PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003 DE UNA EMPRESA DEL SECTOR FINANCIERO

ANDRÉS FERNANDO BENAVIDES ARIAS
JOHN FREDDY VELÁSQUEZ MAYORGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2015

PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003 DE UNA EMPRESA DEL SECTOR FINANCIERO

ANDRÉS FERNANDO BENAVIDES ARIAS
JOHN FREDDY VELÁSQUEZ MAYORGA

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director
FRANCISCO SOLARTE SOLARTE
Ingeniero de Sistemas, Mg. Docencia Universitaria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2015

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Medellín, 19 de septiembre de 2015

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El siguiente documento presenta el desarrollo de una prueba de Intrusión al sistema operativo Windows Server 2003 de una empresa del sector financiero. Se hace un recorrido teórico sobre temas del SO, ataques, metodologías de Intrusión y las herramientas que se utilizan en el test, junto con una demostración práctica.

El documento está organizado de la siguiente manera: del capítulo 1 al 3 presenta los preliminares de la investigación, en el capítulo 4 se muestra la metodología utilizada. El Capítulo 5 se describe el marco de referencia utilizado, en el capítulo 6 presenta el desarrollo de la investigación, en donde se encuentra la ejecución de las pruebas, finalmente en el capítulo 7 se presenta los resultados de la investigación.

Palabras Claves: *Pentest,* Prueba de intrusión, Windows Server 2003, metasploit

INTRODUCCIÓN

"*El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él.*"[1]

La frase anterior de Spafford, sugiere que no se puede hablar de "*Seguridad Informática*", sino más bien de "*Inseguridad Informática*". Todo sistema tiene una vulnerabilidad intrínseca, que se puede descubrir con los suficientes recursos de tiempo y dinero. No por esto, es necesario que las empresas apaguen sus servidores para estar más seguros. Lo que deben hacer es conocer las amenazas, vulnerabilidades y riesgos a los que están expuestas y gestionarlas, para encontrar el equilibrio entre el valor de la información que posee y la inversión que deben realizar para protegerla.

El Pentest o prueba de intrusión, se realiza para detectar aquellas vulnerabilidades desconocidas para la organización, antes de que un atacante las explote. La evaluación de seguridad se puede realizar a cualquier nivel, desde el entorno físico hasta las personas, pasando por las redes, los sistemas operativos, los sistemas de información, las aplicaciones web, etc. Debido a la amplitud que un Pentest puede tomar, en este proyecto se investigará y explotará mediante las herramientas de Kali Linux, las vulnerabilidades de mayor impacto del sistema operativo Windows Server 2003 que ejecuta la empresa SU CRETIDO SA,

---

[1] *Computer Recreations: Of Worms, Viruses and Core War. By A. K. Dewdney in Scientific American, March 1989. p. 110*

Una de las vulnerabilidades mejor documentadas es la **MS08-067,** la cual afecta a todas las versiones de Windows XP y Windows Server 2003 que no han recibido los últimos parches de seguridad. Al explotar dicha vulnerabilidad con herramientas como **Metasploit**, permite el control total del equipo afectado.

La mayoría de los documentos y video tutoriales disponibles en Internet, describen un ambiente simulado (VirtualBox, por ejemplo) para colocar el sistema Victima y el sistema Atacante. La presente propuesta se desarrolla con un Servidor real que ejecuta Windows Server 2003 Enterprise Edición en una dirección IP pública. Además de las actividades iniciales de una prueba de intrusión como el escaneo de la red, identificación de vulnerabilidades y explotación; que se encuentra en la mayoría de video tutoriales, se complementa con otras pruebas como la creación de un troyano, subirlo al sistema, adicionarlo al registro de arranque de Windows y limpieza de huellas.

1. DESCRIPCIÓN DEL PROBLEMA

La empresa SU CRETIDO SA, es una entidad financiera ubicada en la ciudad de Bucaramanga. Uno de sus servidores ejecuta Windows Server 2003 Enterprise Edición para compartir el acceso a internet y gestionar los usuarios mediante el servicio de Directorio Activo.

Con más de 10 años en operación, Microsoft ha anunciado que para Julio de 2015 terminará el soporte a Windows Server 2003[2]. Dejar de darle soporte significa, dejar de corregir los errores que se encuentren en el futuro; todas las máquinas que ejecuten esta versión serán más vulnerables, pues no habría un parche de seguridad por parte del fabricante.

Mientras se desarrollaba esta monografía, Microsoft publicó un boletín[3], sobre una nueva vulnerabilidad llamada MS14-064, la cual podría permitir ejecutar un código arbitrario. Según el informe, esta vulnerabilidad afecta a casi todas las versiones de Windows, desde Windows server 2003 hasta Windows 8.1, pasando por Windows Server 2008 y Windows Server 2012. Esto demuestra el peligro de mantener en operación un sistema operativo que pronto pasara a ser obsoleto.

Los administradores de IT de la empresa SU CRETIDO SA desconocían esta coyuntura y no tienen un plan de migración a una nueva versión del sistema

2 Microsoft. Lead the path to IT innovation today, 2014.

3 Microsoft. Microsoft Security Bulletin MS14-064 – Critical, 2015.

Windows Server u otra plataforma como Linux. Hasta ahora el servidor cumple con su función, por lo cual, creen que continuaran utilizando esta versión mientras analizan todos los detalles técnicos de cualquier cambio. En este momento, no se sabe si el servidor es vulnerable a las nuevas amenazas comentadas o las ya existentes. De Igual manera, se desconoce el impacto que pudiera tener para la organización si un atacante tuviera éxito al explotar una vulnerabilidad. La empresa nunca ha contratado una prueba de intrusión para evaluar la seguridad de sus sistemas. Las consecuencias de tener un servidor vulnerable, bien sea por falta de actualizaciones o configuraciones débiles (por defecto), pueden incluir acceso no autorizado, infección de malware, daño o robo de información, desprestigio, implicaciones legales por violación de protección de datos personales, entre otras.

El lector se puede sentir motivado a utilizar la información suministrada en esta investigación, para realizar estas pruebas contra cualquier sistema, por lo cual, se hace necesario investigar el marco legal para conocer quién y bajo qué circunstancias puede realizar una prueba de intrusión.

1.1 FORMULACIÓN DEL PROBLEMA

¿Presenta el Servidor (Windows Server 2003) de la empresa SU CRETIDO SA alguna vulnerabilidad que permita una intrusión en el sistema; y de ser así, con qué herramientas se pueden identificar y explotar, y a que información se podría acceder?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar una prueba de intrusión al servidor de la empresa SU CRETIDO SA, mediante las herramientas de Kali Linux y la aplicación de una metodología de intrusión, para determinar si es posible acceder información confidencial almacenada en el servidor.

2.2 OBJETIVOS ESPECÍFICOS

- Recolectar y analizar información sobre el Sistema Operativo Windows Server 2003 (licencia, servicios y vulnerabilidades), herramientas de seguridad de Kali Linux (tipo, manejo, comandos, configuración, entre otras) y metodologías de intrusión.
- Elaborar y ejecutar un plan de pruebas que permita determinar las actividades a seguir y las herramientas de Kali Linux a utilizar, para lograr una intrusión al Servidor y acceder a posible información confidencial que contenga.
- Analizar los resultados obtenidos de la prueba de intrusión para elaborar y presentar un informe ejecutivo a la empresa SU CRETIDO SA.

3. JUSTIFICACIÓN

Con la realización de este proyecto, la empresa SU CRETIDO SA podrá conocer cuáles son las vulnerabilidades del sistema operativo Windows Server 2003 y los tipos de ataque que puede recibir para determinar si su servidor se ve afectado o no. Los administradores del sistema podrán conocer la metodología y las herramientas utilizadas, para que la apliquen periódicamente sobre el servidor; además la puede extender a otros servidores y equipos de los clientes. Los usuarios del sistema podrán empezar a aplicar una cultura de la seguridad.

Aunque no se tiene un estudio del número exacto de servidores que ejecutan Windows Server 2003, se cree que este tiene una cuota importante debido a su popularidad y sencillez. Muchas empresas pueden estar en la misma situación que SU CRETIDO SA. En este sentido, el proyecto es importante porque ayuda a divulgar el peligro de mantener en operación Windows Server 2003, además ayuda a los administradores a tomar una decisión, si continuar utilizando esta versión, aceptando los riesgos; o actualizarse a una versión más reciente u otra plataforma.

La seguridad de un sistema no solamente radica en que las aplicaciones y servicios estén actualizados, sino también en tener planes de acción en caso de que se materialice un riesgo. Conocer las vulnerabilidades y su impacto puede ser el insumo para crear planes de contingencia, políticas de continuidad de negocio, de copias de seguridad, entre otros.

Con este proyecto se pueden poner en práctica conceptos de seguridad en Sistemas Operativos y Redes. Los paso a paso de las herramientas utilizadas, pueden ser de gran utilidad para todos los interesados en Seguridad Informática.

4. METODOLOGÍA

4.1 METODOLOGÍA DE INVESTIGACIÓN

El enfoque de la investigación es teórico-práctico, aplicando una metodología cuantitativa, cuasi experimental o descriptiva. Cuantitativa porque se pretende hacer una medición de la seguridad del Servidor, teniendo en cuenta el porcentaje de vulnerabilidades no corregidas del total vulnerabilidades conocidas de Windows Server 2003. Cuasi experimental porque se van a utilizar y a probar diferentes herramientas de escaneo, análisis de vulnerabilidades y de exploits contra el servidor. Descriptiva porque se pretende describir las pruebas, el proceso y los resultados de las mismas.

Técnicas de recolección de información:

- Fuentes primarias: Entrevistas con el administrador del sistema de la empresa y de otras organizaciones. Consultas a expertos en seguridad informática de Colombia y el exterior.
- Fuentes secundarias: Consulta a base de datos especializadas como CVE – Common Vulnerabilities and Exposures, manuales del sistema operativo, libros y otras investigaciones.

4.2 METODOLOGÍA DE DESARROLLO

Para lograr los objetivos de la investigación se proponen las siguientes actividades:

- Utilizar el buscador Google para descargar documentos, videos y herramientas sobre el Sistema Operativo Windows Server 2003 y Kali Linux.
- Realizar entrevistas a los administradores de la empresa, acerca de aplicaciones que ejecuta el Servidor y la infraestructura tecnológica en general.
- Crear un ambiente de pruebas dentro de la empresa que contenga una copia delos programas y servicios instalados en el Servidor a analizar.
- Descargar, Instalar y configurar herramientas de seguridad informática como Kali Linux y Nessus.
- Adaptar una metodología de intrusión para planear las actividades a seguir y las herramientas de Kali a utilizar, teniendo en cuenta la información recopilada anteriormente.
- Utilizar las herramientas y sus opciones según el plan de pruebas anterior, documentando todo el proceso y los resultados obtenidos.
- Realizar las interacciones que sean necesarias con los administradores del sistema, hasta lograr identificar una vulnerabilidad que permita penetrar en el sistema.
- Elaborar un informe ejecutivo a la empresa SU CRETIDO SA de los resultados obtenidos.

5. MARCO REFERENCIAL

5.1 MARCO CONTEXTUAL

SU CRÉDITO SA es una empresa dedicada a la prestación de servicios de recaudo de cartera, verificación de solicitudes de crédito, investigación de bienes, tele mercadeo y actualización de bases de datos para organizaciones públicas o privadas, naturales o jurídicas.

5.1.1 Reseña histórica. SU CRÉDITO SA inicia operaciones en el año 1993 en la ciudad de Bucaramanga, inicia ofreciendo su servicio de recaudo de cartera a la empresa CERGO y posteriormente a GECOLSA del Banco SUDAMERIS. Actualmente SU CRÉDITO SA es una empresa orgullosamente Santandereana con más de 20 años de experiencia en el mercado de cobranza y Call center, acredita la idoneidad y suficiente experiencia en los servicios que ofrece. Durante todo este tiempo de trabajo, SU CRÉDITO SA ha ofrecido sus servicios a los siguientes clientes a saber: BBVA de Colombia, Banco Agrario de Colombia, Banco Citibank de Colombia, Banco Caja Social Colmena, Fondo Nacional de Ahorro, Banco de Occidente, Financiera COMULTRASAN, Banco AV Villas, Banco Davivienda, Banco Gran Ahorrar, Colombia Telecomunicaciones S.A, Telefónica Móviles de Colombia, EBEL, entre otros.

5.1.2 Misión. Su Crédito S.A. es una empresa dispuesta a intermediar en el mercado financiero a través de la prestación de los servicios de administración y recuperación de cartera, CALL & Contact Center, Tele mercadeo, Verificación solicitudes de crédito, para empresas públicas o privadas, naturales o jurídicas. Contando con tecnología de punta en sistemas de información, redes y medios de comunicación e infraestructura, personal altamente motivado y capacitado que

permite obtener rentabilidad financiera y bienestar humano, proyectando a sus clientes confianza, solidez y efectividad.

5.1.3 Visión. Para el año 2015 Su Crédito S.A se proyecta como empresa líder en el mercado en el ámbito regional por su compromiso continuado en la calidad de los servicios ofrecidos y la satisfacción plena en las necesidades del cliente. Logrando así un mayor posicionamiento en el mercado, estabilidad financiera y mejoramiento continuo de los procesos y el capital humano.

5.1.4 Servicios. Los Servicios que ofrece SU CREDITO SA son:

- Recuperación de cartera y de cobro de cartera en las etapas preventiva, administrativa, pre jurídico y castigado.
- Verificación de solicitudes, proceso de validación y/o confirmación de datos básicos y referencias. Comprende además el proceso de informes escritos sobre los resultados obtenidos e inconsistencias encontradas.
- Localización de clientes, gestión de ubicación a través de llamadas en teléfonos registrados en el software de base de datos o demás buscadores virtuales a los cuales el asesor puede acceder a información del solicitante y del Aval.
- Tele Contacto, proceso de contacto telefónico con el cliente recordándole la fecha y el valor a cancelar, verificación puntual de entrega del extracto y actualización de datos.
- Investigación de bienes, Localización cierta y comprobable de los titulares del crédito y de una investigación formal, exhaustiva y confirmada de los bienes e ingresos de los titulares de las obligaciones.
- Tele Mercadeo, proceso de venta telefónica de productos y servicios. Permite contacto instantáneo, en vivo y bidireccional entre el proveedor y el consumidor.

- Visitas domiciliarias, ejecución de visitas a la residencia o sitios de trabajo del deudor, buscando contacto directo, promesas de pago y en caso de no encontrar al titular indagar información de ubicación del mismo.

En la actualidad SU CRÉDITO SA posee 72 empleados de los cuales 59 personas cuentan con puesto de trabajo los cuales constan de equipos equipados con sistema operativo Windows XP debidamente licenciado junto con Office 2007 para el manejo de tareas de oficina, cuenta además con un sistema de gestión el cual se utiliza para llevar registro de los contactos que se realizan vía telefónica con el cliente, ingresando información relevante de las gestiones realizadas por cada uno de los empleados. El servidor de llamadas hace parte de los procesos llevados a diario por los empleados, este es configurado en los equipos mediante un software de telefonía llamado Zoiper – Softphone el cual se encarga de asignar a cada usuario una extensión telefónica para el manejo de las llamadas, dejando almacenado los audios de las llamadas.

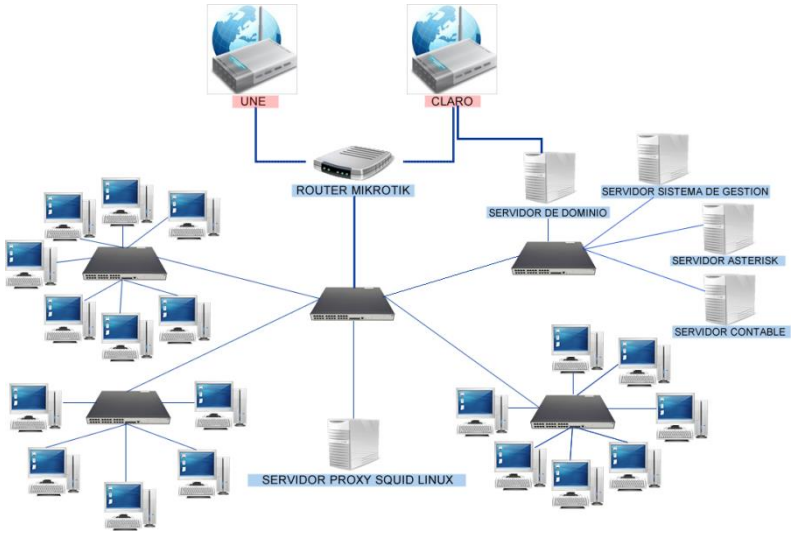
La empresa cuenta con un servidor contable utilizado por el departamento de finanzas para el reporte de los movimientos de dinero que se realizan, así como también de los registros de inventario de los activos. En el servidor de directorio se encuentran cada uno de los usuarios que hacen uso del sistema, por otra parte posee directivas de seguridad para el manejo de contraseñas, accesos restringidos según el tipo de usuario, entre otras políticas de seguridad que buscan garantizar la seguridad de la empresa. Además del servicio de directorio activo, brinda el servicio de internet, el cual, propaga a todos los equipos conectados al dominio que tengan como puerta de enlace la IP de dicho servidor.

La topología de red utilizada es de estrella, tal como se observa en la siguiente gráfica. Las estaciones de trabajo se encuentran conectadas a un conmutador central, por el cual transitan los paquetes de los usuarios, manteniendo el servicio

disponible. Si alguna maquina falla, no afecta el servicio de las demás conectadas al mismo switch. El servicio de internet lo provee dos empresas las cuales son UNE y Telmex (CLARO) de fibra óptica, el primero es de 80 Mbps y el segundo de 30 Mbps, siendo el segundo backup del primero en caso de este fallar.

El cuarto de sistemas posee dos racks, una UPS de 10kva, dos reguladores de voltaje y circuito cerrado de cámaras. El acceso es a través de un sistema biométrico, al cual puede acceder únicamente el personal de sistemas y gerencia. Existe una bitácora de ingreso al departamento de sistemas en el cual se registra el personal que ingresa por algún motivo de mantenimiento o de auditoría externa.

Figura 1. Mapa de red de SU CREDITO SA**.**

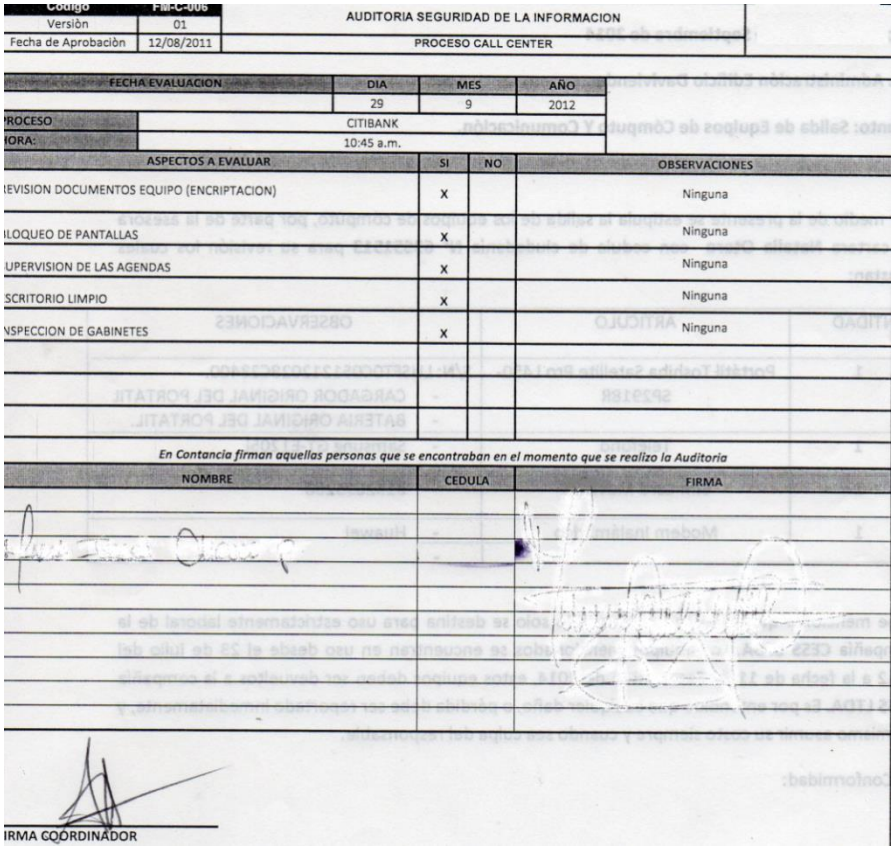


Fuente: Los Autores

La topología estrella de la red, posee un switch capa 2 HP no administrable con cable patch cord categoría 5e debidamente marcados según cada punto de trabajo.

En estos momentos, los controles de seguridad son mediante un formato de lista de chequeo, el cual evalúa sólo ciertos elementos de seguridad y no realiza una inspección a fondo, entre los elementos que evalúan están, escritorio limpio, acceso a páginas de internet no autorizadas, configuración del proxy en el navegador, bloqueo de puertos USB, tal como se observa en el siguiente formato.

Figura 2. Formato de Lista de Chequeo de una Auditoria de Seguridad.



Codigo	FIAFC-006	AUDITORIA SEGURIDAD DE LA INFORMACION
Versiòn	01	
Fecha de Aprobaciòn	12/08/2011	PROCESO CALL CENTER

FECHA EVALUACION	DIA	MES	AÑO
	29	9	2012
PROCESO	CITIBANK		
HORA:	10:45 a.m.		

ASPECTOS A EVALUAR	SI	NO	OBSERVACIONES
REVISION DOCUMENTOS EQUIPO (ENCRIPTACION)	X		Ninguna
BLOQUEO DE PANTALLAS	X		Ninguna
SUPERVISION DE LAS AGENDAS	X		Ninguna
ESCRITORIO LIMPIO	X		Ninguna
INSPECCION DE GABINETES	X		Ninguna

En Contancia firman aquellas personas que se encontraban en el momento que se realizo la Auditoria

NOMBRE	CEDULA	FIRMA

FIRMA COORDINADOR

Fuente: Su Crédito S.A.

5.2 ANTECEDENTES DE INVESTIGACIÓN.

La seguridad informática juega un papel importante en la actualidad en el manejo de la información, por esta razón se hace necesaria la investigación de diferentes entornos en los cuales se haya implementado sistemas de seguridad, que por medio del uso de herramientas de penetración, permitan detectar riesgos y vulnerabilidades a las cuales se encuentran expuestos los sistemas, con el fin de garantizar la disponibilidad, confidencialidad e integridad de los datos.

La recopilación de antecedentes tiene por objetivo, conocer los temas que son utilizados por los investigadores en el desarrollo de mecanismos de seguridad informática, basándose en herramientas de escaneo de vulnerabilidades propias de Linux, las cuales permiten a partir de la detección, crear recomendaciones que sirvan de salvavidas ante situaciones donde la información se encuentre en riesgo.

Los análisis de riesgos y recomendaciones de seguridad forman parte de los mecanismos usados para mantener a salvo la información, los ingenieros Henry Bastidas, Iván López y Hernando Peña (2014), de la Universidad Nacional Abierta y a Distancia, a través de la tesis “Análisis de Riesgos y Recomendaciones de Seguridad de la Información al Área de Información y Tecnología del hospital Susana López de Valencia de la ciudad de Popayán”, tiene por objetivo mejorar los niveles de seguridad informática mediante el análisis y evaluación de riesgos de seguridad informática; el análisis a este documento permitirá conocer las herramientas empleadas en la realización de análisis de vulnerabilidades y ethical hacking a través de resultados ilustrados que se presentan; expone asimismo un resumen detallado de las amenazas y riesgos encontrados durante la ejecución de las pruebas en la entidad pública, la cual alberga gran cantidad de información sensible de pacientes y empleados, la cual por ningún motivo puede ser revelada o caer en manos de un atacante, por ultimo presenta un informe de las

recomendaciones que permitan mitigar o reducir al máximo cada uno de los riesgos y vulnerabilidades descubiertos.

El análisis y gestión de riesgo se realiza para para entender cómo mejorar la protección de la información, la ingeniera Hina Garavito (2015), de la Universidad Nacional Abierta y a Distancia, a través de la tesis “Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, Enfocado en un Sistema de Seguridad de la Información”, tiene por objetivo la ejecución de un análisis de seguridad informática que permita establecer los tipos de riesgos a los cuales están expuestos los sistemas de información misional, es de ayuda conocer las diferentes herramientas empleadas durante el proceso de recolección de vulnerabilidades, así como también los resultados obtenidos una vez ejecutados cada uno de los escaneos; el documento demuestra el nivel de vulnerabilidad que posee la información de la entidad pública, por medio de pruebas de ethical hacking. Una vez terminado el proceso de análisis y evaluación de riesgos mediante MAGERIT, se proponen controles que sirvan de mecanismos de corrección y prevención ante nuevos ataques informáticos.

Conocer de antemano las herramientas y comandos para evaluar la seguridad informática es de vital importancia, los ingenieros Jesús Cifuentes y Cesar Narváez (2004), de la Universidad del Valle, a través de la tesis “Manual de Detección de Vulnerabilidades de Sistemas Operativos Linux y Unix en Redes TCP/IP”, tienen por objetivo dar a conocer definiciones de conceptos básicos de redes y sistemas operativos, además de los diferentes mecanismos de seguridad existentes que permitan blindar la información y mantenerla segura ante posibles ataques informáticos, es de importancia como antecedente puesto que permite aclarar diversos conceptos en temas de ataques y vulnerabilidades y en seguridad a nivel servidor, los cuales permitirán comprender a fondo la importancia que tiene

cada uno de los comandos mencionados en la evaluación de la seguridad de sistemas de información.

El ingeniero Andrés Cárdenas (2011), de la Universidad Carlos III de Madrid, a través de la tesis “Desarrollo de un Entorno para Prácticas de Seguridad Informática”, establece como objetivo la creación de un entorno para la ejecución de exploits, este proyecto es de gran ayuda para la creación de ambientes que no afecten a los sistemas y permitan dar vía libre a la ejecución de diferentes exploits para aprovechar las vulnerabilidades de un sistema y así lograr el objetivo establecido, permite conocer a fondo las diferentes herramientas de seguridad.

5.3 MARCO CONCEPTUAL.

Sistema operativo: “Es un conjunto de programas que gestionan los recursos del sistema, optimizan su uso y resuelven conflictos.”[4].

Vulnerabilidad: “Es un agujero de seguridad en una pieza de software, hardware o sistema operativo, que proporciona un potencial ángulo de ataque a un sistema. Una vulnerabilidad puede ser tan simple como una contraseña débil o tan compleja como un buffer overflow o una inyección de SQL”[5]. Como menciona

4 CANDELA, G. Fundamentos de Sistemas Operativos. Teoría y ejercicios resueltos, 2007.

5 KIRSCH, C. Introduction to Operating System, 2013.

Carlos Santana[6], desde la seguridad informática se establece como vulnerabilidad a toda debilidad de un sistema que afecte su integridad, disponibilidad e integridad.

Exploit: Es un pequeño programa especializado, que toma ventaja de una vulnerabilidad y provee un acceso al sistema.

Payload: Es una pieza de software que permite controlar un sistema después de ser explotado, típicamente se adjunta con el exploit, para garantizar el acceso al sistema a un atacante.

Amenaza: Son agentes que poseen la cualidad de aprovechar una debilidad o vulnerabilidad para llevar a cabo un acto que afecte a un sistema. Las amenazas son directamente proporcionales a las falencias que tenga un sistema, si este posee grandes debilidades en su modo de operar o diseño, las amenazas serán altas y tendrán un gran impacto en el mismo.

Como menciona Araujo[7], las amenazas se clasifican en:

6 SANTANA, C. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?, 2012.

7 ARAUJO, J. Amenazas Informáticas, 2011.

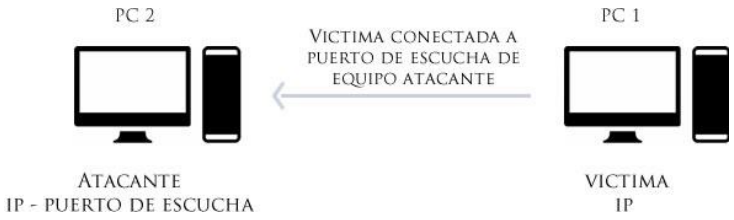
- Intencionales: Son actos realizados con conocimiento previo de las consecuencias que estas tendrán, entre las que se encuentran, sabotaje, atentados informáticos, ejecución de códigos maliciosos, robos de información, espionaje, entre otros.
- Involuntarias: Son realizados sin conocimiento de las repercusiones de los actos, entre los que se encuentran, revelación de información, descarga o propagación de archivos infectados sin conocimiento, alteraciones al sistema por parte de personas inexpertas, entre otros.
- Naturales: Son situaciones fortuitas que se llevan a cabo de repente y que afectan el buen funcionamiento de los sistemas, inclusive a la propia información allí almacenada. Entre estas se encuentran, catástrofes naturales, incendios naturales, inundaciones, entre otras.

Ataque: Intento de una persona o grupo organizado de acceder a un sistema aprovechando la debilidad o falla de un sistema, hardware o del personal, a través de diferentes métodos existentes de ataque. La principal razón de la ejecución de ataques suele ser el factor económico seguido por el espionaje y saboteo, siendo las principales víctimas empresas reconocidas a las cuales el atacante informático pueda obtener algún tipo de beneficio.

Pruebas de Intrusión: Son herramientas ejecutadas en un ambiente real con el fin de medir la protección con que cuenta una organización. Las pruebas de intrusión o Pentest permiten detectar fallas en el sistema de seguridad que pueden resultar catastróficas si son explotados por atacantes informáticos. Para la ejecución de las pruebas de intrusión es necesario contar con el aval de la empresa a la cual se desea probar su sistema de seguridad de información, pues estas pruebas podrían acarrear daños al sistema por los diferentes métodos que se emplean para probar la seguridad y son consideradas ilegales si se realizan sin previa autorización.

Reverse TCP: Modalidad de ataque donde el equipo destino (PC 2) se comunica con la maquina atacante (PC 1) a través de un puerto de escucha que recibe la conexión y permite ejecutar los diferentes comandos de ataque. Ver Figura 3.

