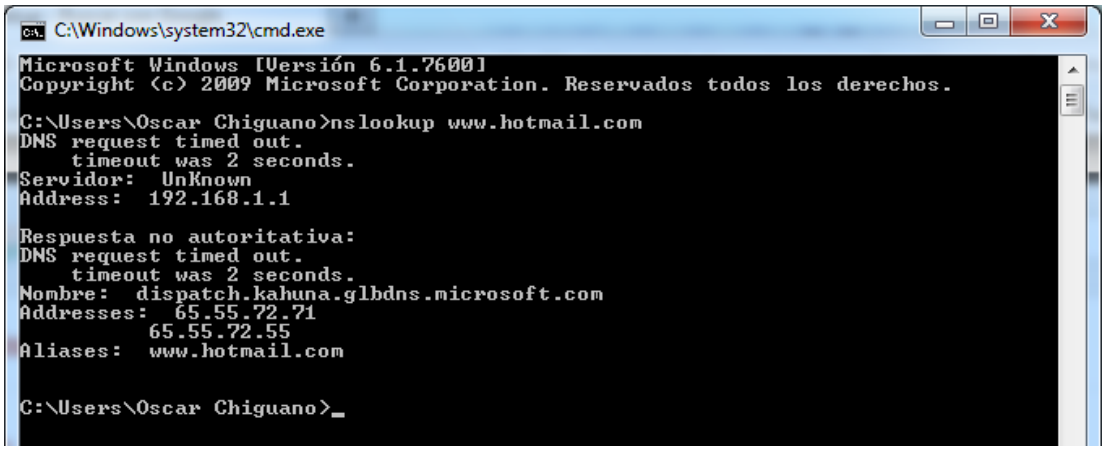
Según la página whois.net/, muestra el perfil público de quien es el propietario de un dominio en particular, así como el nombre del dominio. Whois.net es una página netamente de consulta y acceso a información, esta página garantiza que la información aquí visualizada es veraz y efectiva.

Gràfico3. 1 Whois.net

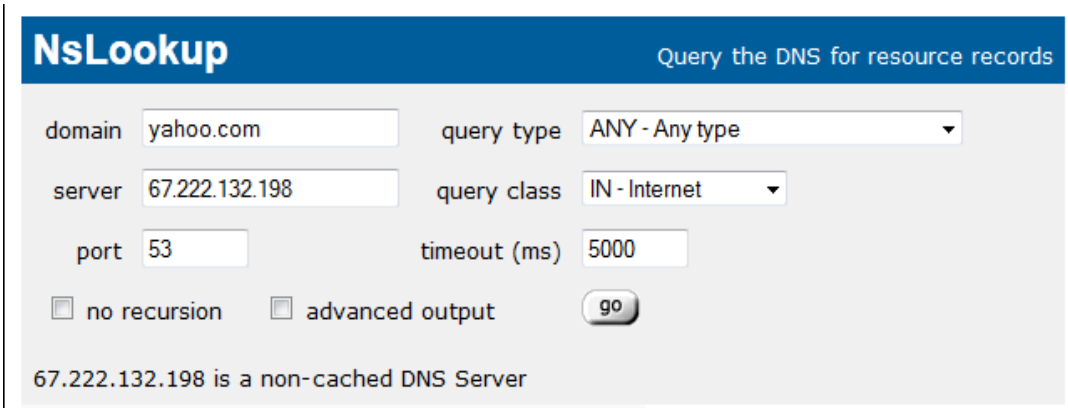
- Nombre dirección y teléfono donde se encuentra registrado el dominio.
- Nombre dirección teléfono de la persona encargada de administrar el dominio.
- Fechas de creación expedición del domino.

3.5 Nslookup

Según la página http://network-tools.com/nslook/, es un comando el cual puede servir tanto en ambiente Windows como el Linux sirve para buscar la dirección Ip del servidor, nombres de un computador en particular, NsLookup también puede ser utilizado via internet en la pajina oficial de esta herramienta.



Gràfico3. 2 Nslookup consola de comandos



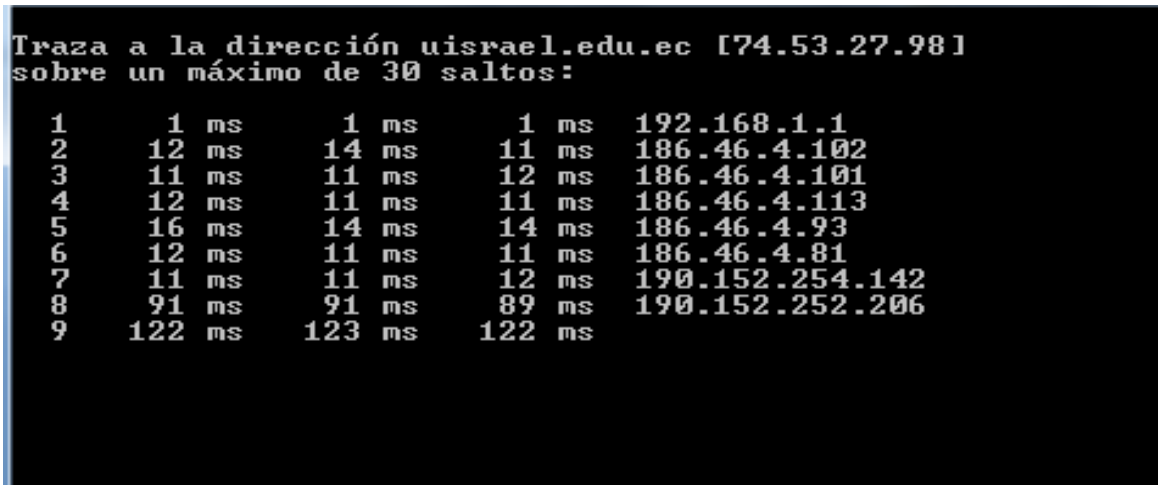
Gràfico3. 3 Nslookup atreves de Internet

3.6 Traceroute

Según la página http://www.traceroute.org/, es una herramienta de diagnostico de redes, que permita realizar el seguimiento de de los paquetes que van desde un host [2]a otro. Esta herramienta es conocida como tracert en ambiente Windows y Traceroute en ambiente Linux.

El número de la primera columna es el número de salto, posteriormente viene el nombre y la dirección IP del nodo por el que pasa, los tres tiempos siguientes son el tiempo de respuesta para los paquetes enviados (un asterisco indica que no se obtuvo respuesta).

Estas herramientas (traceroute y tracert) son órdenes ejecutables en una consola en modo texto.



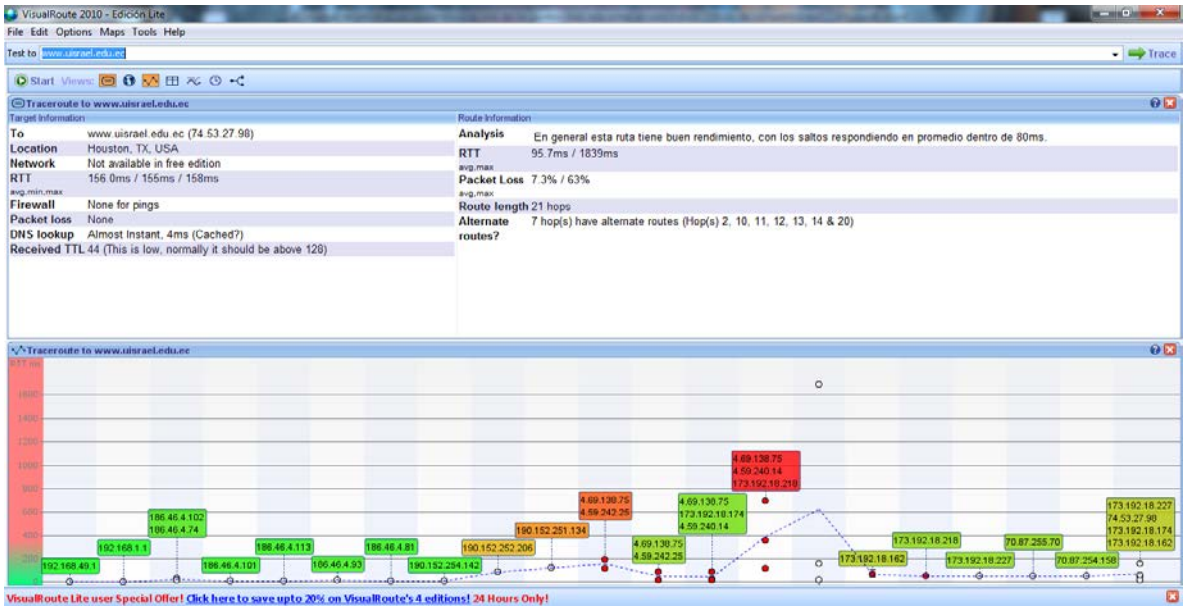
Gràfico3. 4 Traceroute atreves de la consola de comandos

[2] Host: Equipo de Red

3.7 Visual Route

Según la página http://www.visualroute.com/ esta aplicación permite visualizar problemas de conectividad, muestra gráficamente saltos hacia otras direcciones e indica tiempos de respuesta en una escala grafica. Las versiones de este software son comerciales y con un precio en su licencia.

VisualRoute es una potente herramienta de Traceroute, Ping, y Whois que además te muestra gráficamente los resultados sobre un mapa geográfico con todo detalle. El programa puede servirte para localizar una IP o dominio determinado y encontrar posibles problemas de conectividad entre redes.
Y no sólo esto sino que te brindará importante información de los servidores y dominios de destino gracias a su base de datos.

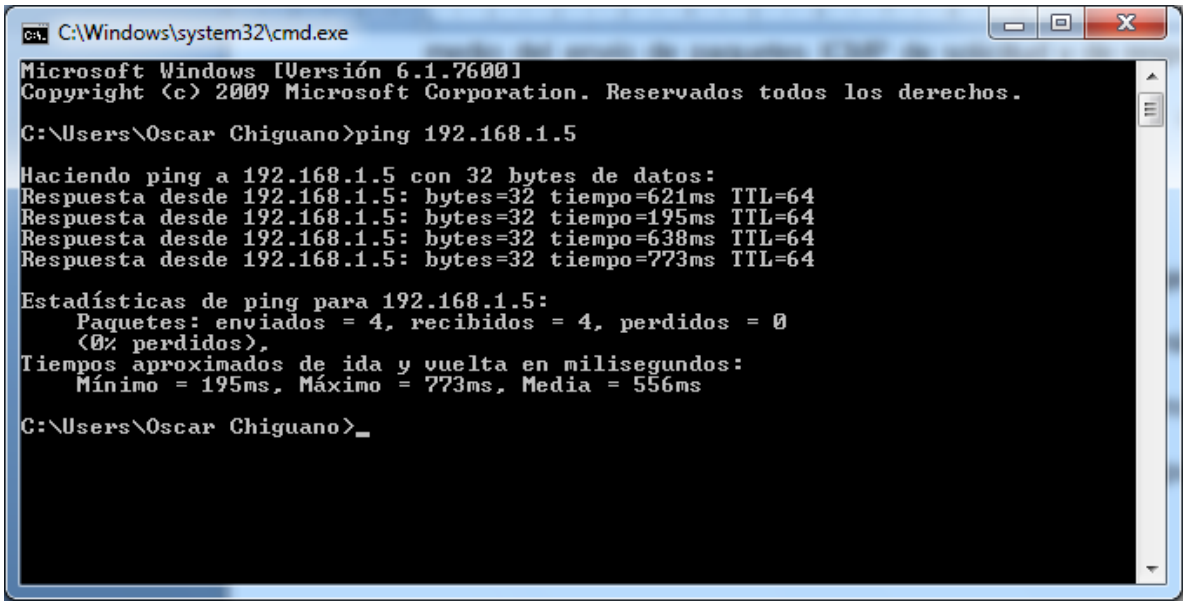


Gràfico3. 5 Visual Route

3.8 Ping

Según la página http://ping.eu/ normalmente, PING el acrónimo de Packet Internet Groper, el que puede significar "Buscador o rastreador de paquetes en redes" Comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta.

