ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD EN INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

Maestría en Seguridad Informática Aplicada

"HACKING ÉTICO PARA DETECCIÓN DE VULNERABILIDADES DE UNA EMPRESA DEL SECTOR DE TELECOMUNICACIONES"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

DIANA MARÍA LÓPEZ ALVAREZ

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios por la fortaleza que me da cada día, a mi familia que siempre me han apoyado y a la Escuela Superior Politécnica del Litoral por darme la oportunidad de crecer profesionalmente.

DEDICATORIA

El presente trabajo lo dedico a mi querida madre, mi ángel de la guarda que con sus oraciones desde el cielo sigue guiando cada paso de mi vida y me da la fuerza para seguir de pie.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR MSIA

Mgs. Karina Astudillo

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

Ing. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El tema del presente trabajo es el hacking ético para detección de vulnerabilidades de una empresa del sector de Telecomunicaciones.

Es importante proteger la información ya que representa una parte fundamental dentro de las instituciones y al ser vulnerable corre el riesgo de ser alterada o robada en su totalidad ocasionando así un enorme impacto negativo para la institución.

El objetivo principal de este proyecto es detectar las vulnerabilidades existentes en los servicios y equipos informáticos auditados de una empresa del sector de Telecomunicaciones mediante el uso y aplicación del hacking ético con la finalidad de evitar los riesgos asociados a las brechas de información.

En el primer capítulo denominado “GENERALIDADES”, se puede visualizar el problema de forma detallada y la solución que el presente trabajo investigativo ha concluido.

En el segundo capítulo denominado “METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN”, se presenta cada una de las fases que se llevan a cabo para la elaboración del hacking ético.

En el tercer capítulo denominado “ANALISIS DE RESULTADOS”, comprende el análisis e interpretación de resultados de este trabajo investigativo.

Con ésta solución se pretende crear conciencia en los usuarios sobre las posibles vulnerabilidades existentes a las que se encuentra expuesta la información de una organización y finalmente proporcionar un informe de la auditoría realizada que expone dichas vulnerabilidades y las recomendaciones de las medidas de seguridad a tomar.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La presente tesina se refiere al tema de Hacking Ético, el cual, se puede definir como una práctica de penetración en los sistemas o equipos informáticos con la finalidad de detectar las posibles vulnerabilidades que existan en éstos.

La importancia del hacking ético es que se considera como una medida preventiva ante las vulnerabilidades que pueda tener un sistema o equipo informático para tomar precauciones y así asegurar y eliminar las brechas y falencias de fuga de información que éstos puedan tener.

Actualmente las empresas utilizan el internet como el principal medio de comunicación para realizar transacciones, movimientos, proveer servicios etc. pero lamentablemente no se ha tomado conciencia en la importancia de la seguridad de la información y debido al continuo avance tecnológico las vulnerabilidades y los ataques son cada vez más frecuentes.

En el presente trabajo se expone las fases del hacking ético que se inicia con el reconocimiento, el escaneo, obtener acceso y finalmente todos estos hallazgos se

reportan en un informe. En el avance del trabajo se presentará de forma más detallada dichas fases, las herramientas utilizadas y los resultados obtenidos.

El objetivo de este trabajo no es explotar, alterar o dañar los equipos auditados sino lograr exponer las brechas de información existentes y brindar posibles soluciones para tratar en la medida posible de asegurar los servicios y con ello ofrecer al cliente un servicio seguro y de calidad.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

De forma general las empresas poseen equipos y sistemas informáticos debido al creciente desarrollo de las tecnologías de información, lo que a su vez hace que éstas quieran ser partícipes de los mejores y últimos avances tecnológicos; de la misma forma el crecimiento de los ataques por parte de crackers se ha disparado en los últimos tiempos en el mundo informático, haciendo así más sensible la seguridad y violación a dichos sistemas.

La fuga de información es una salida no controlada de la data que hace que ésta llegue a personas no autorizadas. Ocurre cuando un sistema de información, equipo o proceso diseñado para restringir el acceso sólo a sujetos autorizados

revela parte del contenido que procesa o transmite debido a errores en los procedimientos de diseño o trabajo.

La carencia de implementación de medidas de seguridad de estos equipos y sistemas ha hecho que el crecimiento de ataques informáticos esté en constante desarrollo con estructuras y habilidades más organizadas que permiten obtener mayores beneficios a sus atacantes.

El hecho de no utilizar una técnica de hacking ético para detectar vulnerabilidades representa un gran riesgo para la información pues ésta puede ser accedida, interceptada, alterada y hasta robada ocasionando así un enorme impacto negativo para la institución.

El tema propuesto hace énfasis en el análisis y evaluación de las vulnerabilidades que poseen algunas Instituciones en sus equipos informáticos y la importancia significativa que esto tiene.

1.2 SOLUCIÓN DEL PROBLEMA

En vista de que todas las empresas deberían contar con fuertes medidas de seguridad para el acceso a todo activo y/o data confidencial a fin de que todos los servicios que ofrece a sus clientes sean seguros y confiables, es importante

recalcar que deben implementarse medidas de seguridad para contrarrestar los riesgos o vulnerabilidades por el uso indebido de la información.

Con ese objetivo se busca brindar las seguridades necesarias para precautelar la información, el hacking ético es una profesión que busca descubrir deficiencias en relación a la seguridad y vulnerabilidades de los sistemas informáticos, a fin de detectar y prevenir posibles ataques de personas no autorizadas.

Ésta solución permite obtener un informe final donde se plasma todos los puntos desarrollados durante el hacking ético, empezando desde el reconocimiento hasta la explotación de las vulnerabilidades encontradas, con esto se busca mostrar de forma organizada los problemas y recomendaciones para evitar un posible ataque informático.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 PLANTEAMIENTO

El continuo desarrollo de las Tecnologías de la Información hace que las empresas privadas y públicas se motiven a ser parte de este crecimiento, pero en los últimos años los ataques de los crackers ha mostrado un creciente y considerable número dirigido a usuarios, dispositivos y sistemas.

La falta de protección ante estos ataques es un problema que ha ido creciendo, considerando que éstos se han ido estructurando de una forma cada vez más organizada.

La empresa de Telecomunicaciones analizada en este trabajo investigativo posee varios servicios los cuales no han sido sometidos a un análisis de hacking ético interno para detectar vulnerabilidades lo que representa un considerable nivel de riesgo de pérdida de información ocasionando un impacto que pueda ser aprovechado por el personal interno que trabaja en dicha institución.

Tal como su nombre lo indica, el hacking interno se ejecuta desde la red interna del cliente, por ejemplo desde el computador de un empleado de la empresa comúnmente se suele encontrar más brechas de seguridad. Astudillo, K. (2012) define los siguiente: “En este tipo de pruebas de intrusión se suele encontrar más huecos de seguridad que en su contraparte externa, debido a que muchos administradores de sistemas se preocupan por proteger el perímetro de su red y subestiman al atacante interno” [1]. Hay que hacer énfasis es la última parte de este texto citado, ya que es un gran error subestimar a los posibles atacantes internos puesto que según las estadísticas la mayor parte de los ataques realizados y considerados exitosos se han ejecutado desde la red interna de una institución.

En base a lo mencionado anteriormente se desarrolla este hacking ético que es una combinación de hacking interno y externo para detectar vulnerabilidades y así mejorar e implementar un plan de acción de protección de información ofreciendo servicios eficientes y seguros ante los posibles ataques de intrusos.

2.2 RECONOCIMIENTO O FOOTPRINTING

La primera fase en la ejecución del hacking es el reconocimiento o también llamado footprinting, el cual consiste en descubrir y recolectar la mayor cantidad de información de la víctima objetivo del ataque. Mientras más minuciosos e ingeniosos seamos, mayor posibilidades hay de encontrar un descuido, objetivo o al lo menos una pista [2].

Entre los objetivos del reconocimiento se puede mencionar:

- Extraer información de la red para tener y encontrar direcciones ip de servidores.
- Encontrar las direcciones ip del servidor de de dominio.
- Encontrar las direcciones ip del servidor de de correo.
- Hacer uso del comando ping para probar conectividad con los servidores detectados.

Primeramente se realizó Footprinting con el famoso buscador *Google*, se utilizó el nombre de la empresa víctima y se obtienen cerca de 390 mil resultados pero el primer enunciado de la lista es el que permite el acceso a la página web deseada.

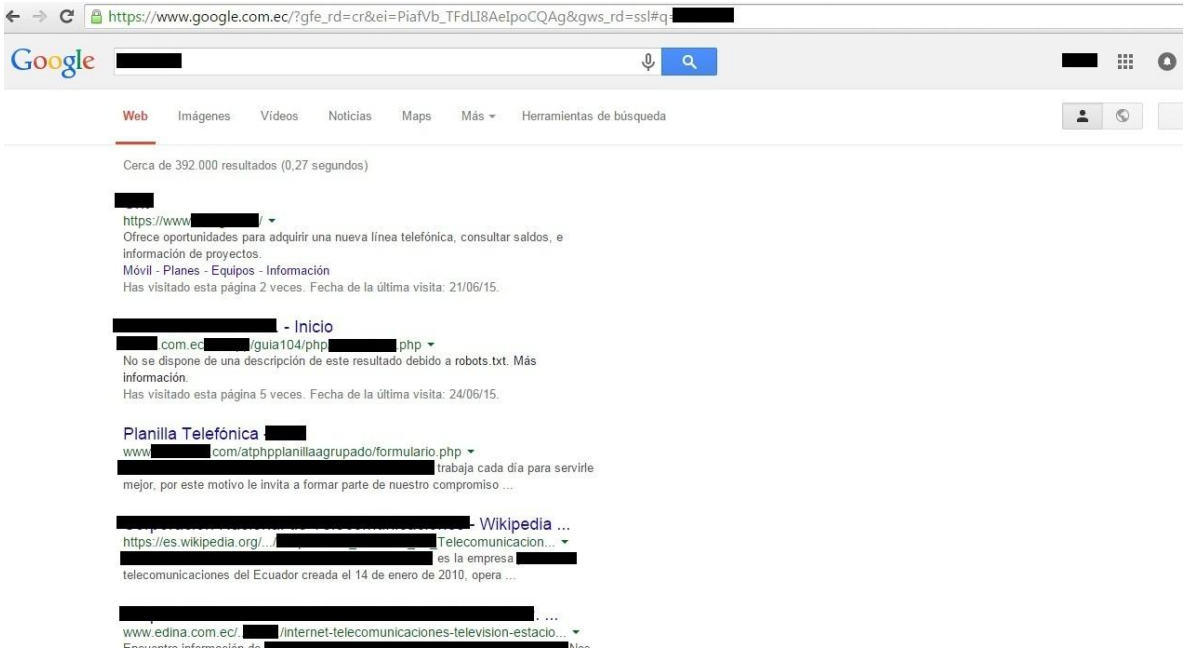


Figura 2.1 Footprinting con Google

El siguiente objetivo es realizar una consulta DNS para conocer la dirección ip y a su vez el rango de ip's pertenecientes a la subred, para esto se hace uso del comando *nslookup* en un shell de windows.