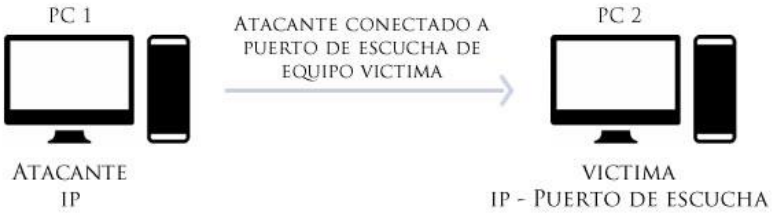
Figura 3. Tipo de conexión Reverse TCP.



Fuente: Los autores.

Bind TCP: Tipo de ataque donde por medio de un puerto abierto en el equipo víctima (PC 2) se realiza una conexión entrante, permitiendo la ejecución de código y sentencias de comandos por parte del atacante (PC 1). Ver Figura 4.

Figura 4. Tipo de conexión Bind TCP



Fuente: Los autores.

PTE: Pruebas de penetración estándar.

Caja Blanca: Son pruebas realizadas en el interior del sistema, conociendo con anterioridad aspectos relevantes que permitan recorrer cada una de las posibles rutas de los procesos llevados a cabo por el sistema, evaluando los bucles del sistema siendo verdaderas o falsas las condiciones, con el fin de poder conocer ambas partes de los procesos y validar que estas cumplan con lo establecido en su diseño.

Caja Negra: Hace referencia a las pruebas que se realizan desconociendo el funcionamiento interno del sistema pero sabiendo sus entradas y salidas, de allí se procede a probar de acuerdo al diseño si este cumple con lo establecido, y levantar registro de los problemas que se evidencien o resultados no esperados. Las pruebas de caja negra se diferencia de caja blanca por desconocer de antemano el funcionamiento del sistema, esto se debe en algunas ocasiones a la complejidad del sistema que se está estudiando, o a la poca información proporcionada por los dueños del sistema.

Caja Gris: Corresponde al punto intermedio de caja negra y caja blanca, se conoce parte del código y funcionamiento de este, además de conocer las salidas el sistema y entradas a manera general. Para llevar a cabo el proceso de caja gris es necesario tener el acceso necesario con los permisos correspondientes para que las pruebas sean sobre un ambiente casi real y se asemeje a los procesos realizados por los usuarios del sistema, “el equipo de pruebas debe ser dotado

con los privilegios adecuados a nivel de usuario y una cuenta de usuario, además de permitirle acceso a la red interna”[8].

5.4 MARCO TEÓRICO

5.4.1 Sistema operativo Windows Server 2003. Microsoft, lo describe como “La pieza fundamental de Microsoft Windows Server System. Se basa en los sólidos fundamentos de Windows 2000 Server y, como en el caso de su predecesor, Microsoft hace un esfuerzo decidido por mejorar la fiabilidad, escalabilidad, rendimiento y facilidad de uso y administración, factores todos ellos relevantes por sí solos, pero que al producirse juntos dentro del mismo producto, reducen drásticamente el coste total de propiedad (TCO) de las infraestructuras informáticas en toda clase de instalaciones, desde las más sencillas (con uno o unos pocos servidores) a las más complejas, compuestas de centenares de servidores en configuraciones de redes distribuidas o grandes Centros de Cálculo con sistemas en clúster y Datacenter.”9 (Información sobre el producto Windows Server 2003, 2006). Entre los servicios que pueden configurarse se encuentra.

8 CABALLERO, A. Hacking con Kali Linux, 2015.

9 Microsoft. Introducción Windows Server 2003, 2006

5.4.1.1 Servicios de Windows Server 2003. Microsoft[10] Los servicios de Windows Server son los siguientes:

- **Servidor de Archivos.** "Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, como un plan de proyecto, podrán tener acceso al archivo del servidor de archivos en lugar de tener que pasarlo entre distintos equipos"[11]. La información es el activo más importante de toda organización, es por esto la importancia de almacenar estos archivos en un sitio que garantice su integridad, confidencialidad y disponibilidad. Una de las ventajas del servidor de archivos es que al encontrarse centralizada la información, esta puede ser compartida asignando permisos de seguridad individuales o totales de los archivos, garantizando que sólo los usuarios con privilegios tengan permisos de escritura, modificación o eliminación.
- **Servidor de impresión:** Brinda la posibilidad de tener en red dispositivos de impresión instalados y configurados para uso local y en internet mediante el uso de MMC (Microsoft Management Console) que emplea Windows. Además

10 Microsoft. Introducción Windows Server 2003. Introducción a la familia de productos, 2006.

11 Microsoft. Microsoft Developer Network. Función de servidor de archivos, 2005.

de compartir impresoras, facilita la administración de estas, permitiendo monitoreo de colas de impresión, reparando fallas en driver o cabezales que podrían llegar a ser requeridas para el mantenimiento de estas. Una vez configurada mediante la línea guiada de instalación de esta función, los usuarios de red podrán hacer uso de los dispositivos que allí se encuentren y ejecutar desde sus puestos de trabajo impresiones que el servidor se encargará de ejecutar a medida que se realicen las peticiones. Mediante el servicio LDP, Windows permite que sistemas operativos de Linux puedan acceder y hacer uso de las impresoras instaladas en el servidor de impresión, lo que permite que todos los equipos de una red Windows y Linux puedan usar este servicio conjuntamente.

- **Servidor de aplicaciones (IIS, ASP.NET):** Mediante el servidor de aplicaciones implementas de Windows Server 2003, permite la agrupación de conexiones de BD y de objetos, proporcionando las tecnologías para trabajar con servicios web de XML. Además permite el acceso a objetos de la organización mediante interfaces de servicios web. Este lenguaje de programación propio de Windows permite a los desarrolladores hacer implementación de sus aplicación es las cuales estarán disponibles a cada uno de los usuarios de la red. Otros de los servicios que brinda el servidor de aplicaciones, es la administración de transacciones distribuidas y la seguridad que implementa.
- **Servidor de correo (POP3, SMTP):** A través de esta función se permite la configuración de correo electrónico el cual se alojará en el servidor y estará disponible a los usuarios de la red que lo requieran. Emplea el servicio POP3 para la recuperación de correo y el servicio SMTP que se encarga de la transferencia rápida al receptor. El servicio SMTP cuenta con la falencia de no poder garantizar que el correo enviado a una cuenta de correo electrónico sea realmente del remitente que lo realiza. La configuración de las cuentas de correo puede realizarse de manera manual o de manera rápida, la cual solo se

requiere el nombre de la cuenta de correo y la contraseña de esta. Windows permite configurar que los correos sean descargados del servidor, o que se deje una copia en el servidor a través de IMAP o POP3. Los correos almacenados en el servidor con extensión .PST permiten tener una copia de seguridad, la cual puede ser restaurada en una nueva cuenta de correo que se mostrará como carpeta de archivos.

- **Terminal Server:** Esta función permite el acceso remoto al servidor como si se estuviera trabajando directamente en él, entre las tareas que se pueden realizar se encuentra, la ejecución de programas, modificación de archivos, y uso de los recursos de la red. Este servicio permite que si una aplicación se configura, todos los usuarios tengan la misma versión, impidiendo que ocurran problemas de compatibilidad en las extensiones de los archivos guardados. En otras de sus funciones está la de almacenamiento de archivos y uso de recursos de la red remotamente.
- **Servidor de dominio (Active Directory):** El directorio activo permite la creación de usuarios, los cuales pueden ser ordenados mediante la creación de carpetas contenedoras y asignarles permisos de administrador o de usuario estándar. Esta función va acompañada de cada una de las GPO que se crean para controlar opciones como la estructura de la contraseña a utilizar, capacidad de almacenamiento de contraseñas, periodo de caducidad, y todas las directivas de grupo que se creen, pueden ser asignadas a los usuarios que se creen en el directorio Activo. La creación de cuentas de usuario permite tener un orden de los usuarios que puedan acceder a los puestos de trabajo, permitiendo crear restricciones a las opciones del sistema operativo, restringiendo la modificación de configuraciones del sistema, hasta el acceso de internet a través de ISA Server, las cuales pueden ser asignadas a los usuarios que existan en el servidor de dominio.
- **Servidor DNS:** Mediante la configuración de esta función se traducirá los nombres de los equipos de la red en direcciones IP, las cuales facilitará tareas

entre usuarios, como compartir archivos o accesos remotos de máquinas. Es un sistema de nomenclatura jerárquica que resuelve a través de una amplia base de datos los nombres de cada equipo, haciendo más fácil reconocer que equipos se encuentran conectados a una red. Su característica principal es la traducción de nombres a direcciones IP, que permita a los usuarios de la red realizar tareas más rápidamente entre equipos, esto es una gran ayuda, pues resultaría complejo y tomaría tiempo realizarlas con las direcciones IP de cada máquina.

- **Servidor DHCP:** Este protocolo de configuración dinámica de host asigna automáticamente direcciones IP en un dominio, sin necesidad de realizarlo manualmente. Al realizar la configuración, se establece el rango de IP que se podrán utilizar al momento de conectar una maquina con IP automática en su configuración. El servidor DHCP trabaja de la siguiente manera, una maquina se conecta a un dominio configurado en Windows Server, este atiende la petición y asigna una IP que se encuentre en el rango DHCP configurado para que el computador pueda realizar tareas en la red, como acceder a carpetas compartidas, accesos remotos, navegación LAN o navegación a internet.
- **Servidor de multimedia de transmisión por secuencias:** Brinda la posibilidad de compartir contenido de audio y video con usuarios de la red, como videos empresariales o de capacitación por ejemplo; basta con tener una maquina conectada a la red que tenga un reproductor con las características de reproducción de Windows para poder ejecutar el contenido multimedia, o simplemente aplicaciones desarrolladas a la medida. Dichas presentaciones almacenadas en el servidor puede ser transmitida vía internet o intranet.
- **Servidor WINS:** La función del servidor WINS, es asignar dinámicamente direcciones IP a nombres de equipos, en caso de que se requiera manejar conexiones mediante el nombre de equipos en vez de direcciones IP, para esto es necesario configurar el servidor WINS, una vez configurado se podrá tener acceso a los recursos mediante el nombre del equipo.

5.4.1.2 Vulnerabilidades de Windows server 2003. Microsoft dispone de un sitio web, donde realiza publicaciones periódicas de las vulnerabilidades descubiertas en todo el software de Microsoft, llamado Boletines de Seguridad.

Las vulnerabilidades son codificadas en un formato **MSAA-XXX,** Donde **AA** es el año de la publicación y **XXX** es un número consecutivo. De este modo, se puede consultar desde el año 2005 hasta el mes actual. Cada boletín contiene un resumen ejecutivo de los problemas que se corrigen, el software afectado, una clasificación de la severidad, el impacto, entre otros datos de interés. Microsoft Clasifica la severidad de una vulnerabilidad en:

Tabla 1. Clasificación de la Severidad de una Vulnerabilidad según Microsoft.

VALORACIÓN	DEFINICIÓN
Crítico	Vulnerabilidad que podría dar lugar a la propagación de un gusano de Internet si no interviene el usuario.
Importante	Vulnerabilidad que podría poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios; o bien la integridad o disponibilidad de los recursos de procesamiento.
Moderado	La explotabilidad podría reducirse en gran medida a través de diversos factores, como una configuración predeterminada, auditoría o dificultad para aprovechar la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

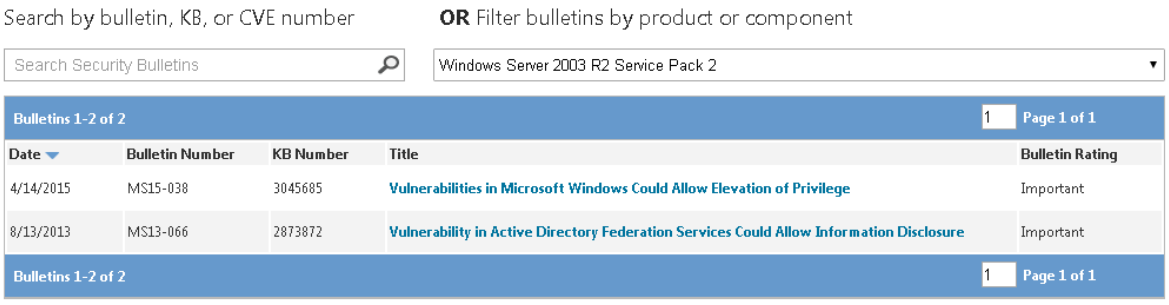
Fuente: Microsoft

El impacto hace referencia al tipo de ataque que se podría ejecutar si una vulnerabilidad no es corregida, según los boletines de seguridad de Microsoft, se encuentran 5 tipos: **Denegación de Servicio, Elevación de Privilegios, Divulgación de Información, Ejecución de código remoto, Suplantación**,

Modificación de datos, Saltos de seguridad. Más adelante en el documento se presenta una descripción de estos y otros tipos de ataque.

Para mejorar el proceso de búsqueda de una vulnerabilidad por diferentes criterios como producto, componente, fecha o número de boletín, Microsoft dispone de un buscador online y un archivo de Excel como se muestra en las figuras 5 y 6.

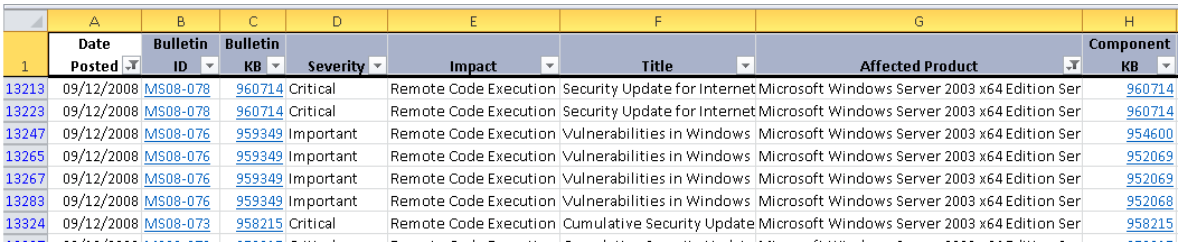
Figura 5. Buscador Online de Vulnerabilidades de Microsoft.



Fuente: Microsoft

Cabe resaltar, que el archivo de Excel contiene 18.491 registros.

Figura 6. Base de datos de vulnerabilidades de Microsoft en Excel.

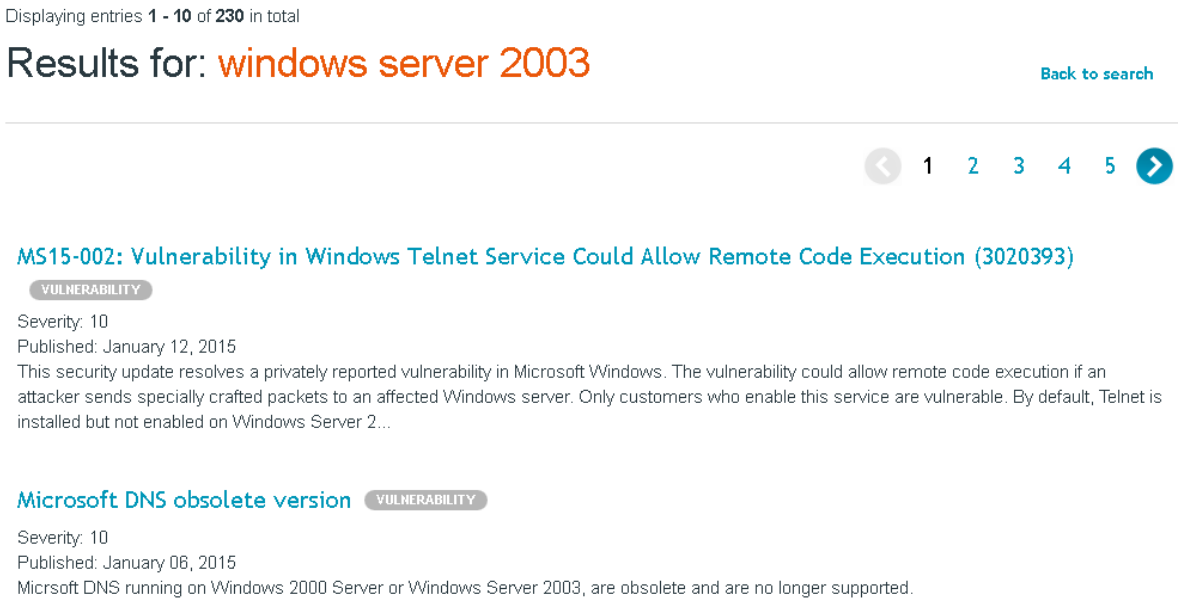


	A	B	C	D	E	F	G	H
1	Date Posted	Bulletin ID	Bulletin KB	Severity	Impact	Title	Affected Product	Component KB
13213	09/12/2008	MS08-078	960714	Critical	Remote Code Execution	Security Update for Internet	Microsoft Windows Server 2003 x64 Edition Ser	960714
13223	09/12/2008	MS08-078	960714	Critical	Remote Code Execution	Security Update for Internet	Microsoft Windows Server 2003 x64 Edition Ser	960714
13247	09/12/2008	MS08-076	959349	Important	Remote Code Execution	Vulnerabilities in Windows	Microsoft Windows Server 2003 x64 Edition Ser	954600
13265	09/12/2008	MS08-076	959349	Important	Remote Code Execution	Vulnerabilities in Windows	Microsoft Windows Server 2003 x64 Edition Ser	952069
13267	09/12/2008	MS08-076	959349	Important	Remote Code Execution	Vulnerabilities in Windows	Microsoft Windows Server 2003 x64 Edition Ser	952069
13283	09/12/2008	MS08-076	959349	Important	Remote Code Execution	Vulnerabilities in Windows	Microsoft Windows Server 2003 x64 Edition Ser	952068
13324	09/12/2008	MS08-073	958215	Critical	Remote Code Execution	Cumulative Security Update	Microsoft Windows Server 2003 x64 Edition Ser	958215

Fuente: Los autores.

Otras fuentes para buscar vulnerabilidades en un producto y su respectivo exploit (si está disponible), son **Metasploit's vulnerability & exploits DB**[12] y **Exploit-DB search**[13] como se muestra en la figura 7 y 8.

Figura 7. Base de Datos de Metasploit's vulnerability & exploits DB



Fuente: Metasploit's vulnerability & exploits DB.

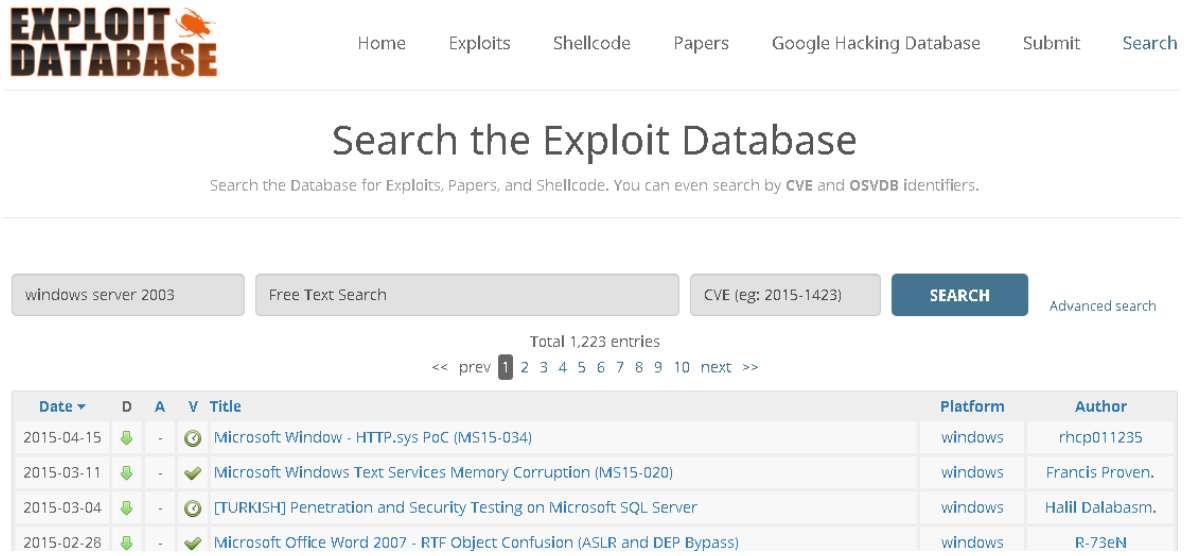
---

13 Rapid7 Security, Vulnerability & Exploit Database. Disponible en: http://www.rapid7.com/db/search.

14 Exploit Database, Offensive Security Exploit Database Archive. Disponible en: http://www.exploit-db.com/search

La segunda fuente, además de indicar si existe una vulnerabilidad en un producto, indica también si está disponible un exploit en la herramienta metasploit.

Figura 8. Base de Datos de Exploit-DB search



Fuente: Exploit-DB search

5.4.1.3 Service pack y actualizaciones de seguridad. El Service Pack es la forma en que Microsoft corrige los problemas más importantes e introduce herramientas adicionales. El Service Pack 1 (SP1) fue lanzando en Marzo de 2005, en el cual Microsoft corrige las vulnerabilidades descubiertas hasta ese momento, y se configura por defecto el firewall que venía deshabilitado en la versión original.

El Service Pack 2 (SP2), se lanzó en Marzo de 2007, entre las nuevas herramientas que se introdujeron están (Microsoft, 2007): Microsoft Management Console (MMC) para una mejor administración de Active Directory.

5.4.2 Clasificación de los ataques. Los siguientes tipos de ataques y su descripción fueron extraídos de la da documentación de la certificación de **CompTia Security**[14], la cual divide los ataques en cuatro categorías: Ataques Activos, Ataques Pasivos, Ataques a Contraseñas y Ataques de código malicioso.

5.4.2.1 Ataques activos. Este tipo de ataques son realizados para causar el mayor daño posible a una red o sistema, mediante la obtención de los servicios, con el fin de detener o modificar la configuración de cada uno de ellos. Los ataques activos son en su mayoría visibles debido a los daños causados, los cuales suelen ser detectados a simple vista, siendo muy notables. En esta categoría se encuentran:

- A.1 Denegación de servicio
- A.2 Bufer Overflows
- A.3 Spoofing,
- A.4 MITM Man in the Middle
- A.5 TCP/IP Hijacking
- A.6 Ingeniería social

15 CROSS, M., NORRIS, L., PILTZECKER, T., SHIMONSKI, R., LITTLEJOHN, D. Comptia Security, 2003.

5.4.2.2 Ataques pasivos. A diferencia de los ataques activos, los ataques pasivos no afectan a la red de la víctima, solo escuchan lo que viaja por la red, recopilando información importante, desde conversaciones hasta claves de seguridad. Entre ellos se tienen:

- B.1 Análisis de vulnerabilidades
- B.2 Escaneo de red y espionaje

5.4.2.3 Ataque a contraseñas o criptografía. Los ataques de contraseña son quizás los más realizados por su facilidad y el gran número de herramientas que existen para hacerlo, en la gran mayoría de casos resulta adivinando la contraseña.

- C.1 Ataque de fuerza bruta
- C.2 Ataque basados en diccionario.

5.4.2.4 Ataque de código malicioso. A través de la historia, los Malware han sobrevivido por su capacidad de cambio para evitar la detección, esto sumado a la versatilidad que posee al poder viajar entre la internet a través de correos electrónicos que se propagan con contenido de temas atractivos a las personas, los cuales acceden a ellos y guardan en sus máquinas, lo que abre el camino al malware de poder llevar a cabo su ataque. Esto sumado al uso generalizado de mecanismos de almacenamiento como USB, que permite que estos se propaguen más fácilmente entre equipos. En esta categoría se encuentran:

- D.1 Virus
- D.2 Troyanos
- D.3 Bombas lógicas

- D.4 Gusanos
- D.5 Puertas traseras

A continuación se presenta una descripción detallada de cada tipo de ataque.

A.1 Ataque de denegación de servicio DoS. Un ataque de **denegación de servicio (DDoS)** aprovecha la capacidad de uso de la red para saturar con envió de solicitudes simultaneas, con el objetivo de superar la capacidad del sitio y de esta forma obstaculizar el buen funcionamiento del mismo. El DDoS funciona de la siguiente manera, los recursos de red, como los servidores web, tienen un número límite de solicitudes que pueden atender simultáneamente. Además del límite de capacidad del servidor, el canal que conecta el servidor con Internet también tendrá un límite de ancho de banda o capacidad. Cuando el número de solicitudes supera los límites de capacidad de cualquier componente de la infraestructura, el nivel de servicio se verá probablemente afectado de una de las formas siguientes: La respuesta a las solicitudes será mucho más lenta de lo normal y existe la posibilidad de que se ignoren algunas (o todas) las solicitudes de los usuarios.

Un tipo especial de DoS es el ***Ataque SYN.*** Este ataque se aprovecha de la debilidad que hay en el protocolo TCP/IP. Cuando dos hosts intercambian SYN | SYN / ACK | ACK en una comunicación, los paquetes SYN enviados son respondidos por el host con SYN/ACK. El atacante envía miles de paquetes SYN al host de la víctima obligándolo a esperar una respuesta que nunca habrá. Mientras el host espera las respuestas no puede aceptar otras solicitudes de procesos reales, dejándolo no disponible, logrando el objetivo de un ataque DoS

A.2 Desbordamiento de memoria. Este es un ataque que aprovecha los errores cometidos por los programadores a menudo por desconocimiento del mismo,

estas deficiencias pueden ser explotadas por este ataque conocido como desbordamiento de memoria, este ataque pretende enviar demasiados datos al buffer con el fin de que este colapse, esta parte del sistema es un área de memoria temporal que almacena datos o instrucciones. Para crear este ataque de desbordamiento de búfer el atacante reemplaza los datos de la memoria por otros datos que la mayoría de veces son caracteres sin orden alguno, ocasionando que el programa deje de funcionar. En algunos casos, las instrucciones almacenadas contienen comandos de instalación de software en el equipo de la víctima, permitiendo al atacante tener control del sistema

A.3 Spoofing. El spoofing proporciona información falsa acerca de su identidad, con el fin de ganar acceso no autorizado a los sistemas. El ejemplo más clásico es *IP spoofing*, en donde el atacante crea un paquete IP con la dirección de origen de otra máquina. En un ataque a ciegas, el atacante sólo puede enviar y tiene que hacer suposiciones o conjeturas acerca de respuestas. Por el contrario, en un ataque con conocimiento se puede controlar y participar en una conversación.

A.4* Ataque *Man in the Middle. Realiza sniffing a una red posicionándose en medio de la puerta de enlace y un servidor o red, esto se logra realizando un ataque al ARP (protocolo de resolución de direcciones) que tome como puerta de enlace la máquina del atacante, para luego cambiar la MAC de la puerta de enlace por la MAC del atacante. Luego de esto todo el tráfico transitará en primer lugar por el atacante, permitiéndole analizar los paquetes recibidos mediante el uso de herramientas como Ettercap.

A.5 TCP/IP Hijacking. El secuestro de sesión TCP, se realiza cuando se intercepta la comunicación entre dos equipos, logrando tener posesión de la conexión en el tiempo que dure la sesión. Este proceso se logra configurando la

ruta que seguirán los paquetes de respuesta a través de direcciones IP mostradas en los Routers.

A.6 ingeniería social. La Ingeniería Social facilita conseguir información de las personas que tiene acceso a un sistema. Se podría definir como una actividad para conseguir de un tercero aquellos datos de interés, para esto, los diseñadores de malware se aseguran de no solo de entrar a sus sistemas por medio del internet, sino que además de esto, se capacitan de habilidades sociales, para poder engañar más fácilmente al usuario.

La Ingeniería Social siempre ha facilitado el método de propagación de ataques informáticos. Estas personas maliciosas son quienes aprovechan las ventajas que tienen para engañar a los usuarios para lograr que éstos den información de cómo acceder a los sistemas y convertirse en victimas de fraudes informáticos. Dejando claro que un sistema puede ser perfecto en toda su programación y evitar por completo un virus o un ataque, los diseñadores de malware solo tiene que ganar la confianza del empleado que maneja el sistema y hacer que el mismo acepte la entrada del virus.

Toda persona es vulnerable ante un diseñador malicioso capacitado para completar un fraude, ya sea que el usuario de encuentre dentro o fuera del sistema informático, o de la red de trabajo. Para estas personas maliciosas la curiosidad, credibilidad, inocencia y confianza de los usuarios se convirtió en su mejor arma. Así la Ingeniería Social logra la confianza de los usuarios para luego poder manipularlas beneficiando a quien la realiza.

B.1 Análisis de vulnerabilidades. Por medio del análisis de vulnerabilidades se puede extraer información de los servicios para determinar si existe algún exploit conocido. Existen herramientas especializadas en encontrar dichas

vulnerabilidades como lo es Nmap, el cual escanea puertos enviando paquetes al host con el fin de recopilar información importante como el tipo del sistema operativo. Es necesario saber de antemano que información se desea recopilar con el fin de escoger la herramienta que más se adapte. Otro ejemplo es Nessus, el cual, permite el análisis de vulnerabilidades por medio de escaneo múltiples sobre diferentes tipos de arquitecturas, los resultados de los análisis son mostrados en un informe de manera detallada, lo que hace aún más fácil detectar que servicios son vulnerables a un ataque, además ofrece recomendaciones para mitigar los riesgos encontrados.

B.2 Sniffing y espionaje. Un Sniffer permite ver que paquetes viajan por la red, sea cableada o inalámbrica. Esta técnica de diagnóstico de problemas en la red se emplea para realizar ataques informáticos, permitiendo encontrar credenciales, incluso contraseñas que son enviadas por la red.

Una herramienta conocida para realizar sniffing es Tcpdump, la cual es utilizada en sistemas UNIX, permite ver todos los paquetes que transitan por la red, obteniendo información del tráfico de la red, enrutamiento, tipos de tráfico, entre otros. Existen otras herramientas como SubSeven y Back Orifice para realizar escuchas ilegales, las cuales capturan todo lo digitado por el usuario y realiza impresiones de pantalla.

C.1 y C.2 Ataques a contraseñas por fuerza bruta y diccionario. Los procesos realizados para este tipo de ataque se realizan por medio de fuerza bruta, mediante diccionarios de datos, que combinados miles o millones de veces logran encontrar la contraseña establecida por el usuario. Es por esta razón que los sistemas han implementado hash en sus contraseñas, haciendo más seguro el proceso.

Las contraseñas se almacenan generalmente en lo que se llama *hash* format. Cuando una contraseña se introduce en el sistema, esta pasa a través de una función hashing de un solo sentido, tales como Message Digest 5 (MD5), y se registra el proceso. Las funciones Hashing son de cifrado de ida solamente, y una vez que los datos han sido 'hash', no puede ser restaurada. Un servidor no necesita saber cuál es su contraseña, solo se necesita saber que el usuario sabe cuál es. Cuando se intenta autenticar, la contraseña pasa a través de la función hash y la salida se compara con el valor hash almacenado, si estos valores coinciden, entonces se autentica.