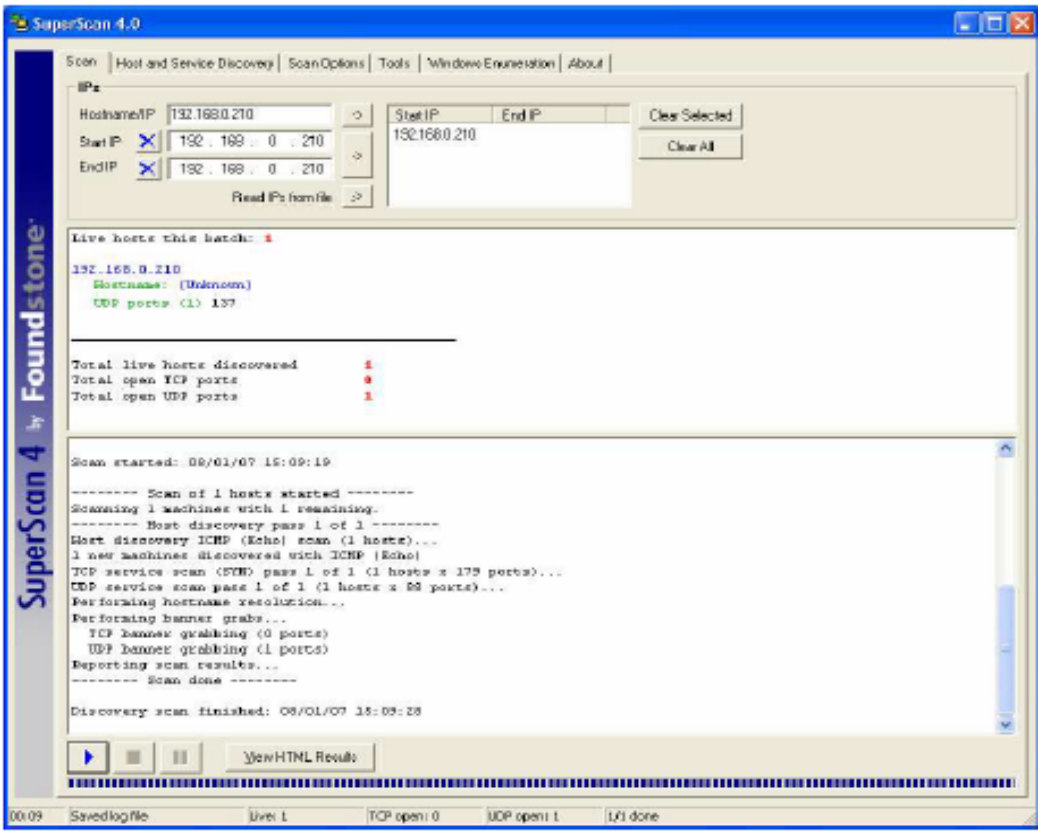
Ejecutando Ping de solicitud, el Host local envía un mensaje ICMP, incrustado en un paquete IP. El mensaje ICMP de solicitud incluye, además del tipo de mensaje y el código del mismo, un número identificador y una secuencia de números, de 32 bits, que deberán coincidir con el mensaje ICMP de respuesta; además de un espacio opcional para datos. Para Linux el comando a digitar es (**ifconfig**).



Gràfico3. 6 Ping médiate consola de comandos Windows

3.9 SuperScan

Según la página http://superscan.archivospc.com/, es un escáner de puertos el cual nos permite realizar una variedad de tipos de operaciones de escaneo. Usando una Ip o utilizando las direcciones ip de un archivo dado. Puede realizar conexiones de cualquier tipo de puerto entre ellos (Ftp, Telnet, Web) además de realizar ping y resolver direcciones de dominio.

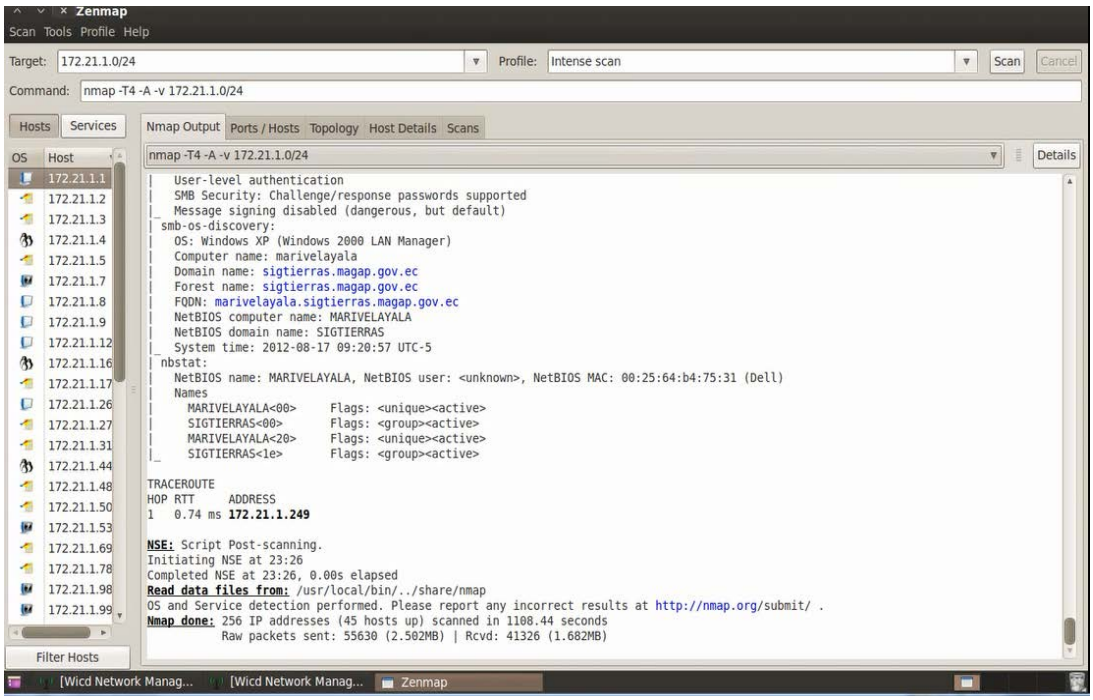


Gràfico3. 7 SuperScan4

3.10 Zenmap (Nmap)

Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.

Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

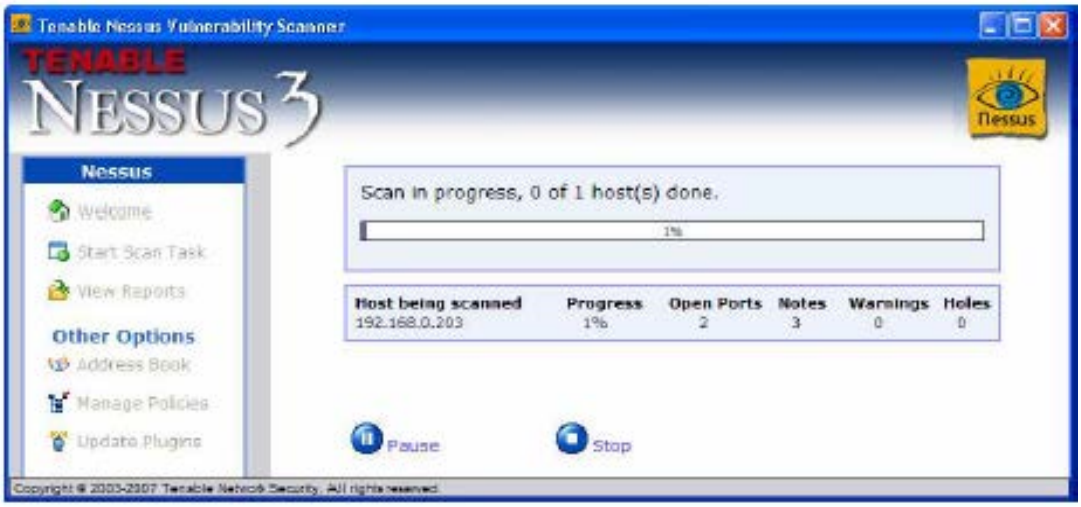


Gràfico3. 8 Znmap Red SigTierras

3.11 Nessus

Según la página http://www.tenable.com/products/nessus, es una de las herramientas más ampliamente implementado del mundo y evaluación de configuraciones de productos, Nessus ofrece alta velocidad de descubrimiento, la auditoría de configuración, el perfil activo, el descubrimiento de datos sensibles, la integración de la gestión de parches, y análisis de la vulnerabilidad de su posición de seguridad con funciones que mejoran la facilidad de uso, la eficacia, la eficiencia y la comunicación con todas las partes de su organización.

Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.

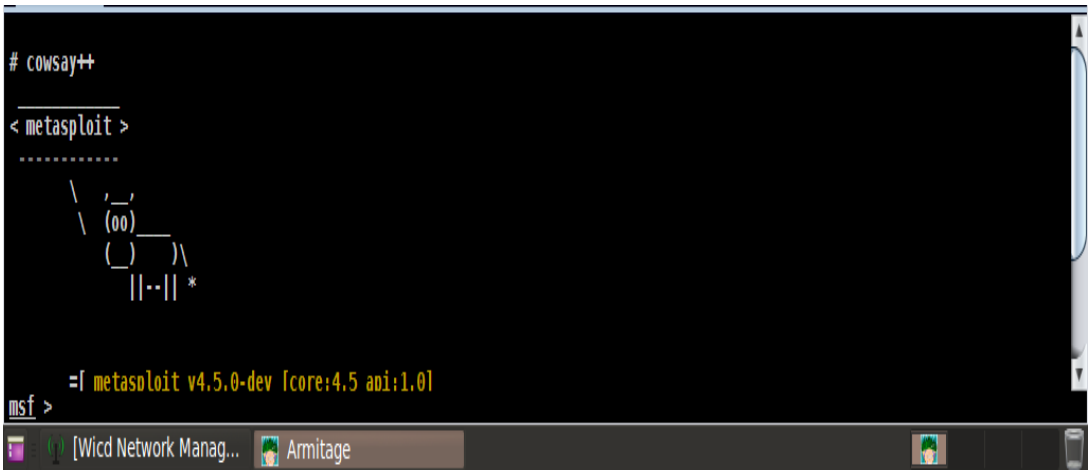


Gràfico3. 9 Nessus Funcionamiento

3.12 Metasploit

Según la página http://www.metasploit.com/, es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos.