Figura 2.2 Resolución DNS con comando nslookup en Windows

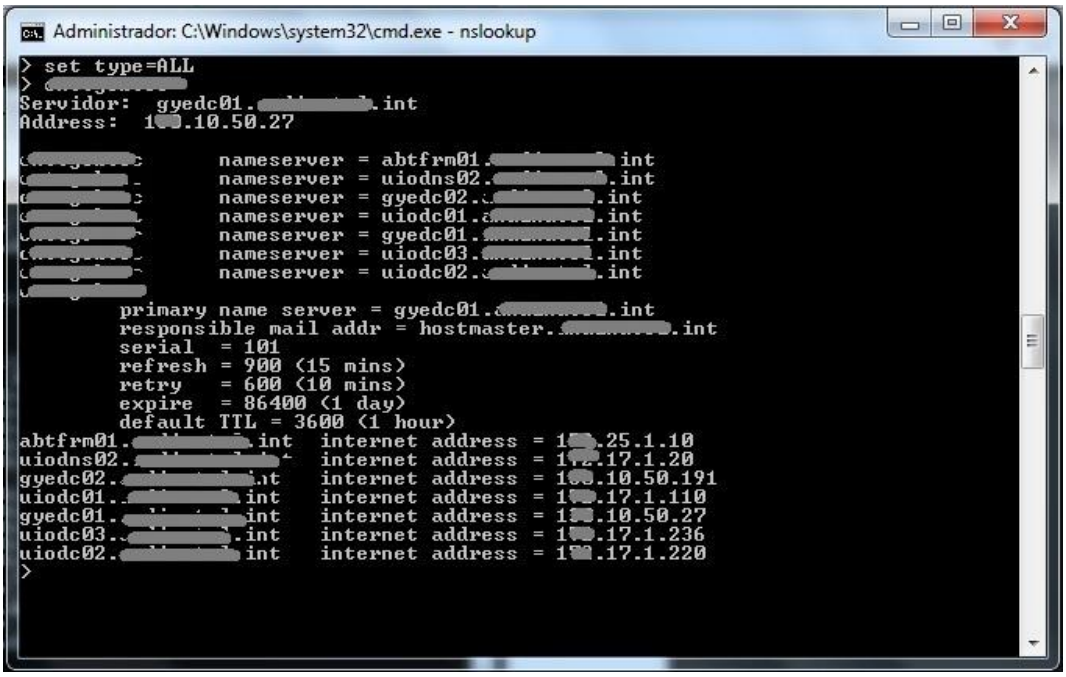
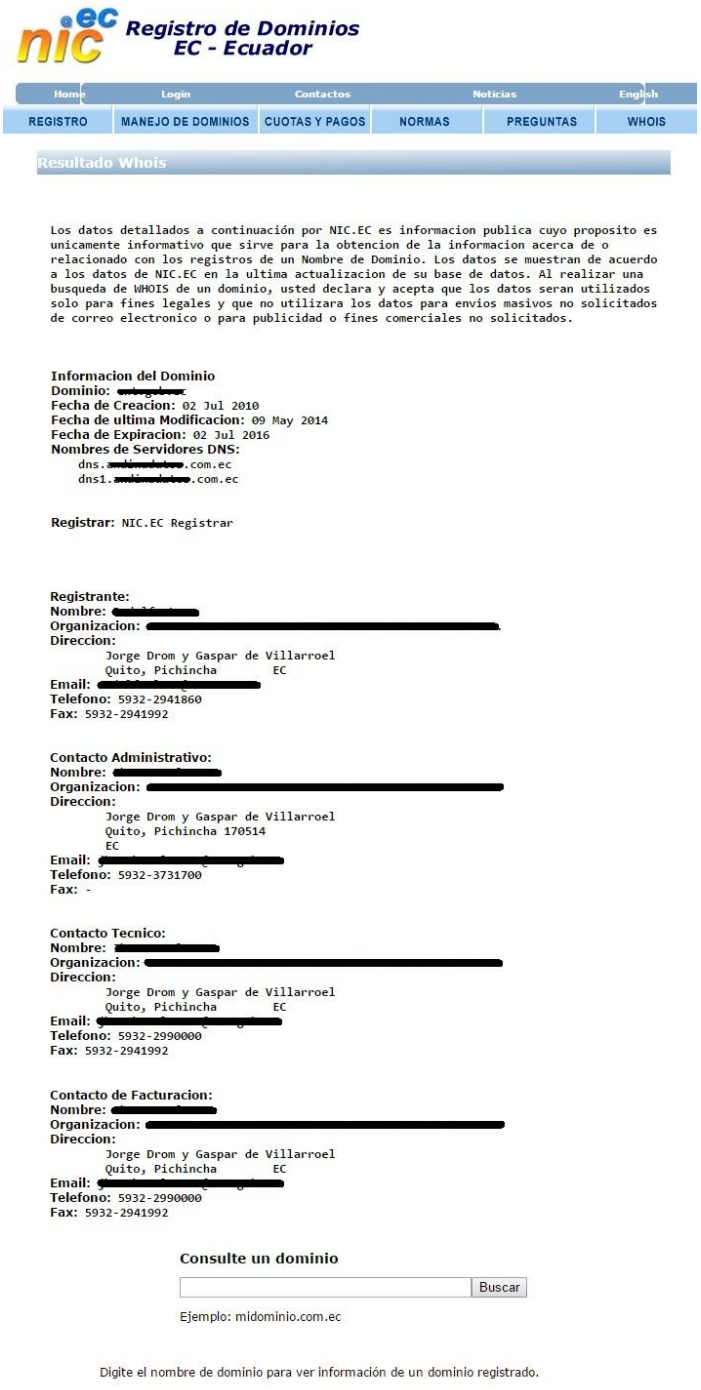


Figura 2.3 Comando nslookup set type=ALL

Con el comando *nslookup* y el tipo de consulta NS se ha obtenido los nombres de los servidores de dominio, así mismo con el tipo de consulta MX se obtuvo el nombre del servidor de correo y con la opción ALL se obtiene la combinación de ambas consultas como se aprecia en la figura 2.3. Por los resultados expuestos se aprecia las ip's de los servidores DNS y SMTP y los nombres. A continuación se realizará reconocimiento con *Who-Is* en el NIC de Ecuador. En la figura 2.4 se muestra la información del nombre de dominio y contactos reales que laboran en la empresa, números telefónicos y correos electrónicos.



Registro de Dominios
EC - Ecuador

Home | Login | Contactos | Noticias | English

REGISTRO | MANEJO DE DOMINIOS | CUOTAS Y PAGOS | NORMAS | PREGUNTAS | WHOIS

Resultado Whois

Los datos detallados a continuación por NIC.EC es informacion publica cuyo proposito es unicamente informativo que sirve para la obtencion de la informacion acerca de o relacionado con los registros de un Nombre de Dominio. Los datos se muestran de acuerdo a los datos de NIC.EC en la ultima actualizacion de su base de datos. Al realizar una busqueda de WHOIS de un dominio, usted declara y acepta que los datos seran utilizados solo para fines legales y que no utilizara los datos para envios masivos no solicitados de correo electronico o para publicidad o fines comerciales no solicitados.

Informacion del Dominio
Dominio: [redacted]
Fecha de Creacion: 02 Jul 2010
Fecha de ultima Modificacion: 09 May 2014
Fecha de Expiracion: 02 Jul 2016
Nombres de Servidores DNS:
dns.[redacted].com.ec
dns1.[redacted].com.ec

Registrar: NIC.EC Registrar

Registrante:
Nombre: [redacted]
Organizacion: [redacted]
Direccion:
Jorge Drom y Gaspar de Villarroel
Quito, Pichincha EC
Email: [redacted]
Telefono: 5932-2941860
Fax: 5932-2941992

Contacto Administrativo:
Nombre: [redacted]
Organizacion: [redacted]
Direccion:
Jorge Drom y Gaspar de Villarroel
Quito, Pichincha 170514
EC
Email: [redacted]
Telefono: 5932-3731700
Fax: -

Contacto Tecnico:
Nombre: [redacted]
Organizacion: [redacted]
Direccion:
Jorge Drom y Gaspar de Villarroel
Quito, Pichincha EC
Email: [redacted]
Telefono: 5932-2990000
Fax: 5932-2941992

Contacto de Facturacion:
Nombre: [redacted]
Organizacion: [redacted]
Direccion:
Jorge Drom y Gaspar de Villarroel
Quito, Pichincha EC
Email: [redacted]
Telefono: 5932-2990000
Fax: 5932-2941992

Consulte un dominio

Buscar

Ejemplo: midominio.com.ec

Digite el nombre de dominio para ver información de un dominio registrado.

Figura 2.4 Datos de contactos obtenidos en NIC.EC

La siguiente herramienta utilizada es *Maltego Community*, la cual, permite obtener datos de una organización con el uso de objetos gráficos a través de transformaciones. Se puede apreciar en las figuras 2.5 y 2.6 los resultados obtenidos al realizar una transformación del dominio de la empresa obtenido anteriormente, se visualizan dominios, ipv4, documentos pdf entre otros.

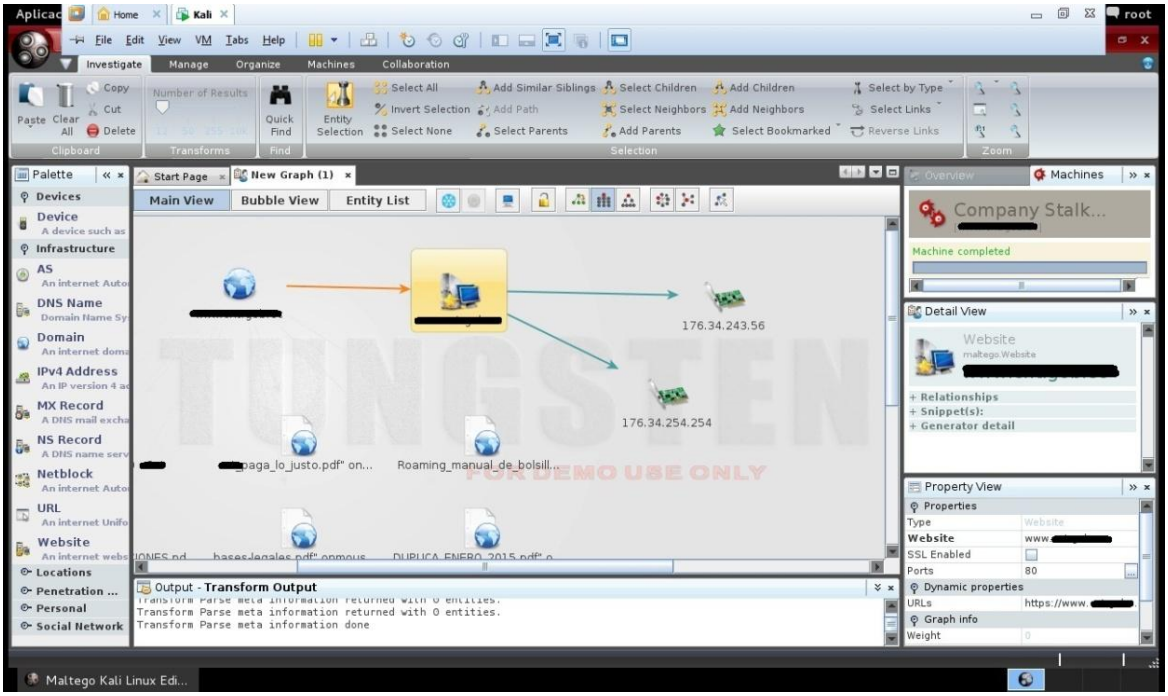


Figura 2.5 Transformación con Maltego

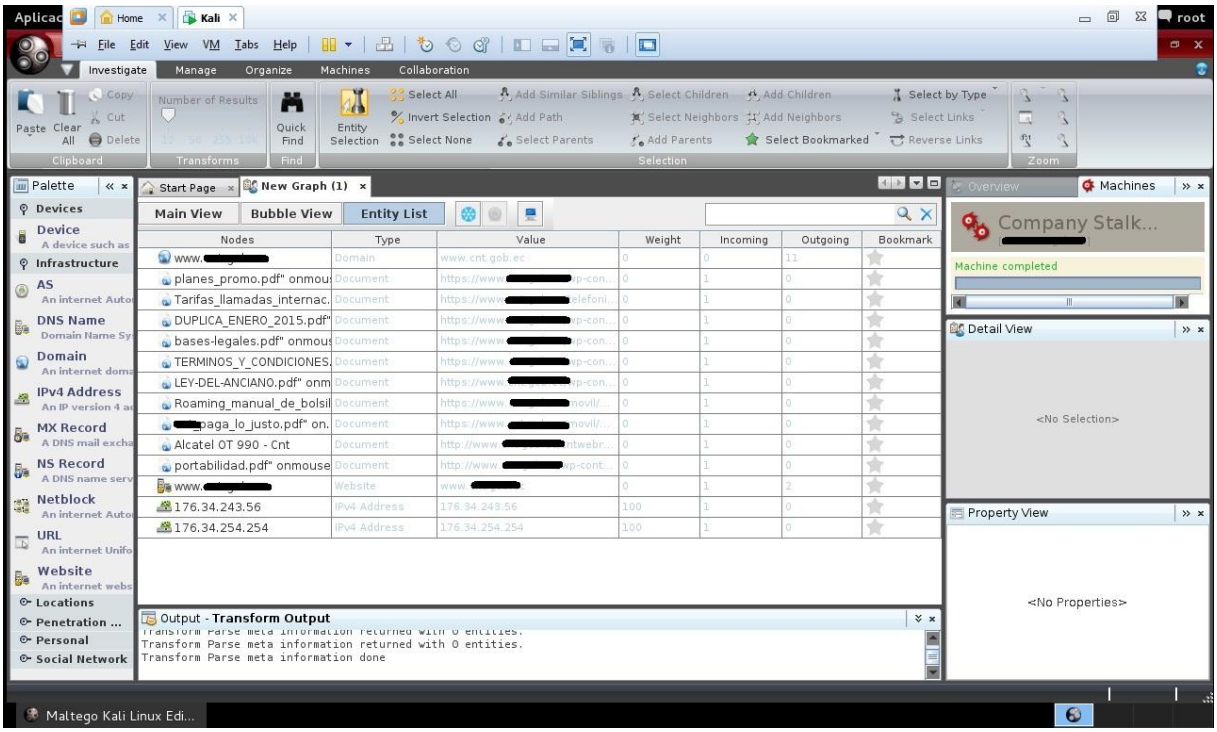


Figura 2.6 Resultado obtenido con Maltego

Continuando con el análisis de reconocimiento resulta útil conocer la ubicación geográfica de la víctima por ejemplo para determinar si los servicios de correo y dns están alojados en la red de la empresa o en algún hosting externo, para esto, se utilizó la herramienta *Visual IP Trace,* el resultado se puede apreciar en la figura 2.7.