D.1 Virus. Los virus son programas como cualquier otro, que necesitan de ser ejecutados para llevar a cabo los procesos. En la mayoría de ocasiones buscan dañar el hardware del sistema, sobrecargando desde la memoria de la maquina hasta el disco duro, Al igual que los troyanos tiene la capacidad de auto replicarse lo que lo hace más autónomo y le ayudan a evadir la detección de antivirus que encuentre a su paso.

Además de infectar a la máquina que dio alojamiento por primera vez al virus, este puede replicarse infinidad de veces aprovechando la red y equipos sin protección alguna, pero a pesar de encontrarse en la red, esto no afecta directamente a las demás máquinas que allí se encuentren conectadas, pues se necesitaría de su ejecución para cumplir con el propósito por el cual fue diseñado.

Los virus se encuentran clasificados de la siguiente forma:

- **Parásitos:** Son aquellos que una vez hayan infectado el registro de la máquina, altera el orden de ejecución para que este sea el primero en ejecutarse.

- **Virus de Sector Bootstrap:** Este tipo de virus como su nombre lo indica se establece en el arranque del disco con el único fin de reemplazar los programas que alojan información y que se ejecutan al inicio del sistema.
- **Multi-partita:** Son virus que añaden la habilidad de los virus del sector de arranque (Sector Bootstrap) con el virus parasito, lo que lo hace más versátil ante cualquier situación y abarca un mayor impacto.
- **Companion:** Este tipo de virus tiene por objetivo robar la identidad de archivos con el fin de parecer idéntico al archivo original para poder más adelante ejecutar su ataque.
- **Link:** Los virus Link o enlace tienen la función de engañar al usuario para que accedan a él y luego infectar el sistema operativo o de los directorios que este almacene.
- **Data file:** Los archivos de datos tienen como fin el apoderarse de los archivos con el fin de manipularlos, inyectando el código malicioso que se replicarán automáticamente a través de macros incrustadas en su estructura.

D.2 Caballos de Troya o Troyanos. Un Troyano es parecido a un virus, pero con unas características relevantes que lo hacen diferenciarse y ganarse una categoría diferente. Como su nombre lo indica, se disfraza de alguna aplicación de utilidad que promete resolver problemas o potenciar instantáneamente aquellas maquinas que andan lentas, u ofrecen entretenimiento, todo lo que pueda llamar la atención y sea atractivo, con el fin de ser descargado y ejecutado. Una vez el archivo es abierto aparentemente no sucede nada o no se muestra el contenido que prometía tener y por el que fue descargado, pero ya en el interior del sistema se procesa el código que infecta al sistema llegando a consecuencias como la pérdida total de la información o daños en sectores del disco.

A diferencia de los gusanos, los Troyanos no se pueden replicar por sí mismo, necesitarían la intervención del usuario el cual descargue el archivo y lo ejecute

por su propia cuenta; entre las acciones del Troyano se puede encontrar abrir una puerta que sirva para acceder remotamente a esa máquina sin que este se percate de tal acción.

D.3 Bombas lógicas. Las bombas lógicas se encuentran en la categoría de malware, con la gran diferencia de ser ejecutadas solo cuando se cumple una condición, esta puede ser un tipo de evento lanzado por la víctima o al cumplirse una fecha, una vez ejecutada se comporta como cualquier malware afectando al sistema operativo y arranques del disco.

Una bomba lógica era conocida como Chernobyl, la cual se extendió a través de disquetes infectados o por medio de archivos infectados, y se replicaban en el sector de arranque del disco. Lo que hizo a Chernobyl diferente de otros virus es que esta no se activaría sino hasta una fecha determinada, en este caso, el 26 de abril, aniversario del desastre de Chernobyl. En ese día, el virus causó estragos al intentar reescribir el sistema de la víctima (BIOS) y borrar información del disco duro.

D.4 Gusanos. Los gusanos se caracterizan por habitar silenciosamente en un sistema, consumiendo los recursos de red y haciendo la maquina más lentas en sus procesos, a diferencia de otros tipos de ataques, los gusanos no se pueden replicar así mismo, por lo que necesitan de la intervención de una víctima para que descargue algún archivo con fachada falsa pero atractiva y lo ejecute en la máquina.

D.5 Puerta Trasera. Una puerta trasera es esencialmente cualquier programa o configuración diseñada para permitir el acceso autenticado a un sistema, este ataque crea un acceso, el cual puede ser utilizado para el robo, modificación o eliminación de información que allí se aloje. Los **rootkits** junto con los troyanos

son los más empleados para llevar a cabo este proceso, que tiene como objetivo crear vórtices por donde viaje la información robada y tener control total del sistema, como si se encontrara frente a él. Un rootkit es una colección de programas que un intruso utiliza para camuflar su presencia. Un típico programa rootkit es T0rnkit, el cual utiliza diferentes versiones para ocultar la presencia del atacante, al tiempo que accede remotamente al sistema.

Los antivirus y firewall resultan de poca utilidad cuando se trata de backdoors o puertas traseras, pues estos no logran diferenciar si los procesos que están siendo llevados a cabo son de forma remota por un atacante o por lo contrario es el administrador del sistema quien se encuentra frente a la maquina procesando diferentes peticiones.

5.4.3 Metodologías de prueba de intrusión. La aplicación de estándares de pruebas de intrusión, permite realizar el proceso de manera ordenada y sistemática. Muchas de ellas son elaboradas por los principales representantes de la industria de la seguridad informática.

5.4.3.1 Pruebas de Penetración Estándar PTE. Están diseñadas para definir una prueba de penetración y asegurar al cliente de la organización un nivel estandarizado de esfuerzo y gasto en una prueba de penetración, la cual puede ser realizada por cualquier persona. El estándar está dividido en siete categorías

con diferentes niveles de esfuerzo requeridos para cada uno, dependiendo de la organización bajo ataque. **Metasploit**[15].

- **Interacciones Pre-compromiso.** Interacciones Pre-compromiso sirve para preparar al cliente, brindándole la oportunidad de imaginar el alcance del test de penetración, dando a conocer lo que se puede y no hacer.
- **Recopilación de Inteligencia.** La fase de recopilación pretende reunir la mayor parte de información posible, la habilidad más importante de un probador de penetración es la cantidad de información que pueda tener al momento del ataque y la forma de acercarse a esta información. Durante la recolección de inteligencia, se intenta identificar qué protección y mecanismos son establecidos, esto ayuda a identificar más el sistema. Para no ser detectados durante las pruebas, se deben realizar exploraciones iniciales para que la dirección IP no se relacione con la del probador.
- **Modelado de Amenazas:** Al realizar el modelado de amenazas lo que se busca es determinar las debilidades en el sistema destino, este modelado de amenazas indicará cual es el ataque más eficiente.
- **Análisis de Vulnerabilidad:** Teniendo claro el método de ataque, se procede a la fase de análisis de vulnerabilidad, el cual combina la información recolectada con las fases mencionadas anteriormente: las exploraciones y los datos de la información recogida de inteligencia.
- **Explotación:** La fase de explotación es a menudo la más estrepitosa, en lo posible sólo se debe utilizar cuando se tiene la convicción de que será exitosa

16 VICENTE, L., BUCIO, J., SOTO, A. Metasploit, 2014.

la prueba. Hay que tener presente que arriesgarse a lanzar una explotación de manera masiva puede que no tenga ninguna recompensa para el probador como para el cliente, por esta razón se debe tener la seguridad de haber planeado el proceso para tener un final exitoso.

- **Explotación Pública:** La explotación pública es un componente que muestra la diferencia de la información importante. Con la explotación, la búsqueda dentro de la penetración puede identificar y valorar los datos que ya se han intentado asegurar. Cada vez que se realiza un ataque, una y otra vez, esto va generando mayor impacto en el negocio.
- **Informes:** Los informes son el elemento más importante de una prueba de penetración, estos revelan cada paso que se realizó durante el ataque, y lo más importante a la organización, el encontrar una vulnerabilidad en la prueba de penetración realizada por el probador. Esta información recolectada durante las fases de prueba es valiosa para garantizar el éxito de la organización en el programa de seguridad y para poder estar seguro frente a posibles ataques. La manera de agrupar la información dentro del informe es presentar a la organización las vulnerabilidades encontradas, corregir los problemas encontrados y actualizar la seguridad del sistema, previniendo fallas futuras. Este informe es presentado en resumen ejecutivo para concluir las técnicas de mejoramiento. Los hallazgos técnicos serán utilizados por el cliente para remediar los agujeros de seguridad. Es deber del probador recomendar al cliente un solución óptima de acuerdo al tipo de vulnerabilidad encontrada en la prueba de penetración.

5.4.3.2 OSSTMM. El manual de la metodología abierta del test de penetración de Seguridad, es uno de los estándares profesionales más completos y generalmente utilizado para revisar la Seguridad de los Sistemas, la metodología está dividida en las siguientes secciones:

- Sección A -Seguridad de la Información
- Sección B -Seguridad de los Procesos
- Sección C -Seguridad en las tecnologías de Internet
- Sección D -Seguridad en las Comunicaciones
- Sección E -Seguridad Inalámbrica
- Sección F -Seguridad Física

5.4.3.3 Information Systems Security Assessment Framework (ISSAF). El Marco de Evaluación de Sistemas de Información de Seguridad, es una metodología más detallada técnicamente que OSSTMM, divide el proceso de evaluación en fases y actividades, que son:

- Fase I – Planeación
- Fase II – Evaluación
- Fase III – Tratamiento
- Fase IV – Acreditación
- Fase V – Mantenimiento

En la Segunda Fase es donde se lleva a cabo la prueba de intrusión. En esta fase se realizan las siguientes actividades:

- Recolección de Información
- Mapeo de la red de trabajo
- Identificación de vulnerabilidades
- Penetración
- Obtener Acceso y escalar privilegios
- Enumeración
- Comprometer usuarios remotos y sitios

- Mantener Acceso

5.4.4 Kali Linux y sus herramientas En Marzo de 2013 hace su aparición Kali Linux, remplazando a la antigua versión de BackTrack. Los cambios más importantes son el paso del entorno Ubuntu a Debian, Se hizo una revisión de las herramientas que contaba BackTrack y eliminaron las innecesarias, quedando un poco más de 350 herramientas. Soporta el sistema de archivos HFS. Soporta arquitecturas basadas en ARMEL y ARMHF.

5.4.4.1 Categorías de las herramientas. Las herramientas de Kali Linux están organizadas en las siguientes categorías, como también se puede observar en el siguiente gráfico:

Figura 9. Herramientas de Kali Linux.

Fuente: Los Autores.

- **INFORMATION GATHERING.** Es la primera categoría de la lista, archiva 57 herramientas, las cuales están compuestas por scripts, analizador de protocolos de red, examinadores DNS, entre otros. Entre las herramientas importantes se encuentran, Amap, la cual permite identificar el puerto sobre el cual se ejecutan las aplicaciones para realizar comparaciones que permitan determinar si son el puerto correcto. Dnsmap, herramienta diseñada para pruebas de penetración, la cual permite recolectar la mayor cantidad de información de la infraestructura analizada, incluyendo nombres de dominio, bloques de red, entre otros.
- **VULNERABILITY ANALYSIS.** Posee herramientas de escaneo en búsqueda de vulnerabilidades en sistemas Cisco en su mayoría. Una de las herramientas para resaltar que se encuentra en el listado es Nmap, el cual es un poderoso escáner que permite descubrir equipos en la red con todas sus características para poder analizarlos y conocer más acerca de ellos.
- **WEB APPLICATIONS.** Categoría que alberga todo lo necesario para lanzar escaneos en internet, compuesto en su mayoría por scripts, poseen cualidades de análisis de bases de datos, inyección de código SQL, captura de elementos de páginas web, entre otros. Entre las herramientas destacadas se encuentra *sqlmap*, su función es detectar y explotar vulnerabilidades en aplicaciones web para realizar ataques de inyección de código SQL.
- **PASSWORD ATTACKS.** Administra 36 herramientas para el ataque de contraseñas, algunas de ellas emplean la fuerza bruta para lograr sus objetivos, que es conocer las credenciales de acceso. Entre estas se destaca *John the Ripper*, la cual es veloz y permite su configuración de acuerdo a las necesidades de búsqueda. Se diferencia de las demás herramientas por poseer sus propios módulos optimizados que emplea para sus ataques.
- **WIRELESS ATTACKS.** Es un listado de 32 herramientas, que en su mayoría permiten el monitoreo de trafico de red. Incluye mecanismos para el análisis de mecanismos que emplean *bluetooth* para la transmisión de datos. Entre estas

se encuentra *BlueRanger*, el cual detecta dispositivos Bluetooth con alta calidad de alcance. Permitiendo ser medida la distancia del dispositivo según la calidad del enlace.

- **EXPLOITATIONS TOOLS.** Listado de herramientas exclusivas para las labores de explotación, en esa lista se incluyen herramientas para realizar pruebas de penetración web, pruebas rápidas y avanzadas en dispositivos vulnerables Cisco, ataques de inyección SQL en aplicaciones web, entre otros.
- **SNIFFING/SPOOFING.** Las herramientas de sniffing son ampliamente requeridas para la búsqueda y explotación de vulnerabilidades de seguridad, este listado posee diferentes instrumentos para hacer uso de esta técnica, entre las cuales se encuentra HexInject, la cual mediante el uso de scripts altera el tráfico de red mediante modificaciones e interceptaciones. Otra herramienta importante en el listado corresponde a *Mitmproxy* que permite visualizar tráfico HTTPS y HTTP, es empleado en el monitoreo en aplicaciones móviles con el fin de detectar envíos realizados.
- **MAINTAINING ACCESS.** Entre las herramientas importantes de mantenimiento de acceso se encuentra *Polenum* que permite la extracción de información de la política de contraseñas de un maquina Windows, Polenum permite realizar estas actividades remotamente. Otra herramienta importante es *WebScarab*, la cual permite disponer de especialistas en seguridad para hallar vulnerabilidades en una aplicación basada en HTTP.
- **REVERSE ENGIEERING.** Listado de herramientas que permiten la realización de ingeniería inversa, realizando la extracción del diseño en algunos casos para comprender el funcionamiento del sistema. Una de las herramientas que se destaca por realizar ingeniería inversa en el listado es *javasnoop*, la cual una vez tiene acceso al código fuente recorre el código realizando cambios de variables y junta toda la información del *Applet* o aplicación.
- **STRESS TESTING.** Entre sus herramientas se encuentra *FunkLoad*, la cual permite realizar pruebas de funcionamiento y de regresión de proyectos web,

prueba de recursos, prueba de carga, entre otras. Así mismo en el listado está *iaxflood*, la cual es una herramienta para saturar el protocolo IAX2 empleado en la PBX Asterisk. Por último y no menos importante se encuentra *inviteflood*, la cual se emplea en el ataque de denegación de servicio (DoS) contra dispositivos SIP, enviando múltiples solicitudes INVITE según la configuración realizada.

- **HARDWARE HACKING.** Herramientas diseñadas para penetrar la parte física de los sistemas con el fin de alterar el código Shell del hardware para afectar su funcionamiento o hacer que funcionen según el deseo del atacante. El listado completo está compuesto por 6 herramientas las cuales son: Android-SDK, apktool, *Arduino*, dex2jar, Sakis3G y smali.
- **FORENSICS.** Conjunto de herramientas para realizar tareas forenses en escenas donde lo importante es conocer las últimas acciones realizadas en el sistema. Entre la lista se encuentra chntpw, la cual permite ver información y modificar contraseñas de usuarios de bases de datos de Windows NT/2000.
- **REPORTING TOOLS.** Listado de 9 herramientas entre las que se encuentra CaseFile, la cual está orientada especialmente a analistas que trabajan en equipo de investigación para lograr un objetivo. La herramienta más parecida a CaseFile es Maltego. Otra herramienta que hace parte de este listado es CutyCapt, su función es capturar formatos PDF, JPEG, GIF, BMP, entre otros, de páginas web. Por otra parte se encuentra Metagoofil, la cual es una herramienta que permite recolectar la mayor cantidad de metadatos posible de documentos con formatos .docx, .pdf, .xls, .ppt, entre otros.

Algunas de las herramientas utilizadas para descubrir y explotar vulnerabilidades son NMAP, NESSUS y METASPLOIT las cuales se van a describir en mayor detalle, debido a su importancia y por su utilización en el proyecto.

5.4.4.2 Nmap (NMAP.ORG, 2014) es uno de los scanner de red más potentes conocido en el mundo. El uso más habitual de esta herramienta es el descubrimiento de equipos activos en la red, la detección del sistema operativo y las aplicaciones y versión que se ejecuta sobre dicho equipo. Con la herramienta *Nmap Scripting Engine NSE*, se extiende las capacidades normales de *scanning* hacía el descubrimiento de redes, explotación y rompimiento de contraseñas. Estas características están disponibles mediante scripts, que se escriben en el lenguaje LUA. Los desarrolladores pueden crear sus propios scripts, y permiten realizar por ejemplo, detección de vulnerabilidades de SQL, ataques a contraseñas mediante fuerza bruta, encontrar proxis abiertos, entre otros. La detección de las aplicaciones se realiza enviado paquetes TCP/IP contra un objetivo-aplicación especifico, y después se analizan las respuestas. El objetivo puede ser una IP, un rango de IPs o un nombre (CNAME). Las aplicaciones se asocian a un número o puerto, algunos son bien conocidos, como 80 HTTP o 22 SSH. Mediante diferentes técnicas de sondeo, Nmap determina cuando un puerto está abierto, cerrado o filtrado. Un puerto abierto, significa que la aplicación está esperando por nuevas solicitudes de conexión.

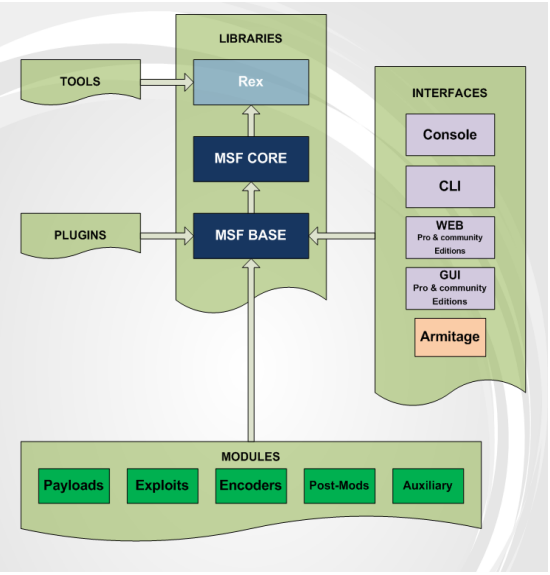
5.4.4.3 Nessus. Es uno de los escáneres de vulnerabilidades más utilizado. Se puede utilizar contra sistemas operativos, aplicaciones web, base de datos, redes, dispositivos móviles, entre otros; en busca de malware, configuraciones erróneas, software desactualizado, entre otras. Entre sus principales características se encuentra que cuenta con una interfaz web, la cual se compone por un servidor http y el cliente web, lo que le permite ser ejecutada en cualquier plataforma, tiene además una base de datos de vulnerabilidades que se actualiza constantemente, permite también generar diversos reportes en que se puede relacionar con *framework* de explotación como Metasploit o *CoreImpact*.

5.4.4.4 Metasploit Es una plataforma para ejecutar programas exploit, además permite el desarrollo, y prueba de los mismos. Metasploit se puede utilizar (con la integración de otras herramientas) para:

- Recolectar información - Escaneo de vulnerabilidades
- Desarrollo de exploit.
- Ataques del lado del cliente.
- Tareas pos explotación: como escalada de privilegios, escritura de archivos, *keylogger*, etc.
- Crear programas para mantener acceso como backdoors.

La utilización de la herramienta se realiza por medio de comandos, aunque existen otras herramientas graficas como *Armitage*, que pueden interactuar con los módulos de Metasploit. La arquitectura de Metasploit se muestra en la figura 10.

Figura 10. Arquitectura de Metasploit Framework



Fuente: Offensive Security

MÓDULOS

- ***Exploit***: Son programas que se aprovechan de alguna vulnerabilidad específica de un sistema operativo y aplicación. Se utiliza como un vector de ataque para enviar y ejecutar un Payload en la víctima, lo que le permita el acceso y control permanente.
- ***Payload***: Son programas que permiten el acceso y control al atacante. También dependen del sistema operativo, pero algunas que se basan en Java, no dependen de la plataforma. El Payload más potente de metasploit es *meterpreter,* el cual muestra una interfaz de línea de comandos.
- ***Auxiliary***: Le permite al framework de metasploit interactuar con otras herramientas externas como escáneres, Sniffer, detección de vulnerabilidades, entre otros.
- ***Encoder***: Son utilizados para camuflar Payload o backdoors y evitar ser detectados por IDS y antivirus.
- ***Post-Mods*:** Contiene herramientas pos explotación como escalada de privilegios, interacción con archivos y procesos, borrado de huellas, entre otros.

INTERFACES

- **Metasploit *Command Line Interface (MSFCLI)*** permite acceder al framework de metasploit de manera sencilla. Permite consultar y utilizar módulos exploits, auxiliares, ofuscadores, entre otros. Además permite conocer cómo utilizar un módulo específico mediante la descripción de sus parámetros.
- **MSFCONSOLE**: Es la interfaz más popular, permite el acceso a todas las opciones del Metasploit Framework. Permite seleccionar un módulo específico, configurarlo y ejecutarlo. Permite asimismo la ejecución de tareas que se pueden colocar en *background* y después retomarlas. Además puede ejecutar comandos externos de Linux.

5.5 MARCO LEGAL

Para la realización de una prueba de intrusión en un entorno real, se debe contar con una autorización por escrito por parte de la empresa, el documento puede incluir el alcance de las mismas, la aceptación de riesgos y los daños que se pueden cometer en el proceso. El Auditor de Seguridad o *Pentester* se compromete a guardar la confidencialidad de toda la información suministrada y la que llegara a descubrir. De esta forma el Pentester puede realizar su trabajo sin temor de infringir alguna de las leyes en materia de seguridad informática, como se menciona a continuación.

5.5.1 Ley 1273 de 2009. La Ley 1273 de 2009 (Congreso de Colombia, 2009) en el capítulo Nro. 1, relacionado a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, entre los diferentes artículos se destacan:

- ***Artículo 269A****: "Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."*
- ***Artículo 269J****: "Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales*

vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa." (Ley 1273, 2009, Capitulo II).

Además de esto se contempla otras infracciones que pueden ser juzgadas y que corresponden a los atentados informáticos, entre los que se encuentran, el hurto de medios informáticos mediante la manipulación de sistemas o redes informáticas para su uso o con ánimo de lucro, caso tal como la venta de información confidencial.

5.5.2 Licencia de Windows Server 2003. Microsoft señala dentro de su modelo de licenciamiento que "Cada copia instalada del software de servidor requiere la compra de una licencia de servidor de Windows. Se requiere una Licencia de Acceso para Cliente de Windows (CAL de Windows) para poder acceder al uso del software del servidor. No se requiere una CAL si el acceso al servidor es a través de la Internet y no está "autentificado", por ejemplo, el acceder a un sitio Web para obtener información general donde no se intercambian credenciales de identificación. Una CAL de Windows (CAL de Dispositivo o de Usuario) puede aún ser designada para su uso con un solo servidor, autorizando acceso por medio de cualquier dispositivo o usuario, cuando la modalidad de software de licencia para el servidor esté definida en "Por Servidor". En esta modalidad, el número de CAL's de Windows es igual al número máximo de conexiones simultáneas. Una CAL de Windows (de Dispositivo o de Usuario) puede ser designada para su uso con cualquier número de servidores, autorizando el acceso por medio de un dispositivo especifico o usuario, cuando la modalidad de licencia del software de servidor este definida en "Por Dispositivo o Por Usuario" (Anteriormente llamada modalidad "Por Asiento"). Se han agregado otras opciones que se detallan a continuación.

Se requiere una licencia de Acceso de Cliente a Terminal Server (CAL TS) para utilizar un Servidor Terminal o de cualquier otro modo hospedar una sesión de interfaz de usuario grafica remota (GUI), excepto para una sesión de consola." (Licenciamiento de Windows Server 2003, 2007)

Las CAL de Windows forman parte primordial en el licenciamiento, cada CAL se vende por separado al momento de adquirir el sistema operativo, las CAL constituyen un permiso de acceso al servidor de tipo lectura o escritura y va sujeto al directorio activo de este.

5.5.3 Licencia de Kali Linux. Al ser Kali una derivación de Debian todo el sistema se encuentra bajo las guías de software libre de Debian, por lo que algunas directrices son "Libre redistribución. La licencia de un componente de Debian no puede restringir a un tercero el vender o entregar el programa como parte de una distribución mayor que contiene programas de diferentes fuentes. La licencia no debe solicitar «royalties» u otras comisiones para su venta.

- Código fuente. El programa debe incluir el código fuente completo, y debe permitir la distribución en forma de código fuente y en forma compilada (binario).
- Trabajos derivados. La licencia debe permitir modificaciones y trabajos derivados y debe permitir que estos se distribuyan bajo los mismos términos que la licencia del programa original.
- Integridad del código fuente del autor. La licencia puede restringir la distribución del código fuente en forma modificada sólo si la licencia permite la distribución de parches para poder modificar el código fuente original del programa en el momento de compilarlo. La licencia debe permitir la distribución del software a partir del código fuente que se haya modificado. La licencia puede obligar a los trabajos derivados a llevar un nombre o número de

versiones diferentes del programa original Esto es un compromiso. El grupo de Debian anima a todos los autores a no restringir ningún fichero, fuente o compilado, de ser modificado.

- No discriminación contra personas o grupos. La licencia no debe discriminar a ninguna persona o grupo de personas.
- No discriminación en función de la finalidad perseguida. La licencia no puede restringir el uso del programa para una finalidad determinada. Por ejemplo, no puede restringir el uso del programa a empresas con fines comerciales, o en investigación genética.
- Distribución de la licencia. Los derechos y libertades de uso asociados al programa deben aplicarse en la misma forma a todos aquellos a los que se redistribuya el programa, sin necesidad de pedir una licencia adicional para estas terceras partes.
- La licencia no ha de ser específica para Debian. Los derechos asociados al programa no deben depender de que el programa sea parte o no del sistema Debian. Si el programa es extraído de Debian y usado o distribuido sin Debian, pero manteniendo el resto de las condiciones de la licencia, todos aquellos a los que el programa se redistribuya deben tener los mismos derechos que los dados cuando forma parte de Debian.
- La licencia no debe contaminar a otros programas. La licencia no debe poner restricciones sobre otros programas que se distribuyan junto con el programa licenciado. Por ejemplo, la licencia no puede insistir que todos los demás programas distribuidos sobre el mismo medio deben ser software libre.” (Contrato social de Debian, 2014).

Todas estas cláusulas permiten al usuario final utilizar cada una de sus herramientas para el análisis y ejecución de pruebas de penetración que permitan cumplir los objetivos de seguridad planteados, permitiendo que el tipo de licencia de Kali no afecte el producto final de dicho análisis.

5.5.4 Leyes internacionales. A nivel internacional existen estatutos que garantizan la integridad, confidencialidad y Disponibilidad de la información y sanciona a aquellos que la incumplan, entre los que se encuentran.

- **RFC 2196 (*Site Security Handbook*)** es una guía para el desarrollo de políticas y procedimientos de seguridad informática para los sitios que tienen sistemas en Internet.
- **ISO / IEC 27001** es un estándar ISO para la formalización de un Sistema de Gestión de Seguridad de la Información (SGSI). Como la norma ISO / IEC 27001 no es un documento de libre acceso y puede ser que sea difícil para las organizaciones a entender y aplicar la norma ISO / IEC" (RFC 2196, 2014). Este manual es base fundamental para el desarrollo de políticas de seguridad en todo el mundo. El estándar ISO 2700x establece "Control y la certificación de seguridad de la información en la empresa. Las empresas tienen que buscar esta certificación para obtener la calidad y cumplimiento en sus departamentos de Tecnología de la Información / Sistemas de Información." (ISO 2700x *Security Standards*, 2011). Es altamente usado ya que se adapta a cualquier tipo de organización sin importar su actividad o tamaño.
- **ISO/IEC 17799** el cual "establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Los objetivos trazados proporcionan una guía general sobre los objetivos comúnmente aceptados de gestión de la seguridad de la información. Contiene las mejores prácticas de los objetivos de control y controles en las siguientes áreas de gestión de seguridad de la información:
    - Política de seguridad.
    - Organización de la seguridad de la información.
    - Gestión de activos.
    - Recursos humanos de seguridad.
    - Seguridad física y ambiental.

- Comunicaciones y gestión de operaciones.
- Control de acceso.
- Sistemas de información de adquisición, desarrollo y mantenimiento.
- Información de gestión de incidentes de seguridad.
- Gestión de la continuidad del negocio.

6. DESARROLLO DE LA INVESTIGACIÓN.

6.1 PLAN DE PRUEBAS.

6.1.1 Creación de un ambiente de pruebas. Para evitar posibles daños en el Servidor a la hora de ejecutar la prueba de instrucción, como perdida de información o suspensión del servicio, se configurará una maquina real (hardware – IP publica), ubicada en el lado de la empresa, con una copia exacta de los servicios y configuración que se ejecutan sobre el Servidor de Producción. A esta máquina se la llamará **Servidor de Pruebas**. Las características principales del Servidor de Producción que se tienen en cuenta para el desarrollo del proyecto son: Sistema operativo *Windows Server 2003 Enterprise Edition* con el ultimo *Service Pack* (2), actualizaciones automáticas activado y Servicio de *Active Directory.*

Por otra parte, se encuentra el equipo del atacante. Se creará un ambiente virtualizado mediante **VirtualBox**, en el cual, una máquina virtual ejecutará Kali Linux, y en otra una máquina virtual, se tendrá imagen del servidor de manera local, para probar y analizar todos los posibles sucesos antes de lanzar el ataque contra el Servidor de Pruebas.

Sera necesario también, configurar **NAT** en el Router del atacante, para poder implementar servicios públicos en una red privada, como un servidor web y puertos para escuchar conexiones entrantes.

6.1.2 Pruebas de mapeo de la red. Tiene como objetivo descubrir el(los) equipos en una red, los servicios que ejecuta y si es posible, la versión del servicio y del sistema operativo. Para ello, se utilizará la herramienta **NMAP.** La empresa SU

CREDITO, dio un rango de direcciones IP en donde se debía buscar el servidor, por lo cual, se tiene una información parcial al respecto.