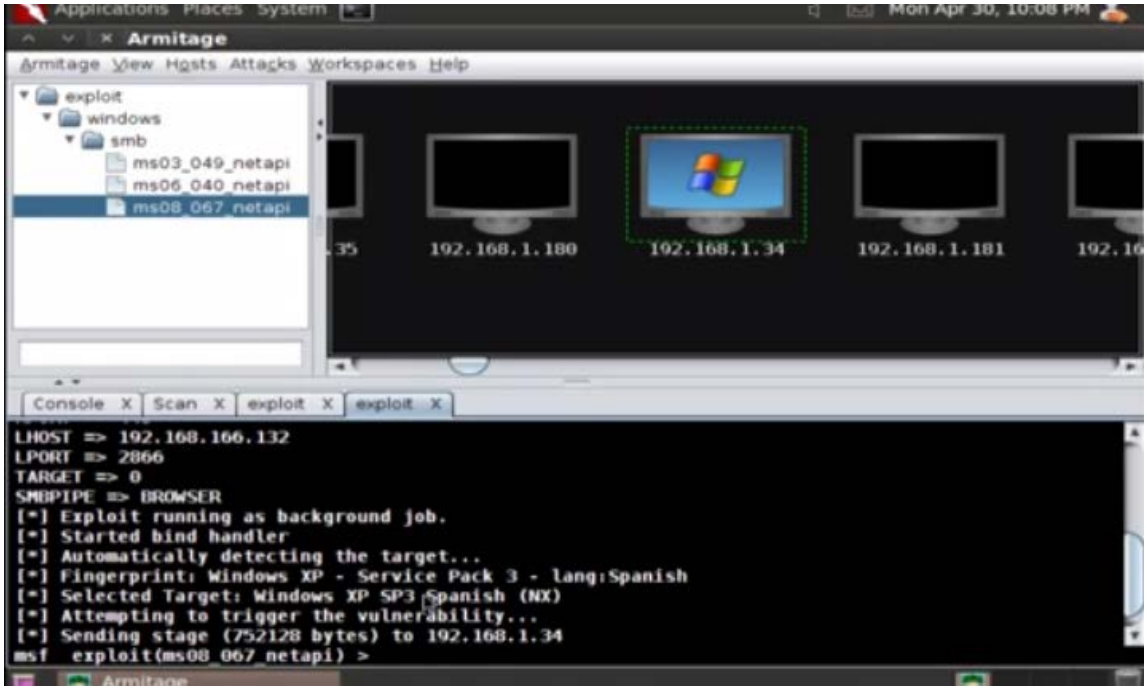
Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Otros subproyectos importantes son las bases de datos de opcodes (códigos de operación).



Gràfico3. 10 Metasploit Captura de Pantalla Propia Autoría

3.13 Armitage

Armitage es una herramienta gráfica de gestión de Metasploit[3] para ciber ataque que visualiza sus objetivos. Armitage tiene como objetivo hacer Metasploit útil para los profesionales de seguridad que comprenden del arte del hacking, pero no el uso de Metasploit.



Gràfico3. 11 Armitage Captura de Pantalla Propia Autoría

[3] Metasploit : Es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad.

3.14 Yamas[4]

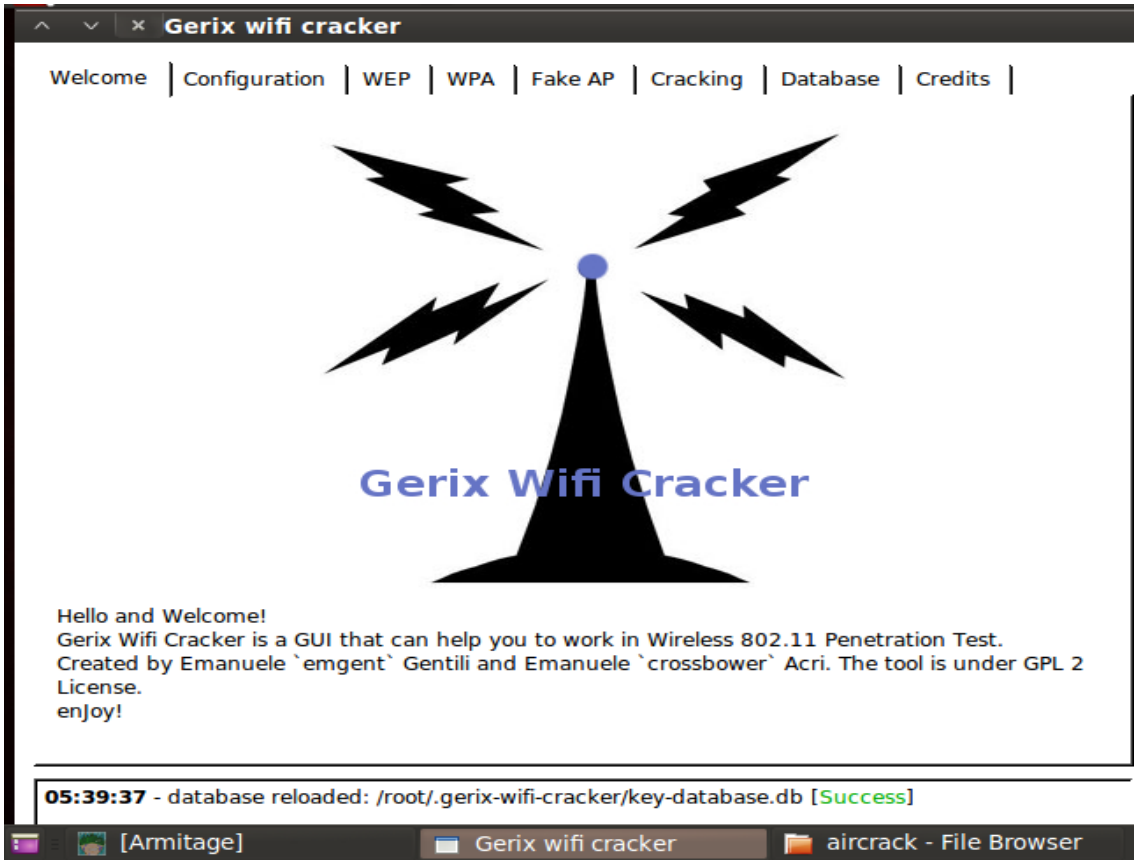
Es una herramienta de BackTrack el cual nos permite cifrar claves a partir de una dirección Ip o de la Ip de una Vlan, este proceso lleva un poco de tiempo ya se debe direccionar a que puerto hay que realizar el ataque o a qué tipo de pagina. Yamas es una de las herramientas preferidas por las personas que realizan Test de Penetración o simplemente desean saber la clave personal de alguno de los programas de redes sociales, por ejemplo Facebook.

Gràfico3. 12 Yamas Captura de Pantalla Propia Autoría

[4] Investigación Propia

3.20 Gerix

Según la página http://belowbit.wordpress.com, una de las herramientas más utilizadas para obtener claves WEP, WPA no sirve para obtener claves cifradas y protegidas con encriptación.



Gràfico3. 13 Gerix Captura de Pantalla

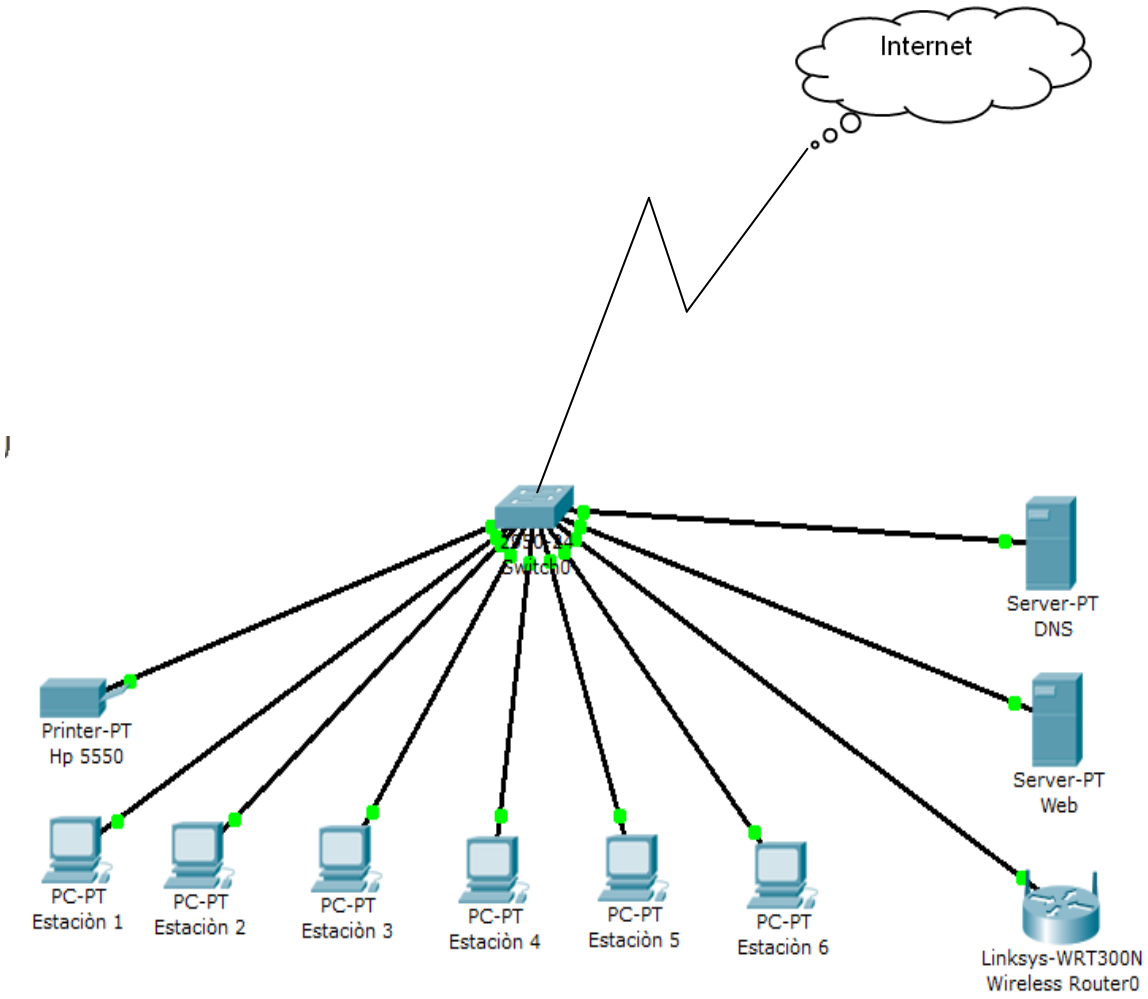
De acuerdo a lo Investigado, el programa que mejor se adecua a las necesidades para el desarrollo del proyecto estudio diseño e implementación de un sistema que permita detectar y corregir vulnerabilidades en la red de datos de la Unidad Ejecutora Magap-Prat Proyecto SigTierras es BackTrack 5 R2 ya que este contiene la gran mayoría de herramientas que se requieren y que fueron analizados para realizar un PentTest.

Además, de acuerdo al Decreto 10-14 [5], emitido por la presidencia de la república donde se pone énfasis a la utilización de software libre en todas las entidades públicas y del estado, y cumpliendo las normativas de la misma y al ser BackTrack es el software que mas cumple con los requerimientos técnicos y aplicables por ley se da por hecho la utilización de este sistema para realizar los diferentes tipos de prácticas, pruebas y análisis que se requieren para llevar a cabo el presente trabajo de Titulación de Grado.

[5] Adjunto en anexos ley 10 14 usos de software libre en entidades públicas.

3.21 Diseño

3.22 Diseño de Red Unidad Ejecutora Magap-Prat[6]



Gràfico3. 14 Diseño de red UE SIGTIERRAS Elaborado por Oscar Chiguano

[6] Diseño Personal

3.23 Equipos que conforman la red de datos de la Unidad Ejecutora Magap Prat[7]

- 12 Equipos portátiles Dell Vostro 1520.
- 26 Estaciones de Trabajo Dell Optiplex 780.
- 1 Servidor Hp Internet.
- 1 Servidor Hp Correo.
- 1 Server hp 790 para servicios Ftp
- 1 Switch Cisco
- 1 Ap Cisco Wireless
- 4 Impresoras Hp 5550 todas funcionando en red
- 2 Scanner Konica Minolta funcionando en red con servicio de escaneo de documentos y recepcion vía correo electrónico.

3.24 Requerimientos Técnicos de equipo para la Instalación de software:

- Equipo con hasta de 4 G de Memoria
- Disco duro de 500 G
- Procesador Cori 5
- Antena Wireless

[7] Investigación Personal

3.25 Requisitos de software

- BackTrack puede ser descargado desde su sitio web oficial http://www.backtrack-linux.org . El software es de código abierto y debe ser capaz de descargar directamente del sitio web.

- Usted necesitará Windows XP, Windows Vista o Windows 7 instalado en uno de los ordenadores portátiles.