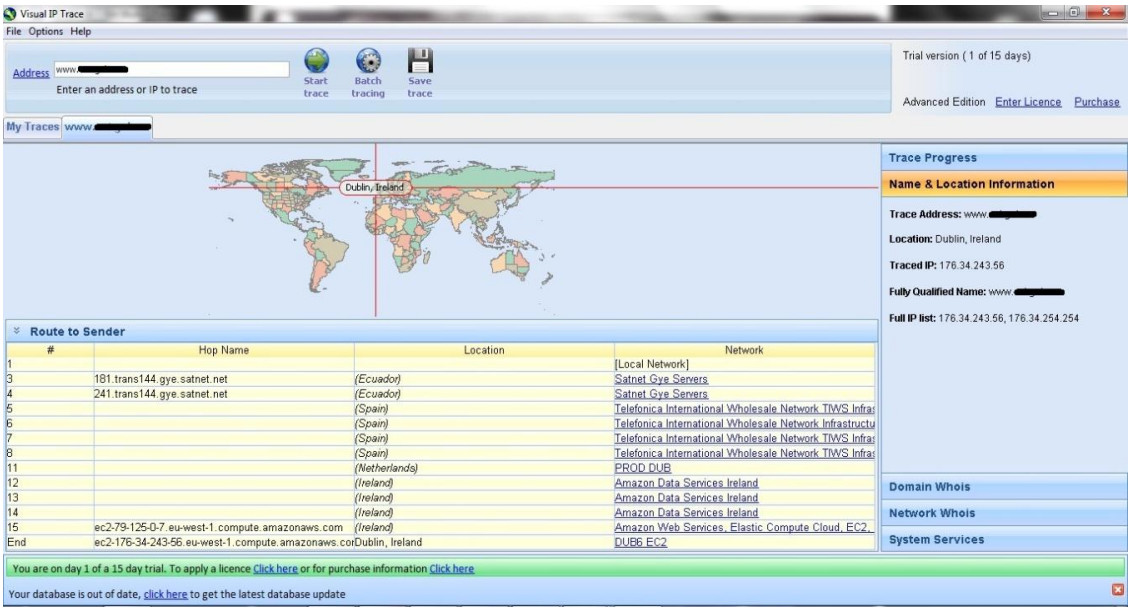


Figura 2.7 Trazado en Visual IP Trace

Después de analizar el resultado obtenido se puede visualizar que se encuentran servicios en Ecuador y en Dublin, Ireland para los servidores DNS, se muestra en la red de Satnet lo que indica que tiene alojamiento con una empresa muy conocida en el Ecuador.

A continuación vamos a realizar un rastreo de un correo electrónico aprovechando el acceso a la red interna, se escoge un correo enviado desde una cuenta interna de un empleado de la empresa objetivo del análisis, dicho correo está dirigido hacia Gmail de un correo personal de prueba, en la figura 2.8 se parecían datos interesantes.

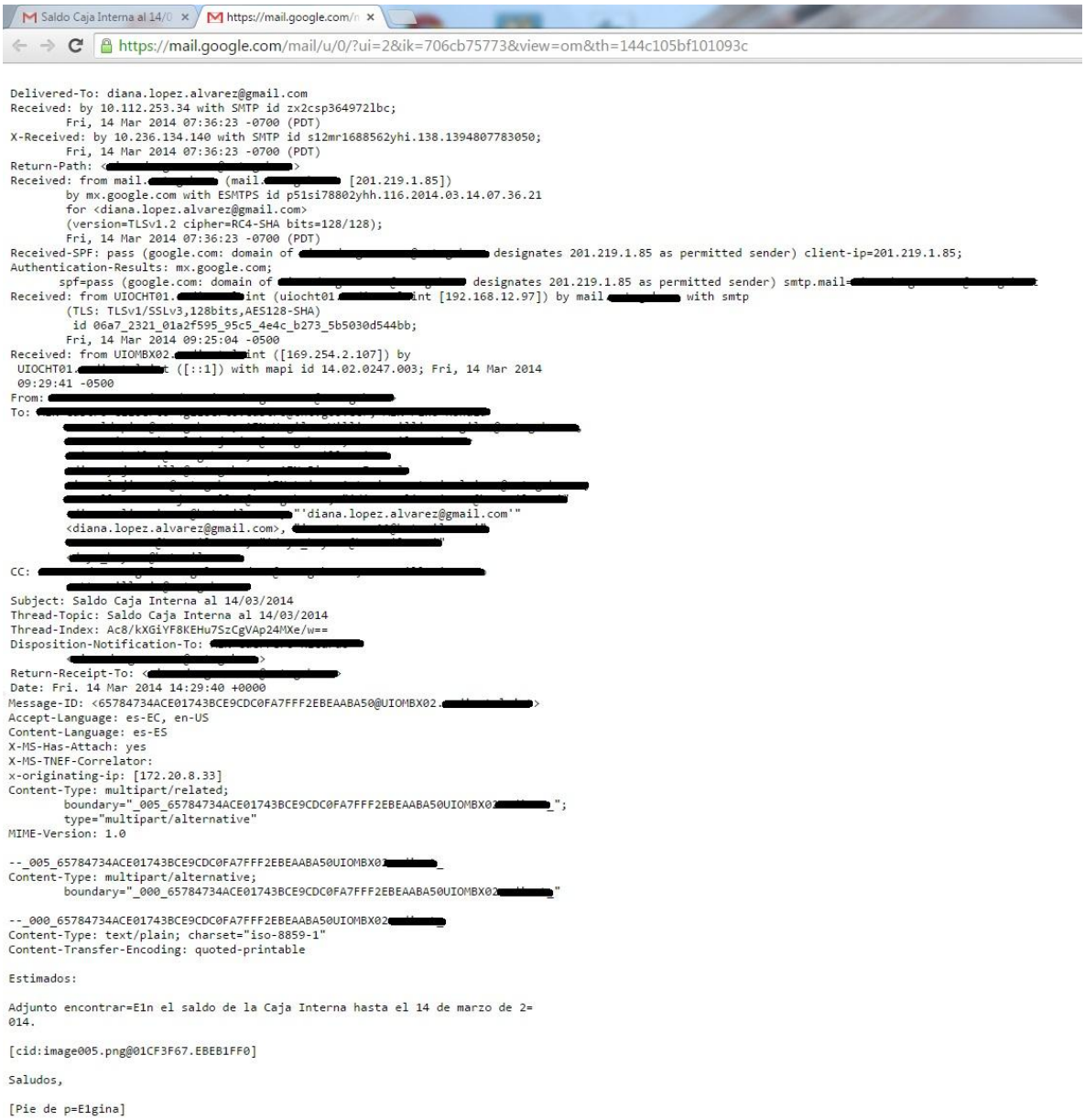


Figura 2.8 Cabecera de mail

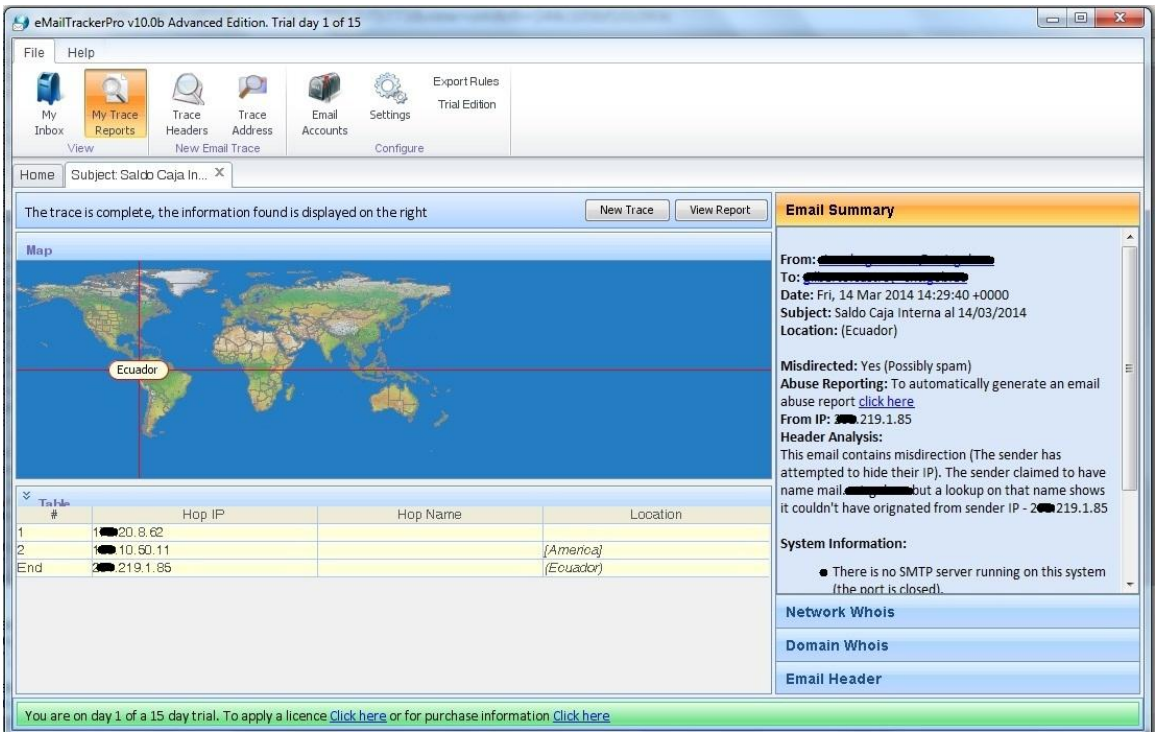
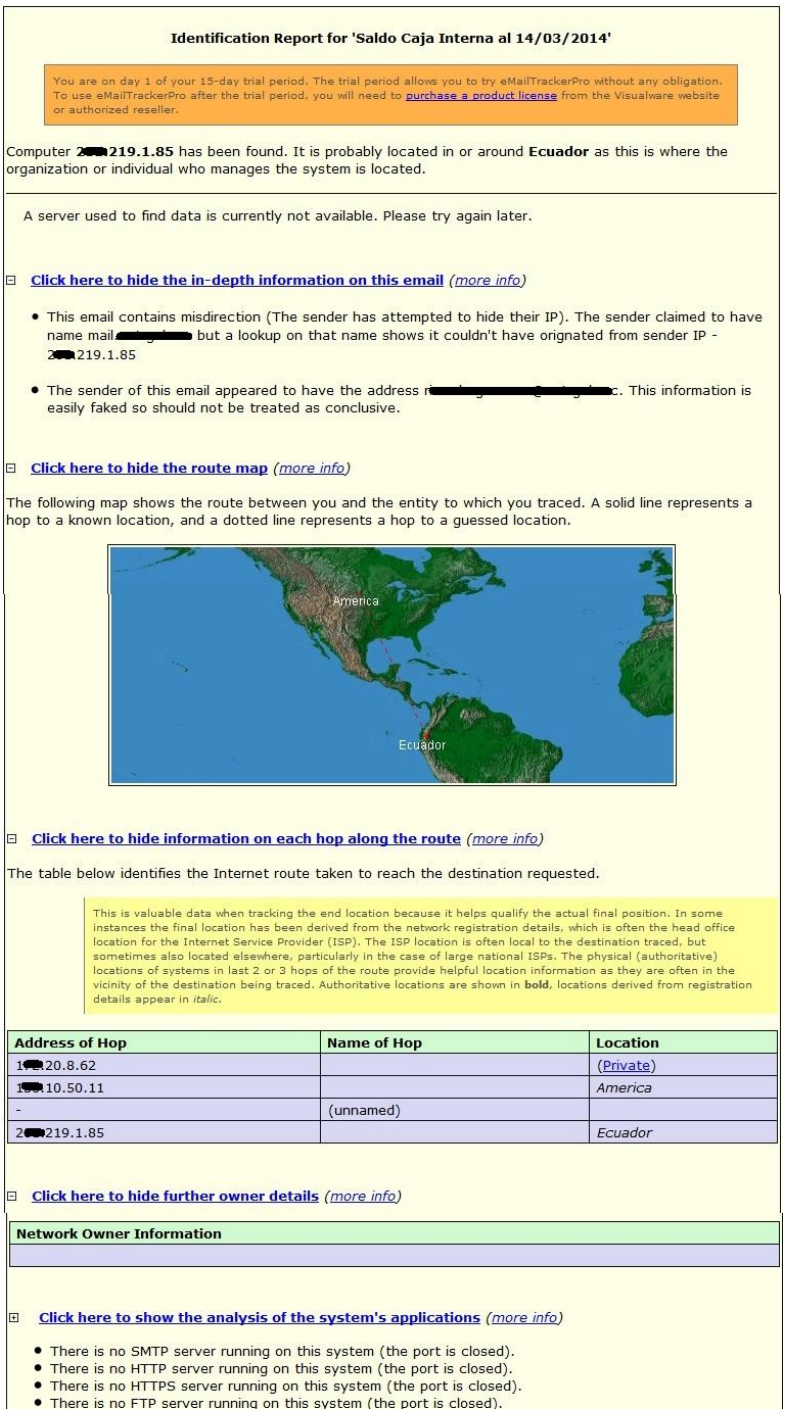


Figura 2.9 Análisis de cabecera de mail con Email Tracker Pro

La figura 2.8 muestra las cabeceras del correo electrónico mientras que la figura 2.9 muestra el análisis del correo con la herramienta *Email Tracker Pro* que ubica el origen del correo en Ecuador con su respectiva tabla de rutas. De la misma forma la figura 2.10 muestra el resumen del análisis del correo. Claramente se aprecia que el correo salió desde la primera ip, posteriormente salió por una ip que aparentemente sería un firewall y finalmente se presenta la ip del servidor de correo que indica que se encuentra en Ecuador, es decir la empresa tiene su servidor de correo de forma local.