6.1.3 Pruebas de identificación de vulnerabilidades. Para descubrir las vulnerabilidades del Servidor, se realizará varios escaneos con **NESSUS** en diferentes momentos: En la instalación por defecto del Servidor, con el Service Pack 1 instalado, con Service Pack 2, y con las demás actualizaciones de seguridad disponibles. Se comprobará si existe alguna vulnerabilidad crítica que permita el ingreso al sistema.

6.1.4 Pruebas de explotación de vulnerabilidades. En esta actividad se seleccionará el **exploit** específico disponible en la herramienta de **Metasploit** para las vulnerabilidades anteriormente descubiertas. Si no se logra tener éxito con un exploit, se escoge otro y se intenta nuevamente. Se tendrá en cuenta que existen otras técnicas de hacking como la **Ingeniería Social.**

6.1.5 Pruebas Pos Explotación. Después de que se logre la intrusión inicial, se emplearán las herramientas de **Meterpreter** para realizar tareas pos explotación como: Elevación de privilegios, desactivar defensas del sistema (antivirus y firewall) y mantener acceso mediante Backdoor, Estas actividades se realizan con el fin de lograr el acceso al sistema, sin tener que repetir los pasos anteriores o por si corrigen la vulnerabilidad presente.

6.1.6. Acceso a información confidencial. El fin del proyecto es poder descubrir información valiosa que se encuentre alojada en el Servidor; y demostrar que es posible que un intruso acceda a ella (crear una copia) siguiendo este plan u otro diferente. Como tiene instalado el Servicio de Active Directory, se interactuará con este servicio mediante las herramientas de comandos que ofrece, para conseguir la información almacenada.

6.1.6 Limpieza de huellas. Todas las actividades anteriormente descritas generan huellas, que básicamente consisten en archivos y eventos generados que se guardan en el registro de Windows. En esta última fase se limpiará los rastros dejados con las herramientas automáticas de Meterpreter. La siguiente tabla resume las actividades propuestas y las herramientas que se proponen utilizar.

Tabla 2. Herramientas propuestas por actividad de la prueba de intrusión.

ACTIVIDAD	HERRAMIENTA
Creación de un Ambiente de Pruebas.	Windows Server 2003. Kali Linux. VirtualBox. OS Router Huawuei HG532e
Pruebas de Mapeo de la Red	NMAP
Pruebas de Identificación de Vulnerabilidades	NESSUS
Pruebas de Explotación de Vulnerabilidades.	Metasploit – MSFCONSOLE
Pruebas Pos Explotación.	Metasploit - Meterpreter CMD
Acceso a Información Confidencial	CMD
Limpieza de Huellas	Metasploit - Meterpreter

Fuente: Los autores.

6.2 DESARROLLO DEL AMBIENTE DE PRUEBAS

Para el desarrollo del proyecto se cuenta con dos máquinas reales: 1) El servidor de pruebas; en donde se ha instalado Windows Server 2003 y 2) la máquina del atacante, el cual tiene un sistema anfitrión Debian 8, y dos máquinas virtuales para Kali Linux y un Windows server para pruebas locales. La siguiente tabla resume las características de los equipos.

Tabla 3. Descripción del Hardware delos equipos utilizados.

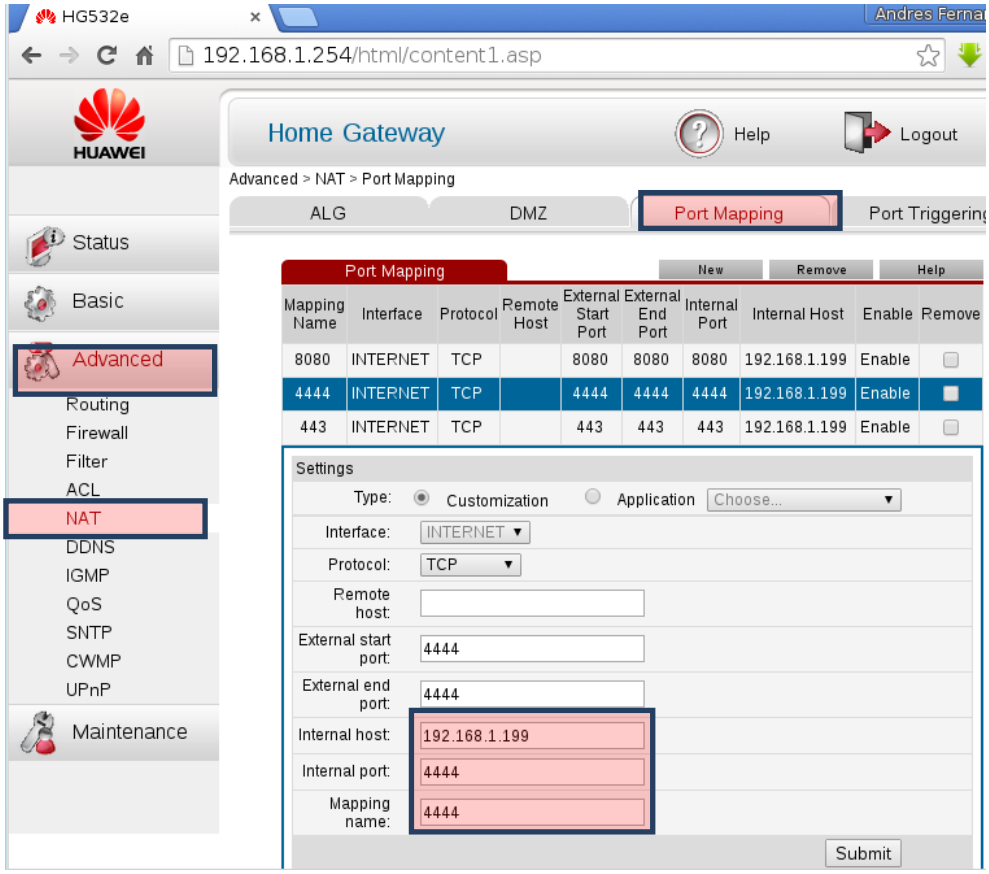
ITEM	**Servidor de Pruebas**	**Atacante**
Procesador	AMD Athlon II X2 2.8 GHz	Intel i5 4510U 2 GHz
RAM	4 GB DDR3	8 GB DDR3
Disco Duro	500 GB	1 TB
IP	XXX.XXX.XXX.XXX (Publica - Fija)	186.159.X.Y (Publica -Variable) 192.168.1.199 (Privada – fija)
Ancho de banda	500 Kbps	110 Kbps

Fuente: Los autores.

Para el desarrollo del proyecto, se necesitan las dos posibles opciones de conexión: **Bind TCP** y **Reverse TCP**, como se explicó en el marco conceptual. El caso de Bind TCP, es la situación más común. El servidor de pruebas ya se encuentra en una IP pública fija, y el atacante intenta conectarse a un puerto específico. Si el atacante desea que el servidor o una víctima, sea quien se conecte a su máquina, también necesita de una dirección IP pública fija; este es el caso de *reverse TCP*.

Debido a la negativa de la empresa UNE, de brindar de una dirección IP pública permanente, se optó por configurar el Router HUAWEI HG532e instalado en el domicilio del Atacante. El servicio de **NAT** permite redirigir las solicitudes desde la IP pública a la red privada. Como se muestra en la figura, el puertos 8080 se utiliza para montar un servicio web malicioso y el 4444, 443 para escuchar las solicitudes de reverse TCP hacia Meterpreter.

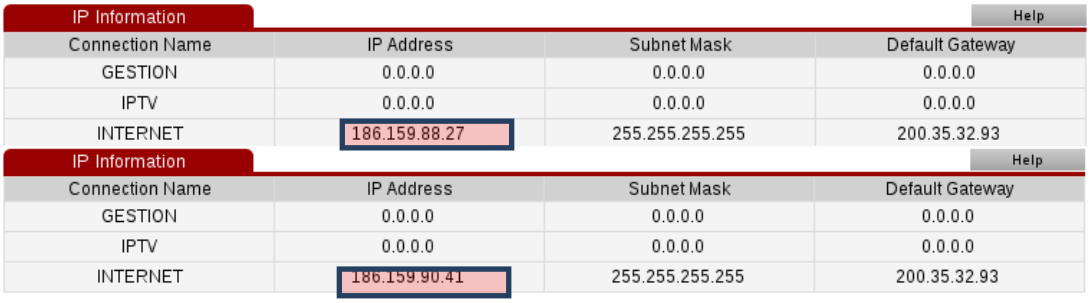
Figura 11. Configuración de NAT en Router HG535e



Fuente: Los autores.

El siguiente problema a resolver, es que la dirección IP pública del Atacante está cambiando constantemente cada vez que se reinicia el router o cada cierto periodo de tiempo, como se puede observar en la siguiente imagen.

Figura 12. Dirección IP publica dinámica en el Atacante.



IP Information — Help

Connection Name	IP Address	Subnet Mask	Default Gateway
GESTION	0.0.0.0	0.0.0.0	0.0.0.0
IPTV	0.0.0.0	0.0.0.0	0.0.0.0
INTERNET	186.159.88.27	255.255.255.255	200.35.32.93

IP Information — Help

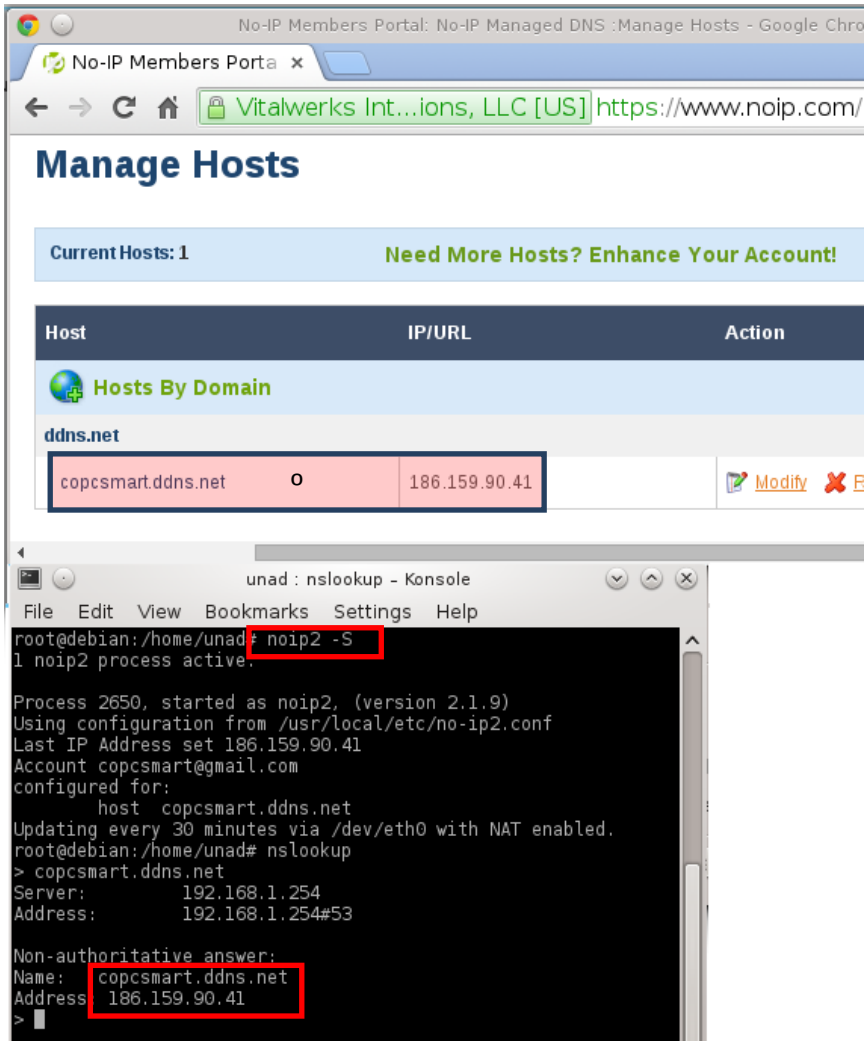
Connection Name	IP Address	Subnet Mask	Default Gateway
GESTION	0.0.0.0	0.0.0.0	0.0.0.0
IPTV	0.0.0.0	0.0.0.0	0.0.0.0
INTERNET	186.159.90.41	255.255.255.255	200.35.32.93

Fuente: Los autores.

Para remediar esta situación se creó una cuenta en **noip.com**, el cual ofrece un servicio DNS gratuito. La configuración de los equipos se puede realizar mediante la interfaz web de la página o mediante una herramienta de línea de comandos como se observa en la imagen.

Se configuro el proceso de NOIP como un servicio, para que se ejecute con cada arranque del sistema y cada 5 minutos, de esta forma se mantiene actualizada la dirección IP relacionada con el dominio seleccionado.

Figura 13. Creación de un dominio para el atacante.



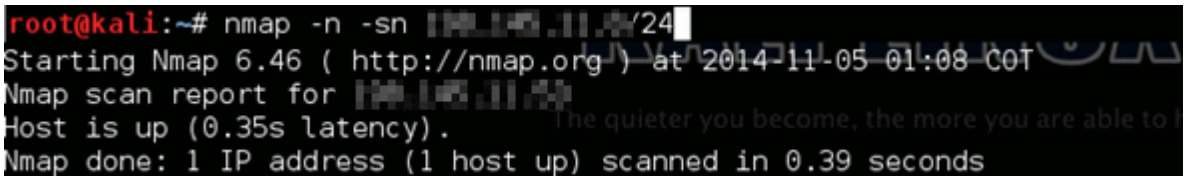
Fuente: Los autores.

Se escogió el nombre del dominio **copcsmart.ddns.net** para tratar de engañar al administrador del sistema, haciéndole creer que se trata de la empresa **PC Smart**, como se verá más adelante. Todas las solicitudes de conexión a este dominio serán redirigidas a la IP privada del atacante.

6.3 PRUEBAS DE MAPEO DE LA RED.

A manera de ejemplo de cómo un Pentester identifica un equipo activo en la red, se ejecutó el siguiente comando de **NMAP** para hacer un sondeo inicial de los equipos activos. Una descripción de las opciones empleadas de esta herramienta se encuentra en el **Anexo 1 – Opciones del Scanner NMAP**.

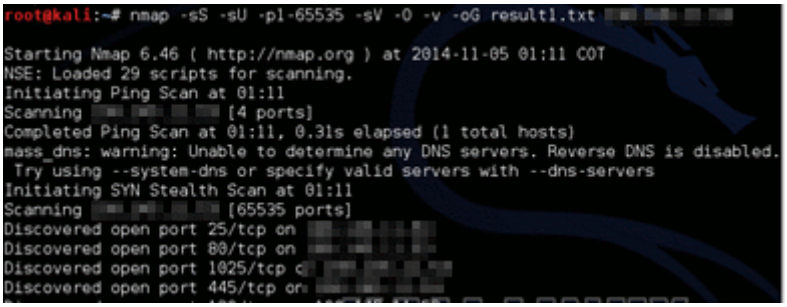
Figura 14. Sondeo de la Red con NMAP.



Fuente: Los autores

Una vez identificado que la IP W.X.Y.Z está activa, se procede a realizar un escaneo más profundo para conocer en detalle los puertos-servicios que están abiertos, y la versión del sistema operativo, mediante el siguiente comando. Los resultados se guardan en un archivo, para su posterior análisis.

Figura 15. Escaneo de los Servicios de Windows Server 2003



Fuente: Los autores

La siguiente tabla presenta una lista detallada de cada puerto descubierto por NMAP.

Tabla 4. Lista de puertos - servicios de Windows Server 2003

PUERTO	SERVICIO
21/tcp	ftp
23/tcp	telnet
25/tcp	Smtp
42/tcp	Nameserver
53/tcp	Domain
80/tcp	http
135/tcp	Msrpc
139/tcp	Netbios-ssn
445/tcp	Microsoft-ds

Fuente: Los Autores.

Por cada uno de los puertos identificados, se puede buscar vulnerabilidades en el código de las aplicaciones que lo ejecutan, para detectar si es posible utilizar un exploit que tome ventaja de dichas vulnerabilidades. Para este análisis se va a utilizar herramientas automáticas como NESSUS, como sigue a continuación.

6.4 PRUEBAS DE IDENTIFICACIÓN DE VULNERABILIDADES.

La herramienta utilizada para la identificación de vulnerabilidades es **NESSUS**, la cual, realiza un análisis de los servicios que ejecuta el servidor por medio de un análisis de puertos. La herramienta presenta los resultados de manera gráfica, con

la opción de exportar un resumen ejecutivo y de integrarse con otras herramientas como NMAP y Metasploit.

Mientras se configuraba el servidor de pruebas, se aprovechó la oportunidad de realizar varios escáneres al momento de instalar las actualizaciones de seguridad como lo son, el Service Pack 1 y 2, y demás actualizaciones de seguridad disponibles. Esto con el fin de conocer la evolución en seguridad que ha tenido Windows Server 2003.

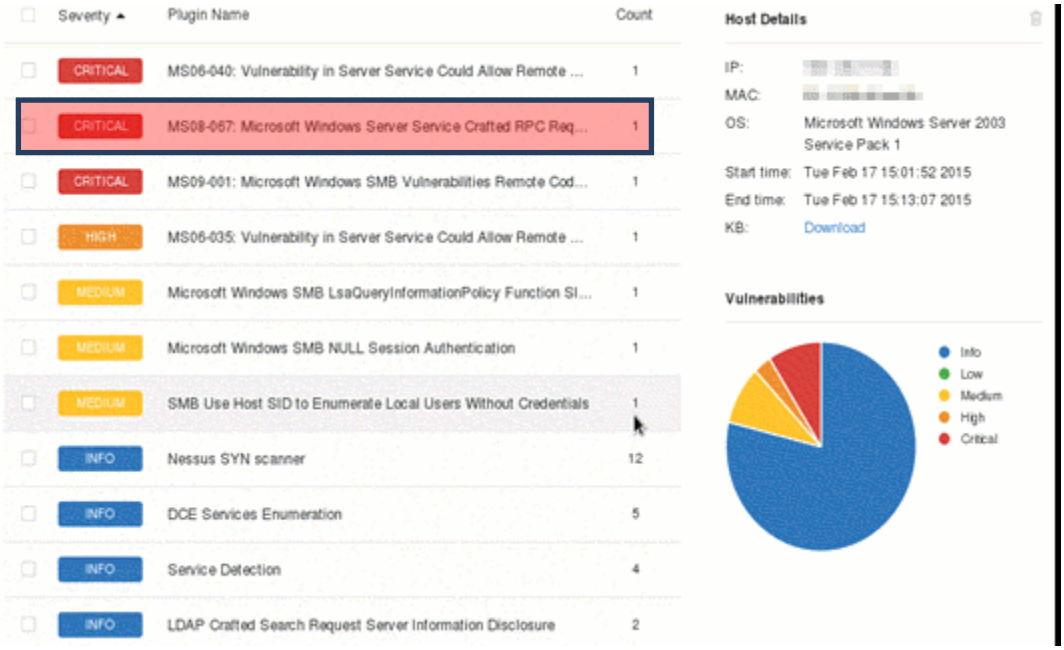
6.4.1 Análisis de vulnerabilidades de Windows Server 2003 SP1. En la siguiente figura se observa un resumen los hallazgos en el Servidor, cuando ejecutaba Windows Server 2003 Enterprise Edition Service Pack 1. En ese momento el sistema presentaba 3 vulnerabilidades críticas que permiten ejecutar un código arbitrario, una de ellas la **MS08-067** como lo muestra en detalle la figura 17. Esta vulnerabilidad es la más ampliamente utilizada por los videos tutoriales y documentos disponibles en Internet, para explicar la utilización de herramientas de explotación como Metasploit. Dicha vulnerabilidad solo está presente en sistemas sin las actualizaciones automáticas,

Figura 16. Resumen de vulnerabilidades del Servidor con SP1

Fuente: Los autores.

La imagen anterior muestra de manera gráfica las vulnerabilidades críticas (marcadas en rojo). Si se hace clic sobre el grafico, Nessus lleva a un informe más detallado, como el mostrado en la siguiente imagen.

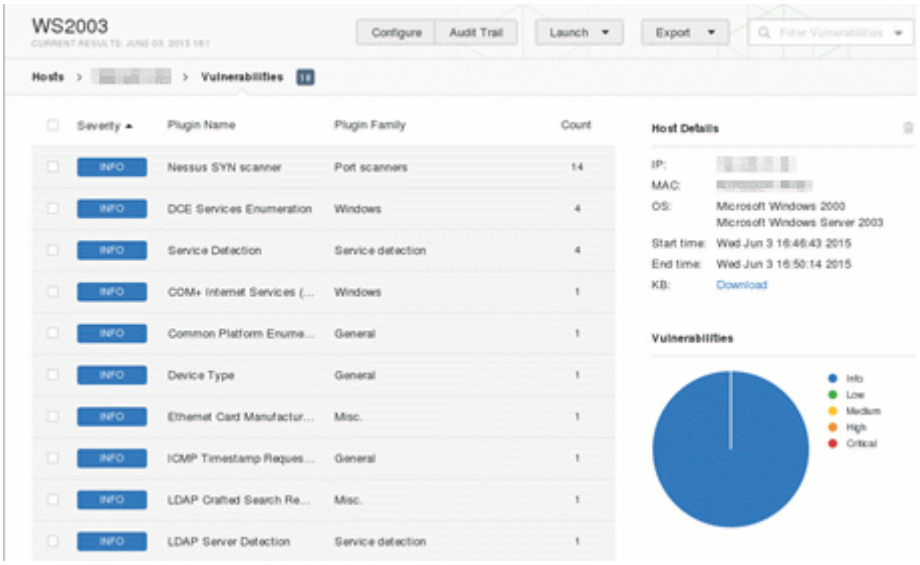
Figura 17. Informe de vulnerabilidades del Servidor con SP1



Fuente: Los Autores

6.4.2 Análisis de vulnerabilidades de Windows Server 2003 SP2 y actualizaciones automáticas activado. El escaneo al servidor con el último Service pack (2) y las actualizaciones automáticas instaladas es más desalentador para el atacante. En la Figura 18, se observa que las vulnerabilidades críticas no están presentes, todos los hallazgos son de tipo INFO (color azul), no se observa ninguna vulnerabilidad crítica en rojo. Si se intenta explotar la vulnerabilidad MS08-067, no tendrá éxito, como se mostrará más adelante.

Figura 18. Informe de Vulnerabilidades con todos los parches de seguridad



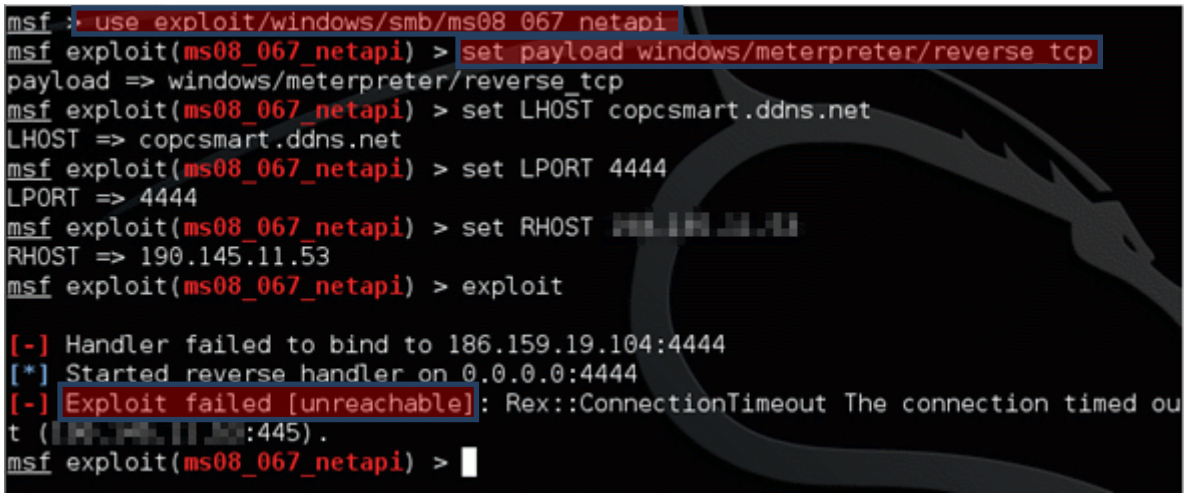
Fuente: Los autores.

Por cada una de las INFO, NESSUS presenta información interesante que se puede analizar en más detalle.

6.5 PRUEBAS DE EXPLOTACIÓN DE VULNERABILIDADES.

6.5.1 Intento de explotación de la vulnerabilidad ms08_067. En la figura 20 se puede observar la serie de pasos realizados para intentar explotar la ya mencionada vulnerabilidad MS08_067. Como describen la mayoría de documentos y videos tutoriales disponibles, primero se utiliza el exploit **ms08_067_netapi** en la consola de Metasploit, después se escoge el Payload de meterpreter. Se configura las variables de la **IP – Puerto** tanto del objetivo como del atacante, y se lanza el exploit.

Figura 19. Intento de explotación de la vulnerabilidad MS08_067



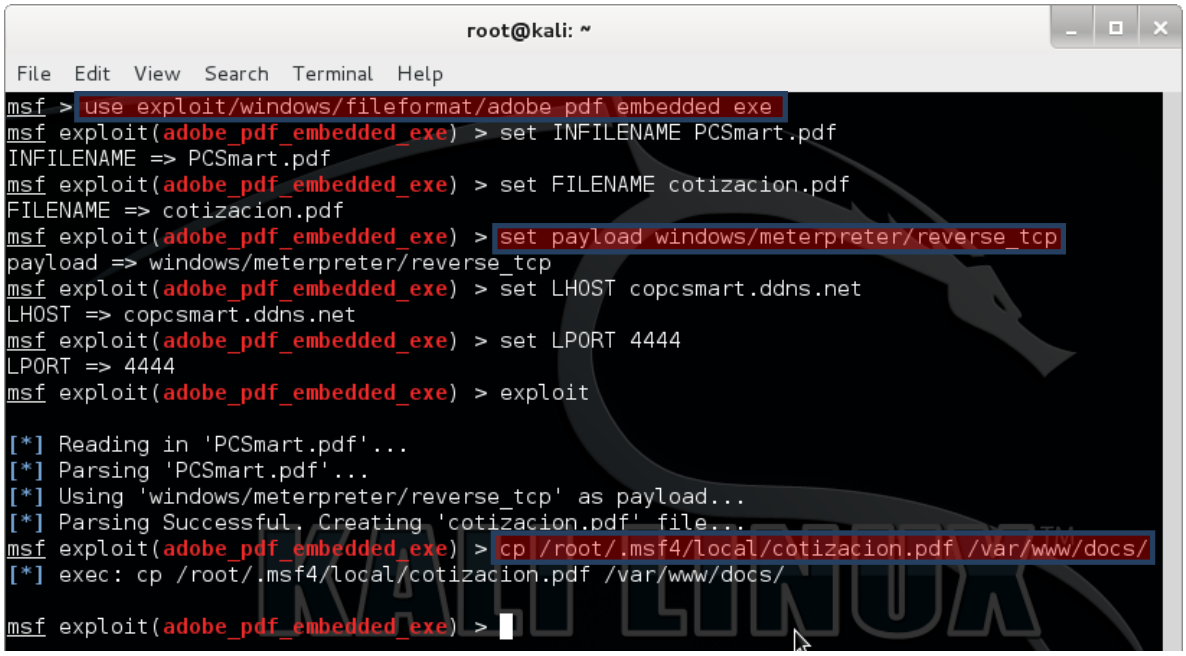
Fuente: Los autores.

El resultado es fallido, debido a que el servidor tiene instaladas las últimas actualizaciones de seguridad. Esta prueba demuestra que en un entorno real, infiltrarse en un sistema no es tan fácil cuando este presenta configuraciones se seguridad mínimas como las actualizaciones automáticas.

6.5.2 Intento de explotación mediante ingeniería social y vulnerabilidad en adobe Reader. En vista de que el análisis con NESSUS no reporta vulnerabilidades críticas en el sistema, se procede a realizar la suposición de que tal vez, exista una vulnerabilidad en el software de escritorio, que generalmente no expone un servicio o abre un puerto para su funcionamiento. En este caso se escogió Adobe Reader, por ser tan popular y porque reporta una alta tasa vulnerabilidades descubiertas que permiten ejecutar un código arbitrario. Este tipo de ataque consiste en crear un archivo PDF malicioso que después se puede enviar por correo electrónico al administrador del sistema; esperar a que lo abra e

iniciar una conexión **Reverse TCP** al atacante. El exploit utilizado es **adobe_pdf_embedded_exe.**

Figura 20. Creación de un PDF malicioso.



Fuente: Los autores.

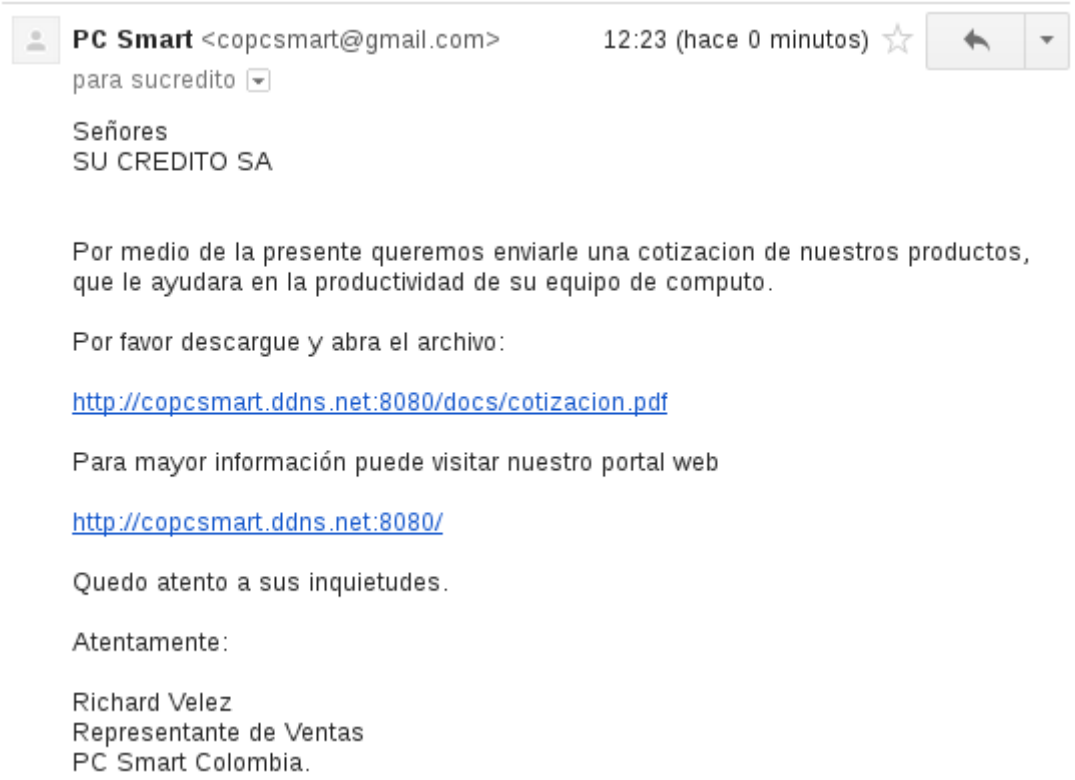
INFILENAME es el PDF inicial en donde se ocultará la carga maliciosa, en este caso un archivo de una cotización de real de la empresa PC Smart.