Es importante señalar que a pesar de que se está utilizando un sistema operativo basado en Windows para nuestras pruebas, las técnicas aprendidas se pueden aplicar a cualquier dispositivo Wi-Fi como teléfonos inteligentes y tabletas, entre otros.

3.26 Aircrack-ng

Aircrack-ng está basado en el estándar 802,11 WEP y WPA-PSK claves de craqueo programa que puede recuperar claves una vez que los paquetes de datos suficientes han sido capturados, lo que hace el ataque mucho más rápido comparado con otras herramientas de cracking WEP.

Aircrack-ng es un conjunto de herramientas para redes inalámbricas de auditoría.

3.27 Preparación de la tarjeta

airmon-ng**:** interfaz inalámbrico devuelve por pantalla el nombre de la tarjeta red que se tiene configurado (wifi0, wlan0, ath0, ra0).

airmon-ng stop ra0**:** monitor mode disable devuelve que la tarjeta tiene el modo monitor desactivado.

ifconfig ra0 down**:** tarjeta de red desactiva**.**

macchanger –mac 00: da la mac original y la falsa que se asignado para luego poder inyectar paquetes.

3.28 Escaneo de redes y clientes asociados

airodump-ng ra0**:** redes y clientes disponibles se despliega una tabla con las redes disponibles con toda la información canal, nombre, calidad de señal, tipo de encriptación, etc.

Se elige una red que tenga buena señal (que vaya capturando #data y tenga buen PWR) se apunta la BSSID, el numero de canal (CHANNEL).

Se para la ejecución del comando pulsando “Control+C”, o cerrando y abriendo otra terminal.

airodump-ng –c NumeroDeCanal –w ArchivoDeCapturas –bssid BBSID ra0:

Por ejemplo una red en canal 11 con BSSID 00:01:02:03:04:C1 que se ha detectado:

airodump-ng -c 11 -w capturaswifi – - bssid 00:01:02:03:04:C1

Capturando paquete se despliega la captura de paquetes así como la señal de la red y los clientes asociados. ESTA TERMINAL NO HAY QUE CERRARLA!

3.29 Inyección de paquetes para agilizar el proceso de capturas de paquetes

Association successful: Permite realizar una autenticación falsa en el router. Para ello en el comando se necesita la BSSID de la red atacada, la mac falsa que puede ser (00:11:22:33:44:55) y el nombre que tiene la red atacada, es decir, la ESSID. Es importante que aparesca el Association Succesful, de lo contrario no se puede inyectar paquetes.

Por ejemplo:

aireplay-ng 1 0 -a 00:01:02:03:04:05 -h 00:11:22:33:44:55 -e WIFI_RED ra0.

aireplay-ng -3 –b BSID –h 00:11:22:33:44:55 ra0:

El envío de paquetes: sale por pantalla el mensaje que están mandando paquetes, para que la inyección sea correcta deben aparecer paquetes ARP recogidos.

Por ejemplo:

aireplay-ng -3 -b 00:01:02:03:04:05 -h 00:11:22:33:44:55 ra0.

Se inicia el proceso de inyección de paquetes, por tanto ESTA TERMINAL NO HAY QUE CERRARLA!

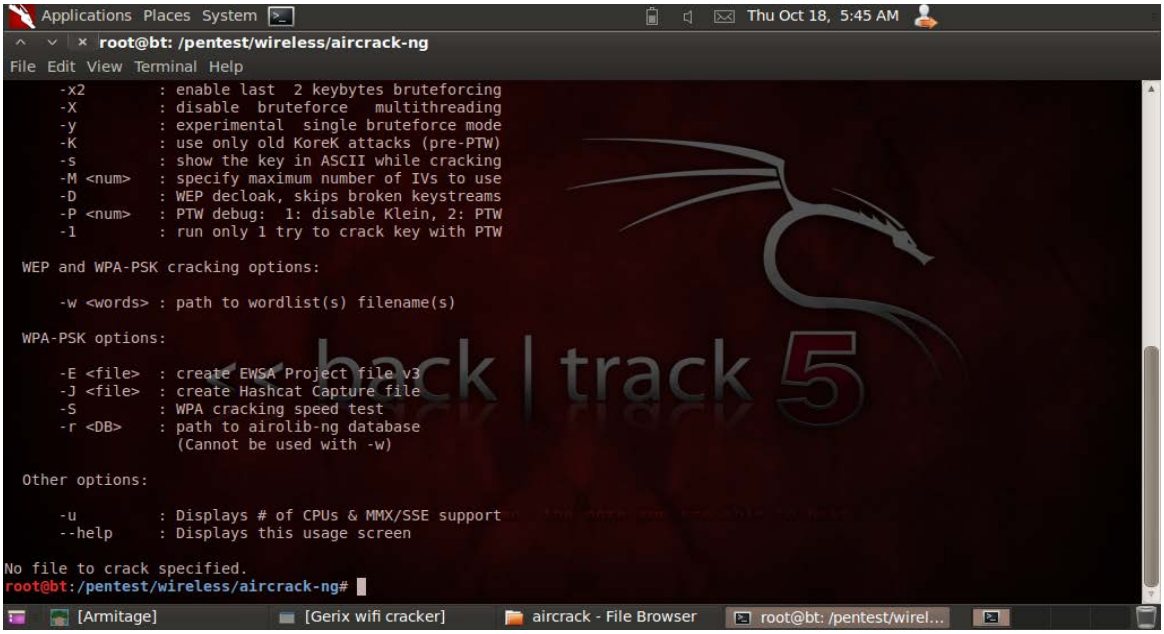
3.30 Crackeo WEP

Para poder obtener la clave WEP es necesario tener un mínimo de paquetes recogidos. El número de paquetes dependerá de la longitud que tenga la clave WEP. Como mínimo se recomienda empezar a intentar conseguir la clave a partir de 30.000.

aircrack-ng –b BSSID ArchivoDeCapturas.cap:

Clave WEP encontrada/no encontrada: El programa empezará a descifrar los paquetes recogidos, y cuando finalice nos dirá si ha encontrado la clave o no.

Si la encuentra nos saldrá: KEY FOUND! y la clave en hexadecimal normalmente.

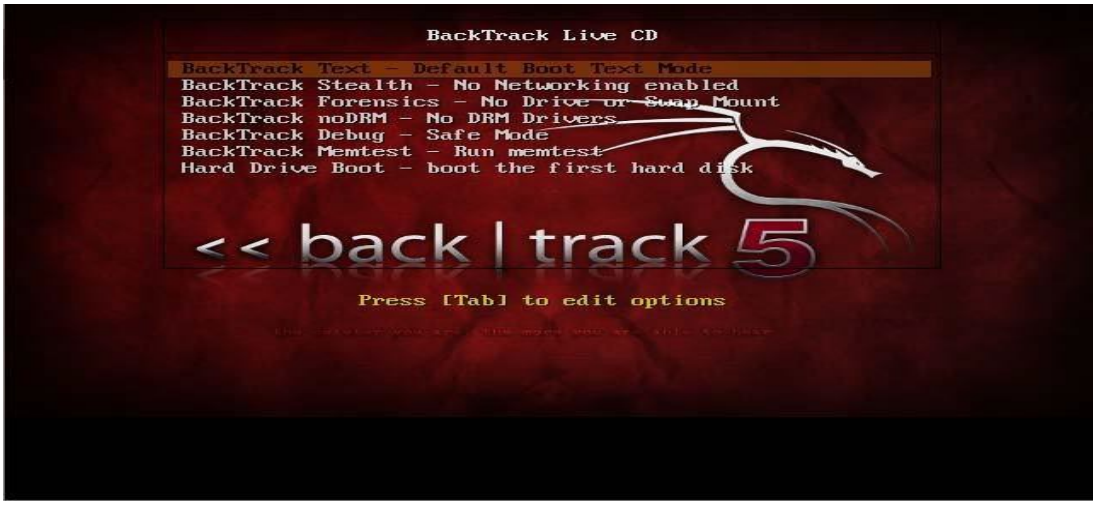


Gràfico3. 15 Aircrack-ng inicio Captura de Pantalla Elaborado por Oscar Chiguano

3.31 Implementación

3.32 Instalación de BackTrack

3.32.1 Grabar la ISO BackTrack (está utilizando BackTrack 5 KDE 32-Bit Edition) que ha se ha descargado en un DVD de arranque. Arrancar el ordenador con el DVD y seleccione la opción BackTrack Text Default Boot Text Mode.



Gràfico3. 16 Instalación BackTrack 5 Captura de Pantalla Elaborado por Oscar Chiguano

3.32.2 Se puede arrancar en el modo gráfico mediante la introducción de startx en el símbolo del sistema.

Gràfico3. 17 Instalación BackTrack Elaborado por Oscar Chiguano

3.32.3 Pantalla de Inicio BackTrack modo Grafico.

Gràfico3. 18 Modo Grafico BackTrack Elaborado por Oscar Chiguano

3.32.4 Hacer doble clic en el icono de instalación de BackTrack a la parte superior izquierda del escritorio. Se iniciará el instalador de BackTrack.

Gràfico3. 19 Instalación Sistema Operativo BackTrack Captura de Pantalla, elaborado por Oscar Chiguano

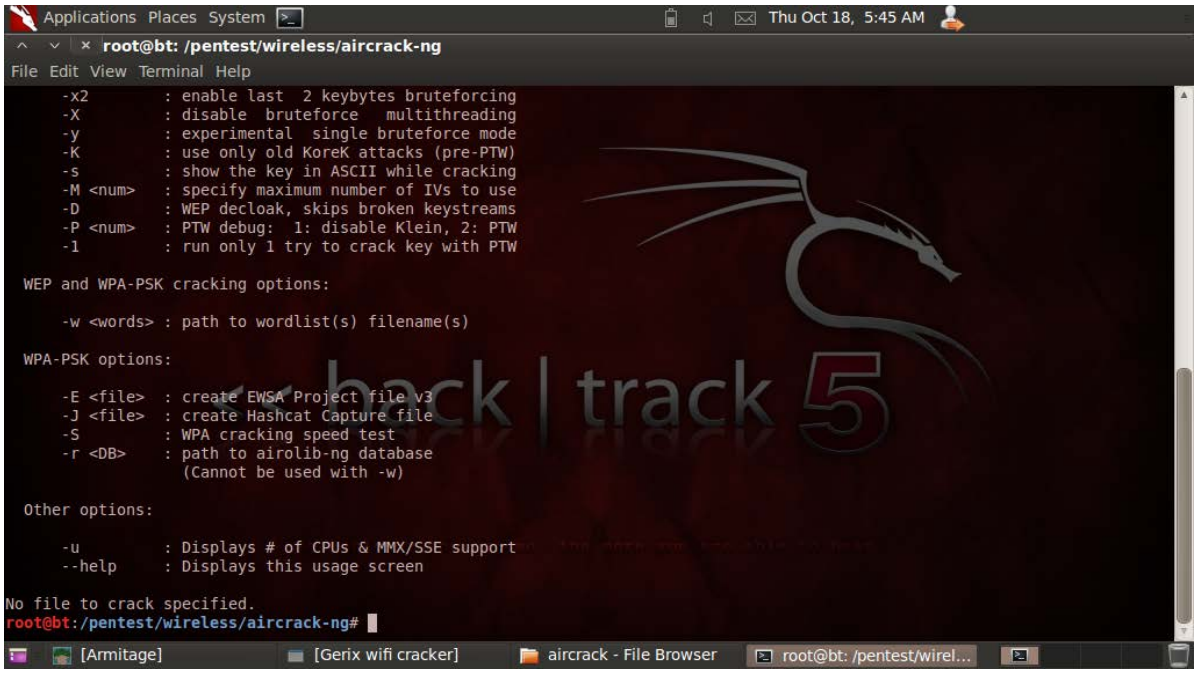
3.32.5 Este programa de instalación es similar a los instaladores basados en GUI de la mayoría de los sistemas Linux. Seleccione las opciones adecuadas en cada pantalla y comenzará el proceso de instalación. Cuando la instalación haya terminado, reinicie el equipo cuando se le solicite y extraiga el DVD.