Identification Report for 'Saldo Caja Interna al 14/03/2014'

You are on day 1 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to purchase a product license from the Visualware website or authorized reseller.

Computer 2[redacted]219.1.85 has been found. It is probably located in or around **Ecuador** as this is where the organization or individual who manages the system is located.

A server used to find data is currently not available. Please try again later.

Click here to hide the in-depth information on this email *(more info)*

- This email contains misdirection (The sender has attempted to hide their IP). The sender claimed to have name mail[redacted] but a lookup on that name shows it couldn't have orignated from sender IP - 2[redacted]219.1.85
- The sender of this email appeared to have the address r[redacted]c. This information is easily faked so should not be treated as conclusive.

Click here to hide the route map *(more info)*

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.

Click here to hide information on each hop along the route *(more info)*

The table below identifies the Internet route taken to reach the destination requested.

This is valuable data when tracking the end location because it helps qualify the actual final position. In some instances the final location has been derived from the network registration details, which is often the head office location for the Internet Service Provider (ISP). The ISP location is often local to the destination traced, but sometimes also located elsewhere, particularly in the case of large national ISPs. The physical (authoritative) locations of systems in last 2 or 3 hops of the route provide helpful location information as they are often in the vicinity of the destination being traced. Authoritative locations are shown in **bold**, locations derived from registration details appear in *italic*.

Address of Hop	Name of Hop	Location
1[redacted]20.8.62		(Private)
1[redacted]10.50.11		*America*
-	(unnamed)	
2[redacted]219.1.85		*Ecuador*

Click here to hide further owner details *(more info)*

Network Owner Information

Click here to show the analysis of the system's applications *(more info)*

- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

Figura 2.10 Resumen de análisis de cabecera de mail con Email Tracker Pro

2.3 ESCANEO

En la fase de escaneo se identifica los hosts activos en base a las ip's encontradas en la fase de reconocimiento y con esto se determina los puertos abiertos en dichos equipos, posteriormente se intentará detectar el sistema operativo y los servicios y aplicaciones que escuchan los puertos.

Con ayuda de la herramienta *Net Scan* haremos un escaneo de puertos como se aprecia en la figura 2.11, además de esto se revelan los servicios ejecutándose en cada uno de ellos, la ip analizada es la del servidor DNS.

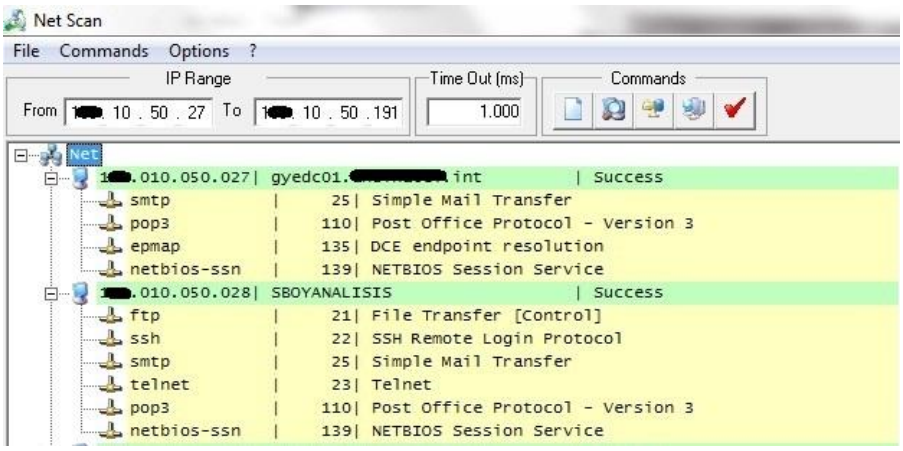


Figura 2.11 Análisis con herramienta Net Scan

Ahora se procede a hacer uso de la herramienta *Nmap*, uno de los escáner de puertos más famosos, se puede realizar un escaneo de puertos desde un Shell o desde la aplicación gráfica. Se realiza un escaneo de tipo connect. Para este

análisis se usará las ip's detectadas en la fase anterior, donde se encontró las ip's: 1XX.10.50.27, 1XX.10.50.11, 2XX.219.1.85.

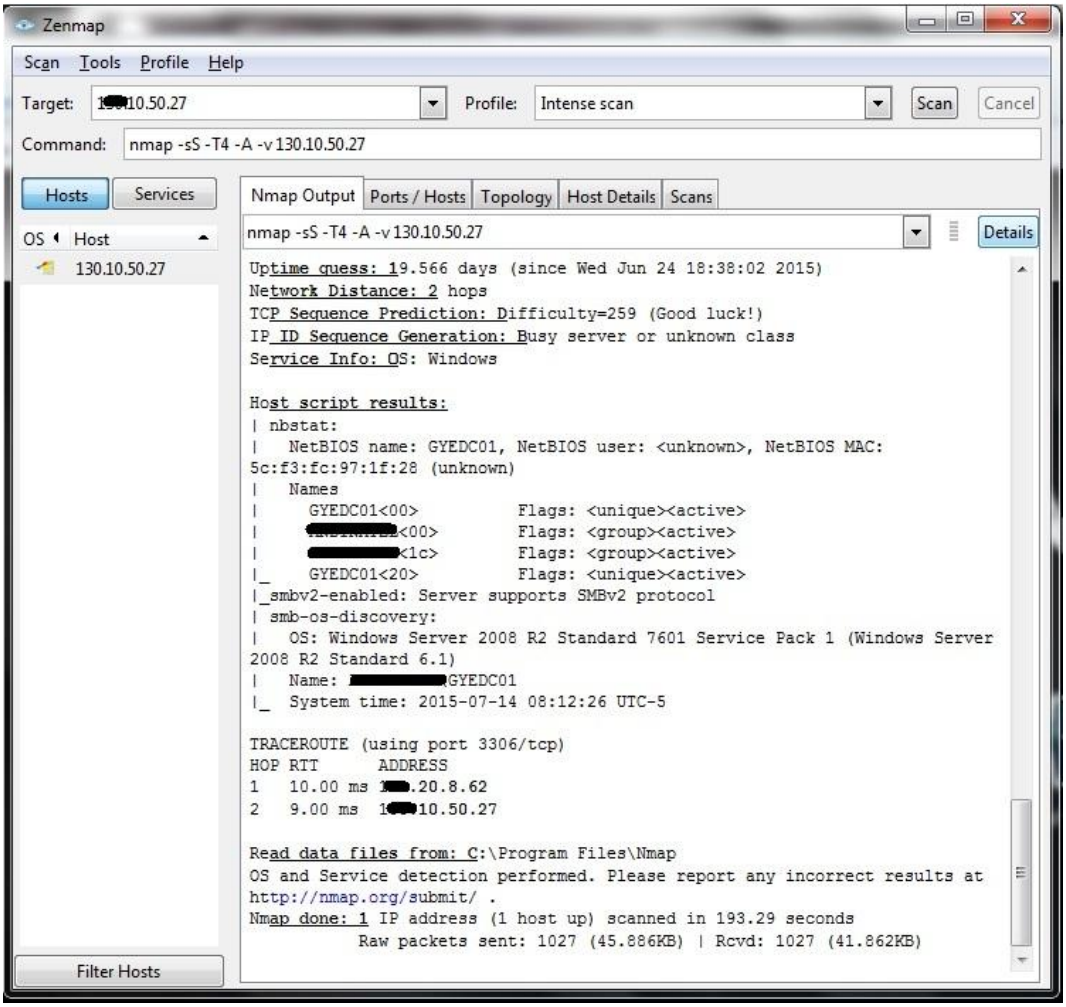


Figura 2.12 Interfaz gráfica ZenMap, escaneo de puertos ip 1xx.10.50.27

Como se puede apreciar en la figura 2.12 *Nmap* permite detectar los nombres del servidor y a su vez muestra el sistema operativo encontrado Windows Server 2008 R2 con SP1.

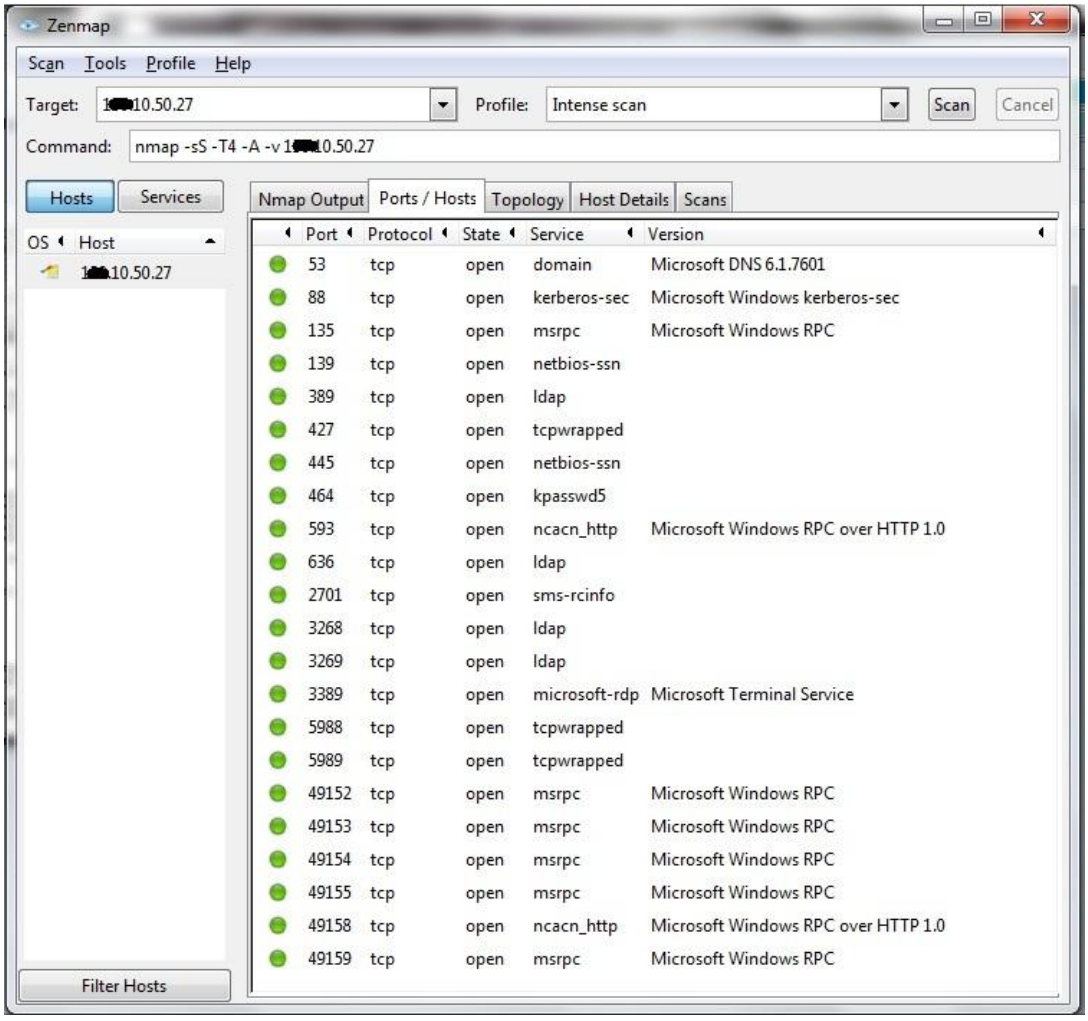


Figura 2.13 Interfaz gráfica ZenMap, detección SO

La figura 2.13 muestra los puertos abiertos y servicios disponibles o para la ip 1XX.10.50.27.