LHOST y **LPORT** es la Red – Puerto donde escucha el atacante por una conexión.

El PDF generado; **cotizacion.pdf**, se cocola en la carpeta del servidor web del atacante que suplanta al de la empresa PC Smart.

El siguiente paso es enviar por correo electrónico la URL de descarga del archivo al administrador del sistema, como lo muestra la Figura 21. Esta es una técnica de ingeniería Social.

Figura 21. Envió del PDF malicioso por correo electrónico.

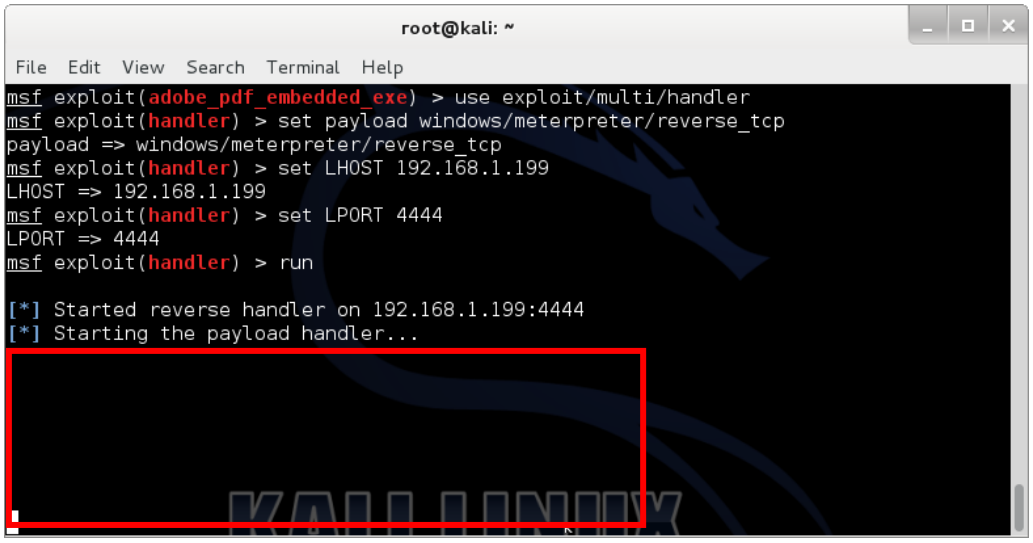


Fuente: Los autores.

Ahora el atacante debe esperar a que el administrador del sistema abra el archivo PDF. Al abrir dicho archivo, ejecuta una serie de instrucciones que se inicia una conexión hacia la IP y puerto del Atacante, por lo cual, es necesario que el atacante configure un escuchador especial **exploit/mult/handler.** Cabe resaltar que el atacante coloca el escuchador en su IP privada, ya que se ha configurado

NAT para hacer la redirección de la IP pública a la IP privada. Cuando se ejecuta el escuchador **(run),** se queda esperando por conexiones entrantes. Como se muestra en la siguiente figura.

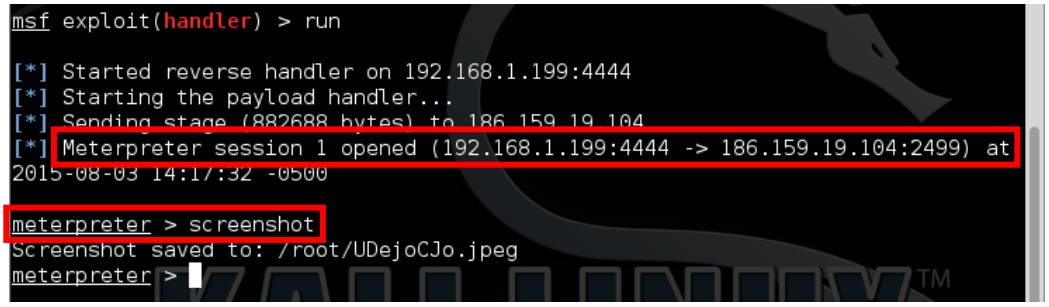
Figura 22. Escuchador de conexión Meterpreter – Reverse TCP.



Fuente: Los autores.

Cuando el usuario del Servidor finalmente abre el archivo, se ejecuta el Payload **meterpreter**, el cual permite tener acceso a la maquina por medio de línea de comandos, como si estuviera en frente de ella. Se observa que el prompt cambia de **msf>** a **meterpreter**>, A partir de este punto se puede interactuar con casi cualquier elemento del sistema, como archivos, procesos, registro, cámara, teclado, etc. La Figura 24, muestra un ejemplo del comando ***screenshot*** que toma una foto a la pantalla el servidor,

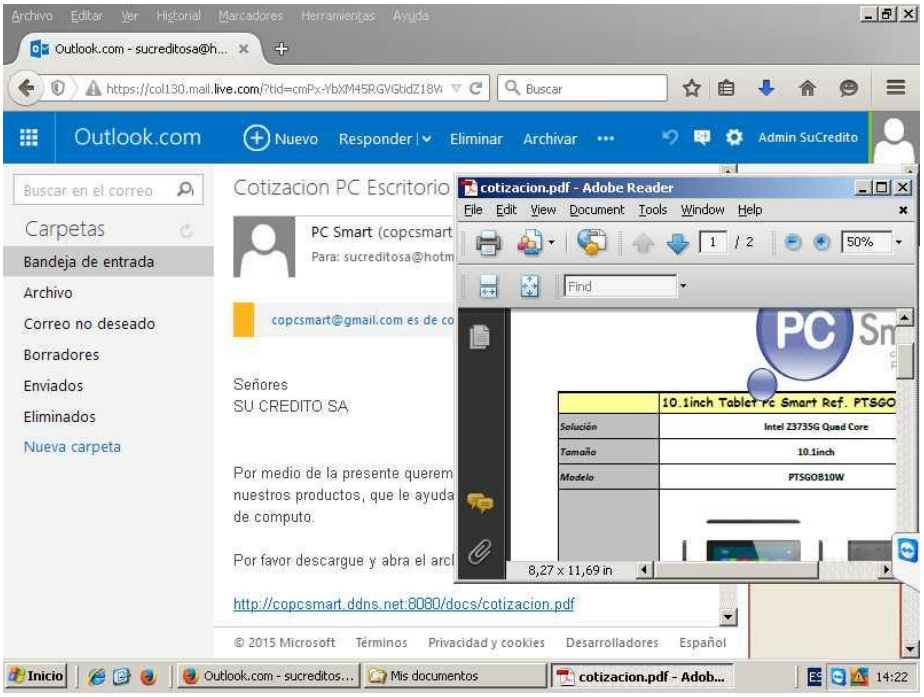
Figura 23. Conexión Entrante cuando se abre el PDF malicioso.



Fuente: Los autores.

La siguiente figura muestra lo que tenía en pantalla el administrador del sistema

Figura 24. Captura de la pantalla del Servidor.



Fuente: Los autores.

A partir de este punto, el atacante ha logrado encontrar y explotar una vulnerabilidad que le permite interactuar con el objetivo por medio de comandos, como se ha comentado anteriormente. El siguiente objetivo es garantizar el acceso al servidor en otro momento, por si el usuario apaga el servidor y se pierde la conexión o si actualiza el software vulnerable. Estas actividades se describen en el siguiente ítem.

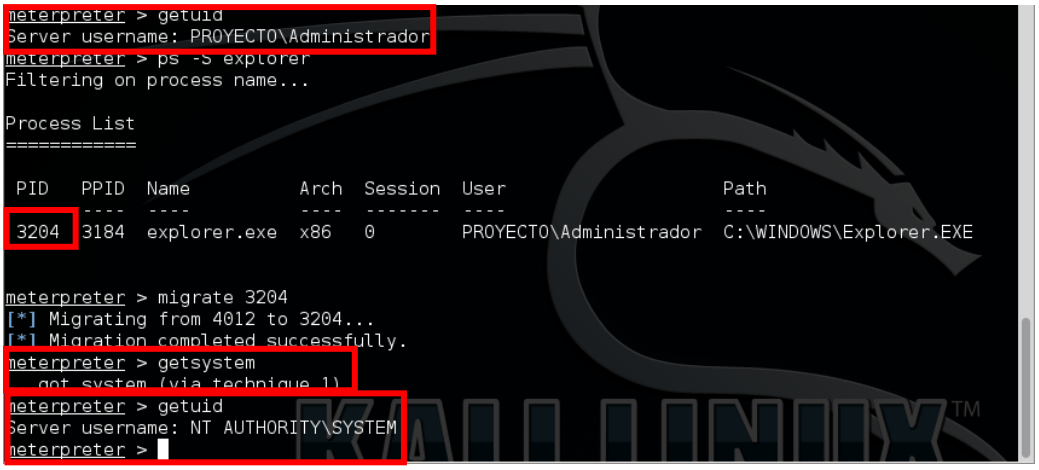
6.6 PRUEBAS POS EXPLOTACIÓN.

Como se comentó anteriormente, el objetivo de estas actividades es asegurar el acceso al sistema en cualquier momento sin tener que esperar a que el usuario abra otra vez el PDF malicioso, o por si realiza una actualización de seguridad en Adobe Reader.

De manera similar a como actúa un virus en el cuerpo humano, se busca atacar las defensas del sistema para prevenir ser detectado o eliminado y así tener control del equipo y poder encontrar información valiosa para el atacante.

6.6.1 Elevación de privilegios. Esta actividad consiste en obtener los privilegios del usuario *System,* el cual puede hacer cualquier cosa sobre el sistema. Por medio del comando getuid se puede saber con qué usuario se abrió el PDF malicioso que inicio la conexión, en este caso, es el usuario por defecto en la instalación de los SO Windows Server Administrador, como muestra la Figura 25. El siguiente paso es *migrar* (migrate) del proceso original en ejecución, a un proceso más o menos permanente y común, como *explorer*, por si el usuario mata el proceso original; para ello se debe conocer el identificador o PID, que se obtiene con el comando ps (la opción –S es para filtrar los resultados por el nombre). El comando getsystem intenta obtener los derechos de System. Esta actividad es satisfactoria.

Figura 25. Comandos para elevación de privilegios.



Fuente: Los autores.

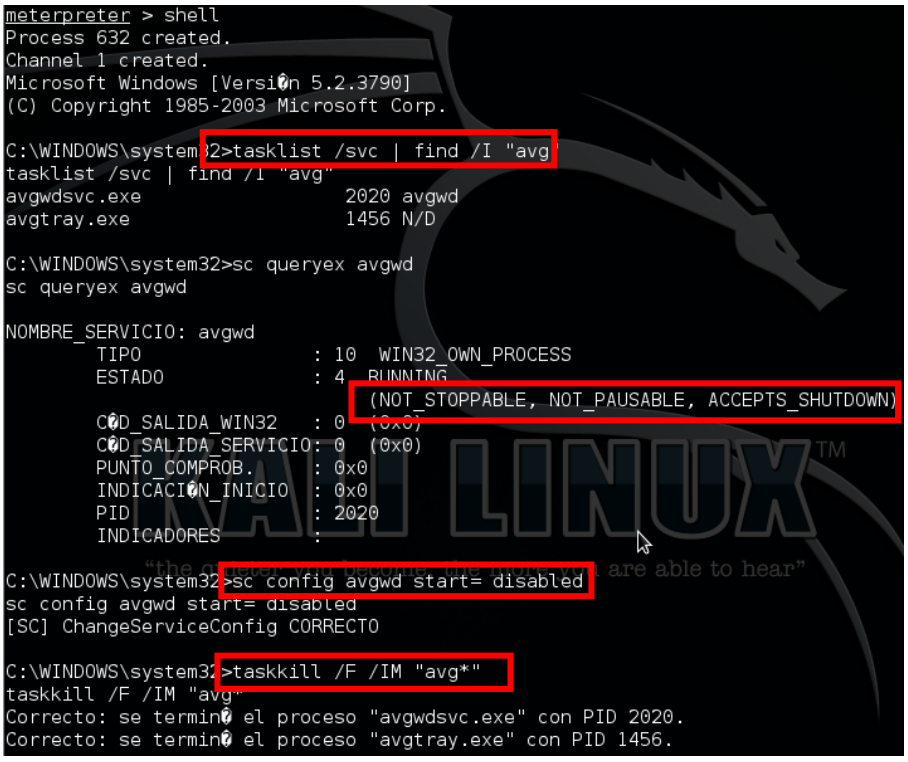
6.6.2 Deshabilitar antivirus, En cualquier momento el antivirus podría detectar y alertar al usuario de las actividades que se intentan realizar sobre el sistema, por lo que el siguiente paso es deshabilitar esta defensa del sistema. Para lograr esta tarea se va a utilizar los comandos que dispone el propio sistema Windows. Se pasa de la interfaz de **meterpreter** a **CMD** por medio del comando **shell**.

El comando **tasklist** lista todos los procesos que se están ejecutando el servidor. Para ahorrar algo de espacio, se evitó la pantalla donde se mostraba que uno de ellos es **avgwdsvc.exe**, el cual nos indica que tiene instalado el **Antivirus AVG**.

Como es habitual, muchos procesos de los antivirus se ejecutan como servicios; si se los mata, el servicio los vuelve a crear o se vuelven a ejecutar al reinicio del sistema. Para comprobar esta situación, se listan los procesos agrupando por el servicio al que pertenecen (opción **/svc**) y filtrando por el nombre de avg (comando **find /I "avg"**). El resultado es el servicio **avgwd**.

El comando que permite consultar e interactuar con los servicios del sistema es **sc**. Para conocer los atributos de un servicio se tiene la opción **query**. Para el caso del servicio de AVG, indica que **no es parable**, **pausable** y **acepta apagado**. Lo que se puede hacer, es configurar el servicio para que no se inicie al siguiente reinicio del sistema, por medio de la opción **config** y estableciendo el atributo **start= disable.** Ahora se puede matar todos los procesos del antivirus mediante el comando **taskkill**y las opciones **/F** (forzar) y **/IM "avg*"** filtrar por el nombre de los procesos que comienzan por avg.

Figura 26. Comandos para deshabilitar Antivirus AVG.



Fuente: Los autores.

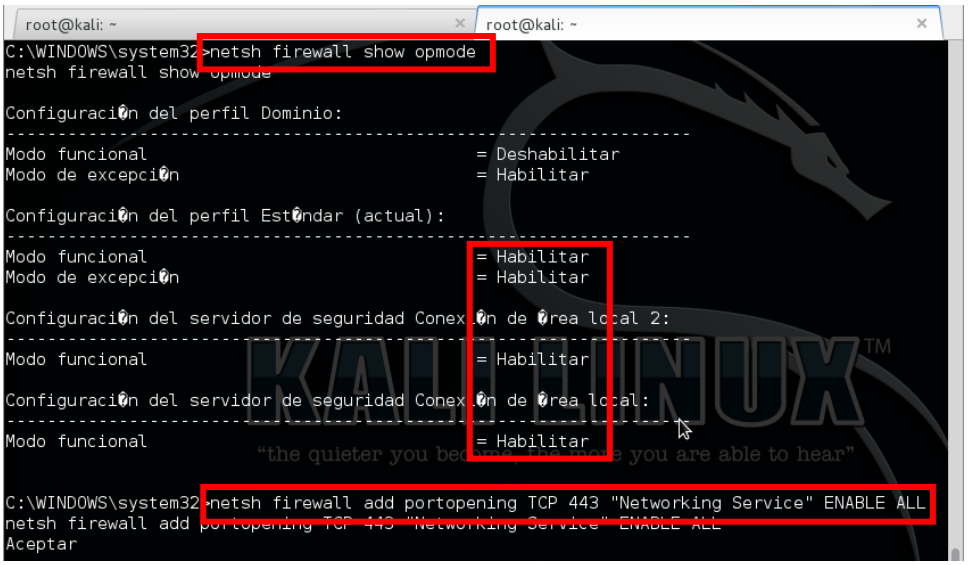
6.6.3 Abrir un puerto en el firewall. Otra de las defensas del sistema es el firewall, el cual permite o bloquea conexiones hacia y desde otras redes. Para

garantizar el acceso al sistema es necesario tener una puerta abierta, que se traduce en un número de puerto habilitado en el sistema atacante.

El comando **netsh** permite configurar muchas opciones de red, entre ellas el firewall. El firewall puede estar en funcionamiento (habilitado) o desactivado (deshabilitado). Para comprobar el estado del firewall se tiene la opción **show opmode.** La figura muestra que el firewall está activado en todos los tipos de redes.

No se desea desactivar completamente el firewall, porque podría alertar al usuario. Para habilitar solo un puerto se tiene la opción **add portopening TCP 443 "Nombre" ENABLE ALL.** Se escogió el puerto 443 para no levantar sospechas, debido a que es el número que se utiliza en las conexiones HTTPS. De esta forma se tiene listo el escenario para instalar un Backdoor.

Figura 27. Comandos para habilitar un puerto en el firewall.

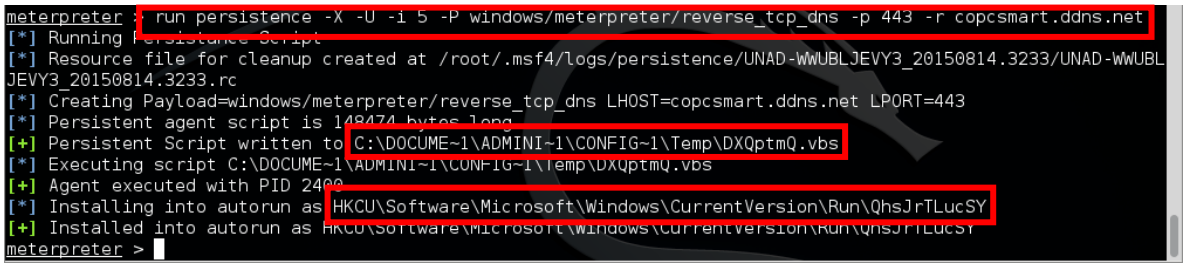


Fuente: Los autores.

6.6.4 Instalación de un backdoor. Un script muy interesante que ofrece metasploit es **persistence,** el cual, crea un Backdoor con meterpreter y lo agrega automáticamente al registro para que se ejecute en cada arranque del sistema o inicio de la sesión. Para poder ejecutar este script, el *antivirus debe estar desactivado* (tarea ya realizada en el punto 6.4.2). A continuación se explican las opciones:

-X El script se ejecute al arranque del sistema y
-U en cada inicio de sesión
-I N Para que se ejecute cada N segundos
-P Payload. Opción para escoger un Payload diferente al por defecto (**reverse_tcp**). El adecuado para el proyecto es **reverse_tcp_dns**, Las siguientes opciones son necesarias con este Payload.
-p Num. Puerto al cual se realiza la conexión. (El mismo número que se abrió en **firewall** en la fase anterior)
-r dominio El nombre de domino creado anteriormente, el cual el sistema debe resolver en una dirección IP.

Figura 28. Comandos para instalación y configuración de un Backdoor.



Fuente: Los autores.

En la imagen se observa que el script agrega una clave llamada **QhsJrTLucSY** al registro en **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**, como se sabe, es la ubicación donde se colocan los programas para que se ejecuten cuando el usuario inicia sesión.

De esta manera se concluyen las actividades que garantizan al acceso al sistema pos la primera explotación. En cualquier momento se puede colocar un escuchador especial, a la espera de que el servidor inicie la conexión hacia el atacante, dándole acceso completo por medio del Payload meterpreter. Como se muestra en el siguiente punto.

6.7 ACCESO A INFORMACIÓN CONFIDENCIAL

Es claro que al momento de la creación una cuenta de usuario en el directorio activo, además del id, se agrega otra información importante, como los son: direcciones, correos electrónicos, teléfonos, entre otras. Si se logra acceder a esta información, se pueden usar las herramientas de Kali Linux junto con técnicas de ingeniería social, para seguir penetrando la red y obtener la información que se almacena en cada equipo de un usuario.

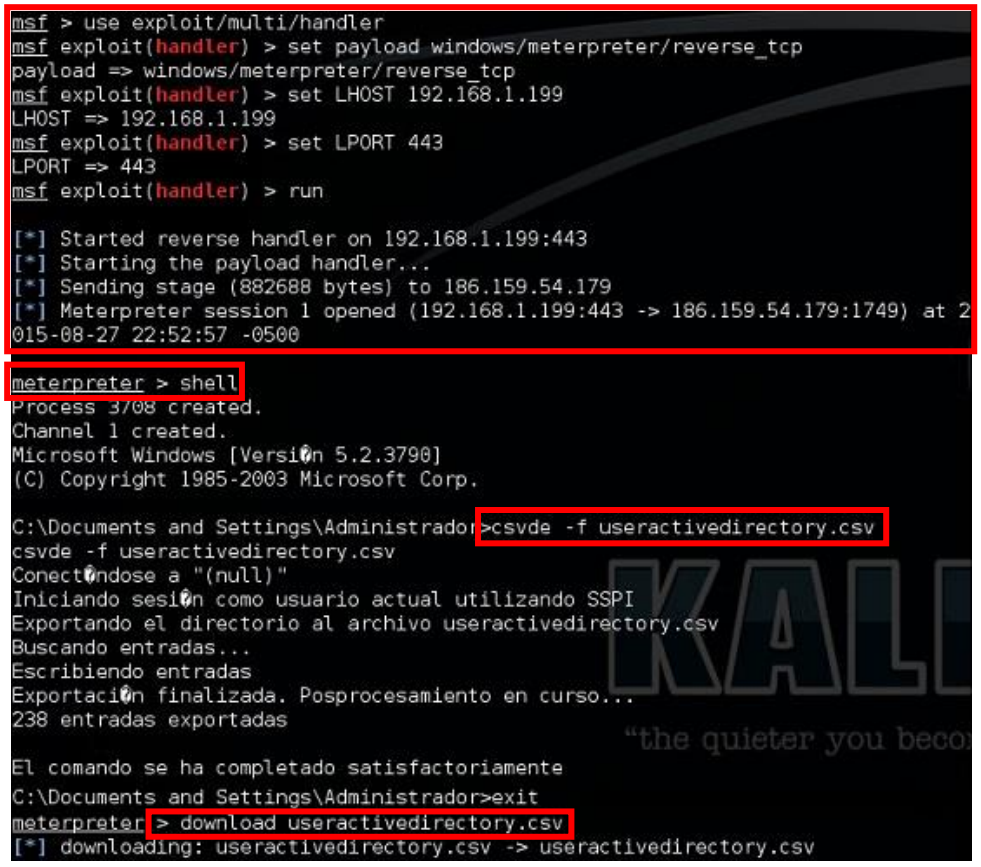
Windows Server dispone de una herramienta de comandos, llamada **csvde,** la cual permite exportarlos datos del dominio de Active Directory en un archivo en formato de valores separados por comas (CSV).

Como se había mostrado en el paso anterior, una vez el servidor se conecta al atacante y se obtiene **meterpreter**, para pasar a **CMD,** se tiene el comando **Shell.** La opción **-f** de csvde, indica el nombre de archivo de exportación. Una vez generado el archivo, para descargarlo al equipo del atacante para su posterior análisis, se tiene el comando **download** en meterpreter, por lo cual, en esta

ocasión, es necesario pasar de **CMD** a **Meterpreter**; basta con ejecutar el comando **exit** para regresar a meterpreter.

Una vez terminado el proceso, se evidencia la cantidad de entradas exportadas al archivo, el cual contiene la información detallada de cada uno de los contactos almacenados en el directorio activo, tal cual como se observa en la Figura 30.

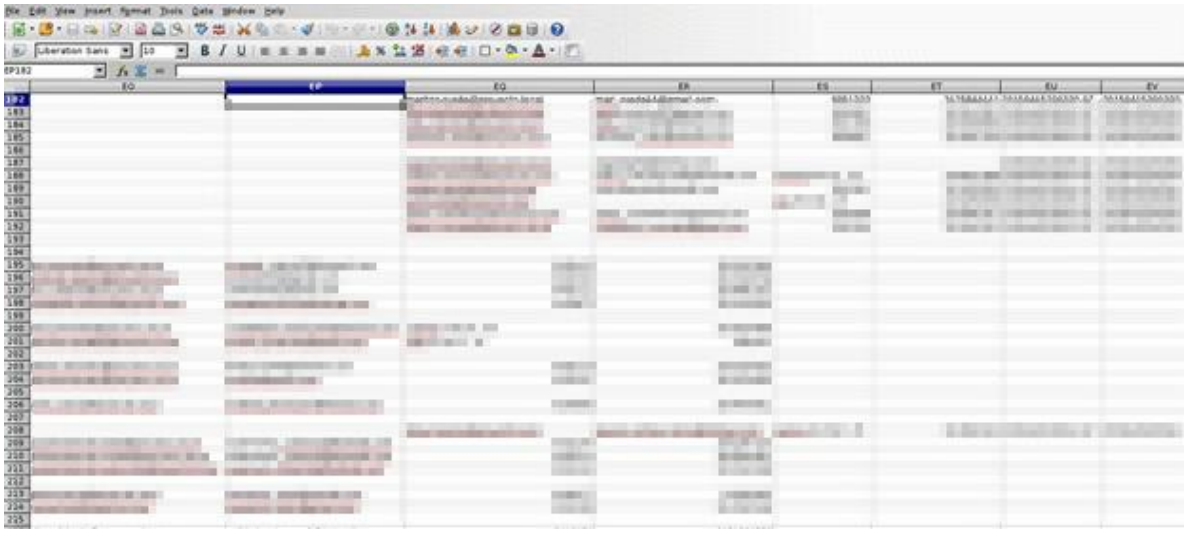
Figura 29. Acceso a la información contenida en el servicio de Active Directory



Fuente: Los autores.

La siguiente figura muestra la información contenida en el archivo, cuando se la abre con openoffice Calc.

Figura 30. Datos personales de los usuarios de Active Directory



Fuente: Los autores.

6.8 LIMPIEZA DE HUELLAS

El último proceso que se realiza en una prueba de intrusión, es eliminar todas las evidencias generadas en las actividades anteriores. Gran parte de las huellas se generan cuando ocurren eventos con los inicios de sesión, el acceso a archivos, carga de controladores, etc. Windows Clasifica los registros en tres categorías: Log de Aplicaciones, Log de Sistema y Log de Seguridad. El comando de meterpreter **clearev**, borra automáticamente dichos registros del sistema.

Los archivos creados durante la ejecución de ciertas herramientas, como el Backdoor o la exportación de los usuarios, son elementos que debe tener en

cuenta el atacante, pues dan pistas de cómo se realizó la intrusión y deben borrarse manualmente.

Para borrar un archivo en meterpreter, se le debe pasar la ruta absoluta al comando **rm**, como se muestra en la figura 32. Igualmente, si se creó una clave en el registro, entonces también hay que eliminarla.

Figura 31. Borrado de huellas

Fuente: Los autores.

7. RESULTADOS DE LA INVESTIGACIÓN

7.1 RESULTADOS DE LAS PRUEBAS

Una vez finalizadas las pruebas, se procede a realizar un análisis de los resultados obtenidos por cada una.

Pruebas de Mapeo de la Red: Se logró descubrir al servidor en el rango de direcciones IP suministradas, por medio de un sondeo inicial. Mediante un escaneo más profundo se logró identificar los servicios y versión de sistema operativo que ejecutaba. La prueba de mapeo de red arrojo 13 puertos abiertos, de aplicaciones como Active Directory y compartir archivos en red.

Pruebas de Identificación de Vulnerabilidades: El análisis de vulnerabilidades con Nessus, no arrojo ninguna vulnerabilidad crítica en los servicios que se están ejecutando en el servidor, ni tampoco alguna configuración errónea que permitiera lograr una intrusión.

Pruebas de Explotación de Vulnerabilidades. El intento de explotación de la vulnerabilidad **ms08_067_netapi** no fue exitoso, debido a que el servidor tiene instalado las actualizaciones de seguridad de Windows. Mediante una técnica de ingeniería social, se envió un PDF malicioso y se logró comprobar que el servidor tiene instalada una versión vulnerable de Adobe Reader, el cual permitió la intrusión inicial, mediante el exploit **pdf_embebed_exe** y el payload **reverse_tcp_dns.**

Pruebas Pos Explotación. Una vez lograda la explotación inicial y haber obtenido la interfaz de meterpreter, se logró realizar las tareas de desactivar el Antivirus,

abrir un puerto en el firewall e instalar un backdoor en sistema. Esto con el fin de garantizar el acceso al sistema en cualquier momento sin repetir el proceso inicial de la prueba. Para lograr estas actividades, además de las herramientas que dispone metasploit, fue necesario también emplear las herramientas Windows.

Acceso a Información Confidencial. En un acceso posterior al sistema, se logró extraer y descargar los datos personales de los empleados de la empresa contenidos en el servicio de Active Directory, mediante herramientas de comandos del propio Windows.

Limpieza de Huellas. Mediante los scripts especializados de Metasploit, se realizó un borrado de todos los elementos generados en las pruebas anteriores.

7.2 INFORME EJECUTIVO

Ver anexo 5 (Informe de resultados).

8. RECOMENDACIONES PARA SU CREDITO SA

Se recomienda a la empresa SU CREDITO SA actualizar el sistema operativo Windows server 2003 a una versión más reciente o migrar a otra plataforma, Tener un equipo de respuesta frete a una intrusión y contar con planes de acción cuando esto suceda.

Disminuir la superficie de exposición mediante la desactivación de servicios innecesarios. Colocar el servidor detrás de un firewall hardware.

Instalar un IPS (*Intrusion Prevension System*) o un Sensor en la interfaz de red, para detectar el alto tráfico generado por los escáneres como Nessus y Nmap. Monitorizar el comportamiento del sistema mediante un IDS (*Intrusion Detection System*), para detectar cambios en el sistema como, creación de archivos, la creación o muerte de procesos, y actividad en el registro de Windows,

No usar por defecto la cuenta de Administrador para administrar el servidor. Usar una cuenta diferente para la administración de cada característica del servidor, configurando los permisos mínimos para realzar esta labor.

Realizar capacitaciones al personal de la empresa en materia de seguridad informática, para advertir que ingresar a sitios web o correos de dudosa procedencia, podría abrir una brecha de seguridad.

Almacenar los eventos generados en el sistema en un servidor externo, para tener una copia de seguridad de todos los eventos generados y así hacer una reconstrucción de los hechos y buscar al atacante, en caso de que se detecte una intrusión.

9. RECOMENDACIONES PARA TRABAJOS FUTUROS.

Ahora que la versión de Windows Server 2003 ha dejado de tener soporte por parte de Microsoft, seguramente será un campo activo de investigación de nuevas vulnerabilidades, que se podrían utilizar para comprometer la seguridad de los equipos que continúen utilizando esta versión.

Para futuros proyectos de pruebas de intrusión, se recomienda tener una amplia conversación con el equipo de asesores, para lograr un buen planteamiento del perfil del proyecto (problema, objetivos, justificación). Ya que en el planteamiento inicial había una falta de entendimiento a la maquina a al cual se le iba a realizar la prueba y el escenario de la misma.

En este proyecto, el servidor está de frente hacia Internet, se puede investigar cómo realizar una intrusión bajo otras circunstancias, como por ejemplo, que él o los servidores estén detrás de una DMZ o firewall, o se hayan implementado otras soluciones de seguridad IDS o IPS. De igual manera, se podría documentar como se pueden utilizar estas herramientas para detectar y detener a un intruso en cada fase de la prueba de intrusión. Sería interesante analizar el funcionamiento de los actuales exploits con que dispone Metasploit o desarrollo de nuevos.

CONCLUSIONES

Con la realización de este trabajo se puede concluir que si fue posible ingresar al servidor de la empresa SU CREDITO SA y acceder a su información. Esta tarea fue posible gracias a la ejecución de herramientas especializadas como Nmap, Nessus y Metasploit, las cuales presentan muchas opciones, que requieren de entrenamiento y practica para su dominio. Para lograr la intrusión no solo fue necesario utilizar herramientas automatizadas, sino también, emplear técnicas como la ingeniería social.

De la revisión de la literatura se puede concluir que mantener en operación el sistema operativo Windows Server 2003 constituye un alto riesgo para cualquier empresa, debido a que dejo de tener soporte por parte de Microsoft y ha tenido un historial de fallas de seguridad que han permito la ejecución de código arbitrario. Las metodologías de pruebas de intrusión consultadas, permitió realizar las pruebas de manera ordenada y sistemática, De igual manera, con el marco legal, se pudo advertir que la realización de estas pruebas sin consentimiento de la empresa, puede acarrear penas legales. Los manuales de las herramientas consultadas permitieron conocer y aplicar las opciones adecuadas para cada una de las fases de la prueba de intrusión.

De la elaboración y ejecución del plan de pruebas, se puede concluir que cuando se realiza una prueba de intrusión desde una red privada es necesario realizar configuraciones adicionales como NAT y creación de un dominio. Este escenario no se toma en cuenta en la mayoría de la documentación disponible sobre pruebas de intrusión, pues generalmente muestran la ejecución de las pruebas en una red privada local o en un entorno virtualizado (el sistema Victima y atacante en la misma máquina). Se concluye además, que los ambientes virtuales, son muy

importantes porque permite reproducir todas las variables a analizar, antes de lanzar el ataque.

Del análisis de las pruebas y de la realización del informe ejecutivo se puede se puede concluir que es muy importante convencer a los gerentes de las empresas de realizar estas pruebas periódicamente para evaluar la seguridad de sus sistemas. De igual manera tener precaución de utilizar un lenguaje excesivamente técnico que no puedan entender los gerentes de una organización.

BIBLIOGRAFÍA

Aharoni, M. (Junio de 2011). *Tutorial de Metasploit Framework.Offensive Securitty.* Recuperado de: http://ns2.elhacker.net/timofonica/manuales/Manual_de_Metasploit_Unleashed.pdf

BSA. (Junio de 2014). *Global Software Survey.* Recuperado de: http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf

Candela, S., Garcia, C., Quesada, A., Santana, F., & Santos, J. (2007). *Fundamentos de sistemas operativos: teoría y ejercicios resueltos.* Recuperadode:https://books.google.es/books?id=fRK3lbTrNy4C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Congreso de Colombia. (Enero de 2009). *Ley 1273 de 2009.* Recuperado de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Kirsch, C. (03 de Septiembre de 2013). *Introduction to PenetrationTesting.* Recuperado de: https://community.rapid7.com/docs/DOC-2248

Microsoft. (Julio de 2002). I*ntroducción a los sistemas operativos Windows Server 2003.* Recuperado de: http://technet.microsoft.com/es-es/windowsserver/bb429524.aspx

Microsoft. (Marzo de 2005). *Microsoft Windows Server 2003 Service Pack 1 (32 bit).*Recuperado de: http://www.microsoft.com/en-us/download/details.Aspx?id=11435

Microsoft. (Diciembre de 2007). *Windows Server 2003 Service Pack 2 (32-bit x86).* Recuperado de: http://www.microsoft.com/en-us/download/details.aspx?id=41

Microsoft. (Noviembre de 2014). *Lead the pathto IT innovation today*. Recuperado de: http://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/

Microsoft. (Noviembre de 2014). *Microsoft Security Bulletin MS14-064 - Critical.* Recuperado de: https://technet.microsoft.com/en-us/library/security/ms14-064.aspx

NMAP. (2014).*Nmap Reference Guide*. Recuperado de: http://nmap.org/book/man.html

Tenable. (2014). *Nessus the Global Standard in Detecting and Assessing Network Data.* Recuperado de: http://www.tenable.com/sites/drupal.dmz.tenable security.com/files/ uploads/documents/whitepapers/using-nessus-to-detect-wap.pdf

VirtualBox. (s.f.). *Why is virtualization useful?* Recuperado de: https://www.virtualbox.org/manual/ch01.html#idp52562720

ANEXO A OPCIONES DEL ESCÁNER NAMP

La sintaxis del comando es la siguiente: http://nmap.org/man/es/

Nmap [<*Tipo de sondeo*>...] [<*Opciones*>] {<*objetivo*>}

<Tipo de sondeo>	<Opciones>	<objetivo>
-sS (TCP SYN) Sondeo por defecto si se cuenta con privilegios de Administrador. Envía un paquete SYN, esperado recibir un SYN/ACK. Funciona si no hay un firewall en medio. **-sT** (TCP Connect) Se ejecuta este sondeo si no se cuenta con privilegios de administrador. Completa el proceso de Tres vías de TCP/IP por lo que podría generar alarmas en un IDS o generar registros en el servidor. Genera gran cantidad paquetes para obtener información, por lo que podría ser lento o denegar el sistema objetivo. **-sU** (UDP) Se utiliza para probar aplicaciones UPD como DNS 53, DHCP 67,68, SMNP 161,162. Se puede combinar con sondeos TCP como SYN. Son más lentos y difíciles que los TCP. **-sN; -sF; -sX** (TCP Null, FIN, Xmas) Activan estas flags para esperar una respuesta RST si está cerrado. **-sA** (TCP ACK) Utilizado para determinar si un puerto esta filtrado y si el tipo de firewall es de estado. Si al enviar un ASK se recibe un RST significa	**-p** (Puerto) Especificar un puerto o un conjunto de puertos. Ejemplo: -p22; -p1-65535; -p U:53, 111 T:21-25,80,139 **-sP** Escanea los host mediante ping. **-O** (Fingerprint) Huellas del sistema operativo. Tratar de determinar el sistema operativo mediante las peculiaridades de la implementación de la pila TCP/IP. **-sV** Tratar de determinar la versión de la aplicación. **-v** Mostrar información detallada del proceso de escaneo. **-sn** (No portscan) No escanear todos los puertos una vez se descubran un host. **-oG**<file> Salida en archivo que se puede utilizar con grep	192.168.1.1 192.168.1.0/24 scanme.nmap.org

que o está abierto o cerrado. Si no se recibe respuesta, significa que esta filtrado. **-sW** (ventana TCP) Similar al –sA analiza el tamaño de la ventana en la respuesta RST para determinar si está abierto o cerrado. No es muy fiable. **-sM** (TCP Maimon) Envía una sonda FIN/ACK, muchos sistemas BSD no responde al paquete, si el puerto está abierto.		

ANEXO B. OPCIONES DE MSFCONSOLE

Opción	Descripción
back	Permite retroceder de un módulo.
exit	Sale de Metasploit
exploit	Una vez configurado el exploit con todos sus parámetros es lanzado con este comando. Existen dos tipos de exploit: Pasivo y Activo. Los pasivos esperan a que la víctima se conecte al atacante. Los activos se siguen ejecutando hasta que se complete u ocurra un error. Dependiendo el Payload el resultado puede ser una Shell o meterpreter (un poderoso Payload analizado más adelante).
info	Muestra información de un módulo.
search	Muy útil comando para buscar un exploit o modulo específico. También se puede combinar con tags como platform, type (exploit, auxiliary), cve
sessions	Cuando se ha logrado la intrusión en un sistema y se ha recibido una Shell, se puede guardar sesión para luego retomarla, por ejemplo con meterpreter, se realiza mediante el comando background. El comando sessions, permite listar, interactuar y matar sesiones.
set	Permite establecer el valor de un parámetro o configuración en un módulo especifico. Los parámetros más comunes en todos los exploit son: RHOST sistema remoto. LHOST sistema local RPORT Puerto remoto LPORT Puerto local
show	Muestra todos los módulos de metasploit, similar a msfcli. Se recuerda que los módulos son auxiliary, exploits, Payload, encoders, nops.

	Cuando se está en un módulo especifico, para ver las opciones del módulo se puede utilizar show options.
use	Permite seleccionar un móduloespecífico. El prompt cambia dependiendo del tipo.

ANEXO C. OPCIONES DE METERPRETER

Opción	Descripción
help	Muestra todas las demás opciones con una pequeña descripción de cada una.
background	Guarda el trabajo en segundo plano para regresar a la consola de msf, con la opción de recuperar el trabajo posteriormente con la opción sessions
cd **pwd** **ls**	Al igual que en DOS y en sistemas UNIX, cd permite cambiar de directorio. El comando pwd muestra el directorio actual. Ls lista los archivos y carpetas.
download **upload**	Download descarga un archivo del sistema remoto al atacante. Upload carga un archivo del atacante al sistema remoto (como por ejemplo un troyano). En ambos casos se debe especificar con doble slash.
migrate	El comando migrate permite migrar de un proceso a otro, es útil en ciertas tareas, como por ejemplo, para guardar las pulsaciones del teclado cuando está en proceso navegador de internet, o cuando inicia sesión.
ps **ps –S nombre**	El comando ps lista los procesos que se están ejecutando en la victima. La opción –S para filtrar por nombre.
Shell	Cambia el prompt a una Shell del sistema para ejecutar comandos propios de este.
webcam_list	Lista las cámaras web disponibles en el atacante.
webcam_snap	Captura una imagen de la cámara. Opciones: -i id de la cámara -v opt mostrar la imagen true o false

ANEXO D. HERRAMIENTAS DE KALI LINUX

INFORMATION GATHERING	
acccheck	Herramienta para el ataque de diccionario de contraseñas de Windows. Se caracteriza por ser un script que requiere de smbclient para su funcionamiento.
ace-voip	Ace VoIP (Automated Corporate Enumerator) es una herramienta enfocada en VoIP, la cual permite obtener información importante semejante a la mostrada en la pantalla de un teléfono IP (nombre, extensión, entre otras características).
Amap	Permiten identificar el puerto sobre el cual se ejecutan las aplicaciones para realizar comparaciones que permitan determinar si son el puerto correcto.
Automater	Automater permite descubrir información relevante de intrusión a partir de una URL, Hash o IP, haciendo de esta herramienta altamente usada por analistas de detección de intrusos.
bing-ip2hosts	Bing-ip2hosts realizado bajo script bash Linux, empleado como primera instancia de reconocimiento en una prueba de penetración. Bing realiza búsquedas de sitios web mediante direcciones IP, bing-ip2hosts enumera todos los host encontrados lo que favorece al analista encontrar una oportunidad mayor de ataque en la práctica.
braa	Escáner snmp en masa, a diferencia de snmpget y snmpwalk, braa realiza rápidas consultas a mayor cantidad de servidores al tiempo. Tiene como cualidad la poca cantidad de recursos de sistema consumidos en el proceso.

CaseFile	Orientado especialmente a analistas que trabajan en equipo de investigación para lograr un objetivo. La herramienta más parecida a CaseFile es Maltego.
CDPSnarf	Escáner de red únicamente para escanear paquetes CDP.
cisco-torch	Permite realizar escaneos de host remotos que ejecutan Cisco Telnet, una vez encontrados permite realizar ataques de diccionario. Permite además explorar a fondo, logrando una mayor efectividad de barrido.
Cookie Cadger	Cookie Cadger supervisael tráfico de wifi y Ethernet, con el fin de interceptar peticiones GET inseguras en un navegador. Brinda reportes gráficos gracias a la suite de Wireshark y Java.
copy-router-config	Realiza el copiado de archivos de configuración de equipos CISCO que emplean SNMP en sus procesos.
DMitry	Herramienta diseñada en C que permite analizar un host de manera detallada, logrando identificar subdominios, cuentas de email, escaneos de puertos, entre otras.
dnmap	Permite la distribución de archivos creados bajo comandos nmap a diferentes usuarios finales.
dnsenum	Script bajo perl que detalla aspectos relevantes de un DNS configurado en un dominio, entre otras funciones.
dnsmap	Herramienta diseñada para pruebas de penetración, la cual permite recolectar la mayor cantidad de información de la infraestructura analizada, incluyendo nombres de dominio, bloques de red, entre otros.
DNSRecon	Entre sus principales características se encuentran, búsqueda de registros de una dirección IP, fuerza bruta en subdominios, visualización de registros DNS en cache, entre otras.
dnstracer	Dnstracer permite hallar información importante de un DNS analizado.

dnswalk	Realiza análisis en consistencia y precisión de un DNS, siendo uno de los depuradores DNS más empleados.
DotDotPwn	Herramienta mexicana incluida en BackTrack Linux la cual permite detectar vulnerabilidades en servidores FTP, TFTP y servidores HTTP.
enum4linux	Escrito en Perl, enum4linux enumera datos de hosts de Samba y Windows.
enumIAX	Empleado mayormente como ataque de diccionario, enumIAX es un protocolo Inter Asterisk Exchange.
exploitdb	Realiza búsquedas directamente en la base de Exploit.
Fierce	Emplea diferentes tácticas para el escaneo rápido de dominios.
Firewalk	Firewalk en términos generales es una poderosa herramienta de seguridad en la red para el reconocimiento de peticiones de protocolos de capa 4, determinando que protocolos pasarán y cuáles serán denegados.
fragroute	Herramienta que ayuda en la prueba de sistemas de detección de intrusos en la red, firewall y TCP/IP.
fragrouter	Fragouter es en esencia un router de fragmentación unidireccional que implementa gran parte de los ataques descritos en el documento de 1998 “Redes Seguras (Inserción, Evasión, y denegación de servicio)”.
Ghost Phisher	Escrito en Python, Ghost Phisher permite realizar auditorías de seguridad en redes Ethernet y Wireless, emulando los puntos de acceso que permitan mejores resultados.
GoLismero	Framework para la realización de pruebas de seguridad web, el cual puede ser enfocado en diferentes exploraciones de seguridad en otros campos.
goofile	Herramienta que presta el servicio de búsqueda de archivos dentro de un dominio seleccionado.
hping3	Herramienta para probar la seguridad en la red y hosts,

	entre sus servicios se encuentran, Escaneo de puertos avanzado, pruebas de red, pruebas de firewall, entre otros.
InTrace	Aplicación para el reconocimiento de red y firewall.
iSMTP	Prueba de enumeración de usuario SMTP, spoofing y relay.
lbd	Herramienta que permite determinar si un dominio utiliza en sus procesos DNS y HTTP.
Maltego Teeth	Programa que se emplea en relaciones entre el cliente y redes sociales, cliente y empresas, entre otros.
masscan	Potente escáner de internet, con la capacidad de transmisión de 10 millones por segundo.
Metagoofil	Herramienta que permite recolectar la mayor cantidad de metadatos posible de documentos con formatos .docx, .pdf, .xls, .ppt, entre otros.
Miranda	Aplicación desarrollada en Python para el descubrimiento e interacciones con dispositivos UPnP.
Nmap	Poderosa herramienta para la detección de redes y auditoria de seguridad.
ntop	Muestra el uso de la red, semejante al comando Top Unix. Su gran ventaja es ser multiplataforma en la gran mayoría de distribuciones UNIX.
p0f	P0f es una herramienta que permite la identificación pasiva de sistemas operativos, identificando la versión de cada equipo conectado al equipo desde el cual se lanza el escaneo, permitiendo visualizar sus actividades, incluyendo el tráfico.
Parsero	Script realizado en Python para lectura de archivos de Disallow, los cuales se encargan de determinar que archivos no deben ser tenidos en cuenta por los motores web de búsqueda.
Recon-ng	Es un marco de reconocimiento web el cual proporciona un ambiente para la realización de pruebas. Se encuentra

	realizado en Phyton lo que permite el apoyo en mejoras del proyecto.
SET	Set de herramientas para la realización de pruebas de penetración de código. Dicho código es abierto y se encuentra disponible para quien desea aportar conocimiento en desarrollo.
smtp-user-enum	Como su nombre lo indica smtp-user-enum permite enumerar los usuarios en Solarios mediante SMTP.
snmpcheck	Herramienta para realizar pruebas de penetración, permite trabajar con dispositivos SNMP, generando formatos de lectura de fácil entendimiento.
sslcaudit	Sslcaudit es una herramienta para comprobar el tamaño de una aplicación o consumo de recursos que utiliza SSL/TLS a través de TCP para su comunicación.
SSLsplit	Herramienta útil para el análisis forense y Pentest.
sslstrip	Analiza el trafico HTTP de una red.
SSLyze	Útil para la identificación de posibles errores en configuración que afecten a servidores SSL.
THC-IPV6	Diseñada para encontrar las debilidades de los protocolos IPV6 e icmp6 mediante ataques.Aprovecha debilidades en protocolos IPV6 e ICMP6 para realizar ataques.
theHarvester	Permite detectar la información que puede ser vista por un atacante, entre ella se encuentra información confidencial como subdominios, puertos abiertos, email, entre otros.
TLSSLed	Evalúa la seguridad de un servidor web mediante su script Linux.
twofi	Twofidevuelve listas clasificadas de resultados de búsqueda.
URLCrazy	Genera intencionalmente errores de dominio con el fin realizar pruebas de phishing y espionaje de información.
Wireshark	Reconocido analizador de tramas de red, permite realizar

	escaneo sobre la red y obtener resultados detallados de cada proceso llevado a cabo en la red. Permite el análisis detallado en un informe completo de todos los procesos y peticiones realizados por cada máquina conectada a una red, que por medio de una tarjeta de red seleccionada se lanza el análisis en tiempo real.
WOL-E	Incluye funciones Wake sobre la LAN de equipos de una red, esta función actualmente se encuentra incluida en dispositivos APPLE.
Xplico	Realiza capturas de tramas de red, para posteriormente realizar un análisis de las aplicaciones en dicho tráfico de internet.

VULNERABILITY ANALYSIS	
BBQSQL	Marco de inyección SQL que explota debilidades encontradas, aprovecha la información proporcionada por el navegador, como lo son las url, cookies, encabezados, proxies, entre otros.
BED	Programa diseñado para la detección de desbordamiento de Bufer.
cisco-auditing-tool	Centra su análisis en la búsqueda de vulnerabilidades en routers Cisco.
cisco-global-exploiter	Realiza pruebas rápidas y avanzadas de seguridad en dispositivos Cisco.
cisco-ocs	Detecta dispositivos Cisco vulnerables.
cisco-torch	Herramienta que detecta host remotos Cisco, NTP, SNMP, entre otros, para posteriormente realizar un ataque de diccionario a las partes vulnerables.
copy-router-config	Realiza el copiado de archivos de configuración de equipos CISCO que emplean SNMP en sus procesos.

DBPwAudit	Herramienta que permite evaluar la seguridad de contraseñas en motores de bases de datos.
Doona	Herramienta diseñada en Australia que comparte algunas característicasde BED para la detección de desbordamiento de búfer.
DotDotPwn	Herramienta mexicana incluida en BackTrack Linux la cual permite detectar vulnerabilidades en servidores FTP, TFTP y servidores HTTP.
Greenbone Security Assistant	Herramienta web diseñada especialmente para la gestión de vulnerabilidades a través de una interfaz de usuario de fácil manejo.
GSD	Cliente de escritorio que se conecta con el Administrador OpenVAS mediante el protocolo OMP.
HexorBase	HeroxBase permite realizar ataques de fuerza bruta a servidores MySQL, Oracle, PostgreSQL, Microsoft SQL Server, entre otros.
Inguma	Conjunto de herramientas limitadas para realizar pruebas de penetración, permitiendo recopilar información importante como usuarios y contraseñas.
jSQL	Permite desde un servidor aislado encontrar información de una base de datos.
Lynis	Herramienta de para auditar la seguridad de código abierto, en la búsqueda permite hallar programas instalado, fallas de configuración, entre otros, a través de controles de seguridad.
Nmap	Poderosa herramienta para la detección de redes y auditoria de seguridad.
ohrwurm	Herramienta practica para la realización de pruebas de números de teléfonos SIP. Además permite obtener información de los números de puerto RTP.
openvas-administrator	Openvas-administratores el modulo para la administración del sistema de evaluación de vulnerabilidades en instalaciones locales y remotas.

openvas-cli	Colección de herramientas de línea de comandos para la administración del sistema de evaluación de vulnerabilidades mediante protocolos.
openvas-manager	Capa para realizar la comunicación entre el escáner de OpenVas y las diversas aplicaciones cliente OpenVas, permitiendo almacenar los resultados de los análisis obtenidos.
openvas-scanner	Openvas-scanner es una herramienta para la realización de auditorías de seguridad, además de ser útil en la verificación de sistemas remotos, detectando que elementos deben realizarse correcciones.
Oscanner	Sistema de evaluación de Oracle que posee plugins para enumerar las funciones de la cuenta, tipo de versión, privilegios de cuenta, políticas de contraseñas, entre otras características útiles.
Powerfuzzer	Dentro de sus fortalezas se encuentra la capacidad de detección de inyección SQL. Es altamente fácil de usar gracias a su diseño.
sfuzz	Herramienta para la realización de pruebas de caja negra mediante una sencilla interfaz que facilita su uso sin importar si no se posee conocimientos del código que se desarrolló. Entre algunas de sus características se encuentra la de brindar un lenguaje script simple para los casos de prueba realizados.
SidGuesser	Pruebas de seguridad para bases de datos basadas en Oracle, mediante el empleo de diccionarios definidos.
SIPArmyKnife	SIPArmyKnife permite detectar mediante la inyección SQL desbordamientos de buffer, cadenas de formato, entre otros elementos.
sqlmap	Detecta y explota vulnerabilidades en aplicaciones web para realizar ataques de inyección de código SQL.
Sqlninja	Logra ingresar a nivel de sistema operativo en el servidor de base de datos para emplearlo como apoyo en la red destino.
sqlsus	Con velocidad logra hacer uso de las funciones de MYSQL, permitiéndole clonar bases de datos, rastrear directorios, entre

	otros.
THC-IPV6	Diseñada para encontrar las debilidades de los protocolos IPV6 e icmp6 mediante ataques. Aprovecha debilidades en protocolos IPV6 e ICMP6 para realizar ataques.
tnscmd10g	tnscmd10ges una sencilla herramienta que analiza el tráfico del puerto tcp 1521.
unix-privesc-check	Script sencillo de ejecutar mediante usuario root o con privilegios locales. Permite su ejecución en sistemas UNIX para el hallazgo de errores de configuración que permitirían a usuarios sin privilegios tener acceso a elementos del sistema restringidos, como por ejemplo, bases de datos, configuraciones del sistema, entre otras.
Yersinia	Marco para el análisis y prueba de redes y sistemas de una organización.

WEB APPLICATIONS	
apache-users	Script que permite visualizar en lista ordenada los usuarios que utilizan Apache.
Arachni	Herramienta de apoyo en pruebas de penetración, ayuda a medir la seguridad de aplicaciones web. Tiene la cualidad de autoaprendizaje de las respuestas HTTP que capta en el proceso.
BBQSQL	Marco de inyección SQL que explota debilidades encontradas, aprovecha la información proporcionada por el navegador, como lo son las url, cookies, encabezados, proxies, entre otros.
BlindElephant	Determina la versión de una aplicación web, midiendo hashes de forma rápida.
Burp Suite	Realiza búsqueda y explotación de vulnerabilidades de seguridad en aplicaciones web.
CutyCapt	Captura formatos PDF, JPEG, GIF, BMP, entre otros, de páginas

	web.
DAVTest	Determina mediante pruebas de penetración rápidas que servicios DAV pueden ser explotados.
deblaze	Permite medir la seguridad de sitios web basados en Flash.
DIRB	Herramienta de apoyo para auditores de aplicaciones web, permite escanear el contenido web para realizar pruebas de seguridad asociadas.
DirBuster	Mediante fuerza bruta detecta nombres de directorios y archivos en aplicaciones y servidores web.
fimap	Pequeña herramienta que permite detectar errores en archivos locales y remotos en aplicaciones web.
FunkLoad	Herramienta que permite realizar pruebas de funcionamiento y de regresión de proyectos web, prueba de recursos, prueba de carga, entre otras.
Grabber	Herramienta para escanear pequeñas páginas web. Al no ser rápida demoraría en escanear una página web pesada.
jboss-autopwn	Herramienta de apoyo la cual despliega una Shell JSP en un servidor JBoss.
joomscan	Permite a los desarrolladores detectar debilidades en seguridad de sitios en Joomla.
jSQL	Permite desde un servidor aislado encontrar información de una base de datos.
Maltego Teeth	Realiza un levantamiento de posibles amenazas encontradas en una organización, mostrando la gravedad que puede tener cada falla.
PadBuster	Permite detectar si una solicitud de Oracle es vulnerable a un ataque.
Paros	Permite evaluar vulnerabilidades de aplicaciones web, integra inyecciones SQL, exploración para XSS, certificados de cliente, entre otros.
Parsero	Script realizado en Python para lectura de archivos de Disallow, los

	cuales se encargan de determinar que archivos no deben ser tenidos en cuenta por los motores web de búsqueda.
plecost	Herramienta que permite analizar una URL o resultados históricos de google, mostrando código de cada plugin encontrado.
Powerfuzzer	Dentro de sus fortalezas se encuentra la capacidad de detección de inyección SQL. Es altamente fácil de usar gracias a su diseño.
ProxyStrike	Permite encontrar vulnerabilidades mientras el usuario navega en una aplicación.
Recon-ng	Marco de reconocimiento web el cual proporciona un ambiente para la realización de pruebas. Se encuentra realizado en Phyton lo que permite el apoyo en mejoras del proyecto.
Skipfish	Herramienta de seguridad de aplicaciones web, los resultados obtenidos son mostrados en un informe que servirá como base para evaluaciones de seguridad de la aplicación.
sqlmap	Detecta y explota vulnerabilidades en aplicaciones web para realizar ataques de inyección de código SQL.
Sqlninja	Logra ingresar a nivel de sistema operativo en el servidor de base de datos para emplearlo como apoyo en la red destino.
sqlsus	Con velocidad logra hacer uso de las funciones de MYSQL, permitiéndole clonar bases de datos, rastrear directorios, entre otros.
ua-tester	Realiza comprobaciones automáticas de URL mediante lista de cadenas provistas por el usuario.
Uniscan	Herramienta de escaneo de vulnerabilidades y de ejecución remota de comandos.
Vega	Proxy de interceptación que permite la depuración de aplicaciones web que interactúan con el usuario.
w3af	Aplicación que mediante interfaz gráfica o de consola permite identificar y atacar las vulnerabilidades de aplicaciones web.
WebScarab	Permite disponer de especialistas en seguridad para hallar vulnerabilidades en una aplicación basada en HTTP.

Webshag	Desarrollada en Python, permite auditar servidores web, entre sus funcionalidades se encuentra, escaneo de puertos, escaneo de URL, entre otros.
WebSlayer	Logra resultados de gran alcance en ejecución de pruebas de aplicaciones web, mediante ataques de fuera bruta en métodos GET y POST, usuarios y contraseñas, entre otros.
WebSploit	Proyecto abierto para diferentes usos, entre los que se encuentran, ataques a USB, ataque a Applet Java, escáner phpmyadmin, entre otros.
Wfuzz	Mediante ataques de fuerza bruta en métodos GET y POST, usuarios, usuarios, contraseñas, inyecciones SQL, permite medir la seguridad de una aplicación web.
WPScan	Escáner de vulnerabilidades y de seguridad para sitios desarrollados en WorPress.
XSSer	Framework que permite detectar y explotar vulnerabilidades XSS en aplicaciones web.
zaproxy	Escáner de vulnerabilidades web, mediante la configuración del proxy en el navegador se procede a lanzar el escaneo.