Gràfico3. 20 Pantalla Sistema Operativo BackTrack Captura de Pantalla, elaborado por Oscar Chiguano

3.32.6 Una vez que se reinicia el equipo, se le presentará una pantalla de inicio de sesión. Escriba en el inicio de sesión "root" y la contraseña "toor". Ahora debe estar logueado en la versión instalada de BackTrack. La clave de inicio es “startx”.

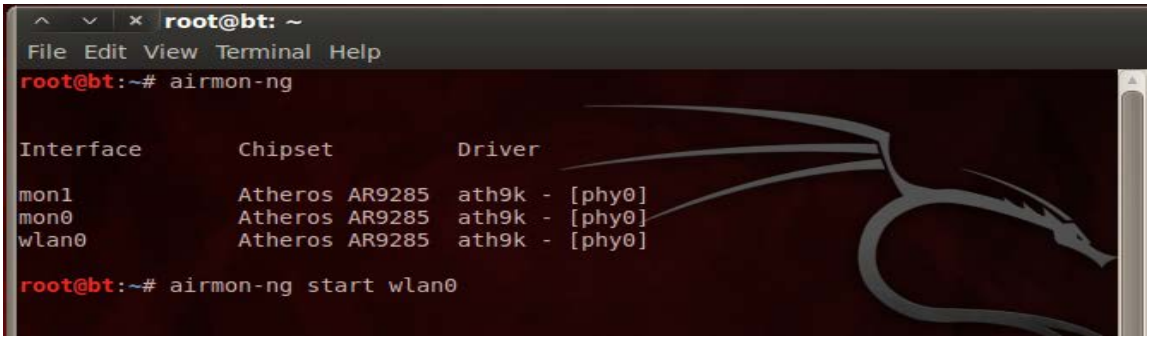
3.33 Aircrack-ng

3.33.1 Ejecutar un nuevo terminal



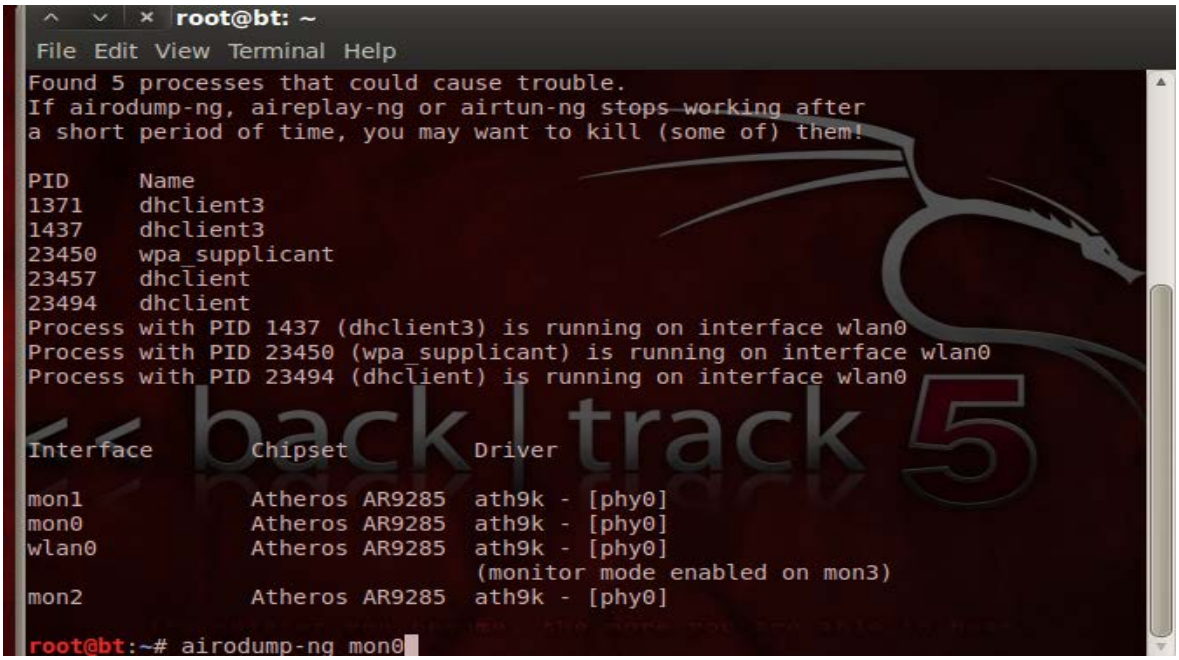
Gràfico3. 21 Ventana de inicio de aircrack-n Captura de Pantalla, elaborado por Oscar Chiguano

3.33.2 Se digita airmon-ng, y aparecen las tarjetas de red.



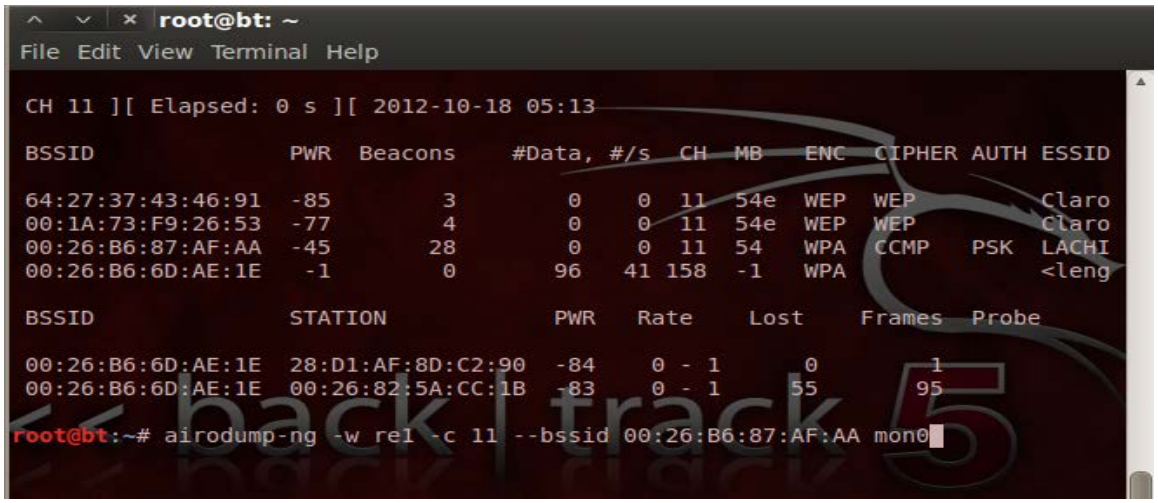
Gràfico3. 22 Airmon-ng interfaz inalámbrico Captura de Pantalla, elaborado por Oscar Chiguano

3.33.3 A continuación se coloca la tarjeta en modo monitor.



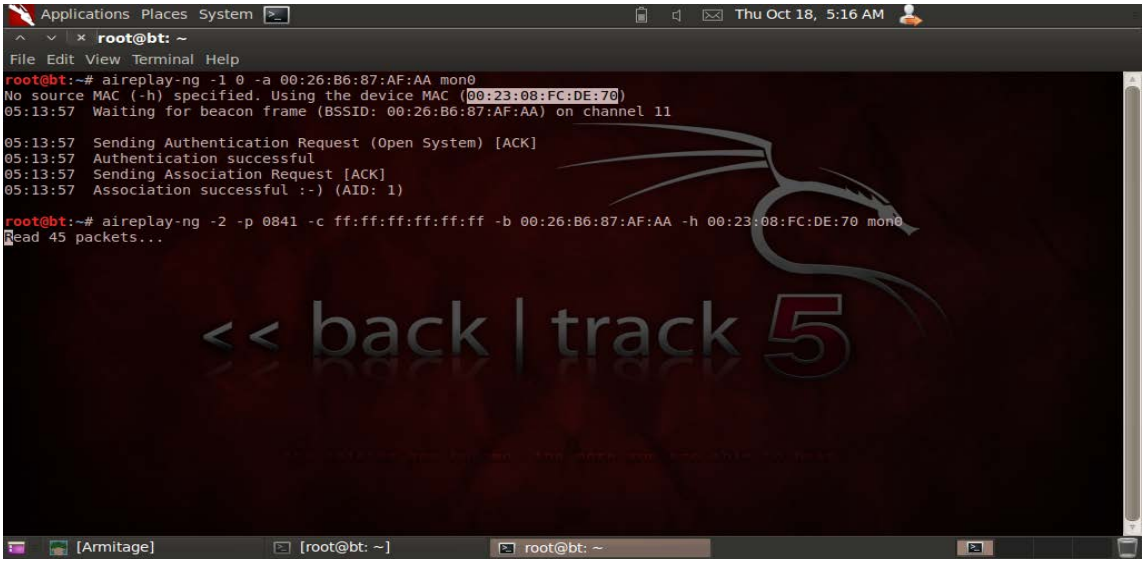
Gràfico3. 23 Airmon-ng Modo monitor Captura de Pantalla, elaborado por Oscar Chiguano

3.33.4 A continuación se coloca la Mac Address.



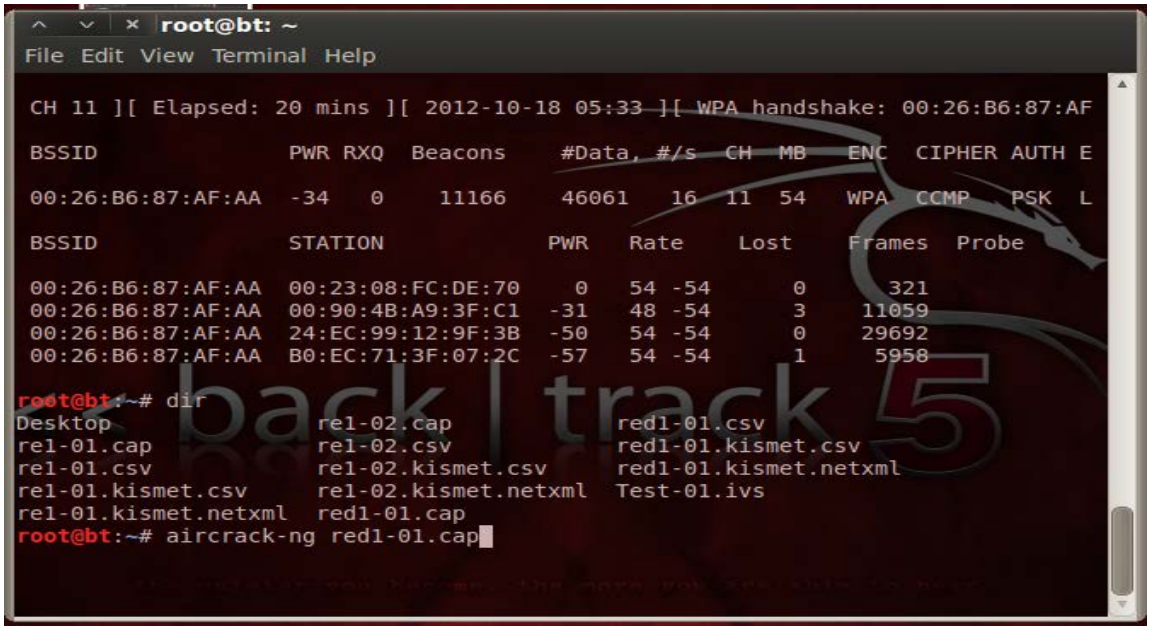
Gràfico3. 24 Airmon-ng colocando Mac Address Captura de Pantalla, elaborado por Oscar Chiguano