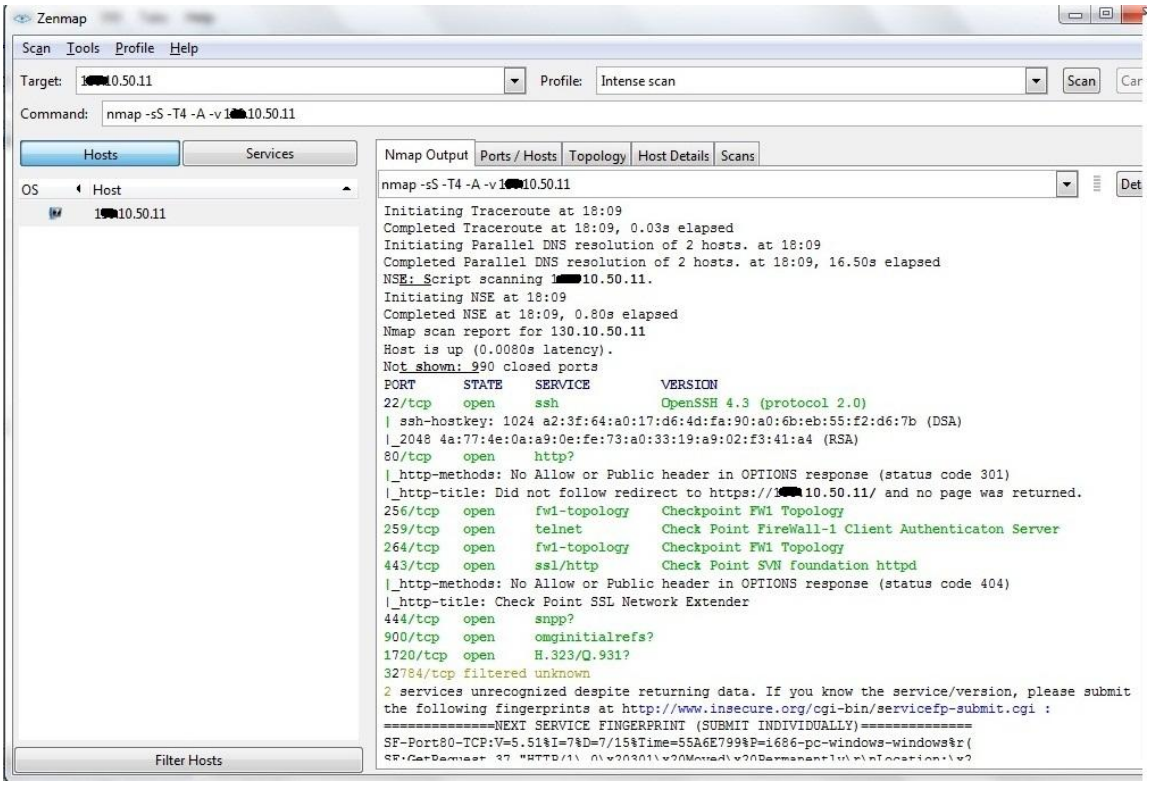


Figura 2.14 Interfaz gráfica ZenMap, escaneo de puertos ip 1XX.10.50.11

En la figura 2.14 se realizó un escaneo de puertos para la ip 1XX.10.50.11 y el resultado obtenido es la identificación de un equipo Firewall Check Point. Se presentan además los puertos abiertos y servicios.

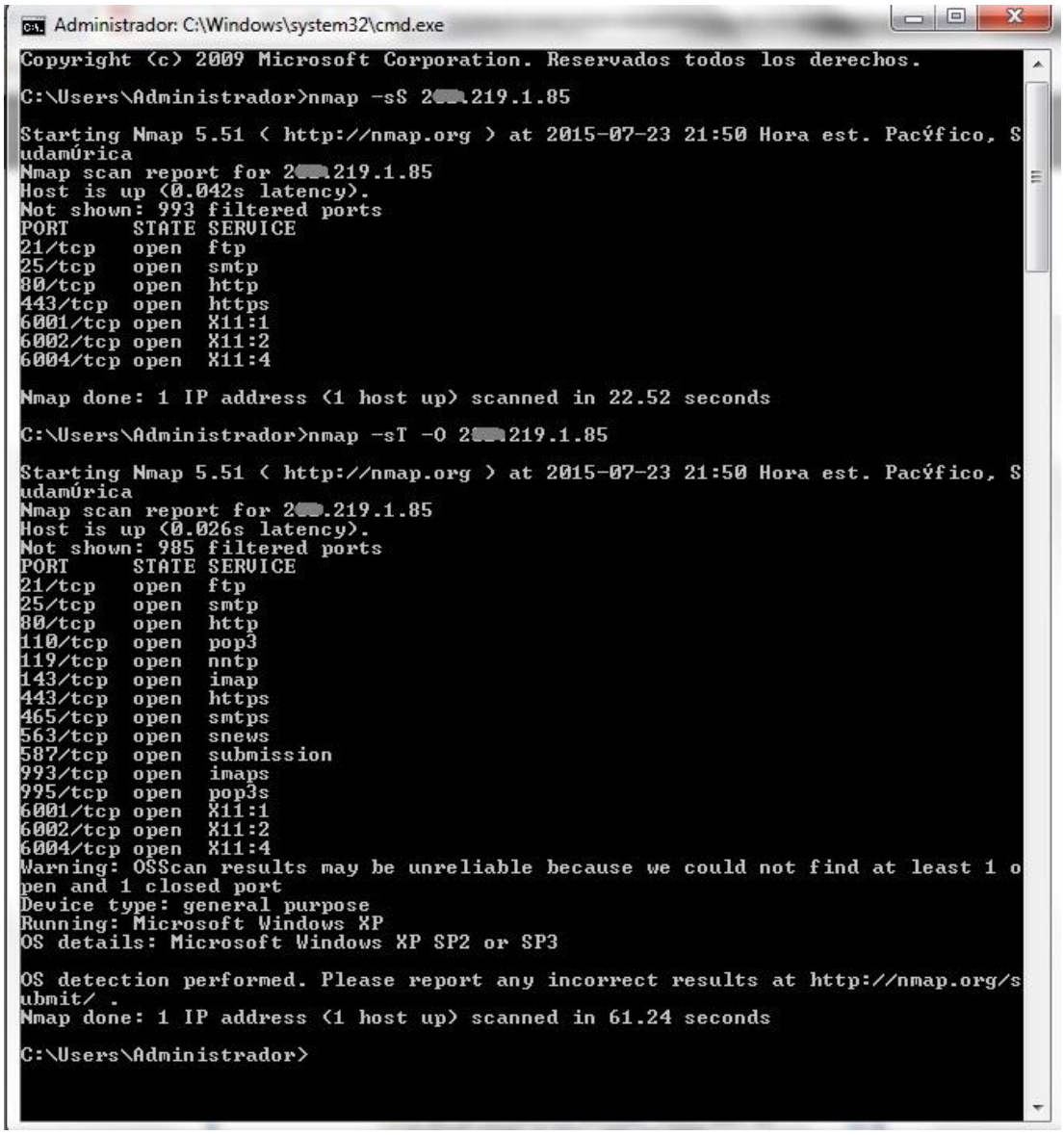


Figura 2.15 NMap desde un cmd de Windows, ip 2XX.219.1.85

Se analiza la ip 2XX.219.1.85, en la figura 2.15 con Nmap desde el Shell de Windows, al realizar un escaneo tipo Connect se detecta los puertos abiertos, así

mismo se obtiene que el sistema operativo aparentemente es Windows Xp. Cabe recalcar que dicho escaneo se ha realizado externamente, es decir, fuera de la red de la empresa.

Ahora vamos a hacer uso de un analizador de vulnerabilidades conocido como *Nessus* en su versión Home Feed gratuita, esto nos permitirá analizar los niveles de riesgo presentes en las ip obtenidas. La ip objetivo será el servidor de correo que hemos detectado hasta el momento 2XX.219.1.85, para lo cual el análisis presenta como resumen los resultados que se observan en la figura 2.16 con un escaneo avanzado con reporte de la información de las vulnerabilidades encontradas.

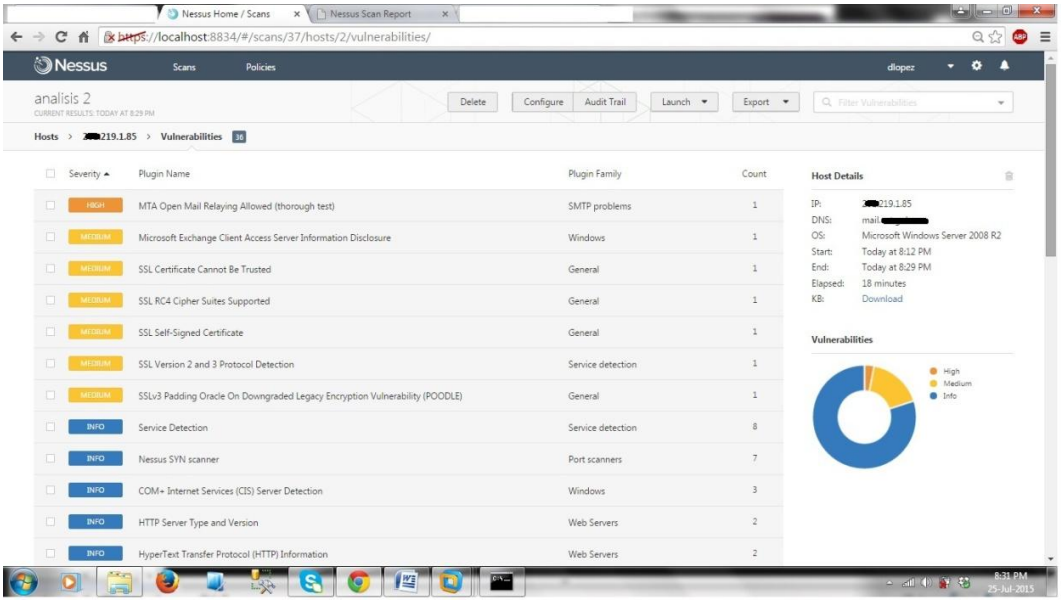


Figura 2.16 Nessus resumen de vulnerabilidades encontradas

Entre lo analizado por *Nessus* existe un riesgo que ha sido calificado como alto, es decir que tiene una vulnerabilidad crítica que podría ser explotada fácilmente, la vulnerabilidad detectada es un Open relay, esto significa que el servidor de correo está mal configurado, de ésta forma alguien podría utilizarlo para hacer spam a través de él. Si esto pasa, las listas RBL (Real-time Blackhole List) incluirán a esta dirección entre los servidores mal configurados y los emails legítimos que se envíen de ese servidor quedarán bloqueados, de ahí la importancia de cuidar la ip del servidor de correo electrónico [3], figura 2.17.

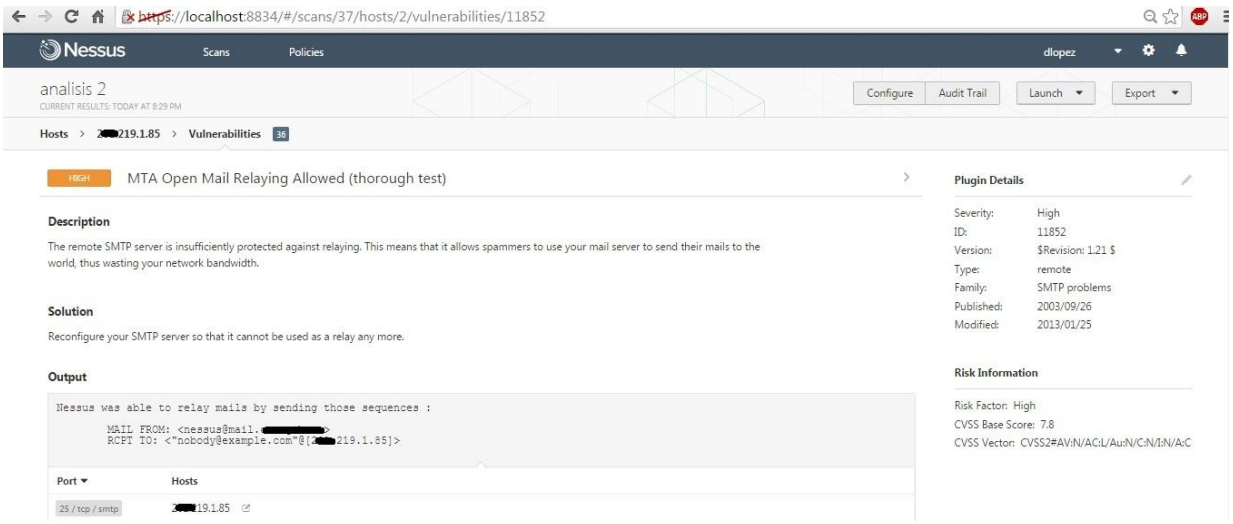


Figura 2.17 Nessus reporte generado

2.4 ENUMERACIÓN

La enumeración es una subfase del escaneo y sirve para encontrar más información de la víctima aprovechando las vulnerabilidades encontradas previamente.

Haciendo uso del comando *net view* podemos realizar enumeración y tratar de obtener una lista de dominios, grupos de trabajo, computadoras o recursos compartidos como se puede observar en la figura 2.18. Primeramente se detecta el dominio de interés y se observa que más adelante se obtiene el nombre de un equipo y se establece una sesión nula, es decir sesiones sin usuario ni clave.