PASSWORD ATTACKS	
acccheck	Herramienta para el ataque de diccionario de contraseñas de Windows. Se caracteriza por ser un script que requiere de smbclient para su funcionamiento.
Burp Suite	Realiza búsqueda y explotación de vulnerabilidades de seguridad en aplicaciones web.
CeWL	Retorna una lista de palabras que pueden ser interpretadas por sistemas como John the Ripper.
chntpw	Permite ver información y modificar contraseñas de usuarios de

	bases de datos de Windows NT/2000.
cisco-auditing-tool	Centra su análisis en la búsqueda de vulnerabilidades en routers Cisco.
CmosPwd	Permite descifrar contraseñas utilizadas para acceder a la BIOS de un computador. Esta herramienta es multiplataforma.
creddump	Extrae credenciales y registros de sesiones de Windows.
crunch	Genera miles de combinaciones posibles de palabras utilizando caracteres de su repositorio Crunch.
DBPwAudit	Herramienta que permite evaluar la seguridad de contraseñas en motores de bases de datos.
findmyhash	Acepta varios algoritmos, entre los que se encuentran algunos muy empleados, SHA256, SHA512, MD5, entre otros.
gpp-decrypt	Script que permite el descifrado de cadenas GPP.
hash-identifier	Permite identificar hashes empleados para el cifrado de información.
HexorBase	HeroxBase permite realizar ataques de fuerza bruta a servidores MySQL, Oracle, PostgreSQL, Microsoft SQL Server, entre otros.
THC-Hydra	Obtiene acceso no autorizado a sistemas remotos. Es muy compatible con el uso actual de tecnología.
John the Ripper	Altamente veloz, permite su configuración de acuerdo a las necesidades de búsqueda. Se diferencia de las demás herramientas por poseer sus propios módulos optimizados que emplea para sus ataques.
Johnny	Entorno grafico de las herramientas de John the Ripper.
keimpx	Verifica credenciales de forma rápida. Se encuentra en código abierto bajo Apache.
Maltego Teeth	Realiza un levantamiento de posibles amenazas encontradas en una organización, mostrando la gravedad que puede tener cada falla.
Maskprocessor	Herramienta de generación de palabras cuya configuración de posiciones es personalizable de acuerdo a las necesidades.

multiforcer	Brinda soporte a diferentes tipos de hash, entre los que se encuentran, SHA1, MD5, entre otros.
Ncrack	Herramienta diseñada para fortalecer la seguridad en las organizaciones, permite detectar contraseñas que no cumplan con los niveles de seguridad adecuados.
oclgausscrack	Su función es descifrar el hash de verificaciones del virus Gauss.
PACK	Analiza las formas comunes de creación de contraseñas de las personas, para a partir de allí crear mejores ataques de fuerza bruta.
patator	Herramienta multifuncional para el ataque de fuerza bruta. Incluye diversos módulos lo que la hace ser aún más eficaz.
phrasendrescher	Herramienta que mezcla varias características importantes para el ataque de fuerza bruta, entre ellas están, ataque de diccionario, multiprocesamientos, multiplataforma, entre otros.
polenum	Permite la extracción de información de la política de contraseñas de un maquina Windows, polenum permite realizar estas actividades remotamente.
RainbowCrack	RainbowCrack emplea un algoritmo especial, capaz de romper diferentes hash.
rcracki-mt	Parte de la versión rcrack, esta nueva versión incluye soporte multi-core.
RSMangler	Su funcionamiento es semejante a John The Ripper, la diferencia radica en el orden de ejecución de los procesos.
SQLdict	Su función es atacar SQL Server.
Statsprocessor	Generador de palabras que permite generación de ataques por posición.
THC-pptp-bruter	Enfoca su accionar en el puerto tcp 1723, su función es atacar a través de la fuerza bruta las debilidades de una aplicación.
TrueCrack	Posee diversas funcionalidades, entre ellas, lanzar ataques de diccionario y de alfabeto según la longitud ingresada.
WebScarab	Permite disponer de especialistas en seguridad para hallar

	vulnerabilidades en una aplicación basada en HTTP.
wordlists	Lista de palabras y símbolos almacenados en Kali Linux.
zaproxy	Escáner de vulnerabilidades web, mediante la configuración del proxy en el navegador se procede a lanzar el escaneo.

WIRELESS ATTACKS	
Aircrack-ng	Captura paquetes de datos con el fin de recuperar claves, realiza el proceso de manera rápida a comparación de otras herramientas de crackear WEP.
Asleap	Permite realizar ataques al protocolo PPTP.
Bluelog	Herramienta para monitoreo de tráfico, se enfoca principalmente en la detección de dispositivos bluetooth en un área determinada.
BlueMaho	Alertas de sonido e informes estadísticos hacen parte de esta herramienta diseñada para realizar pruebas de seguridad en dispositivos bluetooth.
Bluepot	Una de sus funciones es monitorizar ataques a través de una interfaz gráfica con variedad de herramientas.
BlueRanger	BlueRanger detecta dispositivos Bluetooth con alta calidad de alcance. Permitiendo ser medida la distancia del dispositivo según la calidad del enlace.
Bluesnarfer	Herramienta que permite detectar dispositivos vulnerables a Bluesnarfing. Esto son dispositivos que poseen falla de seguridad la cual admite la conexión a datos almacenados sin realizar ningún alerta al propietario.
Bully	Basado en el ataque de fuerza bruta WPS, aprovechándose de las vulnerabilidades del diseño de WPS.
coWPAtty	Herramienta para la realización de ataque de diccionario sobre redes WPA/ WPA2.

crackle	Aprovecha fallas en procesos BLE para realizar ataques de fuerza bruta.
eapmd5pass	Una vez realiza el análisis de una interfaz de red, extrae las autenticaciones EAP-MD5 para posteriormente generar un ataque a la contraseña del user.
Fern Wifi Cracker	Su función es servir como programa de ataque inalámbrico, realiza auditorias de seguridad en descifrado y recuperación de claves.
Ghost Phisher	Escrito en Python, Ghost Phisher permite realizar auditorías de seguridad en redes Ethernet y Wireless, emulando los puntos de acceso que permitan mejores resultados.
GISKismet	Se caracteriza por ser una herramienta inalámbrica que utiliza SQLite para sus bases de datos y GoogleEarth en las gráficas de sus archivos.
Gqrx	Sistema receptor de radio, emplea interfaz gráfica para el uso de diferentes herramientas, entre ellas, Modo FM Especial, Cambio de frecuencia, grabación y reproducción de audio, etc.
gr-scan	Muestra señales encontradas en un rango de frecuencias, se encuentra desarrollado en lenguaje C++.
kalibrate-rtl	También conocido como Kal, realiza búsquedas de estaciones GSM.
KillerBee	Herramientas para encontrar en su mayoría vulnerabilidades de ZigBee.
Kismet	Entre sus funcionalidades se encuentra, detección de intrusos, permite realizar escaneo en la red permitiendo leer los resúmenes encontrados y además descubre redes inalámbricas.
mdk3	Permite crear redes wifi falsas con el fin de saturar redes que realizan sus conexiones vía wifi.
mfcuk	Se enfoca en exponer pruebas y material de libnfc y crapto1.
mfoc	Su función es la de recuperar claves de tarjetas MIFARE Classic.
mfterm	Diseñada para el trabajo con Mifare Classic.
Multimon-NG	Permite descifrar transmisiones, entre las cuales están, POCSAG,

	EAS, MORSE CW, entre otros.
PixieWPS	Herramienta para realizar ataques de fuerza bruta con PIN a WPS (Facilita conexiones a redes WIFI a través de la asignación de código PIN de 8 dígitos.).
Reaver	Realiza un ataque de fuerza bruta al PIN de WPS con el fin de obtener la contraseña WPA/WPA2.
redfang	Mediante el ataque de fuerza bruta, redfang detecta dispositivos Bluetooth ocultos.
RTLSDR Scanner	Analizador de espectros, mediante una interfaz permite realizar escaneo de frecuencias.
Spooftooph	Su función es clonar información de sistemas Bluetooth, entre sus características se encuentran, cambiar perfil Bluetooh, Clonación de información Bluetooth, entre otras.
Wifi Honey	Script que permite la creación de puntos de acceso falsos.
Wifitap	Permite pasar por alto denegación de accesos en redes wifi mediante la inyección de tráfico.
Wifite	Herramienta de auditoría inalámbrica, entre sus funciones se encuentran, ajustes personalizables, resúmenes de sesiones, registro de contraseñas en archivo .txt.

EXPLOITATIONS TOOLS	
Armitage	Herramienta que sirve de apoyo a Metasploit mediante secuencia de comandos que permiten aumentar el impacto sobre las operaciones realizadas en la red**.**
Backdoor Factory	Parche de binarios ejecutables, permitiendo la inyección de código de una forma más rápida y eficaz.
BeEF	Herramienta cuyos servicios son para la realización de pruebas de penetración en navegadores web.
cisco-auditing-	Centra su análisis en la búsqueda de vulnerabilidades en routers

tool	Cisco.
cisco-global-exploiter	Realiza pruebas rápidas y avanzadas de seguridad en dispositivos Cisco.
cisco-ocs	Detecta dispositivos Cisco vulnerables.
cisco-torch	Herramienta que detecta host remotos Cisco, NTP, SNMP, entre otros, para posteriormente realizar un ataque de diccionario a las partes vulnerables.
crackle	Aprovecha fallas en procesos BLE para realizar ataques de fuerza bruta.
jboss-autopwn	Herramienta de apoyo la cual despliega una Shell JSP en un servidor JBoss.
Linux Exploit Suggester	Script que permite realizar seguimiento a vulnerabilidades en pruebas de penetración realizadas.
Maltego Teeth	Realiza un levantamiento de posibles amenazas encontradas en una organización, mostrando la gravedad que puede tener cada falla.
SET	Social-Engineer, permite lanzar pruebas de penetración en corto tiempo.
ShellNoob	Herramienta de apoyo para escritura de Shellcode.
sqlmap	Detecta y explota vulnerabilidades en aplicaciones web para realizar ataques de inyección de código SQL.
THC-IPV6	Diseñada para encontrar las debilidades de los protocolos IPV6 e icmp6 mediante ataques. Aprovecha debilidades en protocolos IPV6 yICMP6 para realizar ataques.
Yersinia	Marco para el análisis y prueba de redes y sistemas de una organización.

SNIFFING/SPOOFING	
Burp Suite	Realiza búsqueda y explotación de vulnerabilidades de seguridad en aplicaciones web.
DNSChef	DNS para el envío de solicitudes falsas y demás configuraciones como parte de pruebas de penetración.
fiked	Tiene como función servir de extensión de Cisco en la búsqueda de vulnerabilidades en configuraciones con ayuda de un demonio IKE no real.
hamster-sidejack	Hamster-sidejack tiene por objetivo secuestrar cookies olfateadas en la red para luego reemplazarlas por otras y hacer uso de esas sesiones.
HexInject	Mediante el uso de scripts altera el tráfico de red mediante modificaciones e interceptaciones. Funciona a manera de escáner (Sniffer).
iaxflood	Herramienta para saturar el protocolo IAX2 empleado en la PBX Asterisk.
inviteflood	Emplea el ataque de denegación de servicio (DoS) contra dispositivos SIP, enviando múltiples solicitudes INVITE según la configuración realizada.
iSMTP	Prueba de enumeración de usuario SMTP, spoofing y relay.
isr-evilgrade	Permite inyectar actualizaciones falsas aprovechando vulnerabilidades en parches y actualizaciones.
mitmproxy	Mitmproxy permite visualizar tráfico HTTPS y HTTP, es empleado en el monitoreo en aplicaciones móviles con el fin de detectar envíos realizados.
protos-sip	Se enfoca en medir la seguridad de SIP (Protocolo de Inicialización de Sesión)
rebind	Ataque de re vinculación de registros DNS.
responder	Herramienta que permite obtener credenciales pasivas, desplegando servidores falsos con el fin de obtener contraseñas en

	la red.
THC-IPV6	Aprovecha debilidades en protocolos IPV6 e ICMP6 para realizar ataques.
WebScarab	Permite disponer de especialistas en seguridad para hallar vulnerabilidades en una aplicación basada en HTTP.
Wifi Honey	Script que permite la creación de puntos de acceso falsos.
Yersinia	Marco para el análisis y prueba de redes y sistemas de una organización.
zaproxy	Escáner de vulnerabilidades web, mediante la configuración del proxy en el navegador se procede a lanzar el escaneo.

Maintaining Access	
CryptCat	CryptCates una herramienta UNIX que puede ser empleada por otros programas y scripts para la lectura de datos a través de conexiones de red, empleando los protocolos UDP y TCP.
Cymothoa	Mediante el empleo de la biblioteca ptrace permite la manipulación de procesos, a través de la inyección de código.
dbd	Dbdes una herramienta portable que ofrece un cifrado robusto para sistemas UNIX y Windows. Gracias a cifrados como SHA1, reconocido por su cifrado seguro. Dbd se encuentra bajo licencia pública GNU.
dns2tcp	Herramienta de red diseñada para la transmisión de conexiones TCP a través de tráfico DNS.
http-tunnel	Permite el envío de solicitudes a través de proxy HTTP, permitiendo tener conexión detrás de firewall a internet. En la actualidad existen diferentes páginas web que brindan este servicio.
HTTPTunnel	HTTPTunnel es una herramienta semejante a http-tunnel, especializado en realizar conexiones mediante servidores proxy,

	empleando métodos GET y POST.
Intersect	Intersectes un módulo de administración que permite al usuario crear sus propios menús de módulos según sus gustos, además de brindar la opción de importación y personalización.
Nishang	Nishangposee un listado de scripts para el uso de PowerShell el cual permite potenciar la seguridad ofensiva y la ejecución de pruebas de penetración.
polenum	Permite la extracción de información de la política de contraseñas de un maquina Windows, polenum permite realizar estas actividades remotamente.
PowerSploit	PowerSploitbrinda mecanismos durante la ejecución de pruebas de penetración, los cuales son secuencias de comandos útiles al momento de llevar a cabo los Pentest.
pwnat	Pwnates una herramienta que permite a un número de clientes detrás de NAT comunicarse con un servidor.
RidEnum	Ataque de fuerza bruta para la detección y enumeración de cuentas de usuario a través de sesiones nulas.
sbd	Sbdes una herramienta semejante a dbd, diseñado para realizar cifrado robusto mediante el empleo de hash tipo AES y SHA1, además de brindar la opción de portabilidad.
U3-Pwn	Reemplaza archivo iso original por otros de ejecución automática para la automatización de ataques de inyección de dispositivos USB.
Webshells	Colección de webshells para ASP, ASPX, CFM, JSP, Perl y servidores PHP.
Weevely	Weevelyes una herramienta web PHP que permite simular conexiones telnet para la explotación de aplicaciones web, a través de la creación de puertas traseras para la manipulación de cuentas web.
Winexe	Winexe ejecuta remotamente comandos en Windows NT / 2000 / XP sistemas de GNU / Linux.

Reverse Engieering	
apktool	Apktool es una herramienta para la realización de ingeniería inversa, ampliamente utilizadas para aplicaciones Android.
dex2jar	Dex2jar posee un conjunto de herramientas para la lectura y traducción de archivos dex, además de herramientas para trabajar con archivos .class y modificar archivos .apk
diStorm3	diStorm3es una biblioteca C para la descompresión de archivos, puede ser usado en módulos integrados o kernel.
edb-debugger	Herramienta similar del depurador Olly de la plataforma Windows paraLinux, posee una interfaz gráfica de usuario de fácil manejo, además de un fácil análisis de instrucciones.
jad	Jad es un descompilador de JAVA
javasnoop	Programa realizado en Java para la reversión de aplicaciones en aquellos casos en los que no se puede tener acceso al código fuente de la aplicación,
JD-GUI	JD-GUI es una utilidad gráfica que permite observarel código fuente de archivos .class de Java.
OllyDbg	Se caracteriza por ser un depurador que analiza el código binario útil en casos que la fuente no se encuentra disponible para Microsoft Windows.
smali	Smalies un ensamblador y desensamblador para aplicaciones Android de Java en formato dex Dalvik.
Valgrind	Valgrind es un sistema para la depuración de programas de Linux. Permite detectar errores de gestión de memoria para fortaleces el desarrollo de programas más estables.
YARA	Describegrupos de malware basado en texto o patrones binarios contenidos.

Stress Testing	
DHCPig	Permite iniciar un ataque avanzado DHCP que además analiza las IPs de una LAN.
FunkLoad	Herramienta que permite realizar pruebas de funcionamiento y de regresión de proyectos web, prueba de recursos, prueba de carga, entre otras.
iaxflood	Herramienta para saturar el protocolo IAX2 empleado en la PBX Asterisk.
Inundator	Inundatorpermite la detección de intrusos anónimos que realizan ataques contra falsos positivos.
inviteflood	Emplea el ataque de denegación de servicio (DoS) contra dispositivos SIP, enviando múltiples solicitudes INVITE según la configuración realizada.
ipv6-toolkit	Conjunto de herramientas para la evaluación de la seguridad y solución de problemas de herramientas IPv6.
mdk3	Permite crear redes wifi falsas con el fin de saturar redes que realizan sus conexiones vía wifi.
Reaver	Realiza un ataque de fuerza bruta al PIN de WPS con el fin de obtener la contraseña WPA/WPA2.
rtpflood	Herramienta de línea de comandos utilizada para inundar dispositivos procesadores de RTP.
SlowHTTPTest	SlowHTTPTestes una herramienta configurable que permite la simulación de capas de aplicacionespara ataques del servicio. Posee además la cualidad de ser multiplataforma.
t50	t50 es un protocolo múltiple de herramientas para realizar ataques de inyección para sistemas * nix.
Termineter	Termineteres un framework que ofrece una plataforma de pruebas de seguridad de contadores inteligentes.
THC-IPV6	Diseñada para encontrar las debilidades de los protocolos IPV6 e icmp6 mediante ataques. Aprovecha debilidades en protocolos

	IPV6 e ICMP6 para realizar ataques.
THC-SSL-DOS	Herramienta para la verificación de rendimiento de SSL.

Hardware Hacking	
android-sdk	SDK de Android que aporta bibliotecas API y herramientas de desarrollo necesarias para construir, probar y depurar aplicaciones para Android.
apktool	Apktool es una herramienta para la realización de ingeniería inversa, ampliamente utilizadas para aplicaciones Android.
Arduino	Arduinoes una plataforma de prototipos electrónicos de código abierto para medir su flexibilidad, hardware y software, está enfocada para diseñadores de entornos interactivos
dex2jar	Dex2jar posee un conjunto de herramientas para la lectura y traducción de archivos dex, además de herramientas para trabajar con archivos .class y modificar archivos .apk
Sakis3G	Sakis3Ges una herramienta para establecer una conexión 3G con cualquier combinación de módem o de operador.
smali	Smalies un ensamblador y desensamblador para aplicaciones Android de Java en formato dex Dalvik.

Forensics	
Binwalk	Herramienta que permite realizar búsqueda de imágenes de firmware dada para archivos incrustados y de código ejecutable.
bulk-extractor	Herramienta que permite la extracción de características como direcciones de correo electrónico, números de tarjetas de crédito, direcciones URL, y otros tipos de información de archivos de evidencia digitales.

Capstone	Permite el desmontaje en el motor de disasm para el análisis binario en procesos de seguridad.
chntpw	Permite ver información y modificar contraseñas de usuarios de bases de datos de Windows NT/2000.
Cuckoo	Cuckooes un sistema de análisis de malware, permite visualizar resultados detallados que describen lo que existe en cada fichero cuando se ejecuta dentro de un entorno aislado.
dc3dd	dc3dd es una versión parcheada de GNU con características adicionales para la informática forense.
ddrescue	Ddrescueposee una función simple, la cual consiste en realizar copia de datos de un archivo o dispositivo de un bloque a otro.
DFF	DFFes una fuente de informática forense de software libre y de código abierto desarrollada sobre una interfaz de programación de aplicaciones dedicadas (API).
diStorm3	diStorm3es una biblioteca C para la descompresión de archivos, puede ser usado en módulos integrados o kernel.
Dumpzilla	Dumpzillapermite extraerinformación forense importante de navegadores Firefox, Iceweasel y SeaMonkey.
extundelete	Extundeletees una utilidad que puede recuperar archivos borrados de una partición ext3 o ext4.
Foremost	Foremostes una herramienta que permite recuperar archivos perdidos en función de sus encabezados, pies de página, y las estructuras de datos internas.
Galleta	Herramienta forense que examina el contenido de los archivos cookie producidos por Microsoft de Internet Explorer.
Guymager	Herramienta generadora de imágenes forenses de libre adquisición de medios de comunicación.
iPhone Backup Analyzer	Herramienta diseñada para navegar fácilmente a través de la carpeta de copia de seguridad de un iPhone (o cualquier otro dispositivo iOS).
p0f	P0f es una herramienta que permite la identificación pasiva de

	sistemas operativos, identificando la versión de cada equipo conectado al equipo desde el cual se lanza el escaneo, permitiendo visualizar sus actividades, incluyendo el tráfico.
pdf-parser	Herramienta que analizaun documento PDF para identificar los elementos fundamentales utilizados en el archivo analizado.
pdfid	Herramienta de escaneode archivos con el fin de detectar palabras claves en PDF para verificar su contenido.
pdgmail	Herramienta que permite el análisis de elementos de gmail con el fin de detectar contactos, correos electrónicos, últimos accesos, direcciones IP, entre otros.
peepdf	Peepdfes una herramienta desarrollada en Python para explorar archivos PDF con el fin de averiguar si el archivo puede ser perjudicial o no.
RegRipper	RegRipperes una herramienta de código abierto, para la extracción y análisis de información de claves y datos de registros para realizar un posterior análisis de los mismos.
Volatility	Volatility es un conjunto de herramientas de código abierto para la extracción de artefactos digitales de memorias RAM.
Xplico	Realiza capturas de tramas de red, para posteriormente realizar un análisis de las aplicaciones en dicho tráfico de internet.

Reporting Tools	
CaseFile	Orientado especialmente a analistas que trabajan en equipo de investigación para lograr un objetivo. La herramienta más semejante a CaseFile es Maltego.
CutyCapt	Captura formatos PDF, JPEG, GIF, BMP, entre otros, de páginas web.
dos2unix	dos2unixposee una suite de herramientas, entre las que se encuentran,unix2dos, dos2unix, mac2unix y unix2mac para

	conversión de archivos de texto entre formatos UNIX (LF), DOS (CRLF) y Mac (CR).
Dradis	Aplicación web que proporciona un repositorio de información para realizar un seguimiento de lo que se realiza, y lo que está por realizarse durante evaluaciones de seguridad.
KeepNote	Herramienta multiplataforma que permite almacenar apuntes de cualquier tipo, útiles durante la ejecución de procesos de Pentest.
MagicTree	Herramienta que permite la generación de informes, diseñada para consolidación de datos.
Metagoofil	Herramienta que permite recolectar la mayor cantidad de metadatos posible de documentos con formatos .docx, .pdf, .xls, .ppt, entre otros.
Nipper-ng	Herramienta que permite realizar observaciones acerca de configuraciones de seguridad de diferentes tipos de dispositivos como routers, firewalls y switches de una red.
Pipal	Herramienta para la realización de estadísticas para ayuda en el análisis de contraseñas.

ANEXO E. INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN A SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

Mediante el siguiente informe, se realiza una prueba de penetración al Servidor Windows Server 2003, sobre accesos no autorizados y la posible pérdida de información en SUCREDITO S.A

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

INTRODUCCIÓN

La seguridad informática tiene por objetivo garantizar la disponibilidad, integridad y confidencialidad de la información almacenada en un sistema.

La pérdida de datos o robo de información mediante accesos no autorizados puede ocasionar graves problemas que afectarían la información sensible y confidencial de la empresa y de sus clientes.

Mediante una prueba de intrusión, se puede detectar aquellas vulnerabilidades desconocidas para la organización, antes de que un atacante las explote, lo que permite realizar una evaluación de seguridad en entornos físico, personas, redes, sistemas operativos, sistemas de información, aplicaciones web, entre otros.

En el presente resumen se presentarán los resultados de la explotación de las vulnerabilidades de mayor impacto del sistema operativo Windows Server 2003 que ejecuta la empresa SUCREDITO SA, mediante las herramientas de Kali Linux.

OBJETIVO

Analizar los resultados obtenidos de la prueba de intrusión al servidor de la empresa SUCREDITO SA mediante el uso de herramientas de Kali Linux.

FORMULACIÓN DE PROBLEMA

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

¿Presenta el Servidor (Windows Server 2003) de la empresa SUCREDITO SA vulnerabilidades reconocidas; y de ser así, con qué herramientas se pueden identificar y explotar?

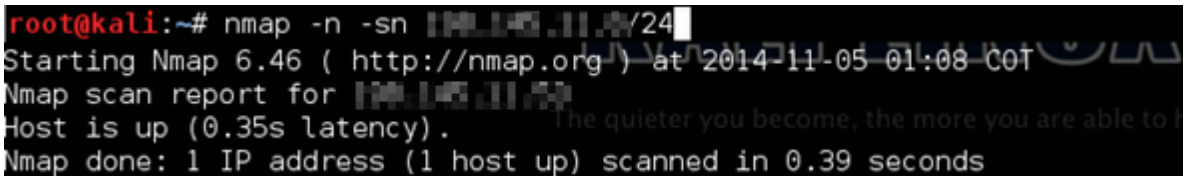
A continuación se detalla cada uno de los procesos llevados a cabo durante la prueba de penetración, describiendo el objetivo de cada herramienta usada y un posterior análisis de los resultados obtenidos.

RESULTADOS

FASE 1. PRUEBA DE MAPEO DE RED

Este tipo de prueba tiene por objetivo descubrir equipos en una red, los servicios que ejecuta, entre otros aspectos.

Mediante la herramienta NMAP se realizó el mapeo de red, a partir de un rango de direcciones IP proporcionadas por SUCREDITO S.A., los resultados obtenidos fueron los siguientes:



Al identificar la IP W.X.Y.Z activa, se procede a realizar un escaneo más profundo para conocer en detalle los puertos-servicios que están abiertos.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

La siguiente tabla presenta una lista detallada de cada puerto descubierto por NMAP.

PUERTO	SERVICIO
21/tcp	ftp
23/tcp	telnet
25/tcp	Smtp
42/tcp	Nameserver
53/tcp	Domain
80/tcp	http
135/tcp	Msrpc
139/tcp	Netbios-ssn
445/tcp	Microsoft-ds
1035/tcp	Multidropper
1039/tcp	Sbl
3389/tcp	Ms-wbt-server
8099/tcp	unknown

A partir de los puertos encontrados, mediante la herramienta NESSUS se da inicio al escaneo en busca de vulnerabilidades.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

FASE 2. PRUEBAS DE IDENTIFICACIÓN DE VULNERABILIDADES.

A través de escaneos mediante el uso de NESSUS, se pretende descubrir vulnerabilidades del Servidor.

A continuación se detalla 2 tipos de escaneos llevados a cabo:

1) En la instalación por defecto del Servidor con el service pack 1.
2) Con la instalación de todas las con las actualizaciones de seguridad disponibles, incluyendo el service pack 2.

FASE 2.1. ESCANEO EN LA INSTALACIÓN POR DEFECTO DEL SERVIDOR, CON EL SERVICE PACK 1.

En la siguiente grafica se observa un Informe de vulnerabilidades del Servidor. El sistema presentaba 3 vulnerabilidades críticas que permiten ejecutar un código arbitrario, una de ellas la *MS08-067,* dicha vulnerabilidad solo está presente en sistemas sin las actualizaciones automáticas.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

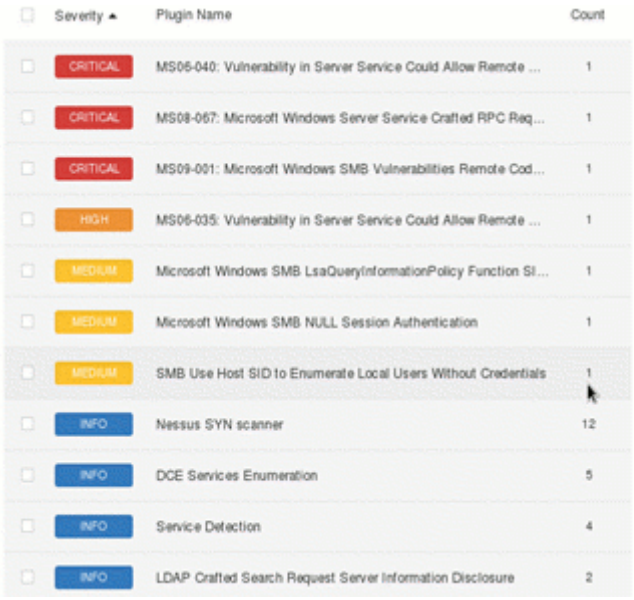
Colombia - Medellín

2015

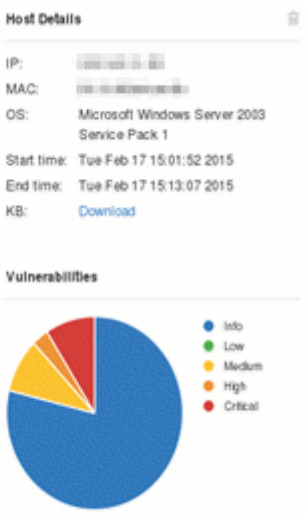
INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015



Severity	Plugin Name	Count
CRITICAL	MS06-040: Vulnerability in Server Service Could Allow Remote ...	1
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Req...	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Cod...	1
HIGH	MS06-035: Vulnerability in Server Service Could Allow Remote ...	1
MEDIUM	Microsoft Windows SMB LsaQueryInformationPolicy Function SI...	1
MEDIUM	Microsoft Windows SMB NULL Session Authentication	1
MEDIUM	SMB Use Host SID to Enumerate Local Users Without Credentials	1
INFO	Nessus SYN scanner	12
INFO	DCE Services Enumeration	5
INFO	Service Detection	4
INFO	LDAP Crafted Search Request Server Information Disclosure	2



Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

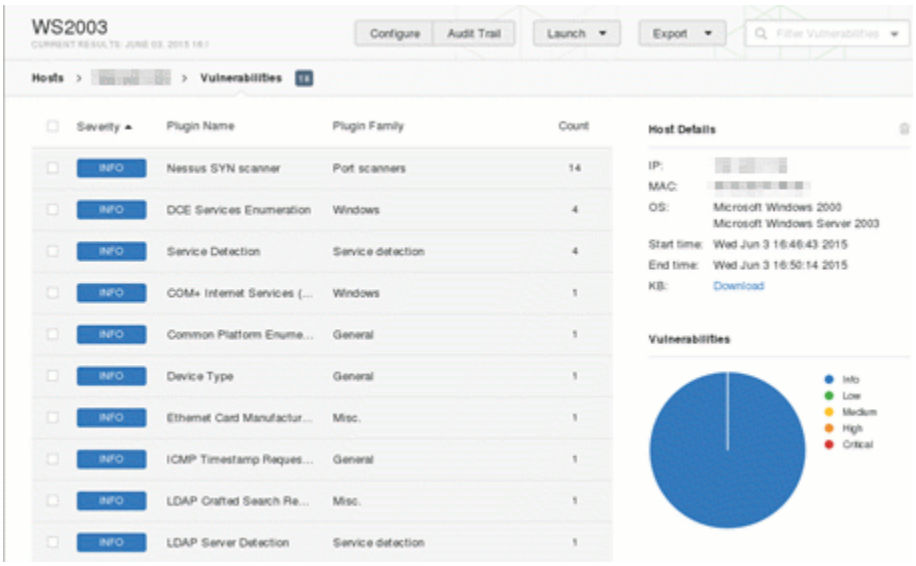
INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

FASE 2.2. ESCANEO CON LAS ACTUALIZACIONES DE SEGURIDAD DISPONIBLES INCLUYENDO SERVICE PACK 2.

El escaneo llevado a cabo al servidor con Service Pack 2 y las actualizaciones automáticas instaladas, no presenta vulnerabilidades críticas presentes, todas son de tipo información, tal como se observa a continuación.



Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

FASE 3. PRUEBAS DE EXPLOTACIÓN DE VULNERABILIDADES.

Una vez realizado el escaneo de vulnerabilidades, se procedió a probar los diferentes exploits.

FASE 3.1. INTENTO DE EXPLOTACIÓN DE LA VULNERABILIDAD MS08_067.

Al ejecutar el exploit **ms08_067_netapi** desde la consola de Metasploit, se obtuvo un resultado fallido, debido a que el servidor tiene instaladas las últimas actualizaciones de seguridad.

Por este motivo se replanteo la manera de realizar la explotación y se implementaron las siguientes pruebas que se describen en las siguientes fases.

FASE 3.2. INTENTO DE EXPLOTACIÓN MEDIANTE INGENIERÍA SOCIAL Y VULNERABILIDAD EN ADOBE READER.

Los resultados obtenidos por parte de NESSUS, no arrojaron vulnerabilidades críticas, por lo que se procedió a realizar pruebas en software de escritorio, en este caso se escogió Adobe Reader, partiendo de estadísticas que demuestran una alta tasa de vulnerabilidades descubiertas que permiten ejecutar un código arbitrario, este tipo de ataque consiste en crear un archivo PDF malicioso que después se puede enviar por correo electrónico al administrador del sistema, esperar a que lo abra e iniciar una conexión **Reverse TCP** al atacante.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

Mediante el exploit **adobe_pdf_embedded_exe**, se estableció los parámetros de configuración antes de realizar el ataque, añadiendo un nombre de PDF inicial en donde se ocultó la carga maliciosa y la adición de puertos de escucha.

El PDF generado: **cotizacion.pdf** se colocó en la carpeta del servidor web del atacante que suplanta al de la empresa PC Smart.

El siguiente paso consistió en utilizar una técnica de ingeniería social, enviando las URL de descarga del archivo al administrador del sistema por correo electrónico, tal como se evidencia a continuación:

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

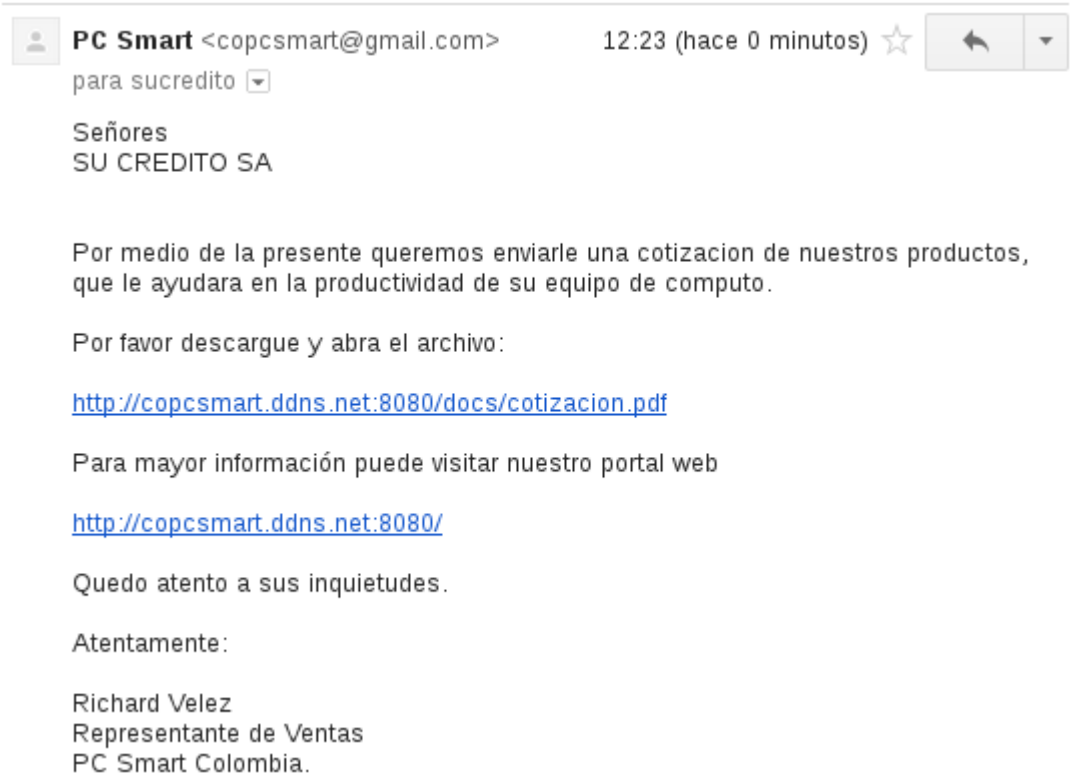
Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015



PC Smart <copcsmart@gmail.com> 12:23 (hace 0 minutos)

para sucredito

Señores
SU CREDITO SA

Por medio de la presente queremos enviarle una cotizacion de nuestros productos, que le ayudara en la productividad de su equipo de computo.

Por favor descargue y abra el archivo:

http://copcsmart.ddns.net:8080/docs/cotizacion.pdf

Para mayor información puede visitar nuestro portal web

http://copcsmart.ddns.net:8080/

Quedo atento a sus inquietudes.

Atentamente:

Richard Velez
Representante de Ventas
PC Smart Colombia.

Una vez enviado el correo se realizó un tiempo de espera, mientras el administrador del sistema abriera el archivo PDF, al realizarse la apertura del archivo, se ejecutó dicho archivo, se ejecutó una serie de instrucciones que inició una conexión hacia nuestra IP y puerto.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

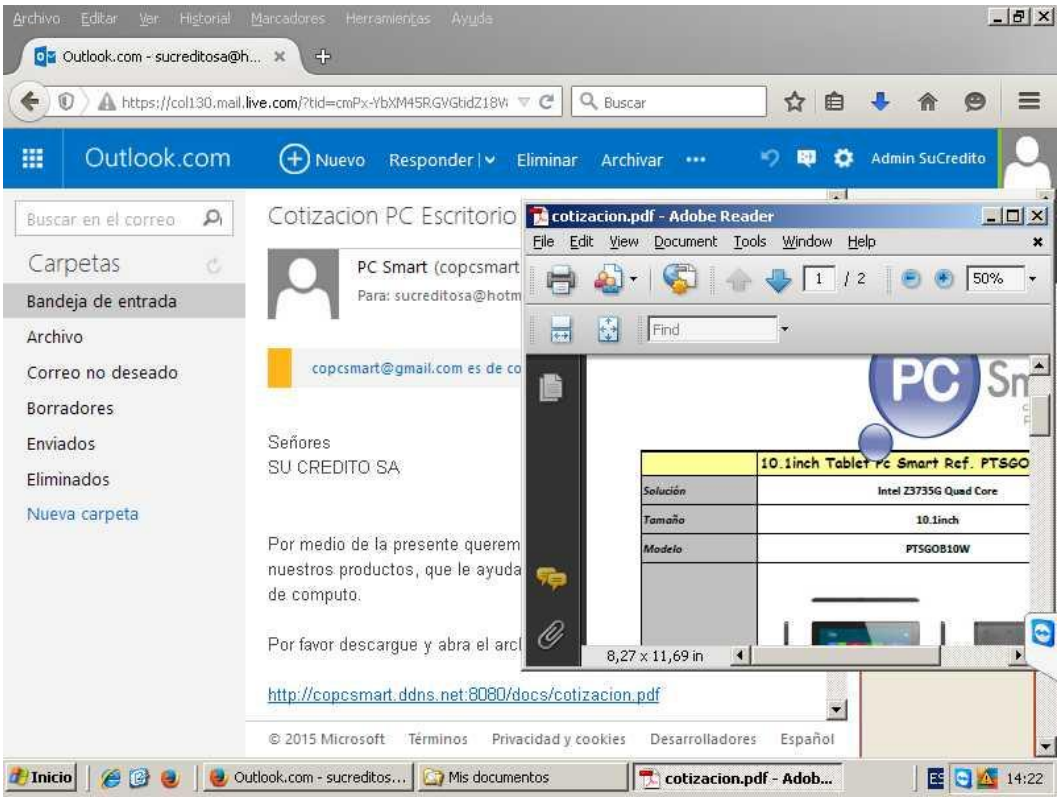
Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015



Ademas de lo anterior, la apertura del archivo PDF por parte de la persona de sistemas al que fue enviado, permitió que se ejecutara un payload meterpreter, el cual permite tener acceso a la maquina por medio de línea de comandos, como si estuviera en frente de ella, ademas de poder interactuar con casi cualquier elemento del sistema, como archivos, procesos, registro, cámara, teclado, entre otros.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

Lo anterior evidenció una vulnerabilidad que una vez explotada permitió interactuar con el objetivo por medio de comandos.

El siguiente objetivo fue garantizar el acceso al servidor en otro momento, por si el usuario apagara el servidor y se perdiera la conexión o si actualiza el software vulnerable.

FASE 4. PRUEBAS POS EXPLOTACIÓN.

Con el fin de garantizar el acceso al sistema en cualquier momento sin tener que esperar a que el usuario abra otra vez el PDF malicioso, por si realizara una actualización de seguridad en Adobe Reader, se realizaron los siguientes procesos descritos a continuación:

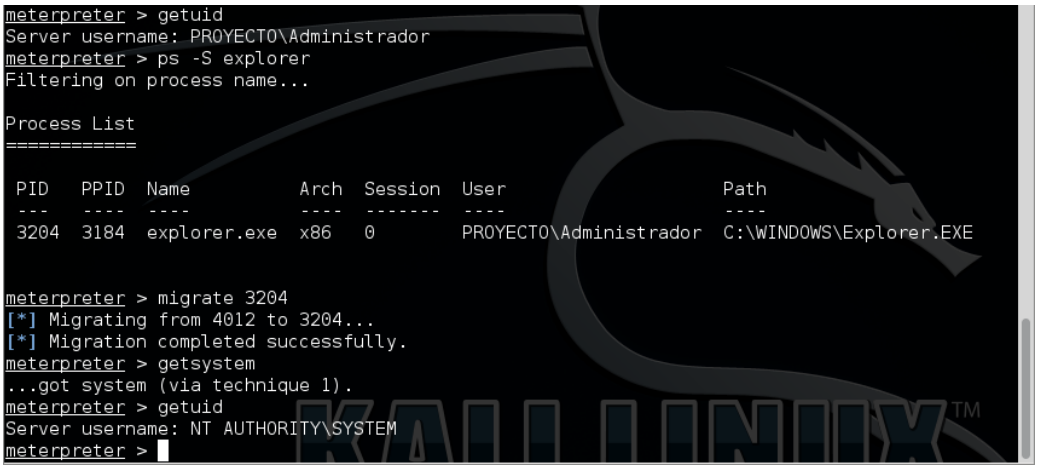
FASE 4.1. ELEVACIÓN DE PRIVILEGIOS.

Por medio de comandos de consola se obtuvieron privilegios de usuario System, el cual tiene dominio total del sistema, el primer paso realizado fue obtener el nombre del usuario que realizó la apertura del archivo PDF, posteriormente se migró el proceso original en ejecución a un proceso explorer, el cual es medianamente permanente, los resultados obtenidos fueron satisfactorios.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015



FASE 4.2. DESHABILITACIÓN DE ANTIVIRUS.

En cualquier momento el antivirus podría detectar y alertar al usuario de las actividades que se intentaban realizar sobre el sistema, por lo que el siguiente paso fue deshabilitar esta defensa del sistema.

El comando **tasklist** lanzado mediante la opción Shell de Meterpreter, se visualizó en la lista de procesos ejecutados en el servidor, el proceso del Antivirus AVG.

Como es habitual, muchos procesos de los antivirus se ejecutan como servicios; si se les mata, el servicio los vuelve a crear o se vuelven a ejecutar al reinicio del sistema, para comprobar esta situación, se listaron los procesos agrupando por el servicio al que pertenecen y filtrando por el nombre de avg, obteniendo el resultado del servicio.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

El siguiente paso consistió en a través de un comando interactuar con los servicios del sistema, lo que se obtuvo del servicio de AVG, indicó que no es parable, pausable y acepta apagado, por lo que se pudo determinar que la manera de realizar el proceso era mediante la configuración del servicio para que no se iniciara al siguiente reinicio del sistema.

Posteriormente se mataron los procesos correspondientes al antivirus AVG, los cuales una vez listados, se clasificaron por las palabras avg, el proceso se realizó mediante sentencias de comandos, a continuación evidenciadas:

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

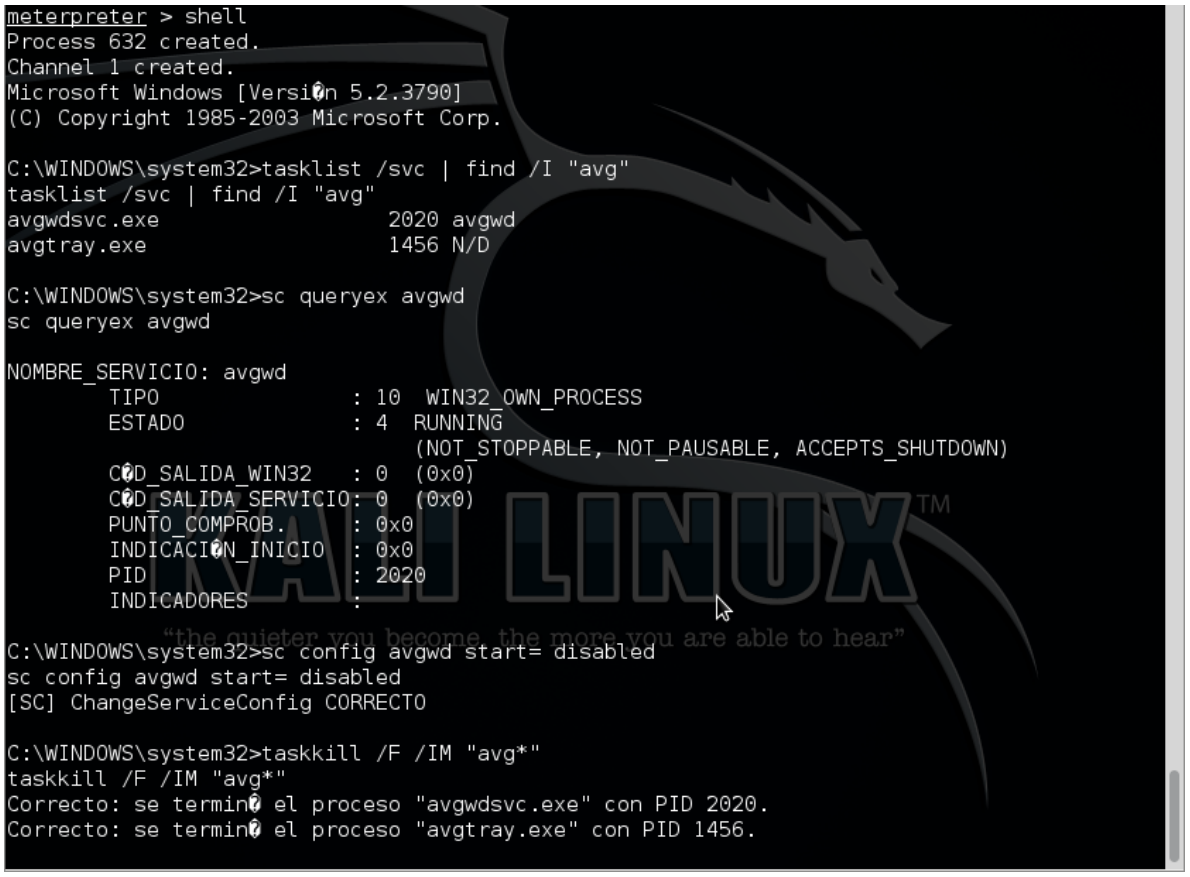
Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015



Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015

FASE 4.3. APERTURA DE PUERTO EN EL FIREWALL.

Se tuvo en cuenta una de las defensas del sistema, llamada firewall, el cual permite o bloquea conexiones hacia y desde otras redes. Para garantizar el acceso al sistema es necesario tener una puerta abierta, que se traduce en un número de puerto habilitado en el sistema.

Mediante la ejecución del comando netsh, el cual permite configurar muchas opciones de red, entre ellas el firewall, se ejecutó la verificación del estado del mismo, para comprobar si este se encontraba habilitado o deshabilitado a través de la opción show opmode, lo que permitió evidenciar que el firewall se encontraba activo en todos los tipos de redes.

No se deseaba desactivar completamente el firewall, porque podría alertar al usuario, por lo que se decidió habilitar solo un puerto mediante la ejecucion de sentencia de comandos, el puerto escogido fue el puerto 443 para no levantar sospechas, debido a que es el número que se utiliza en las conexiones HTTPS.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

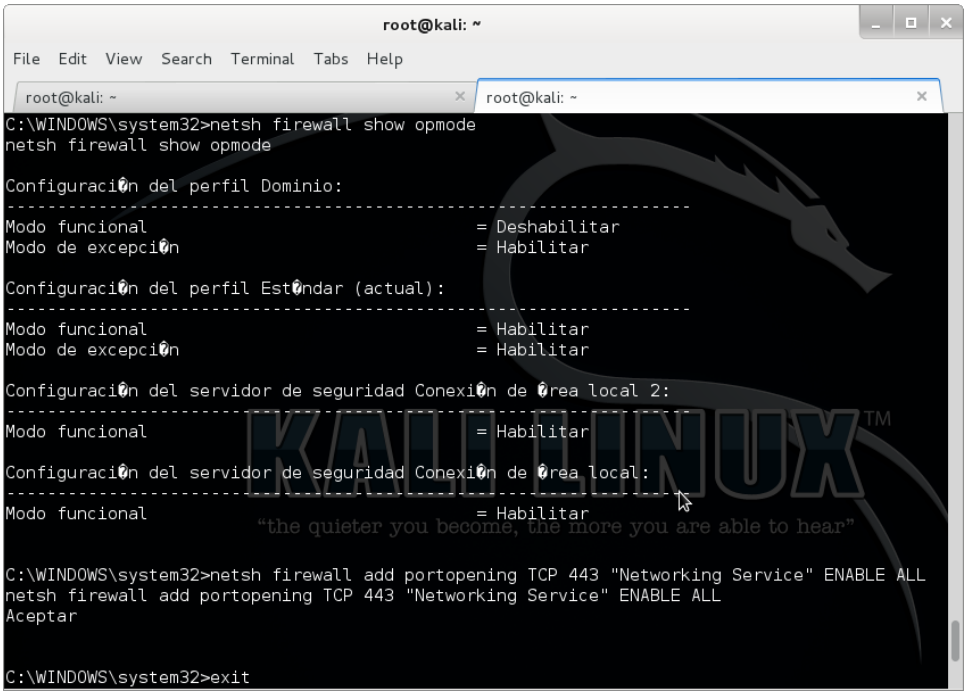
Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015



Las anteriores actividades prepararon el escenario para instalar un backdoor, como se describe a continuación:

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

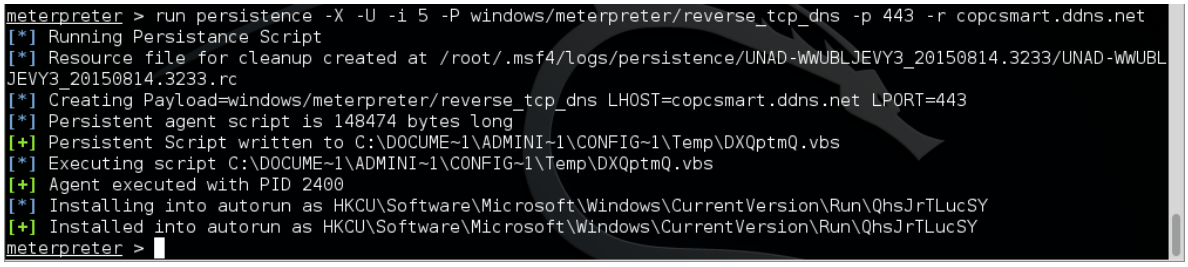
Colombia - Medellín

2015

FASE 4.4. INSTALACIÓN DE UN BACKDOOR.

Mediante la ejecucion del script *persistence* de metasploit se creó un backdoor con meterpreter y se agregó automáticamente al registro para que se ejecutara en cada arranque del sistema o inicio del sesión, la realizacion de esta fase implicó la desactivacion del antivirus, descrita anteriormente en el informe ejecutivo.

Los parámetros configurados previos a la ejecución del script fueron: ciclo en segundos de la ejecución, puerto al cual se realiza la conexión, nombre de dominio, opción de arranque al iniciar el sistema, entre otros, a continuación se evidencia dicha configuración:



Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

FASE 5. ACCESO A INFORMACIÓN CONFIDENCIAL.

Una vez llevadas a cabo cada una de las fases descritas anteriormente, se procedió a extraer información confidencial que es agregada al momento de la creación de usuarios en el directorio activo, como los son: direcciones, correos electrónicos, teléfonos, entre otras; una vez se logró ingresar a la información como se evidencia más adelante, se podría usar más herramientas de Kali Linux combinadas con técnicas de ingeniería social, para seguir penetrando la red y obtener la información que se almacena en cada equipo de un usuario.

El proceso se realizó mediante una herramienta propia de Windows, lanzada desde meterpreter, la cual permite acceder a la terminal y ejecutarla, la cual agregando ciertos parámetros de configuración permite la exportación en un archivo separado por comas, conocido como CSV.

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

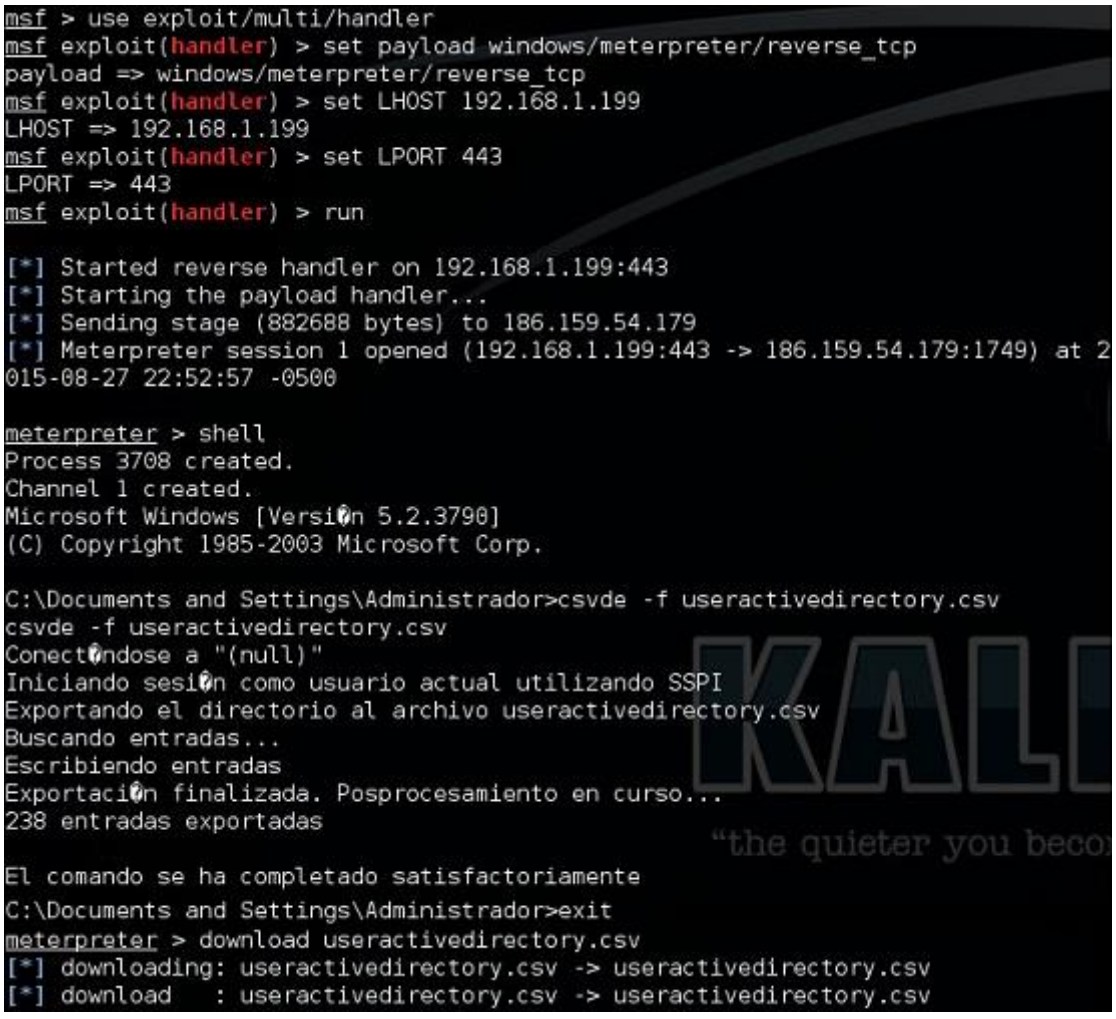
Colombia - Medellín

2015

INFORME EJECUTIVO DE PRUEBA DE INTRUSIÓN AL SISTEMA OPERATIVO WINDOWS SERVER 2003

SUCREDITO S.A

UNAD 2015



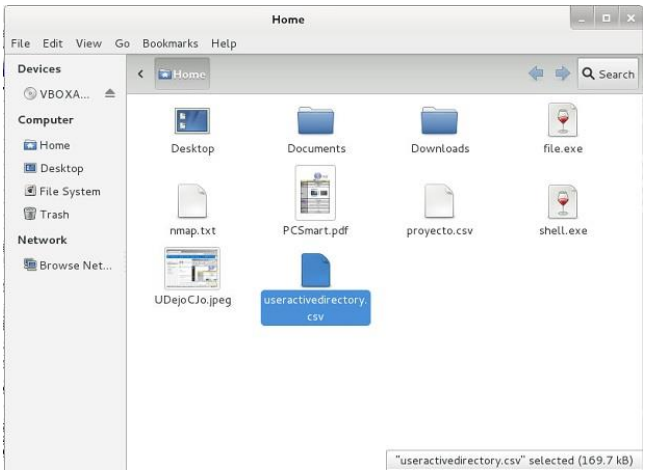
Una vez generado el archivo, se procedió a realizar la descarga del mismo localizado en el servidor Windows, para su posterior análisis desde Linux. Los resultados obtenidos como se observa en la gráfica siguiente, es información confidencial, la cual podría ser utilizada

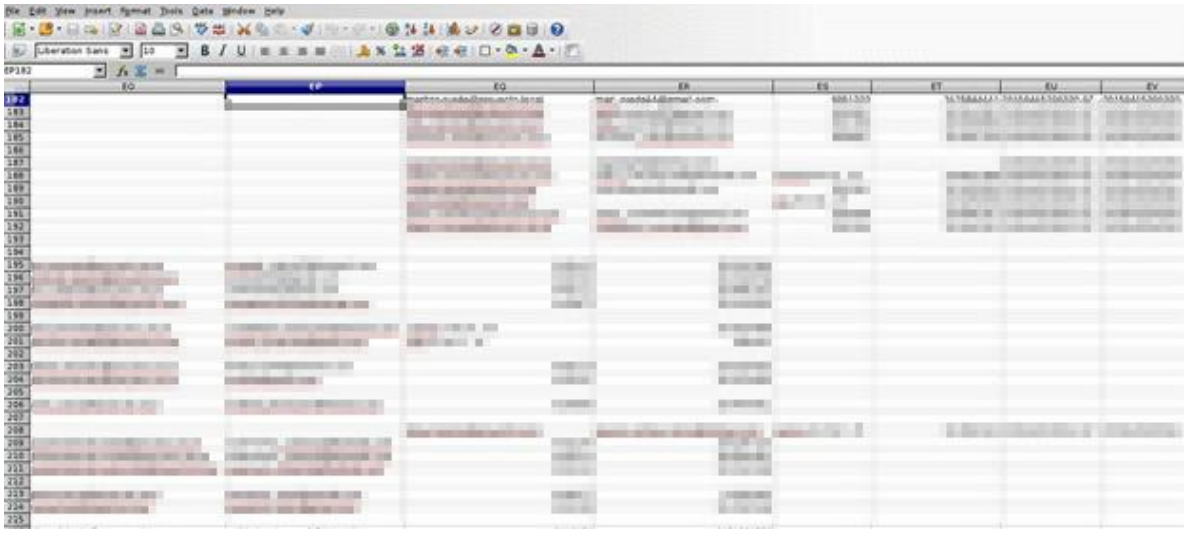
Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

en cualquier evento delictivo, lo cual infringiría contra las normas de seguridad de la información, integridad y confidencialidad.





Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

FASE 6. LIMPIEZA DE HUELLAS.

Finalmente al realizar la prueba de intrusión descrita anteriormente, se procedió a eliminar todas las evidencias generadas en las fases mencionadas; Gran parte de las huellas se generan cuando ocurren eventos con los inicios de sesión, el acceso a archivos, carga de controladores, etc. Windows Clasifica los registros en tres categorías: Log de Aplicaciones, Logs de Sistema y Logs de Seguridad.

Al igual que los anteriores procesos, la limpieza de huellas se realizó mediante la ejecución de un comando de meterpreter llamado *clearev*, el cual borra automáticamente dichos registros del sistema, a continuación se evidencia el proceso llevado a cabo:

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015

RECOMENDACIONES

Como elementos de recomendación, se propone lo siguiente:

- No abrir correos o sitios web de dudosa procedencia
- Revisar el software que no se actualice por defecto (en este caso Adode reader 9)
- Colocar el servidor detrás de hardware firewall,
- Instalar IDS-IPS en la red y en el servidor,
- No utilizar la cuenta Administrador por defecto,
- Monitorear los eventos y procesos del sistema,
- Generar una copia en línea de los eventos del sistema (por si borran las huellas, poder recuperarlas, para análisis de la intrusión).

Elaborado por: Ing. Andrés Fernando Benavides Arias, Ing. John Freddy Velásquez Mayorga.

Colombia - Medellín

2015