3.33.5 Empieza la captura de paquetes con aireplay-ng.



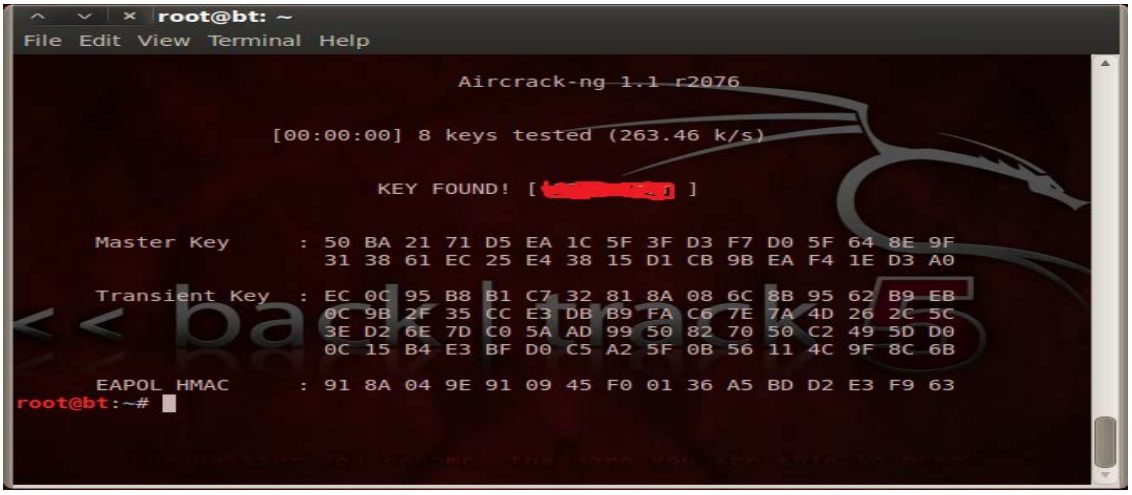
Gràfico3. 25 Airmon-ng captura de paquetes con aireplay Pantallazo, elaborado por Oscar Chiguano

3.33.6 Inyección de paquetes para el cifrado de la clave.



Gràfico3. 26 Airmon-ng inyección de paquete Captura de Pantalla , elaborado por Oscar Chiguano

3.33.7 Captura de clave wireless

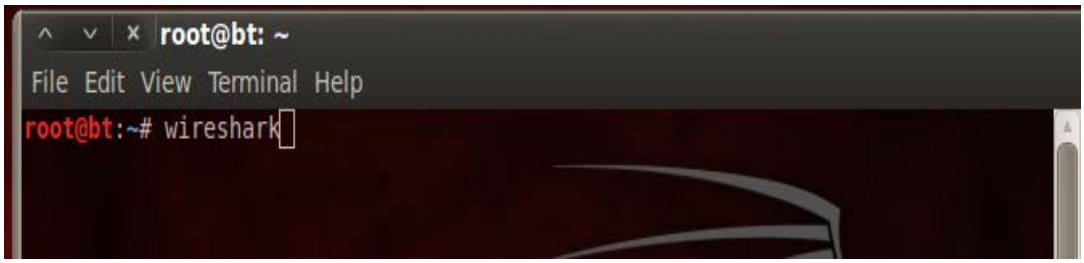


Gràfico3. 27 Airmon-ng inyección de paquetes Captura de Pantalla , elaborado por Oscar Chiguano

3.34 Whireshark

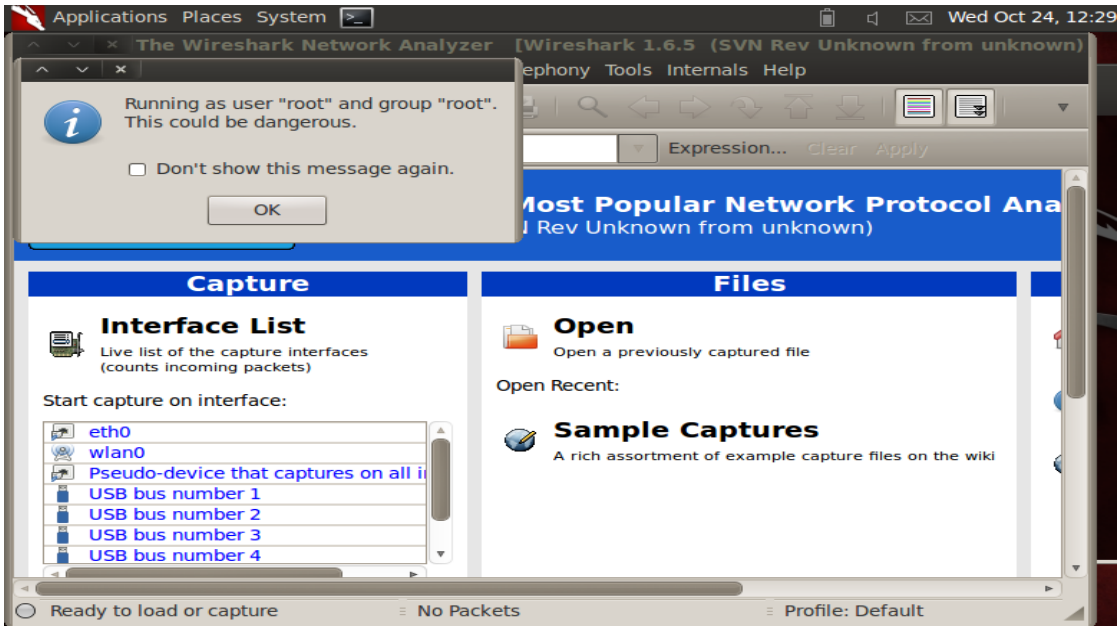
Antes conocido como Ethereal, es el mejor analizador de redes (sniffer) de la actualidad. Es capaz de diseccionar gran cantidad de protocolos, SMTP, HTTP, POP3, 802.11, 802.3 (Ethernet), entre otros. Su arquitectura modular facilita la creación e integración de nuevos decodificadores (dissectors) de protocolo, y por esto existe una gran comunidad que suele agregar un decoder para casi cualquier tipo de protocolo existente. Además de sus capacidades de decodificación, también son destacables sus diversas funcionalidades para la obtención de datos desde las capturas, gráficos y tendencias. Una de sus características más importantes son los filtros que permiten filtrar la información obtenida desde la red y de esta manera llegar a comprender los datos más relevantes.

3.34.1 Inicio de Wireshark



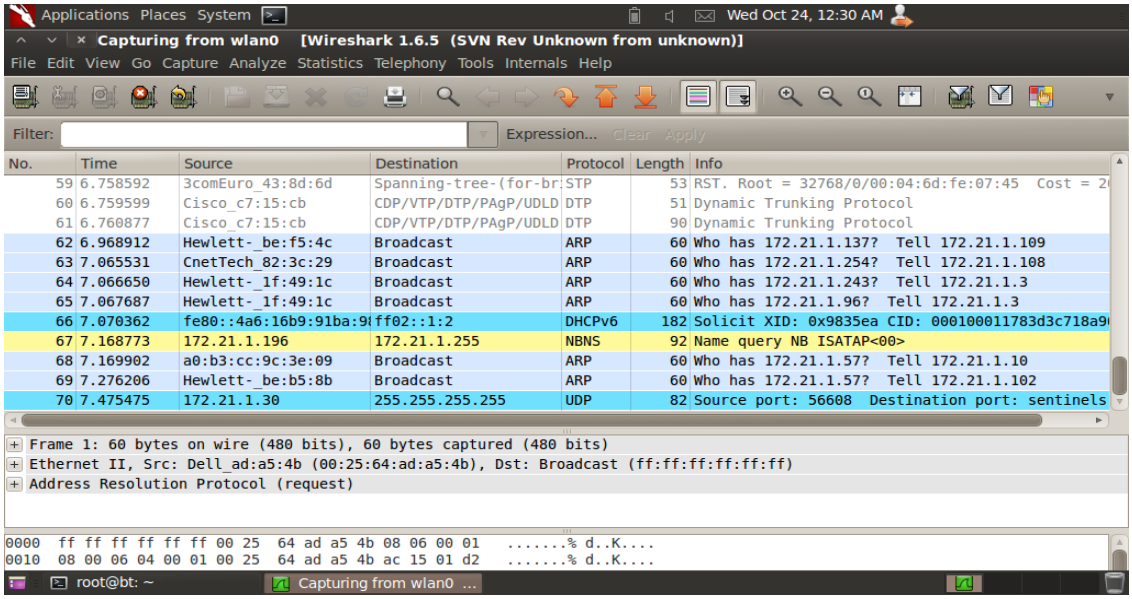
Gràfico3. 28 Llamada a wireshark , elaborado por Oscar Chiguano

3.34.2 Ejecución de Wireshark en Backtrack



Gràfico3. 29 Interfaz de Inicio, elaborado por Oscar Chiguano

3.34.3 Captura de paquetes



Gràfico3. 30 Captura de Paquetes y Tráfico de red Captura de Pantalla, elaborado por Oscar Chiguano

3.35 Zenmap

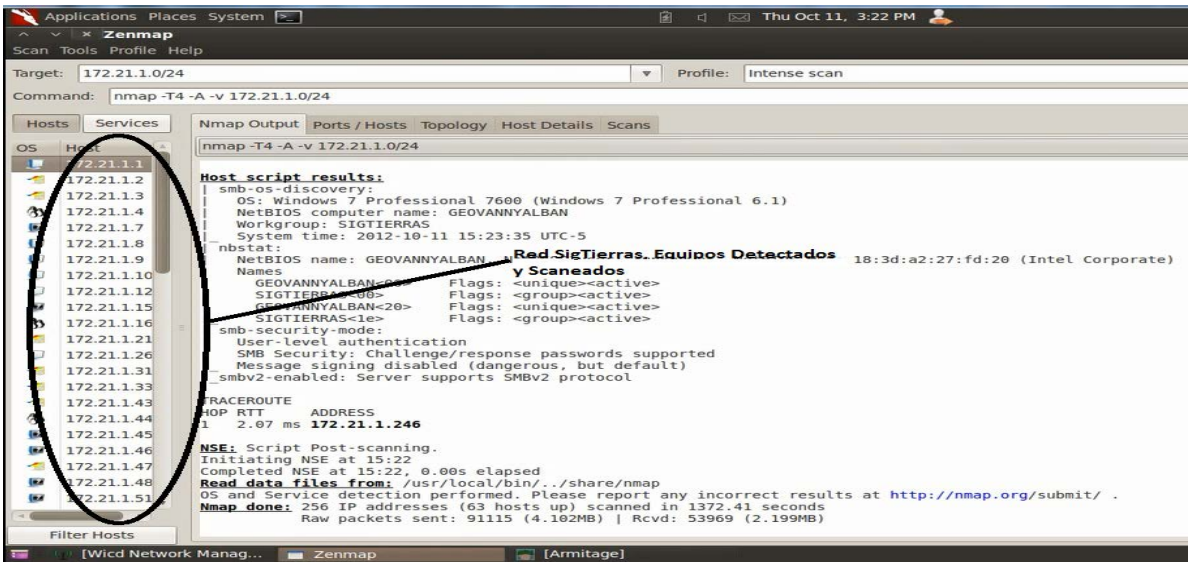
Escaneo de puertos, se ingresa la dirección de red la cual se requiere hacer el escaneo luego se procede a realizar el escaneo total.