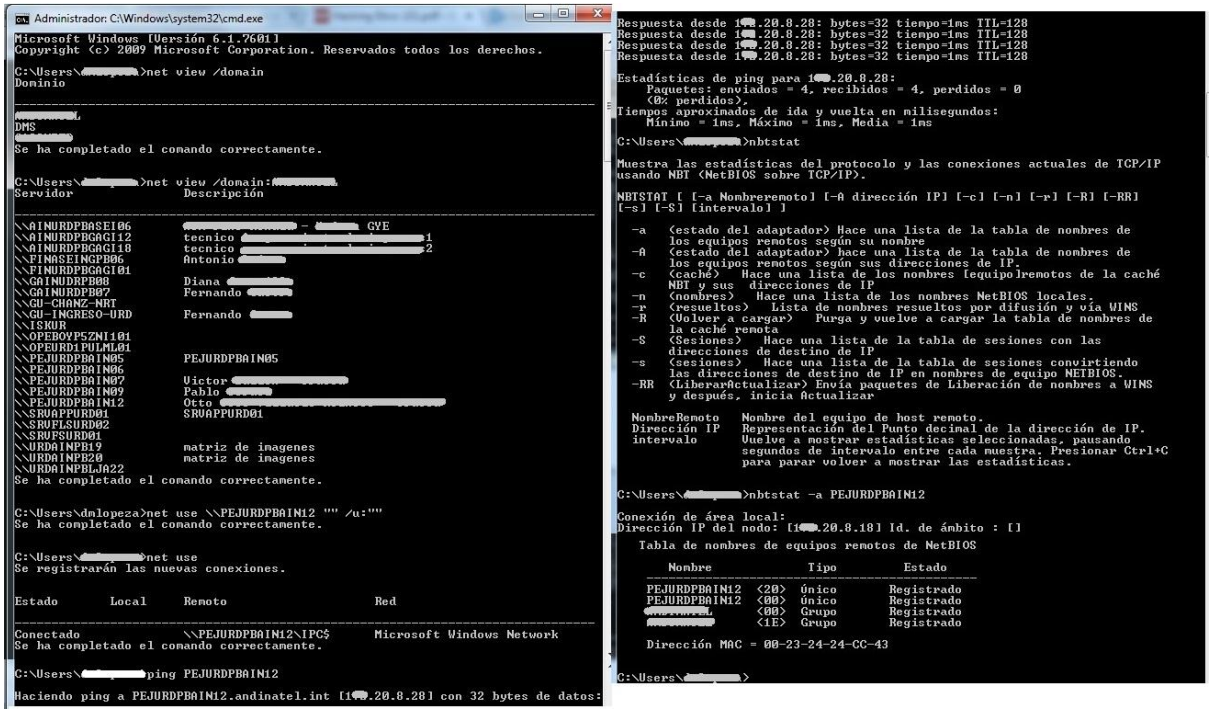


Figura 2.18 Enumeración con Netview

En base a la tabla 1, se puede visualizar como dato importante que se obtuvo el nombre del dominio y un servidor de archivos.

Tabla 2.1 Sufijos de NetBIOS (extracto)

Nombre	Número(h)	Tipo	Uso
<computername>	0	U	Servicio de estación de trabajo
<computername>	1	U	Servicio Messenger
<\\--__MSBROWSE__>	1	G	Examinador principal
<computername>	3	U	Servicio Messenger
<computername>	6	U	Servicio Servidor RAS
<computername>	1F	U	Servicio NetDDE
<computername>	20	U	Servicio Servidor de archivos
<computername>	21	U	Servicio Cliente RAS
<domain>	1B	U	Examinador principal de dominio
<domain>	1C	G	Controladores de dominio

Para listar usuarios, grupos, servicios, se hizo uso de dos herramientas conocidas como *Dumpsec* y *Hyena* como se puede observar en las figuras 2.19 y 2.20.

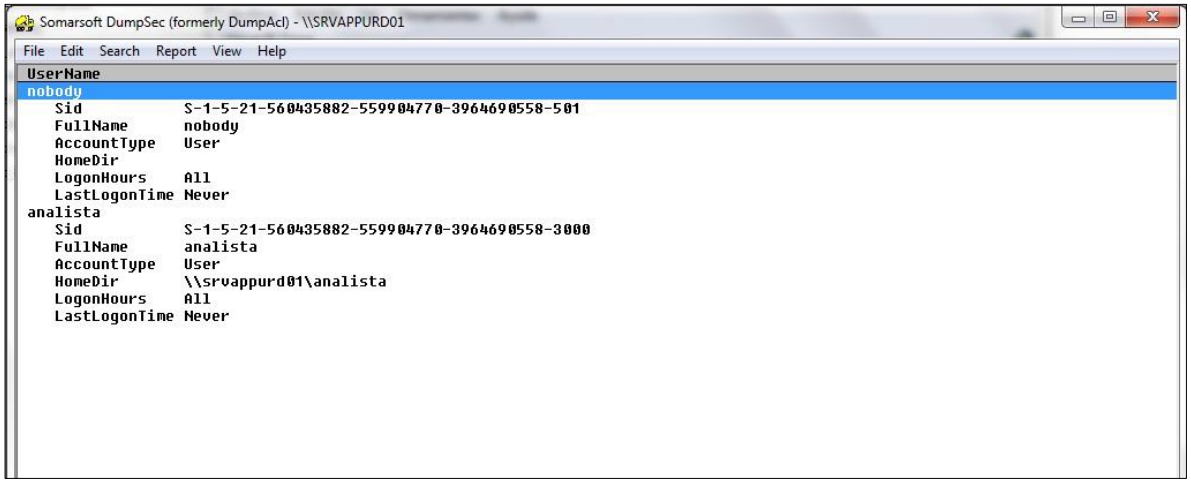


Figura 2.19 Listado de usuarios con DumpSec

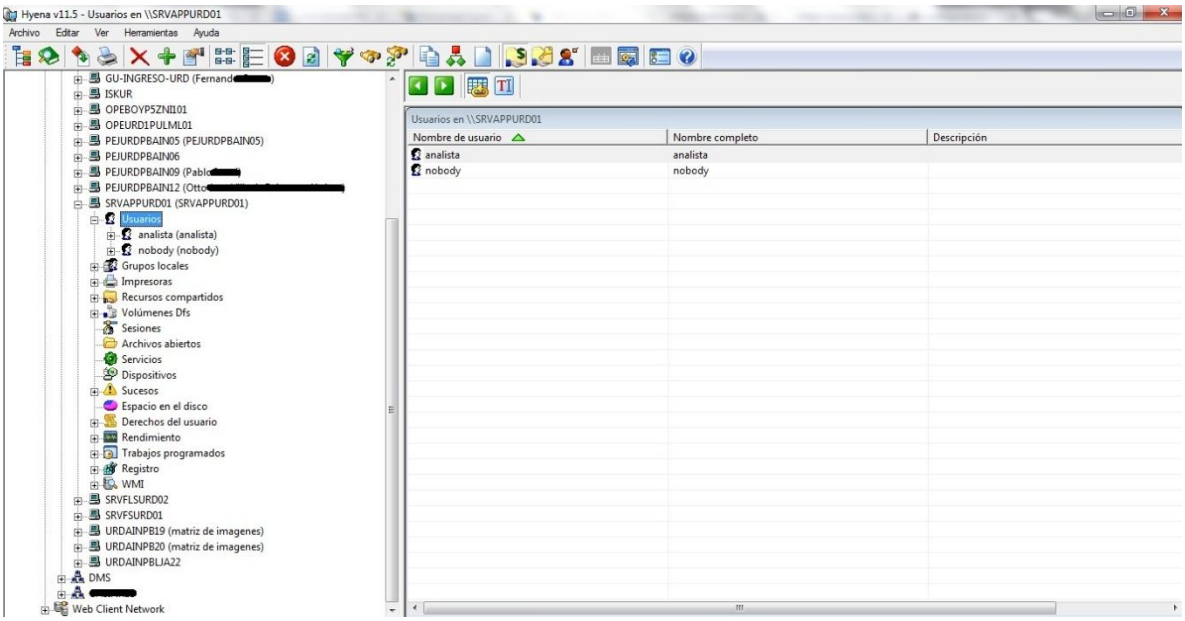


Figura 2.20 Enumeración con Hyena

Éstas son herramientas antiguas pero útiles a la hora de realizar enumeraciones. Como dato interesante se puede acotar que al llevar una laptop y conectar un cable de red a ella se asignó una ip automáticamente lo que permitió estar dentro de la red sin necesidad de configurar nada adicional, con esto se obtuvo acceso a realizar el escaneo desde la red interna de la institución.

2.5 EXPLOTACIÓN O HACKING

Hemos llegado a la fase de hacking o llamada también explotación, en la cual, se puede hacer uso de exploits manuales y automáticos. Es recomendable hacer

énfasis que al ser éste un Hacking ético lo que se pretende no es atacar causando por ejemplo alguna denegación de servicios, el objetivo es encontrar las vulnerabilidades presentes en los equipos auditados y los posibles riesgos que pueden enfrentar.

Para realizar esta fase se hizo uso de la herramienta *Metasploit Framework Community* que es una versión gratuita aunque limitada que proporciona información sobre vulnerabilidades y permite realizar exploits. Antes de acercarse o realizar una prueba de penetración es recomendable tener todo listo ”afilando las herramientas” y actualizándolas, como lo dijo Abraham Lincon: "Si yo tuviera ocho horas para cortar un árbol, me gustaría pasar los primeros seis de ellos afilando mi hacha."[4].

Vamos a concentrarnos en el servidor de correo SMTP, al encontrarse localmente en Ecuador trataremos de explotar las vulnerabilidades encontradas, con ayuda de *Nessus* se logró detectar que dicho servidor tiene una vulnerabilidad calificada como Alta de Open Relay, primeramente subimos el reporte generado con *Nessus* y vemos las vulnerabilidades encontradas, todo esto lo almacenamos en un workspace y posteriormente detectamos las vulnerabilidades con ayuda del comando Vulns.

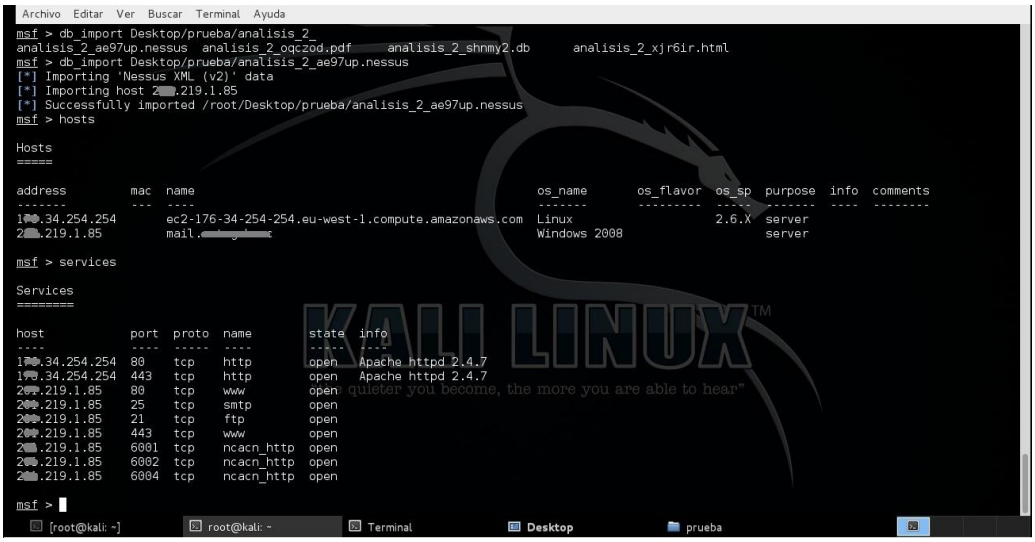


Figura 2.21 Metasploit carga reporte de Nessus

Como se aprecia en la figura 2.21 se realizó la importación del reporte de *Nessus* y con el comando *hosts* se verifica que la ip analizada ha sido incorporada al workspace, con el comando *services* se lista los puertos abiertos y servicios activos dentro del servidor de correo. En la figura 2.22 se hace uso del comando *vulns* que presenta la lista de las vulnerabilidades que fueron detectadas.

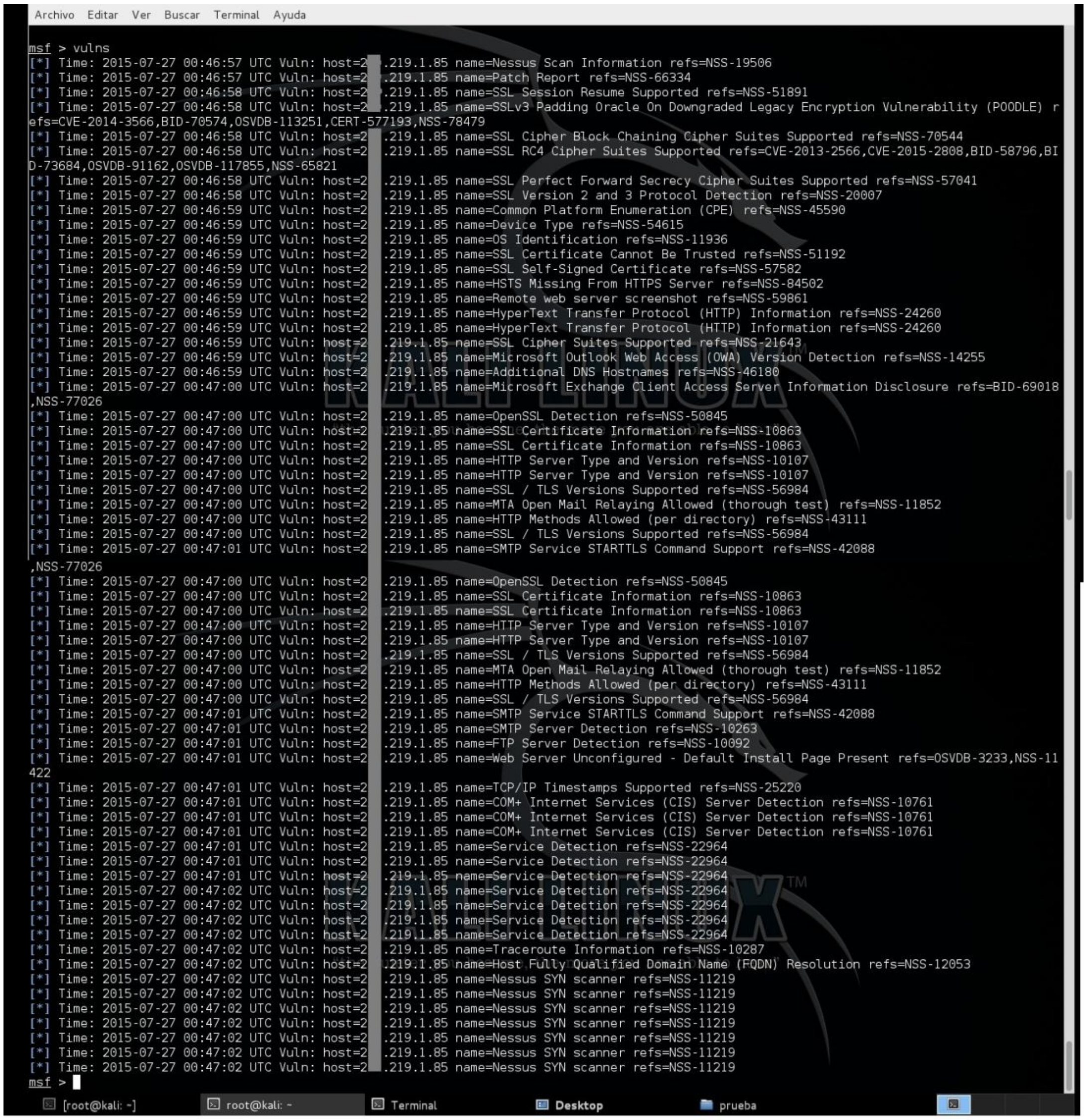


Figura 2.22 Metasploit, uso de comando Vulns

Como habíamos detectado la vulnerabilidad de Open Relay, hacemos uso del módulo auxiliar de mestasploit “smtp_relay” como se aprecia en la figura 2.23.

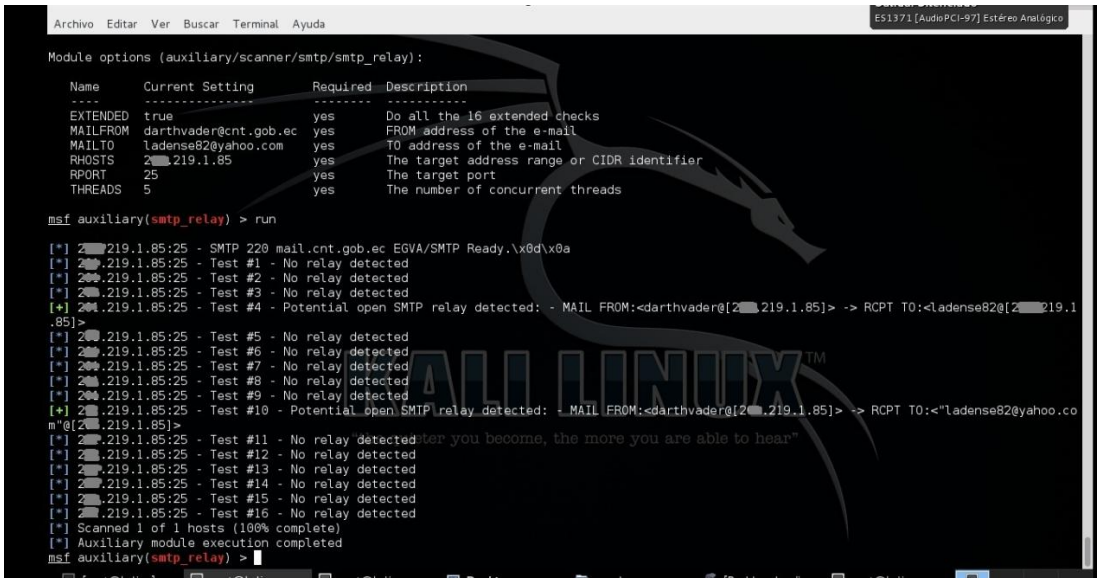


Figura 2.23 Metasploit, uso de módulo auxiliar smtp_relay

Ahora procedemos a probar con ayuda de *telnet* el envío de correos desde el servidor, para esto primero ingresamos y hacemos un HELO al servidor, vemos que nos responde y le seteamos el remitente y destinatario recibiendo como respuesta un Ok, lo cual indica que el correo pudo ser enviado exitosamente, figura 2.24.

De ésta manera hemos podido comprobar que el envío de correos se pudo hacer ocasionando así la comprobación de Open Relay.

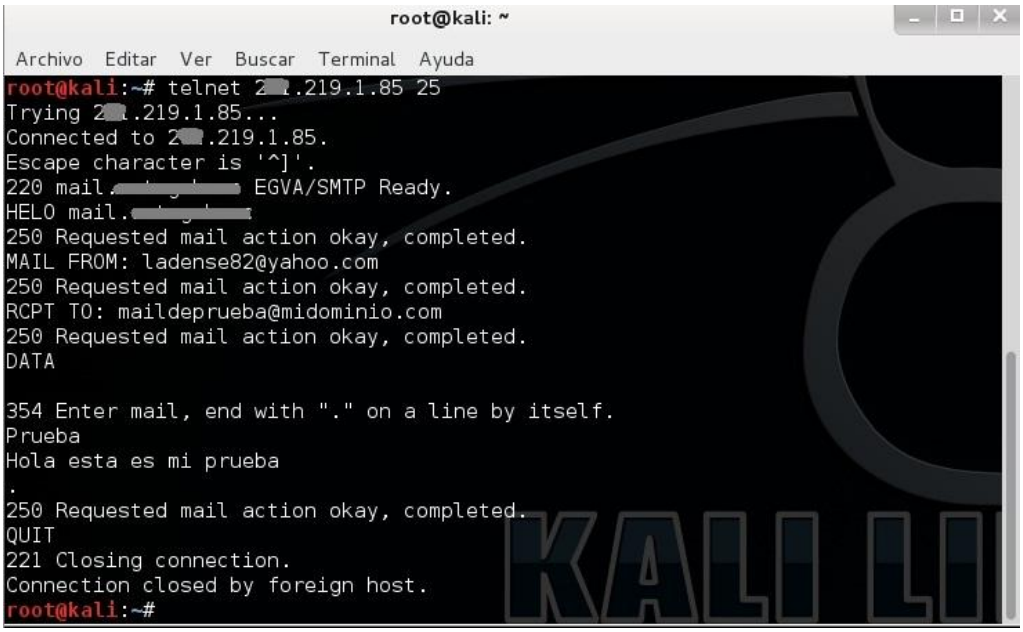


Figura 2.24 Telnet, envío de correo

Ahora con ayuda de la herramienta *Ethercap* se pueden realizar varias operaciones, entre ellas se realizó un escaneo de hosts y se logra capturar las mac address y descripciones/nombres de los equipos, figura 2.25.

Finalmente se realiza un ataque DoS(Denial of Service) a la intranet de la empresa cuya ip fue detectada en las fases anteriores, en la figura 2.26 se aprecia el resultado exitoso, el ataque fue detenido inmediatamente .

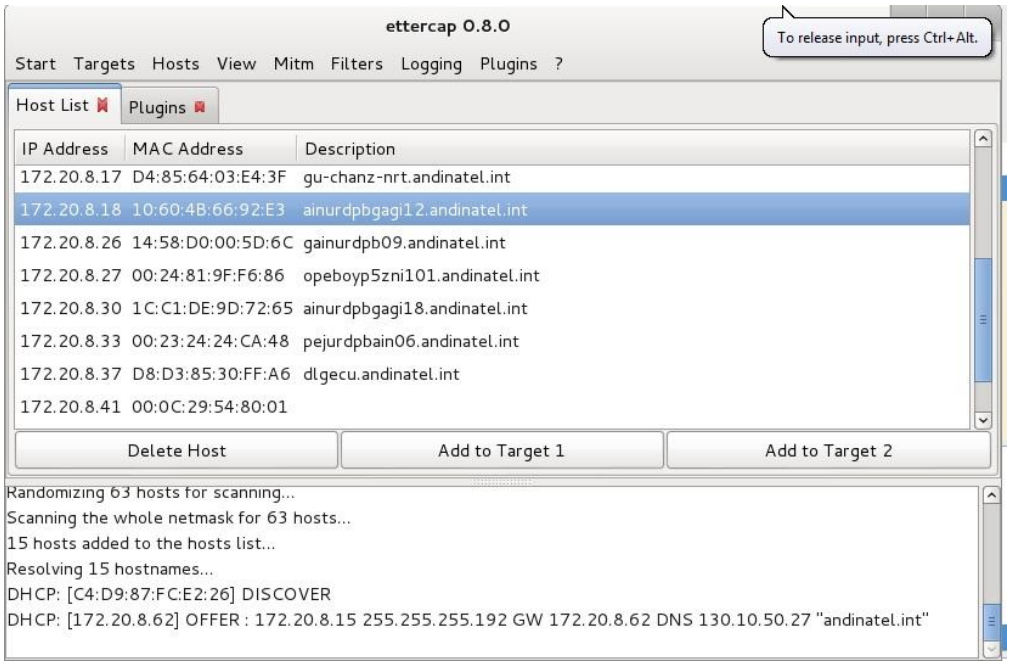


Figura 2.25 Ethercap, escaneo de hosts

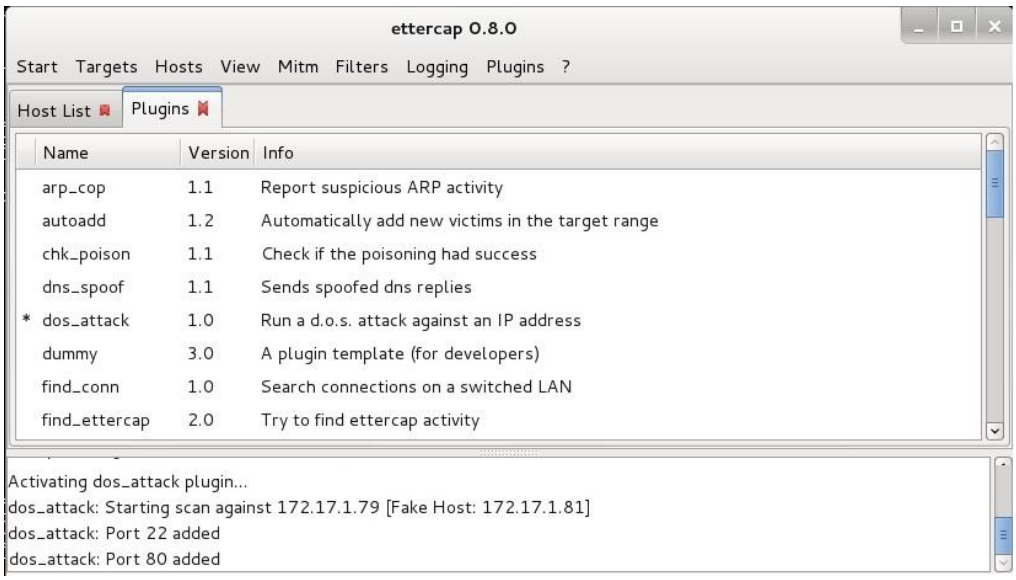


Figura 2.26 Ethercap, ataque DoS a intranet

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

La confidencialidad es la capacidad de un sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él. En este trabajo se analizaron cuatro vectores de ataques que puede comprometer la confidencialidad de la información según la siguiente tabla.

Tabla 3.1 Vectores de ataque a la confidencialidad

Confidencialidad	
Vector de ataque	**Resultado**
Recopilación de información	1
Escaneo de puertos	1
Acceso a la interfaz web de intranet	0
Acceso a la red	1

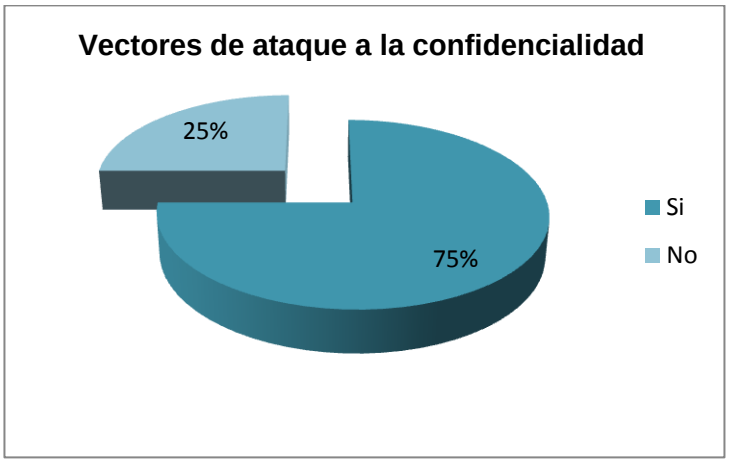


Figura 3.1 Vectores de ataque a la confidencialidad

La integridad, permite asegurar que la información no se ha alterado, es decir, que los datos recibidos son exactamente los que fueron enviados sin haberse producido ningún cambio o modificación. Existen 2 vectores de amenazas que pueden comprometer de alguna forma la integridad como se muestra en la siguiente tabla.

Tabla 3.2 Vectores de ataque a la integridad

Integridad	
Vector de ataque	**Resultado**
Edición de archivos de pcs	0
Manipulación de correos electrónico	1

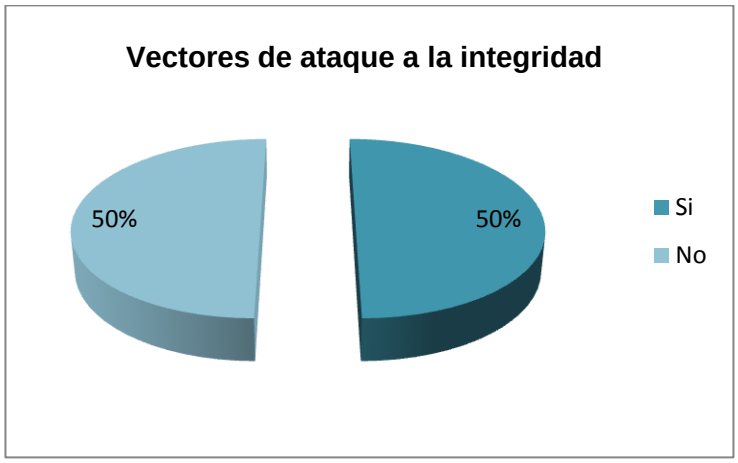


Figura 3.2 Vectores de ataque a la integridad

La disponibilidad es la característica de que un sistema se mantiene funcionando de forma eficiente y en caso de fallo es capaz de recuperarse rápidamente. Par el análisis se emplearon 2 vectores de ataques como se muestra a continuación.

Tabla 3.3 Vectores de ataque a la disponibilidad

Disponibilidad	
Vector de ataque	**Resultado**
Ataque DoS (denegación de servicios)	1
Autenticarse para acceso a intranet	0

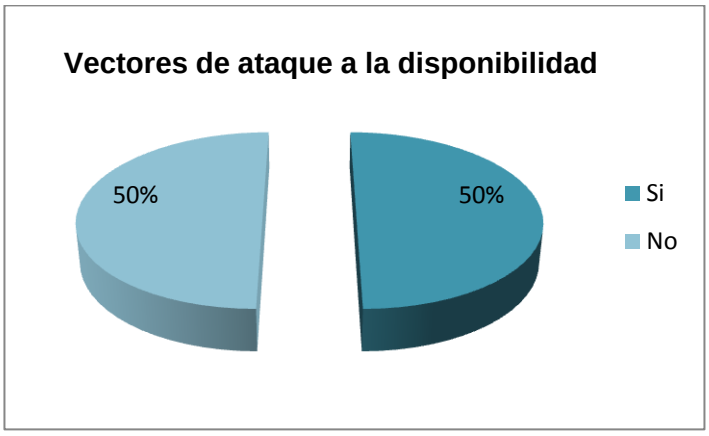


Figura 3.3 Vectores de ataque a la disponibilidad

Todos estos conceptos son conocidos como los principios básicos de la seguridad de la información, la correcta gestión de la seguridad de la información busca mantener y establecer programas y políticas que tengan como objetivo conservar la confidencialidad, integridad y disponibilidad, si alguna de éstas características fallara no se tendría un sistema seguro.

Una vez realizadas las fases del hacking ético en el capítulo anterior podemos descubrir que es muy factible violentar los principios básicos de la seguridad de la información lo cual es un aspecto muy serio para analizar y tomar así las debidas precauciones.

3.2 ANÁLISIS CUALITATIVO Y CUANTITATIVO

Para determinar la necesidad y estado actual de la seguridad de la información ante la elaboración de un hacking ético a la empresa se realizó un análisis cualitativo y cuantitativo basándose en los resultados obtenidos mediante los vectores de ataque realizados, se obtiene que existe un 75% de probabilidad de ataques que podrían poner en riesgo la confidencialidad de la información. Para el análisis de la integridad existe un 50% de porcentaje que indica que es factible realizar un ataque que posibilite alterar la información. Para el análisis de los ataques a la disponibilidad existe un 50% que afirma que es posible comprometer la funcionalidad del sistema.

3.4 INFORME DE AUDITORÍA

3.4.1 RESUMEN EJECUTIVO

Durante el proceso de Hacking Ético realizado para la empresa de Telecomunicaciones se pudieron encontrar vulnerabilidades de seguridad informática en algunos equipos evaluados con niveles de riesgo alto, medio y bajo.

Las vulnerabilidades con un riesgo alto se concentra principalmente en el servidor de correos ya que fue posible detectar la ip y haciendo uso de herramientas de

vulnerabilidades se pudo encontrar el sistema operativo que maneja, los puertos que tiene abiertos y un caso de open relay que podría permitir a un atacante enviar miles de correos y afectar el ancho de banda además de que alguien podría utilizar el servidor para enviar spam a través de él, esto podría ocasionar que las listas RBL incluyan estos mails entre los mal configurados y los emails legítimos que se envíen del servidor podrían quedar bloqueados.

Así mismo otra de las vulnerabilidades encontrados fue el ataque DoS a la página web de la intranet, lo que provocó una pérdida de la conectividad a la misma.

Como se puede visualizar en la tabla 3.4, se presentan las vulnerabilidades encontradas de forma general.

Tabla 3.4 Equipos auditados y puertos

IP	Equipo/ Servicio	Sistema operativo detectado	Puertos abiertos
2XX.219.1.85	Correo	Windows Server 2008 SP2	21,25,80,110,119,143,443,465,563, 587,993,995, otros
1XX.10.50.11	Firewall	-	22,80,256,259,264,443,444,900 otros
1XX.10.50.27	DNS	Microsoft Windows Server 2008 R2 SP1	53,88,135,139,389,427,445,464,593 ,636 otros
1XX.17.1.79	Intranet	Windows Server 2003 SP1	22,80,81,82,83,135,139,445,otros

Adicionalmente se localizó un servidor de aplicaciones dentro de la red interna, el cual presenta vulnerabilidades al permitirnos detectar los usuarios que tiene y los SID de éstos.

Como dato importante es necesario recalcar que en ningún momento se realizó una explotación que afecte de forma permanente y/o grave al funcionamiento de los equipos o servicios ya que el objetivo de este trabajo es señalar las vulnerabilidades para que se tomen las precauciones necesarias ante eventos de posibles ataques internos y/o externos.

3.4.2 BITÁCORA DE ACTIVIDADES

- Los análisis realizados se hicieron por medio de una laptop la cual fue ingresada y conectada a un punto de red de la empresa, la ip fue asignada automáticamente y no se requirió de más configuraciones.
- Se realizó la fase de footprinting o reconocimiento con ayuda de herramientas como Google, Nic EC, *nslookup*, Maltego, Visual IP Trace, Email Tracker Pro.
- Para la fase de Escaneo se utilizó herramientas como Net Scan, Nmap y Nessus, por medio de ellas se pudo detectar puertos abiertos, servicios activos, ip’s y vulnerabilidades latentes.
- En la fase de enumeración se usó *net view,* DumpSec y Hyena.

- Para la fase de explotación se usó Metasploit y Telnet, se hizo uso de módulos auxiliares.
- Además se hizo uso de las herramienta Ethercap con lo que se logró realizar una denegación de servicios.
- Se capturan pantallas de los resultados ante el uso de las herramientas mencionadas en los puntos anteriores.
- Se realiza un análisis de los resultados obtenidos y se registra los equipos detectados con el servicio que realizan, el sistema operativo funcional y los puertos abiertos.

3.4.3 RESUMEN DE HALLAZGOS

- Se pudo detectar por medio de Nic.ec registra información de contacto de la empresa, mails, nombres, teléfonos, direcciones y cargos desempeñados.
- Con *nslookup* se pudo detectar las ip's tanto del servidor de dominio como de correo, así mismo los nombres de éstos equipos, con ayuda de *Nmap* se detectaron puertos abiertos y versiones de sistemas operativos, así como el tipo de dispositivos escaneados y las vulnerabilidades con riesgos altos, medios y bajos del servidor de correo; además se confirmó el sistema operativo de los equipos.
- Con ayuda de *net view* se pudo establecer sesiones nulas, además con el uso de *Hyena* se detectó los usuarios del servidor de aplicaciones encontrado en

una subred interna y con ayuda de *Dumpsec* se pudo establecer cuáles son los usuarios y sus SID's en dicho servidor.

- En la explotación se halló que se puede realizar un envío masivo de correos desde el servidor SMTP, lo que podría causar un disparo en el consumo de ancho de banda [5] y a su vez colocar en listas negras a las direcciones del servidor lo que ocasionaría un bloqueo de salida de emails.
- Se pudo realizar una denegación de servicios con *Ethercap* en el acceso a la página web de la intranet de la empresa lo que causó que este recurso sea inaccesible a los usuarios.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. No se puede evitar de forma total que se realice un ataque de reconocimiento hacia la empresa víctima.
2. Los accesos hacia varios servicios y/o equipos no cuentan con las debidas seguridades lo que pone en riesgo un posible ataque.
3. No se cuenta con las políticas de seguridad adecuadas para salvaguardar la información y el acceso a ésta, las políticas existentes no se cumplen a cabalidad.
4. Al tener una vulnerabilidad de *open relay* el servidor SMTP presenta una amenaza ya que algún *spammer* podría aprovecharse de esto y enviar miles de correos no solicitados a costa de este recurso sin autenticación y hacia cualquier dominio SMTP, y con esto el ancho de banda podría sufrir un gran impacto y colocar en listas RBL a las direcciones del servidor bloqueando así su salida.
5. La página web de la Intranet presenta vulnerabilidad ante un ataque de denegación de servicios lo que permite a un atacante dejar sin conectividad o acceso a ésta, con esto se concluye que la misma no presenta seguridades a un ataque interno.

RECOMENDACIONES

1. Es recomendable hacer público solo lo que sea estrictamente necesario acerca de la empresa, por ejemplo para evitar ataques de reconocimiento se recomienda pagar por privacidad en los servicios de directorios como Who-Is, así mismo los servidores de correo, nombres, etc. deben estar en una zona desmilitarizada.
2. Un servidor solo debe tener instaladas las aplicaciones y servicios que sirven para el fin previsto de éste.
3. Se recomienda filtrar accesos a puertos no autorizados desde las subredes internas o desde internet por medio de configuraciones de reglas en los firewalls.
4. Se debe ejecutar análisis de vulnerabilidades y auditorías en equipos, sistemas operativos y servidores de forma continua para detectar posibles amenazas de seguridad y así poder tomar precaución y correcciones efectivas.
5. Se recomienda capacitar o dictar charlas preventivas a los trabajadores de las empresas sobre la seguridad de la información y los ataques de seguridad a los que se exponen.
6. Es recomendable hacer uso del hacking ético para detectar posibles vulnerabilidades en la intranet de la empresa ya que con esto se puede detectar fallas de seguridad y así se podrá brindar soluciones para evitar algún ataque de integridad o confidencialidad.

BIBLIOGRAFÍA

[1]. Astudillo, K. (2012). Hacking Ético 101, 11-12

[2]. Tori, C. (2008). Hacking Ético, 47.

[3]. Alonso, Ch. (2009). El lado del mal http://www.elladodelmal.com/2009/06/por-que-mis-correos-llegan-como-spam.html, fecha de publicación Junio 2009.

[4]. Aharoni, M. (2011). Metasploit Unleashed, Mastering the Framework, 8..

[5]. Open relay. Wikipedia, https://es.wikipedia.org/wiki/Open_Relay.