3.35.1 Ejecutar un nuevo Terminal y se llama a zenmap.

Gràfico3. 31 Ingreso a Znmap Captura de Pantalla , elaborado por Oscar Chiguano

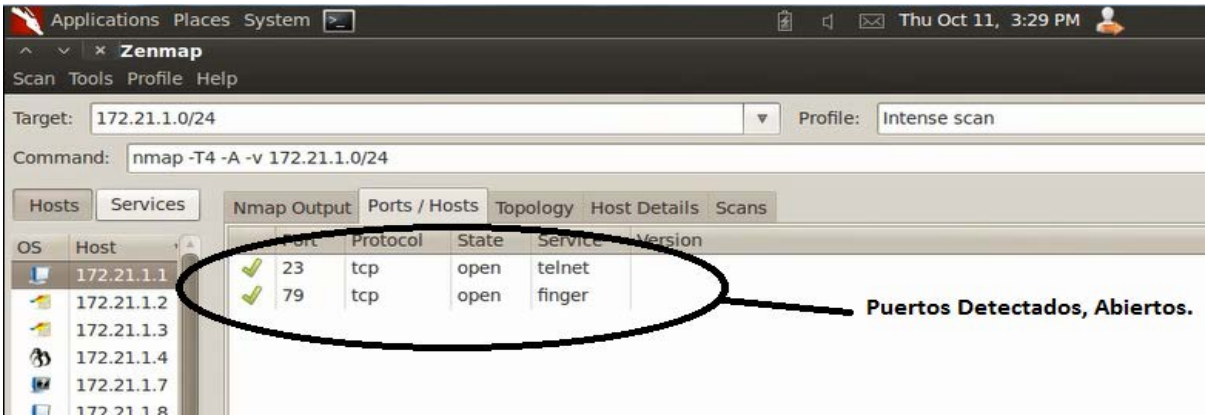
Gràfico3. 32 Escaneo de puertos con Zenmap Captura de Pantalla , elaborado por Oscar Chiguano

3.35.2 Se procede a realizar Intense Scan



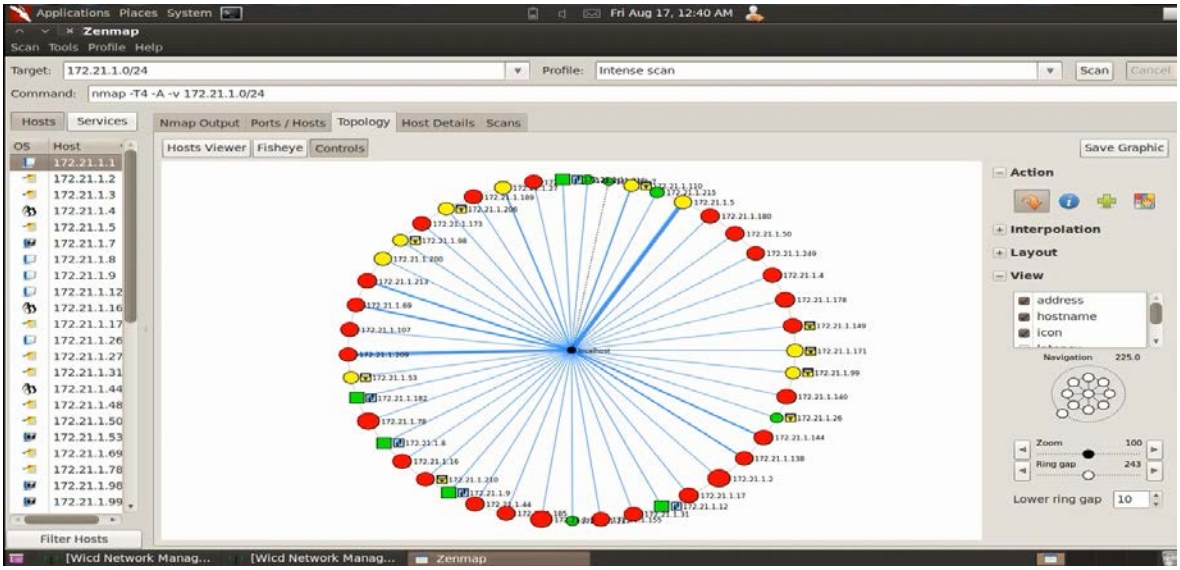
Gràfico3. 33 Primer Resultado Escaneo de puertos con Zenmap. , elaborado por Oscar Chiguano

3.35.3 En este caso en particular la red de datos del SigTierras presenta varios tipos de puertos abiertos.



Gràfico3. 34 Escaneo de puertos con Zenmap, puertos abiertos en la red. , elaborado por Oscar Chiguano

3.35.4 Visualización de la Topología completa de red con sus direcciones Ip`s latencia, hostname, latencia.



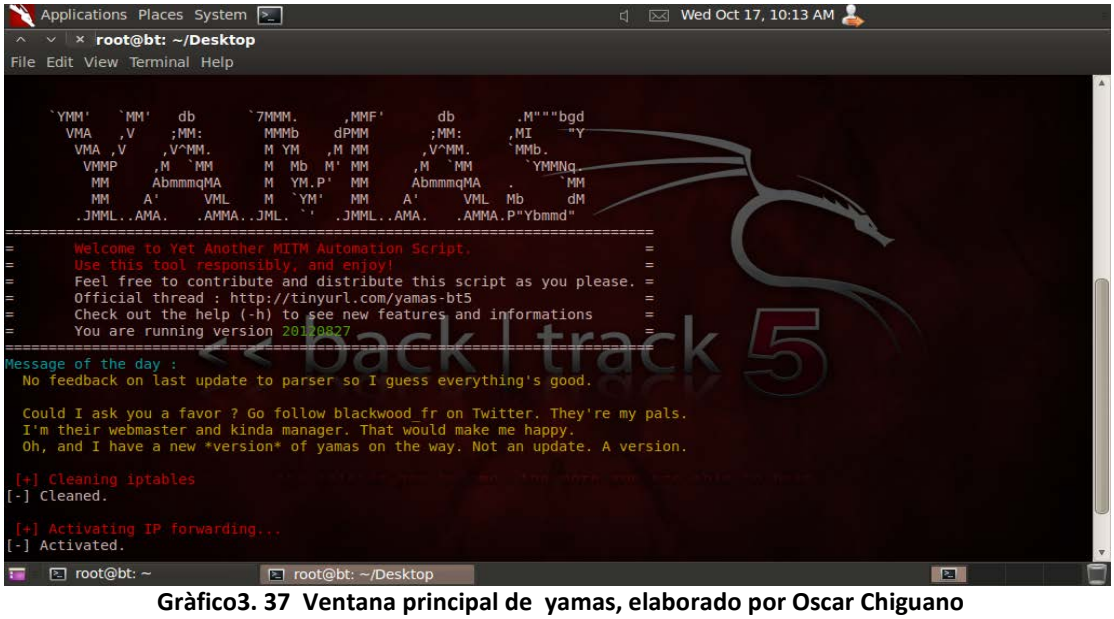
Gràfico3. 35 Topología de Red con Zenmap, elaborado por Oscar Chiguano

3.36 Yamas

3.36.1 Actualización paquete yamas.sh indispensable para el correcto desempeño del software.

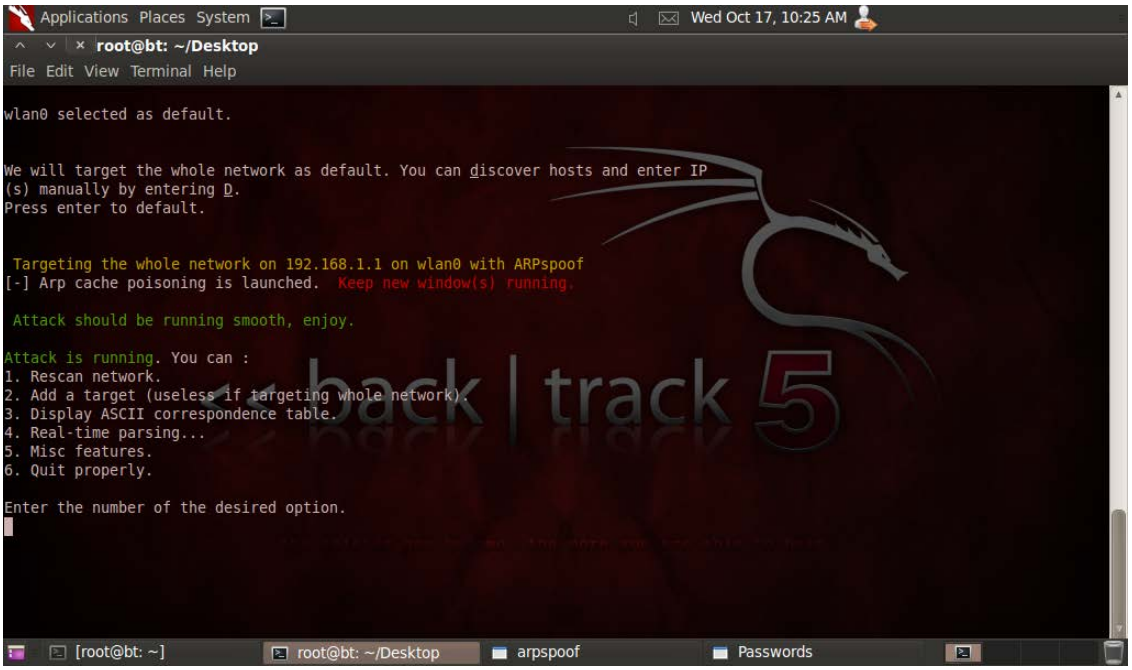
Gràfico3. 36 Actualización paquete yamas.sh, elaborado por Oscar Chiguano

3.36.2 Abrir un nuevo terminal y se llama a nuestro software digitando yamas.



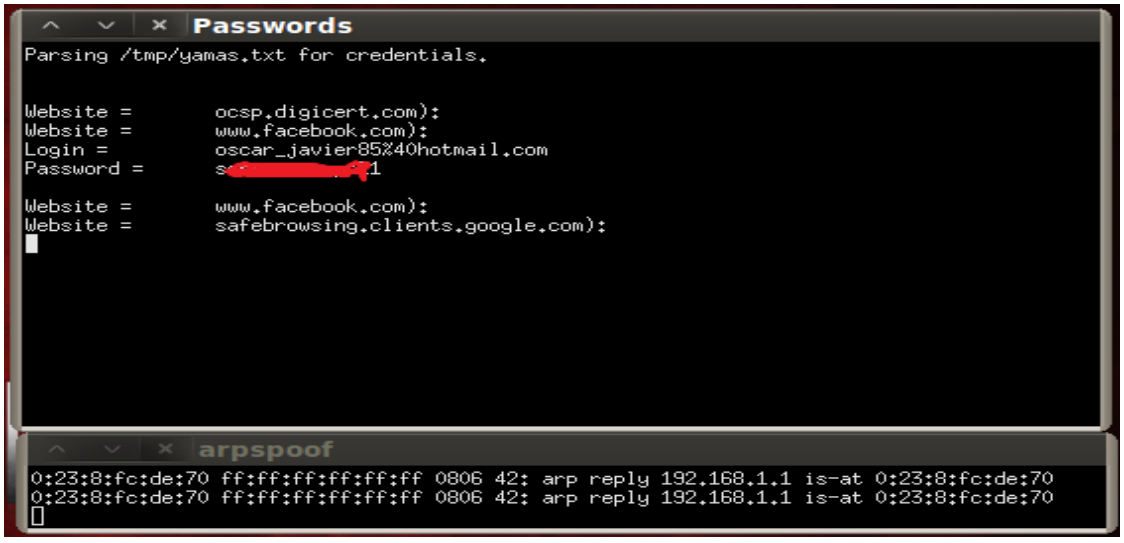
Gràfico3. 37 Ventana principal de yamas, elaborado por Oscar Chiguano

3.36.3 Opciones para escoger el puerto, maquina, red que se quiere atacar, en este caso se atacara a una cuenta de Facebook.



Gràfico3. 38 yamas opciones de ataque, elaborado por Oscar Chiguano

3.36.4 Captura de clave ejem: Facebook.



Gràfico3. 39 yamas captura de clave Facebook, elaborado por Oscar Chiguano

CAPÌTULO IV

4. Introducción

En el siguiente capítulo se realizó el análisis económico el cual arroja la idea de cuánto seria la inversión para la implementación del Sistema BackTrack el cual nos permitirá realizar el Test de Penetración el cual permitirá valorar el estado de la red de la Unidad Ejecutora Magap-Prat.

4.1 Análisis económico

4.1.1 Costos Directos

DESCRIPCION	UNID	CANTIDAD	SUBTOTAL	TOTAL
DELL OPTIPLEX 790: LicenseSpanish/ Garantía 3 años	1	1	995,00	995,00
MONITOR DELL FLAT PANEL 17" WIDE	1	1	227,81	227,81
Tarjeta Wireless N Wifi Adaptador Usb D-link Dwa-125 150mbps	1	1	19,00	19,00
Router E3000 Cisco Tecnologia N	1	1	280,00	280,00
Rollo de cable Utp cat 5	1	1	118,00	118,00
Conectores Rj 45	100	100	10,00	10,00
SUBTOTAL				1531,00
IVA				183,72
TOTAL				1714,72

Tabla 3 Análisis Económico Costos Directos Elaborado por Oscar Chiguano

4.1.2 Costos Directos

DESCRIPCION	Modalidad	Horas	SUBTOTAL	TOTAL
CCNA Módulo 1	Presencial	240	290,00	290,00
CCNA Módulo 2	Presencial	240	290,00	290,00
CCNA Módulo 3	Presencial	240	290,00	290,00
CCNA Módulo 4	Presencial	240	290,00	290,00
CCNA Security	Presencial	150	150,00	150,00
Curso Seguridad en Redes Eduacanet	Presencial	40	450,00	450,00
SUBTOTAL				1571,43
IVA				188,57
TOTAL				1760,00

Tabla 4 Análisis Económico Costos Indirectos Elaborado por Oscar Chiguano

4.2 Análisis Foda

Tabla 4Análisis Foda

Factores Internos / Factores Externos	**Lista de Fortalezas**	**Lista de Debilidades**
	F1. Software Libre F2. No pago Licencias F3.Codigo abierto F4. Completo compendio de Aplicaciones para Test Penetración.	A1. Actualización Cotidiana A2. Nuevas herramientas para Test de Penetración. A2. Personas entendidas en el manejo y uso del sistema, pueden utilizarlo para realizar hackeo.
Lista de Oportunidades O1. El presente Proyecto se puede aplicar a cualquier tipo de empresa. O2. Por sus costos bajos el presente proyecto es aplicable en redes de pequeñas y grandes dimensiones.		
Lista de Amenazas A1. Creación de nuevas herramientas para análisis y Test de Penetración. A2. Que los costos de licencias y software disminuyan.		

Tabla 5 Análisis Foda Elaborado por Oscar Chiguano

CAPÌTULO V

5. Introducción

Una vez realizado el estudio diseño e implementación del sistema BackTrack que permite realizar detectar y corregir vulnerabilidades en la red de datos de la Unidad Ejecutora Magap-Prat Proyecto SIGTIERRAS, se procedió a realizar las siguientes conclusiones y recomendaciones.

5.1 Conclusiones

- Se elaboró el PentTest el cual ayudará a detectar, analizar y corregir las vulnerabilidades que se presenten en la red de la Unidad Ejecutora Magap-Prat.

- Se implementó el sistema BackTrack, y se realizó diferentes pruebas de validación con diferentes tipos de software, los cuales ayudaron a sacar como conclusión que la red de datos de la Unidad Ejecutora **MagapPrat es Vulnerable** por lo tanto la presenta red está expuesta a ser blanco fácil de diferentes tipos de Ataque.

- Los equipos y la información que se almacena en los equipos informáticos que conforman la Unidad Ejecutora Magap-Prat corren gran riesgo, ya que si una persona con conocimientos y que desee cuásar algún tipo de perjuicio en esta red, lo podrá hacer sin ningún tipo de impedimento.

- El campo de la seguridad Informática es muy variante, por lo tanto los Administradores de red, Hacker Ético debe mantenerse al día, lo cual requiere autoeducación y estudios continuos. además de un entrenamiento apropiado para manejar y administrar las herramientas que van apareciendo.

- La elaboración de pruebas anunciadas es un modo eficiente de verificar los controles de seguridad de los que dispone la empresa. Esto crea un ambiente de trabajo seguro y orientado a la seguridad y permite a los usuarios de la red experimentar directamente en la red de datos la presencia de un intruso.

- Las pruebas sin previo anuncio son las que más se deben tomar en cuenta, ya que permite al administrador de red verificar el verdadero estado de la red además de saber el tráfico de red que ahí se encuentra.

- Las políticas de seguridad son importantes ya que se instruye a los usuarios a limitar accesos a sitios indebidos, además de permitir a los usuarios a ser más precavidos y responsables.

- Las políticas para una autenticación segura deben ir de la mano con una administración segura, se debe capacitar a los usuarios la manera segura de cómo administrar claves de acceso para los diferentes sistemas o cuentas que se manejen.

- Actualmente una de las vulnerabilidades más usadas en las redes de datos es las contraseñas, es por eso se debe implementar una política el cual obligue a los usuarios a utilizar caracteres especiales en sus contraseñas o usar las bien llamadas (Claves Tontas).

5.2 Recomendaciones

- Se recomienda la utilización de encriptación AAA en para incrementar seguridad en el Switch.

- Habilitar SSH para mejorar seguridad.

- Crear grupos de trabajo los cuales tendrán diferentes tipos de privilegios, así como el bloqueo de servicios dependiendo la actividad que ellos realicen.

- La implementación de Puertos Seguros, y la habilitación de registro de MacAddress para evitar que cualquier intruso pueda ingresar y conectarse con nuestra red de datos.

- Es necesario concienciar a los administradores de red, acerca del uso o el mal uso que se pueda dar a las herramientas utilizadas para realizar el Test de Penetración o Hacking Ético en el presente proyecto de titulación de grado. Y no realizar actividades que están penadas por la ley.

- Las herramientas de seguridad son actualizadas diariamente por lo que los administradores de red están en la obligación de mantenerse al tanto de las últimas actualizaciones que se publican para así poder realizar trabajos óptimos.

- Es necesario recordar a los usuarios de la red de datos que no se debe apuntar claves, contraseñas en papeles que estén al alcance de cualquier persona mal intencionada la cual puede provocar que se violenten los sistemas de seguridad.

- Se debe definir grupos de trabajos y marcar límites y privilegios para cada uno de estos grupos, ya que así se puede limitar a los usuarios a ingresar a sitios indebidos.

GLOSARIO

PenTest: El Test de Penetración, también llamado a veces “hacking ético” es una evaluación activa de las medidas de seguridad de la información.

Host: es usado en informática para referirse a los computadores conectados a la red.

Experto en Seguridad: persona dedicada a investigar sobre los amenazas que existen en la red, posee habilidades de un hacker, y de un cracker.

Vulnerabilidad: En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Cracker: Contrario de hacker, seguridades. Crea programas o cracks. Pirata informático.

Ap: Access Point. Función Bridge ó puente de acceso a internet inalámbrico.

Interfaz: punto en el que se establece una conexión entre dos elementos, que les permite trabajar juntos. La interfaz es el medio que permite la interacción entre esos elementos.

PacketTracer: es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA.

MacAddress: (Media Access Control address o dirección de control de acceso al medio) es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red.

Hacker, Hack: se refiere a la acción de resolver un problema de manera creativa e incluso divertida.

Lammer: se pondría decir que es un aprendiz o persona que presume tener conocimientos de algo que no domina.

BIBLIOGRAFIA

- Libro Acurio Normas y Standares
- Referencias norma 10-04
- CCNA Exploration4.0 protocolos y enrutamientos.
- CCNA Exploration4.0 Aspectos de redes.
- CCNA Exploration4.0 Redes wireless.
- CCNA Security.
- Educa net: 03 - Seguridad en Firewalls.
- Educated: 04 - IDS & IPS Best Practices.
- Educa net: 06 - Arquitectura de red segura.
- Fiscalía general del estado: Ley de delitos Informáticos.
- Libro Seguridad en Redes.
- Cobit Reglas

Web Bibliográfica

- http://www.cert.org/
- http://www.backtrack-linux.org/downloads/
- http://www.fiscalia.gob.ec/
- http://www.wireshark.org/
- http://nmap.org/man/es/
- http://www.aircrack-ng.org/
- http://www.contraloriageneraldelestado.gob.ec
- http://www.elcomercio.com
- http://www.iab.org.br/index.php?option=com_content&view=category&id=57&layout=blog&Itemid=19.
- whois.net/,
- http://network-tools.com/nslook/
- http://www.traceroute.org/
- http://www.visualroute.com/
- http://ping.eu/
- http://superscan.archivospc.com/
- http://www.tenable.com/products/nessus
- http://www.metasploit.com/
- http://belowbit.wordpress.com

Anexos

Nº 1014

RAFAEL CORREA DELGADO

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

CONSIDERANDO:

Que en el apartado g) del numeral 6 de la Carta Iberoamericana de Gobierno Electrónico, aprobada por el IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, realizada en Chile el 1 de Junio de 2007, se recomienda el uso de estándares abiertos y software libre, como herramientas informáticas;

Que es el interés del Gobierno alcanzar soberanía y autonomía tecnológica, así como un significativo ahorro de recursos públicos y que el Software Libre es en muchas instancias un instrumento para alcanzar estos objetivos;

Que el 18 de Julio del 2007 se creó e incorporó a la estructura orgánica de la Presidencia de la República la Subsecretaría de Informática, dependiente de la Secretaría General de la Administración, mediante Acuerdo N°119 publicado en el Registro Oficial No. 139 de 1 de Agosto del 2007;

Que el numeral 1 del artículo 6 del Acuerdo Nº 119, faculta a la Subsecretaría de Informática a elaborar y ejecutar planes, programas, proyectos, estrategias, políticas, proyectos de leyes y reglamentos para el uso de Software Libre en las dependencias del gobierno central; y,

En ejercicio de la atribución que le confiere el numeral 9 del artículo 171 de la Constitución Política de la República;

DECRETA:

Artículo 1.- Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos.

Artículo 2.- Se entiende por Software Libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a) Utilización del programa con cualquier propósito de uso común
b) Distribución de copias sin restricción alguna.
c) Estudio y modificación del programa (Requisito: código fuente disponible)
d) Publicación del programa mejorado (Requisito: código fuente disponible).

Artículo 3.- Las entidades de la Administración Pública Central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software.

Artículo 4.- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de Software Libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Para efectos de este decreto se comprende como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa del patrimonio nacional.

Nº 1014

RAFAEL CORREA DELGADO

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

a) Sistema en producción funcionando satisfactoriamente y que un análisis de costo beneficio muestre que no es razonable ni conveniente una migración a Software Libre.

b) Proyecto en estado de desarrollo y que un análisis de costo - beneficio muestre que no es conveniente modificar el proyecto y utilizar Software Libre.

Periódicamente se evaluarán los sistemas informáticos que utilizan software propietario con la finalidad de migrarlos a Software Libre.

Artículo 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica.
b) Regionales con componente nacional.
c) Regionales con proveedores nacionales.
d) Internacionales con componente nacional.
e) Internacionales con proveedores nacionales.
f) Internacionales.

Artículo 6.- La Subsecretaría de Informática como órgano regulador y ejecutor de las políticas y proyectos informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de este Decreto.

Para todas las evaluaciones constantes en este decreto la Subsecretaría de Informática establecerá los parámetros y metodología obligatorias.

Artículo 7.- Encárguese de la ejecución de este decreto los señores Ministros Coordinadores y el señor Secretario General de la Administración Pública y Comunicación.

Dado en el Palacio Nacional en la ciudad de San Francisco de Quito, Distrito Metropolitano, el día de hoy 10 de abril de 2008

Rafael Correa Delgado
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA