UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Pruebas de penetración y análisis de vulnerabilidades

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Abigail Gabriela Hernández Pereda

ASESO DE INFORME

Ing. Alberto Templos Carbajal

Ciudad Universitaria, Cd. Mx., 2019

Contenido

I. Objetivos

Generales

- Dar a conocer las actividades realizadas como consultor de Seguridad Informática.
- Plasmar un breve desarrollo de un ejercicio de pruebas de penetración.

Particulares

- Desarrollar un ejercicio de pruebas de penetración haciendo uso de la metodología PTES.
- Dar a conocer el uso de algunas herramientas para realizar pruebas de penetración

II. Introducción

Actualmente para las empresas de cualquier sector es importante contar con una presencia dentro de Internet que les permita tener interacción con los usuarios brindando el acceso a plataformas para realizar actividades que el día de hoy se consideran cotidianas tales como transacciones bancarias, envío de información, compras en línea, entre otras; generando día a día cantidades masivas de información circulando dentro de la red. Es necesario contar con una gran cantidad de equipos y conexiones que permitan la comunicación dentro de una empresa y fuera de ella, para facilitar el envío de información, la cual se ha vuelto un recurso valioso, objetivo de los atacantes.

En algunos casos, las empresas no cuentan con una cultura de seguridad que les permita protegerse ante los atacantes debido a una falta de controles que regulen y brinden protección a los sistemas que utilizan, generando así pérdidas de miles de millones de dólares por ciberataques, afectando no sólo al aspecto económico sino también a la credibilidad y reputación de las empresas ante los consumidores.

Es importante que las empresas inviertan cierto porcentaje de sus ingresos en cubrir necesidades del sector de la seguridad informática, tales como configuraciones seguras, uso de un Sistema de Gestión de la Seguridad de la Información, realizando auditorías de forma continua, entre otras actividades que le permitan reforzar sus puntos débiles ante ciberatacantes.

1. Descripción de la empresa

Durante un período de seis meses estuve laborando en una empresa orientada a seguridad informática, la cual cuenta con una serie de servicios entorno al ámbito de la seguridad informática, en donde desempeñé una serie de actividades, las cuales están descritas en el presente documento.

Para conocer acerca del entorno y giro de la empresa se detallarán aspectos de las actividades desempeñadas, no obstante, debido al acuerdo de confidencialidad establecido con la empresa, se mantendrá en anonimato la identidad de ésta, así como los procesos utilizados e información serán ofuscados, o bien no establecidos en su totalidad.

Actualmente la empresa de seguridad cuenta con una serie de servicios orientados al sector tecnológico, haciendo un gran énfasis en la seguridad informática con el principal objetivo de brindar soluciones para el manejo de riesgos digitales, brindando una gran eficiencia en la operación del negocio utilizando procesos de mejora con enfoque al negocio y su operatividad, teniendo soluciones en ámbitos de seguridad defensiva y ofensiva, así como en el manejo e implementación de soluciones digitales.

1.1 Organigrama institucional

El siguiente esquema muestra las actuales relaciones organizacionales dentro de la empresa (veáse figura 1.1), en donde el área en el que me desempeñé como Consultor de Seguridad Informática en el área de Seguridad Ofensiva.

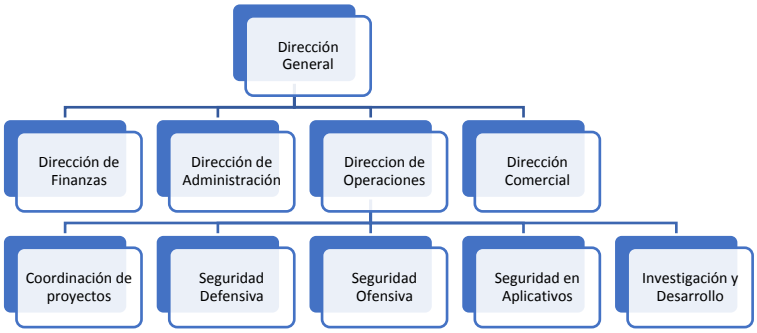

Figura 1.1 Organigrama institucional

A continuación, una pequeña descripción de las principales actividades a desempeñar por cada una de las áreas representadas en el organigrama:

- **Dirección General:** La principal función de esta área es fungir con actividades relacionadas a la administración, gestión y coordinación de cada una de las áreas en la empresa, liderando las principales actividades a realizar.

- **Dirección de Finanzas:** Tiene a su cargo labores relacionadas con la gestión de gastos y recursos económicos, en esta área se lleva a cabo la contabilidad de la empresa, así como los registros y movimientos financieros.

- **Dirección de Administración:** Las labores de reclutamiento, búsqueda de talento, así como recursos humanos se encuentra gestionada por esta área la cual desarrolla actividades relacionadas con la contratación, manejo de personal.

- **Dirección de Operaciones:** Es el principal eslabón del área en la que estuve laborando. El líder tiene a su cargo la dirección, administración y gestión de los proyectos a realizar por parte de cada una de las subáreas descritas a continuación.

- **Coordinación de Proyectos:** Como principal labor es la coordinación y gestión de proyectos a realizar por el área, estableciendo los tiempos, actividades a desempeñar por las demás subáreas.

- **Seguridad Defensiva:** Desempeña labores relacionas a la ejecución y diseño de pruebas de seguridad, así como la realización de monitoreo e identificación de amenazas.

- **Seguridad Ofensiva:** En esta área, me estuve desempeñando como consultor de seguridad informática, las actividades a desempeñar están relacionadas con el escaneo, análisis de vulnerabilidades y pruebas de penetración.

- **Seguridad en Aplicativos:** Área que se dedica a realizar pruebas orientadas a aplicativos web y aplicaciones móviles con el afán de detectar vulnerabilidades y llevar a cabo su correspondiente reporte.

- **Investigación y Desarrollo:** En el mundo de la tecnología, es importante estar a la vanguardia en cuanto a herramientas, actualizaciones, fallas de seguridad, entre otros, en esta área su principal obligación es realizar actividades con principal enfoque a la investigación y desarrollo de nuevas técnicas para la realización de actividades.

- **Dirección Comercial:** Área dedicada a la gestión de proyectos en colaboración con otras empresas.

1.2 Consultor de seguridad informática

Como principal responsabilidad un consultor de seguridad informática debe de estar en constante actualización acerca de las normativas, herramientas, vectores de ataques, ataques, así como tener conocimiento de las nuevas tecnologías que van surgiendo.

En este caso mis actividades como consultor de seguridad informática están dedicadas a realizar labores de Seguridad Ofensiva, las cuales están relacionadas con las actividades que realiza un atacante externo. Las empresas de diversos sectores suelen contratar este servicio para garantizar y validar que sus estrategias de seguridad podrían hacer frente a los ataques que un inexperto, persona con experiencia o bien propios colaboradores llevarán a cabo y terminen afectando a la reputación de la empresa en imagen, financieramente, entre otros.

Una mala práctica que se lleva a cabo es considerarlo juez y parte de la solución de las brechas detectadas, debido a que la labor de un consultor pues como tal el consultor es una persona externa y para crear un plan de trabajo que evite esta serie de riesgos es responsabilidad de la empresa contratante determinar cuál sería la solución más viable sin afectar a la operación.

A continuación brindaré una descripción acerca de las actividades y responsabilidades que estuve realizando durante mi estadía en esta empresa:

- Realizar análisis exhaustivos de aquellas vulnerabilidades que puedan comprometer el valor del negocio de una institución, para ello se hace uso de herramientas libres y comerciales, con el objetivo de encontrar posibles vectores de ataque internos y externos.
- Conocer acerca del avance de las nuevas tecnologías y con ello el surgimiento de las nuevas amenazas, es decir tener conocimiento de la forma de interacción con las vulnerabilidades de día cero.
- Realizar reportes en donde señale los hallazgos encontrados, así como posibles vectores de ataque y escenarios de riesgo que pudiesen comprometer los activos. Si bien, al realizar un pentest el consultor de seguridad no puede ser juez y parte, puede brindar una recomendación que podría mitigar la vulnerabilidad.

2. Antecedentes

De acuerdo con el SANS Institute la seguridad de la información queda definida como:

> *Todos aquellos procesos y metodologías diseñadas e implementadas para proteger la información impresa, electrónica o cualquier otra forma de información confidencial, privada y sensible o de acceso no autorizado (SANS Institute, 2018).*

La seguridad informática cuenta con cinco principios básicos que se encuentran definidos como: (véase figura 2.1)

Figura. 2.1 Pilares de la seguridad

- **Integridad**: Delimita que únicamente la información puede ser modificada por los usuarios autorizados de manera controlada.
- **Confidencialidad**: Sólo los involucrados son aquellos que deben contar con el acceso a la información, evitando la divulgación a usuarios no involucrados.
- **Disponibilidad**: La información debe estar utilizable cuando sea requerida.
- **No repudio**: Válida que tanto la parte emisora como receptora sea quienes hayan emitido la información
- **Autenticación**: Permite validar que el usuario involucrado sea al que le pertenece la información.

2.1 Amenazas cibernéticas

Al hablar de seguridad informática es importante tener presente una serie de conceptos que se encuentran definidos a continuación.

2.1.2 Amenaza

Se caracteriza por ser toda acción que puede valerse de aprovechar una vulnerabilidad atentando a la seguridad de la información, teniendo un efecto negativo sobre algún sistema.

2.1.3 Tipos de amenazas cibernéticas

A continuación, una breve descripción de las amenazas cibernéticas más conocidas.

2.1.3.1 Ingeniería Social

Mediante una serie de técnicas un atacante intenta manipular a un individuo con el afán de obtener algún beneficio, en la mayoría de los casos la información del usuario, enfocado al ámbito tecnológico un atacante se puede valer de correos electrónicos, llamadas telefónicas con el afán de hacer caer a la víctima

2.1.3.1.1 Phishing

Es una técnica utilizada por un ciberatacante valiéndose de correos electrónicos usurpando la entidad de alguna empresa o persona, enviando un mensaje hasta cierto punto convincente en donde haciendo uso de páginas falsas obtiene información del usuario, tales como correos, cuentas de tarjetas bancarias, entre otros.

2.1.3.1.2 Smishing

Al igual que el phishing, el smishing hace uso de mensajes de texto plano en donde envía un mensaje en donde valiéndose de un enlace recortado, tratan de obtener información del usuario para comprometer su información.

2.1.3.1.13Pharming

Valiéndose de un malware un atacante puede modificar el archivo host de un usuario para posteriormente redireccionarlo a un sitio falso para poder recopilar información que le permita falsificar la identidad de la víctima.

2.1.3.2 Malware

Es la abreviatura de “Malicius Software”, en esta clasificación se encuentra todo tipo de software malicioso que tiene como finalidad afectar a la disponibilidad, integridad y confidencialidad de un sistema informático. A continuación una breve descripción de los más conocidos.

2.1.3.2.1 Troyano

Es un tipo de malware que tiene como principal objetivo alterar el funcionamiento de la computadora del usuario provocando acciones tales como bloqueo, modificación, copia o eliminación de datos, si bien este tipo de malware no se multiplica, su forma de distribución es simular ser un software legítimo y posteriormente proceder con la instalación en el equipo de la víctima.

Existen diversas variantes de troyanos tales como backdoors, exploit, rootkits, troyanos bancarios, troyanos espías, cada uno de ellos tiene una función diferente, no obstante, su objetivo es común.

2.1.3.2.2 Ransomware

Software malicioso que tiene como finalidad bloquear la pantalla o bien cifrar información de los usuarios, desde archivos con extensiones predefinidas, el MBR o bien el disco duro, poniendo como condición el pago de una suma de dinero para obtener la llave que descifra la información cifrada, por lo regular este pago suele ser solicitado en criptomonedas.

El método de infección en su mayoría suele ser mediante el uso de ingeniería social, que, redirigiendo a algún enlace, logran hacer que el usuario descargue este software que puede ser dañino para el usuario computadora.

2.1.3.2.3 Virus

Software malicioso que tiene como principal objetivo hacer uso de los recursos del dispositivo y tomar el control de los principales procesos, sus principales métodos de infección suelen ser acceso a sitios infectados, redes sociales, phishing, consiguiendo así que el usuario descargue este código y lo ejecute en su ordenador.

- Bombas de tiempo: Se activan en un momento determinado para causar algún daño en el ordenador.
- Bot: Se activan al iniciar el sistema.
- Gusanos: Tienen la facilidad de replicarse y distribuirse por cualquier medio tal como, dispositivos externos, correos electrónicos, redes de datos, etc.

2.1.3.2.4 Red de bots

Mediante un dispositivo central y haciendo uso de un canal de comunicación en denominado ***comand and control*** (CC) es posible hacer uso de los recursos de dispositivos infectados de forma remota. Tal fue el caso de la red de bots Mirai basada en IoT, que logró realizar los ataques de denegación de servicios más importantes hasta el momento.

2.2 Vulnerabilidad

Es una falla o debilidad que puede permitir a un atacante comprometer la integridad, disponibilidad y confidencialidad de un sistema. Pueden tener su origen en malas configuraciones, falta de procedimientos, errores de diseño.

Es posible encontrar vulnerabilidades que no se encuentren registradas o de reciente descubrimiento por parte del fabricante, durante el período en el que se descubre la vulnerabilidad y se libera un parche o solución se le conoce como día cero, se suelen liberar exploits que permiten explotar la vulnerabilidad poniendo en riesgo (léase el apartado 2.3) los sistemas utilizados por el usuario final. (véase figura 2.2)

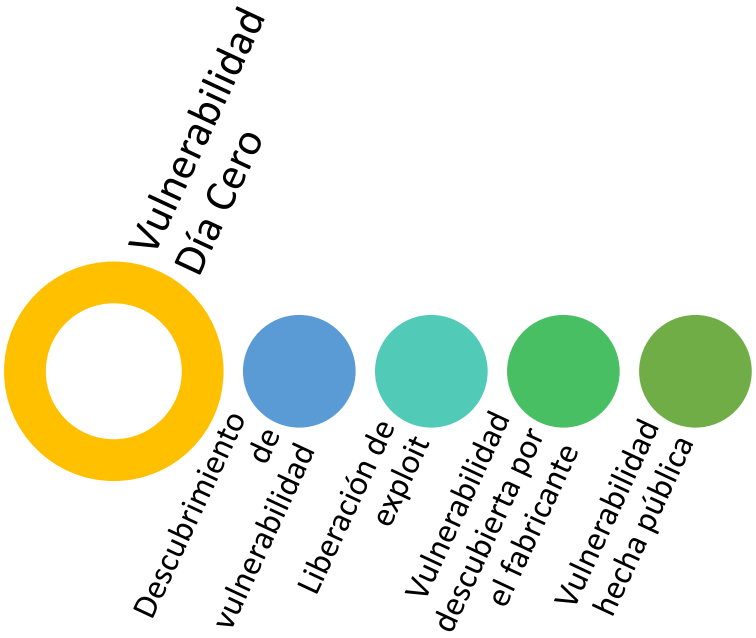

Figura. 2.2 Ciclo de vida de una vulnerabilidad

2.3 Riesgo

Se define como la probabilidad de que un incidente de seguridad suceda, es decir la materialización de una amenaza y el impacto esta cause. Depende de tres factores: la probabilidad, la amenaza y el impacto que tenga.

Al evaluar el riesgo en una empresa se cuenta con dos tipos de riesgo: el técnico y el operacional. El primero está relacionado con las vulnerabilidades que se puedan encontrar en un sistema así como su posible impacto a nivel técnico relacionado con escalación de privilegios, inyecciones de código, falta de parches, por mencionar algunos, mientras que el riesgo operacional está relacionado con el impacto al negocio que pueda tener el que un atacante acceda o comprometa la integridad, disponibilidad y confidencialidad de un sistema y la afectación a nivel reputacional de la misma empresa, para ello se realiza una clasificación de activos en dónde se determina cuáles son los de mayor y menor impacto para empezar a determinar un plan de control de riesgos.

2.4 Vectores de ataque

Son los medios de los cuales se vale un ciberatacante para afectar la disponibilidad, integridad y confidencialidad de la información que maneje un usuario y/o persona, valiéndose de fallas, vulnerabilidades o debilidades dentro de un sistema que le permite a un atacante realizar un análisis detallado del objetivo de ataque validando aspectos como la codificación, configuraciones, explotación de vulnerabilidades que faciliten el comprometer un sistema.

El contar con un plan de seguridad dentro de una institución debe estar dirigido a disminuir vectores de ataque, vulnerabilidades, amenazas y por consecuencia los niveles de riesgo con los que se cuenten.

3. Pruebas de penetración

Durante el desarrollo de los proyectos se lleva a cabo una serie de pruebas para intentar acceder a los sistemas de acuerdo con el enfoque solicitado en el contrato del proyecto el cual es acordado previamente con el cliente, con el objetivo principal de obtener una radiografía a nivel de seguridad de los equipos con los cuales cuenta una institución, para detectar los principales riesgos y amenazas.

En un ambiente operativo la mayoría de los dispositivos con los que se cuentan se encuentran en producción, debido a ello las pruebas que se realizan a estos aplicativos se solicita no comprometan la disponibilidad del servicio (desbordamiento de buffer o ataques de denegación de servicio), no obstante, esto no exime a los servicios realizar este tipo de pruebas las cuales se llevan a cabo de la mano de los administradores de TI para recuperar el sistema en caso de algún inconveniente.

3 .1 Metodología utilizada

Para llevar a cabo las pruebas de penetración se hace uso de la metodología establecida como Penetration Testing Execution Standard conocida por sus siglas en inglés como PTES, la cual delimita una serie de procedimientos a seguir para llevar a cabo una prueba

de penetración en sistemas definidos, esta prueba consta de siete secciones que involucran la información desde la comunicación inicial hasta la parte de desarrollo de informes.

Las secciones están definidas de forma estándar señalando los puntos: (véase figura 3.1)

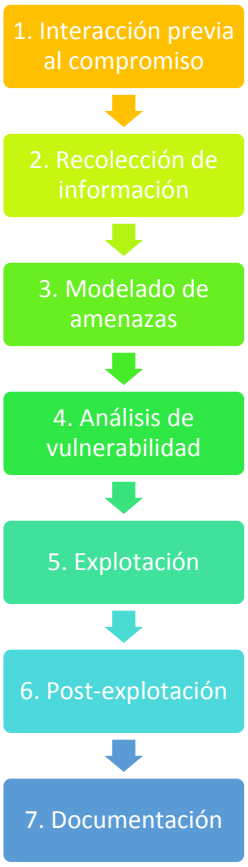

Figura. 3.1 Metodología PTES

A continuación, se describirá cada una de las fases de la metodología.

3.1.1. Interacción previa al compromiso

Durante esta etapa se define cual será el alcance de las pruebas de penetración, estableciendo si se llevara a cabo una prueba interna y/o externa; para la primera se realiza una prueba dentro de los límites de la organización, la segunda se limita exclusivamente a toda aquella información que se encuentre disponible desde Internet y que pueda comprometer la imagen o estructura de la empresa, dentro de estas pruebas se pueden definir tres clasificaciones:

- Pruebas de caja blanca: Se recibe información acerca de los sistemas tales cómo direcciones IP, servicios, claves de acceso, diseño de la infraestructura, permite validar parches de seguridad en servicios o servidores, realizar una prueba exhaustiva del código fuente, el cliente proporciona accesos a los dispositivos de interés para llevar a cabo las actividades.

- Pruebas de caja gris: El cliente brinda sólo algunos datos de información relevantes que podrían ser de ayuda al consultor a realizar la prueba, otros tantos es responsabilidad del consultor detectarlos y reportarlos.

- Pruebas de caja negra: En este tipo de pruebas el consultor no cuenta con información alguna para realizar la prueba, tratando de simular el acceso de un atacante externo.

Herramienta por utilizar: Google Hacking Data Base (GHDB)

El uso de herramientas como GHDB (Google Hacking Data Base) en este proceso, permite encontrar información indexada en el motor de búsqueda de Google evitando así compartir el punto y ubicación de búsqueda de información de datos, así como detectar la información que se encuentra de manera pública que pueda ser de carácter confidencial, o bien accesos a plataformas de administración expuestas, acceso a respaldos que brinden información de credenciales de administración, entre otros.

La herramienta Google Hacking Database permite acceder al contenido indexado en este motor de búsqueda, haciendo uso de *dorks,* es posible recopilar información específica que

pueda brindar un vector de ataque, tal es el caso de formularios, bases de datos, puntos de restauración, acceso a consolas expuestas en Internet, información confidencial relacionados con una empresa.

Básicamente es realizar una búsqueda avanzada en el motor de búsqueda con elementos más complejos que permiten filtrar el contenido que podría mostrar el buscador y brindar solo aquella información relacionada con sitios específicos.

A continuación, se muestra un listado, así como su funcionamiento de los principales operadores de GHDB (véase Tabla 3.1)

Listado de dorks

Haciendo uso de identificadores es posible realizar búsquedas orientadas a tener información específica, a continuación, una descripción de los operadores que hace uso la herramienta. (véase Tabla 3.1)

Operador	Descripción
allintext	Permite buscar alguna cadena de texto dentro del contenido en una página web
allintitle	Permite buscar alguna cadena de texto en el título de alguna página web, no es posible utilizar haciendo uso de otros dorks.
intitle	Permite buscar una cadena dentro del título de una página web, a diferencia del anterior es posible hacer uso de otros dorks.
allinurl	Permite buscar una cadena de texto solo en la url, no es posible utilizar haciendo uso de otros dorks.
inurl	Permite buscar una cadena de texto en la url, a diferencia del anterior es posible hacer uso de otros dorks.
author	Permite realizar obtener información relacionada a algún nombre o dirección de correo indicada,

Operador	Descripción
cache	Permite realizar búsqueda dentro del contenido cache almacenado en Google, es útil para acceder a contenido borrado.
link	Permite realizar búsquedas de sitios asociados con determinado punto web.
related	Permite realizar búsquedas de páginas relacionadas, no es posible utilizar haciendo uso de otros dorks.
site	Permite realizar búsquedas relacionadas exclusivamente con el dominio señalado.
ext	Permite realizar búsquedas de archivos con la extensión señalada.
filetype	Permite realizar búsquedas por el tipo de archivo
info	Permite mostrar información relacionada con el sitio web
define	Permite proporcionar una definición de palabras que definan una frase en el orden que se han escrito

Tabla. 3.1 Descripción de dorks

Para poder combinar los dorks y tener resultados más específicos, la herramienta de GHDB cuenta con una serie de operadores lógicos, los cuales se describen a continuación (véase Tabla 3.2)

Operadores lógicos

Operador	Símbolo	Descripción
NOT	-	Permite excluir cadenas dentro de la búsqueda

OR	|	Permite realizar búsquedas

Operador	Símbolo	Descripción
AND	+	Permite realizar búsquedas de más de dos palabras asociadas a la búsqueda
Precisión de búsqueda	“ ”	Permite realizar búsquedas de manera exacta mostrando solo aquel contenido relacionado con la cadena entre comillas.

Tabla. 3.2 Descripción de operadores lógicos

3.1.2. Recolección de información

En esta etapa el objetivo principal es recabar la mayor cantidad de información del objetivo, con el afán de detectar aquellos datos que podrían convertirse en punto de explotación o bien brindar información que pudiese comprometer la continuidad del negocio permitiendo alguna entrada al sistema de información de forma física y/o electrónica, de acuerdo con la información que se obtenga durante esta fase se podrá hacer uso de vectores de ataque.

La información obtenida dentro de esta etapa es obtenida de fuentes públicas como buscadores, redes sociales, entre otros, detectando así información expuesta en dichas fuentes.

Herramienta por utilizar: Nmap

Nmap es una herramienta *open source*, que permite realizar una serie de escaneos dentro de una red, esta herramienta es multiplataforma, brindando a un administrador de red, a un consultor de seguridad o cualquier persona interesada en la información de su computadora realizar un escaneo acerca de los puertos de red, así como lanzar una serie de scripts para detectar posibles vulnerabilidades en el equipo escanear. Dependiendo de la bandera que se utilice se puede realizar un escaneo que brinde información detallada tal como, puertos abiertos, sistema operativo, realizar un escaneo sin inundar la red de paquetes, entre otros.

Para descubrir los servicios dentro de un sistema, con ayuda de la herramienta de Nmap es posible escanear los puertos para determinar los servicios que se encuentran a la escucha, por defecto se escanean los puertos bien conocidos, es decir del 1-1024, la definición de los puertos 1025-65535 se encuentran listados en el archivo Nmap-services se incluyen el listado de puertos de 1025-65535, no obstante, es posible definir un rango de puertos a analizar durante el escaneo. En el caso de descubrimiento de puertos Nmap cuenta con seis estados los cuales se encuentran descritos a continuación:

- **Abierto**: Acepta conexiones de tipo TCP y UDP, es posible detectar el servicio que se encuentra corriendo.
- **Cerrado**: Este tipo de puertos no cuentan con algún servicio o aplicación para aceptar peticiones, no obstante, son puertos que pueden ser accesibles al cambiar su configuración.
- **Filtrado**: En este caso, no es posible determinar el estado del puerto debido a que puede que la comunicación se encuentre filtrada por algún *firewall*.
- **No filtrado**: Los puertos no filtrados son accesibles, pero no es posible determinar su estado.
- **Abierto | Filtrado**: Debido a que no es posible determinar el estado del puerto es posible que se clasifique en este estado, por lo regular en este tipo de análisis los puertos abiertos no emiten respuesta.
- **Cerrado | Filtrado**: Cuando no es posible determinar si un puerto se encuentra cerrado o filtrado es posible clasificarlo.

En las siguientes figuras (véase figura 3.2 y 3.3) se puede apreciar el funcionamiento de la herramienta desde la interfaz gráfica y a nivel de comandos, así como una breve descripción de las banderas utilizadas en ese momento.

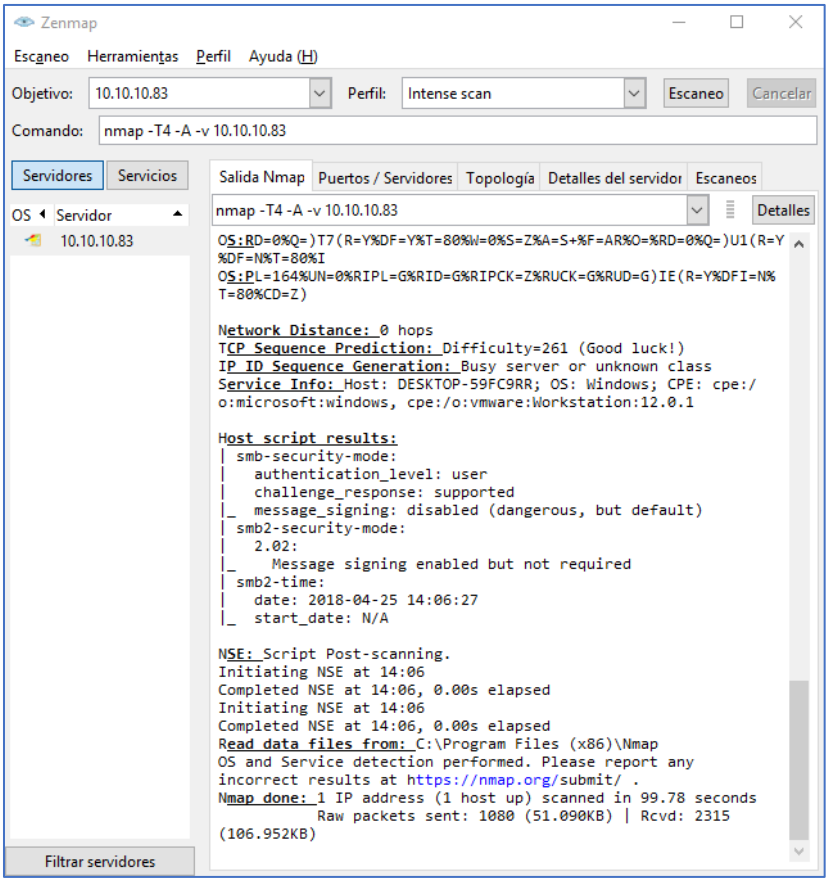

Figura. 3.2 Ejemplo escaneo de dispositivo haciendo uso de Nmap

La herramienta de Nmap cuenta con una serie de utilerías que permiten identificar información a nivel de red tales como puertos, sistemas operativos, vulnerabilidades, información de certificados, entre datos que pueden ser utilizados por un administrador de red, así como para obtener información en un pentest.

En la figura 3.3 se muestra un ejemplo de uso de la herramienta Nmap desde comandos, en donde se realiza un análisis de puertos específicos al servidor de búsquedas de Google, en la tabla 3.3 se visualiza la descripción de cada una de las banderas utilizadas en el comando.

```
root@kali:~# nmap -sS -sV -p 25,80,443 www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 18:00 EDT
Nmap scan report for www.google.com (216.58.194.100)
Host is up (0.027s latency).
Other addresses for www.google.com (not scanned): 2607:f8b0:4000:80f::2004
rDNS record for 216.58.194.100: dfw06s48-in-f100.1e100.net

PORT    STATE    SERVICE   VERSION
25/tcp  filtered smtp
80/tcp  open     http      gws
443/tcp open     ssl/https gws
2 services unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi
?new-service :
```

Figura. 3.3 Resultados del escaneo al portal de Google haciendo uso de herramienta Nmap

En la tabla 3.3 se muestra una descripción de las banderas utilizadas en el ejemplo.

Opción	Descripción
-sS	Permite realizar un sondeo sigiloso de puertos debido a que no a completa las conexiones por TCP, muestra el estado de la conexión.
-sV	Permite detectar la versión del servicio que se encuentra corriendo.
-p	Permite realizar un escaneo a la lista de puertos definida.

Tabla. 3.3 Descripción de banderas de Nmap

3.1.3 Modelado de amenazas

Una vez recabada la documentación importante se clasifican los activos en primarios y secundarios con el fan de identificar todo aquello que desde la perspectiva de seguridad podría significar un riesgo. Esta actividad debe ser planificada para identificar posibles amenazas y vulnerabilidades en los activos primarios y secundarios.

Para poder realizar un modelado de amenazas a alto nivel se deben considerar los siguientes aspectos:

- Documentar información relevante obtenida en pasos previos
- Identificar y clasificar cuáles serán los activos primarios y secundarios

- Identificar cuales serán las posibles amenazas de los activos primarios y secundarios

Herramienta por utilizar: En esta etapa se realiza la clasificación e identificación conforme a la información recabada, es decir, es un proceso manual.

3.1.4 Análisis de vulnerabilidad

Esta etapa permite evaluar y descubrir fallas en sistemas que pudiesen ser explotadas por un atacante, este tipo de fallas está regularmente asociadas a la configuración incorrecta de algún servicio, manejo de sistemas sin soporte, uso de aplicaciones expuestas, hasta una incorrecta administración y gestión de controles.

3.1.4.1 Ciclo del análisis de vulnerabilidades

Al realizar un análisis de vulnerabilidades es necesario incluir cinco etapas, las cuales ayudan a detectar y remediar las vulnerabilidades presentes en los dispositivos, a estas etapas se les conoce como el ciclo de análisis de vulnerabilidades el cual se puede visualizar en la figura 3.4.

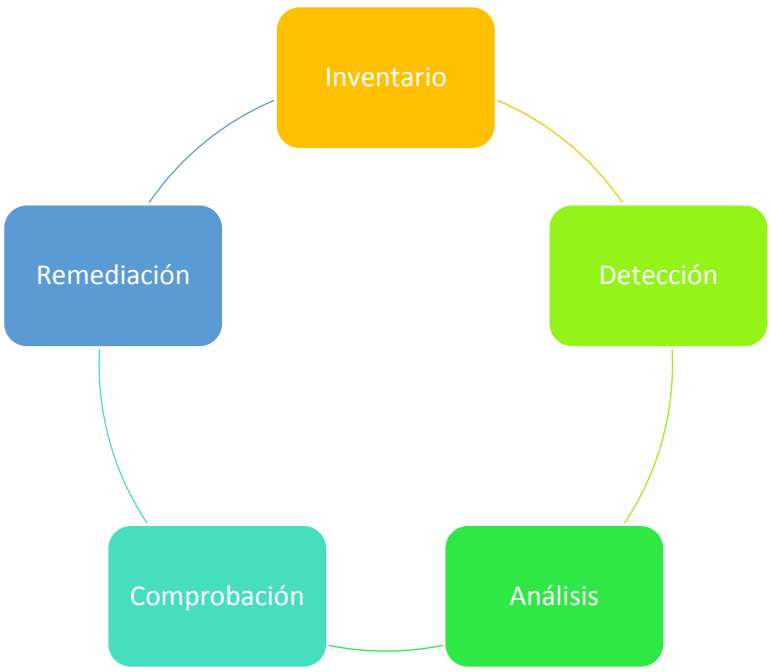

Figura. 3.4 Ciclo del análisis de vulnerabilidades

- **Inventario:** Se define el listado de dispositivos a valorar durante el análisis de vulnerabilidades.
- **Detección:** Haciendo uso de alguna herramienta de seguridad informática, se realiza un escaneo a los dispositivos listados en el paso anterior.
- **Análisis:** Se clasifica de acuerdo con el riesgo que pueda tener cada una de las vulnerabilidades en caso de ser explotada.
- **Comprobación:** Debido a que las herramientas automatizadas pueden señalar falsos positivos, es necesario comprobar que las vulnerabilidades detectadas en el paso anterior correspondan a las tecnologías instaladas en el equipo.
- **Remediación:** Aplicar alguna acción correctiva tal como aplicación de parches, acceso por listas blancas, configuración de firewall, entre otras que permita eliminar la vulnerabilidad.

Herramienta por utilizar: Nessus

La herramienta de Nessus es un escáner de vulnerabilidades a nivel sistema operativo y aplicativo, cuenta con módulos específicos que permiten validar vulnerabilidades presentes en los objetivos definidos dentro de un escaneo

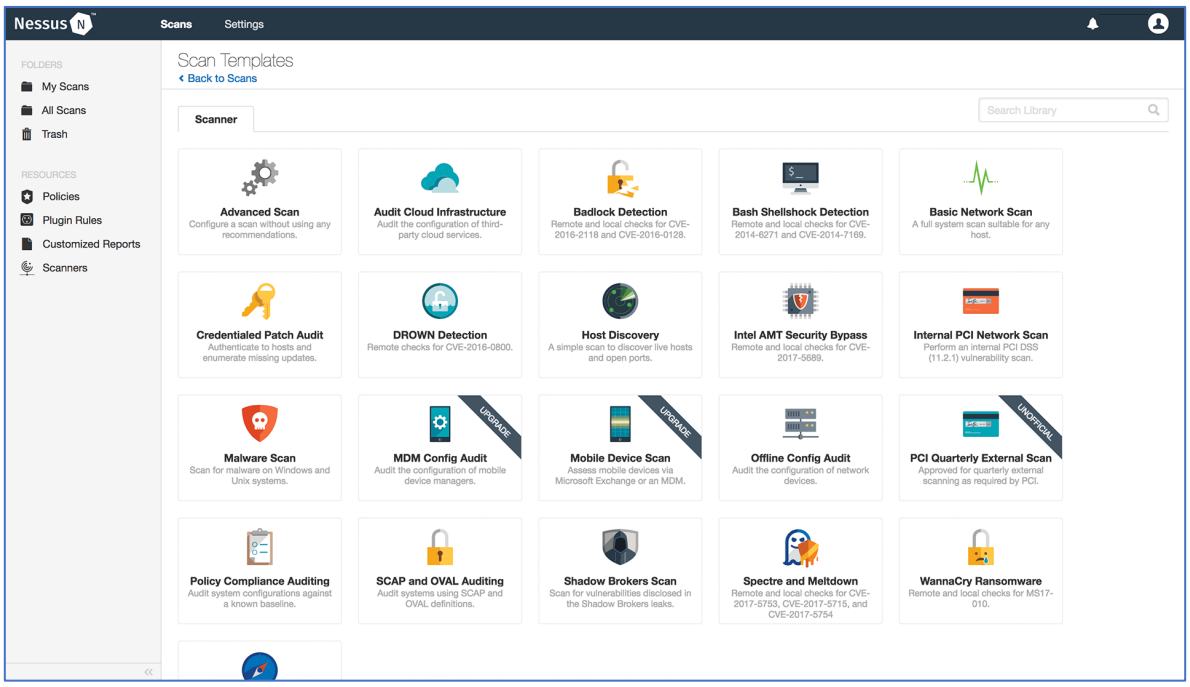

Figura. 3.5 Portal de administración de Nessus

3.1.5 Explotación

En esta fase se busca ganar acceso a un sistema o bien evadir restricciones de seguridad, se tiene como principal objetivo identificar los principales activos, que se pueden identificar en la etapa previa.

Existen una serie de procedimientos que pueden dificultarla realización de esta etapa como lo son los antivirus, la codificación, el cifrado, acceso mediante listas blancas, uso de dispositivos como WAF, entre otros.

Durante esta etapa es posible desarrollar técnicas de evasión, tratando de similar un escenario de riesgo de un atacante real, que permita validar la correcta aplicación de controles.

Herramienta por utilizar: Metasploit

Es un proyecto de código abierto que cuenta con una serie de módulos para validar e identificar riesgos, así como el explotar algunas de las vulnerabilidades existentes.

Figura. 3.6 Ejemplo herramienta Metasploit

3.1.6 Post-explotación

Durante está etapa se tiene como principal objetivo el obtener información del equipo comprometido que pueda brindar valor al activo tales como la lista de usuarios en la máquina, permisos, interfaces y segmentos de red, herramientas disponibles, procesos corriendo, entre otros, también es de interés realizar cierta persistencia en el equipo posterior al ataque haciendo uso de algún proceso habilitado.

En esta fase es donde se hace uso del concepto de puertas traseras o por su pronunciación en inglés “back door” que permiten al usuario que tenga conocimiento de ello acceder al equipo, mientras unos están dedicados al mantenimiento de equipos los cuales están colocados con esta finalidad, otros son creados por atacantes para ganar persistencia dentro del equipo comprometido

Herramienta por utilizar: Metasploit

3.1.7 Documentación

En esta fase se lleva a cabo la realización de un informe ejecutivo, en donde es prescindible lograr transmitir la importancia acerca de los hallazgos obtenidos en etapas previas, así como el posible impacto al negocio; establecer aspectos como el riesgo e impacto dentro de la organización, el cual puede ser delimitado mediante una escala o puntaje que permitirá clasificar cada uno de los hallazgos obtenidos. Este reporte puede contar con una serie de recomendaciones, sin embargo, es importante señalar que no es posible ser juez y parte al momento de realizar una prueba de penetración

4. Desarrollo del proyecto

En la empresa “Empresa X” se solicitó realizar un análisis de vulnerabilidades y pruebas de penetración al equipo de consultores, en donde se requería un análisis de caja negra con el afán de obtener toda la información que un atacante externo e interno fuera capaz de recabar.

Para lograr el objetivo del proyecto se dividió en dos fases, un análisis externo el cuál recababa toda la información que fuese pública y de acceso desde cualquier nodo de red y la segunda fase un análisis interno en dónde desde la infraestructura de la “Empresa X” se recabó toda la información accesible desde un nodo de red proporcionado.

4.1 Análisis externo

Las empresas cuentan con información qué es de dominio público, es decir, se puede acceder desde Internet brindando a un usuario externo una serie de vectores de ataque que podrían comprometer información de la empresa, afectar su operación, disminuir su productividad y/o dañar la reputación de esta.

Este servicio involucra analizar el escenario que se tiene desde fuentes de dominio público, es decir, toda aquella información que se pueda acceder desde un navegador tal

como información en redes sociales, páginas web accesibles desde Internet, archivos públicos, información indexada en motores de búsqueda, entre otros.

La información proporcionada por Internet, sino se cuenta con un control de acceso delimitado, puede brindar una gran serie de vectores de ataque en este caso, haciendo la búsqueda de información sensible tal como usuarios, contraseñas.

Haciendo uso de herramientas como GHDB se trata de acceder a información como lo son archivos con información sensible tales como usuarios y contraseñas, archivos de configuración, consolas de administración expuestas o bien información de clasificación confidencial pero que se encuentre pública. (véase figura 4.1, 4.2, 4.3, 4.4)

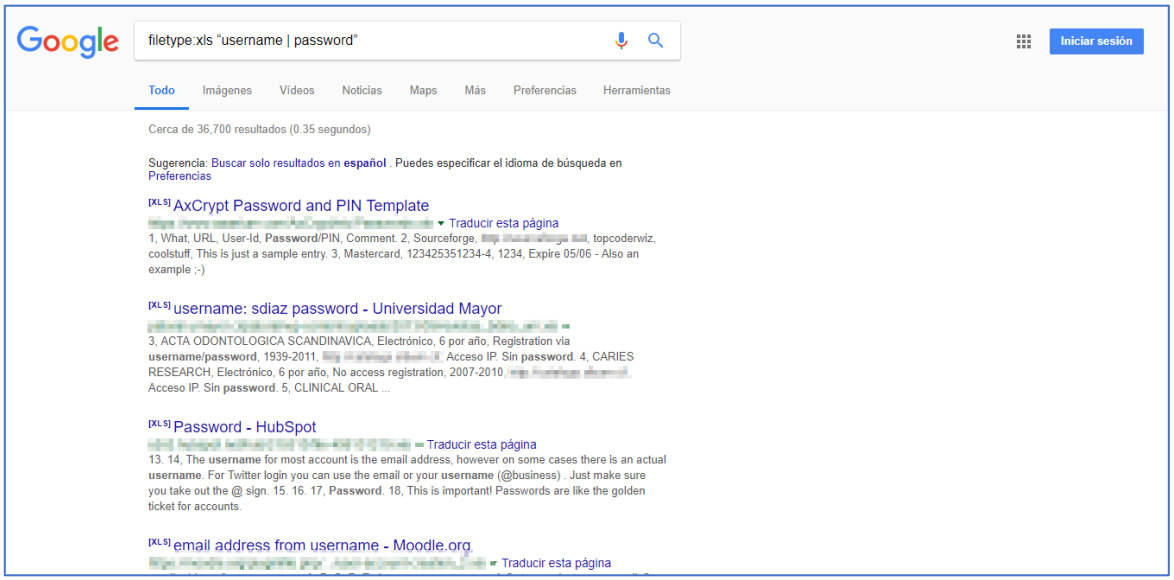

Figura. 4.1 Uso de dorks en Google

Es posible, haciendo uso de dorks, encontrar información sensible tales como carpetas, archivos de configuración e inclusive hasta un listado de correos electrónicos, permitiendo a un atacante externo conocer información acerca de la empresa.

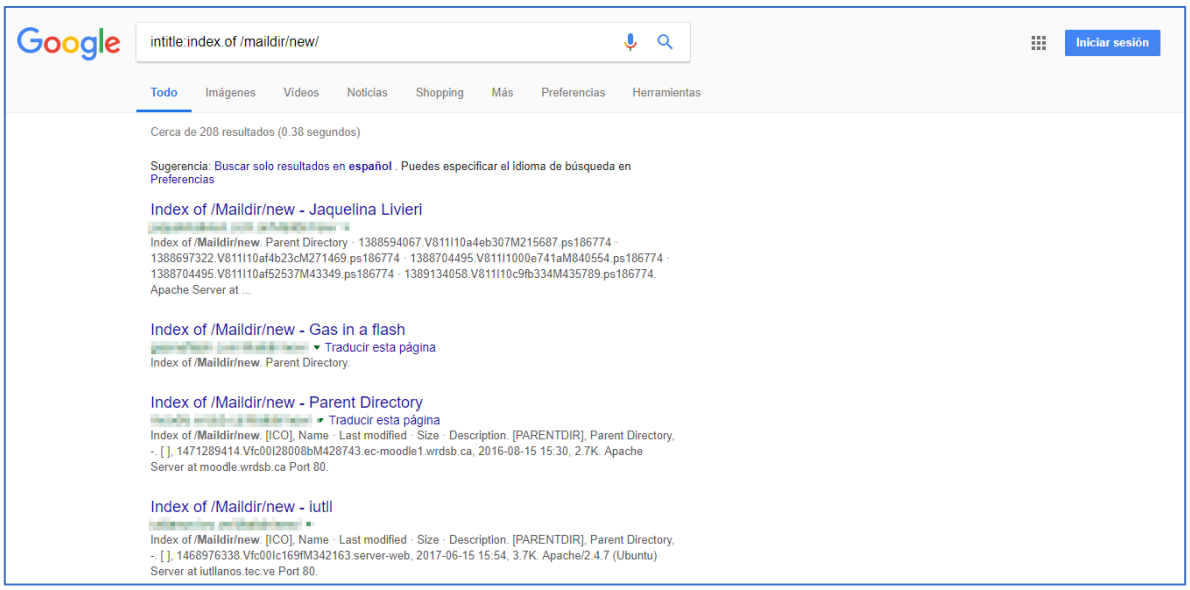

Figura. 4.2 Uso de dokers en Google

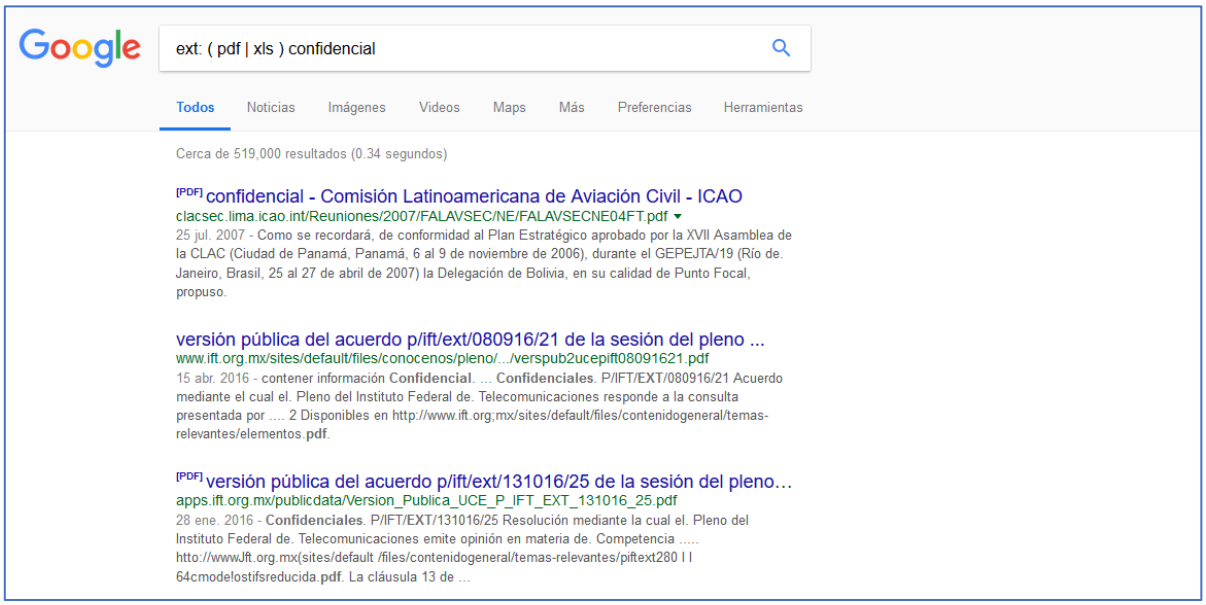

Figura. 4.3 Uso de dokers en Google

Al realizar una recolección de información es posible encontrar acceso a portales de administración o a consolas de configuración, las cuales podrían ser uno de los principales vectores de ataque.

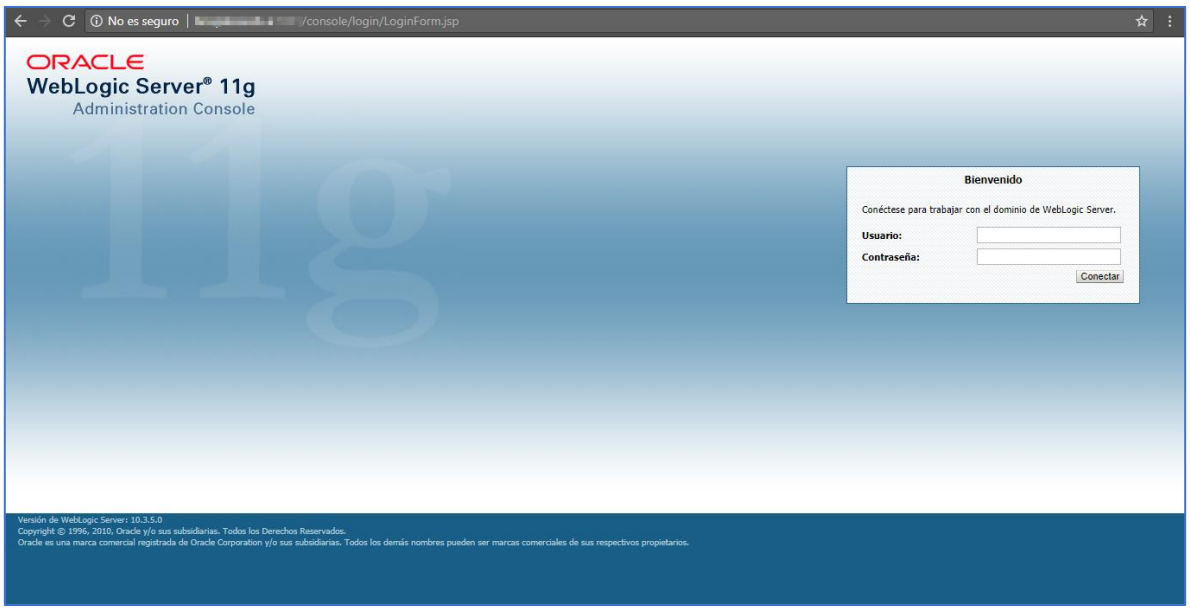

Figura. 4.4 Portal público de consola de administración

Parte del análisis externo es obtener información de todos aquellos portales públicos accesibles desde Internet pertenecientes al cliente y que puedan ser objetivo de un atacante. Una vez obtenida la lista de dispositivos se realiza un reconocimiento acerca de las tecnologías con las que cuenta, configuraciones por defecto, puertos abiertos (véase figura 4.5), dispositivos y sitios relacionados, nombres de dominio y de ser posible información acerca de contactos de confianza de la empresa.

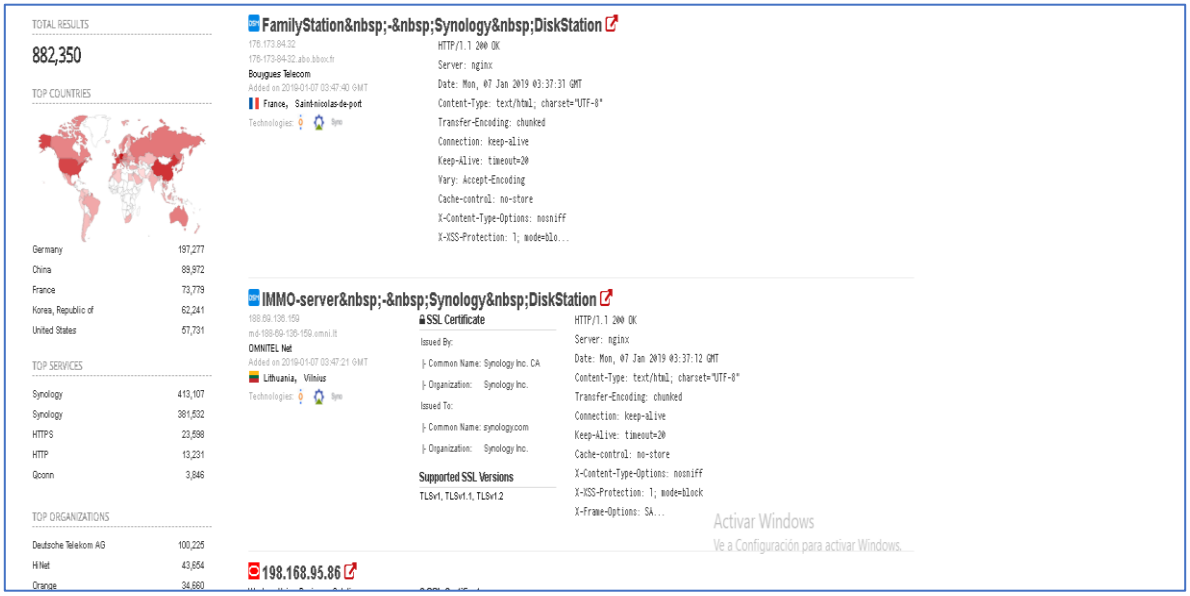

Figura. 4.5 Ejemplo de búsqueda pública

En el caso de portales públicos es de interés del consultor validar posibles inyecciones de código en aplicaciones que puedan comprometer la confidencialidad, integridad o disponibilidad, así como la reputación de una empresa. En la figura 4.6 se puede apreciar una inyección de código en una página web, en donde un atacante podría comprometer la imagen de la empresa, obtener acceso a bases de datos con información sensible de clientes, acceso desde configuraciones por defecto, suplantación de identidad de la empresa o usuario.

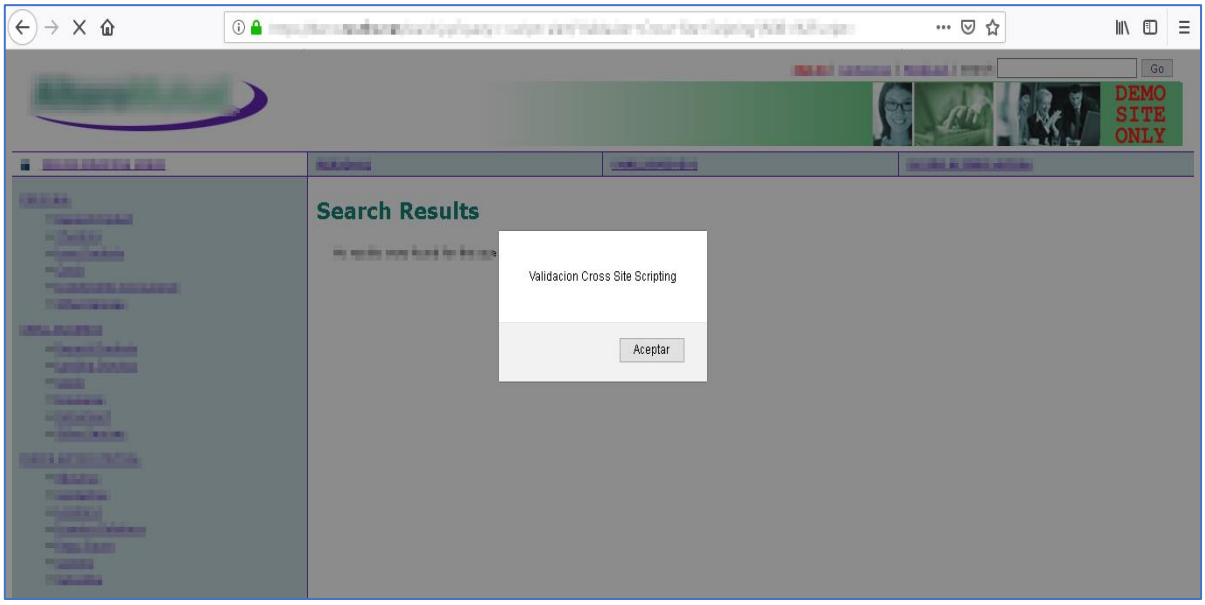

Figura. 4.6 Validación de inyección de código en portal

4.2 Análisis interno

Esta fase se lleva a cabo en la red interna de la empresa, con el afán de detectar posibles brechas de seguridad que permitan comprometer la integridad de la empresa, desde el funcionamiento de la red interna, funcionamiento de equipos o información confidencial, básicamente la realización de este ejercicio tiene como objetivo simular a algún atacante interno y prever el riesgo dentro de la institución.

Muchas veces las empresas cuentan con sistemas operativos obsoletos lo cual les hace susceptibles a una serie vulnerabilidades que podrían comprometer el nivel de operación,

debido a que pueden ser blanco de una serie de ataques tales como denegación de servicio, inyección de código o bien brindar un acceso remoto a un atacante.

En el caso de las pruebas de negra es de suma importancia descubrir la arquitectura de la red en la que se está trabajando, es decir, encontrar los segmentos de red dentro de la empresa, así como los activos que pertenecen a los mismos.

Para conocer algunos de los segmentos que conforman la red, llevado a cabo su descubrimiento con herramientas como tracert o Nmap.

La herramienta traceroute es utilizada para realizar un diagnóstico de redes, debido a que permite realizar un seguimiento de los paquetes que se envían desde el host destino al host origen, en el sistema operativo Windows es posible hacer uso de esta herramienta utilizando el comando tracert mientras que en sistemas como Unix, Mac y GNU/Linux es posible encontrarla como traceroute.

En la figura 4.7 se muestra la ejecución de esta herramienta, así como las opciones con las que cuenta para obtener información relacionada a los segmentos de red.

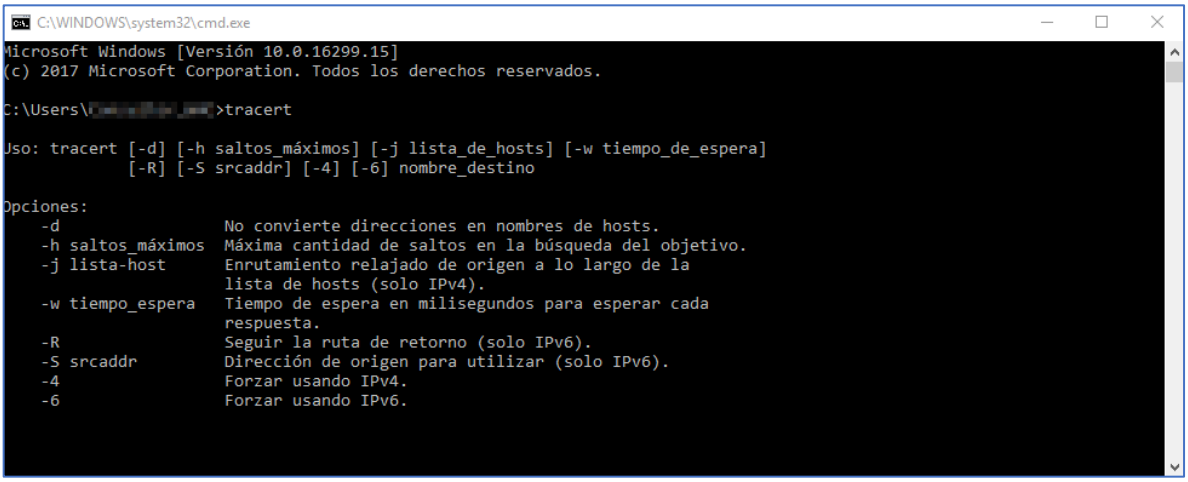

Figura. 4.7 Ejemplo comando tracert

Dependiendo de la arquitectura de red es posible que haciendo uso de esta herramienta se encuentren segmentos internos de la red, debido a que nos permite identificar la serie de saltos de forma interna antes de llegar a la salida a Internet.

Una vez proporcionada la información de la red por parte de la empresa a evaluar “Empresa X”, se obtiene una dirección IP dentro del segmento, se identifica si hay algún servicio de DHCP activo o bien se establece una dirección estática que permita la comunicación con los demás equipos.

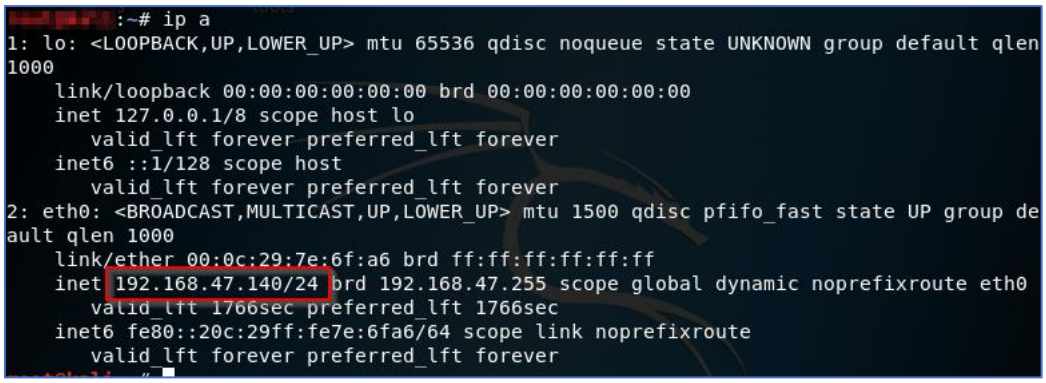

Figura. 4.8 Asignación de Dirección IP

Es necesario identificar los equipos activos dentro de la red, en este caso se parte de un segmento de red192.168.47.0/24 para encontrar aquellos equipos que estén activos y poder determinar también los servicios con los que cuentan, para ello se realiza un escaneo de red y de equipos.

Durante esta fase es importante reconocer los servicios que se encuentran corriendo de los dispositivos, para ello es importante conocer los puertos y el estado en el que se encuentran, con la herramienta de Nmap como se muestra en la figura 15 podemos realizar un escaneo específico para encontrar servicios haciendo uso del filtrado por puertos con el objetivo de detectar posibles vectores de ataque

En la siguiente figura (véase figura 4.9) se puede visualizar el uso de la herramienta Nmap desde comandos, muestra el escaneo que se realiza a un segmento de red 10.10.10.0/25 con el afán de detectar todos los hosts activos, así como información de cada uno de ellos.

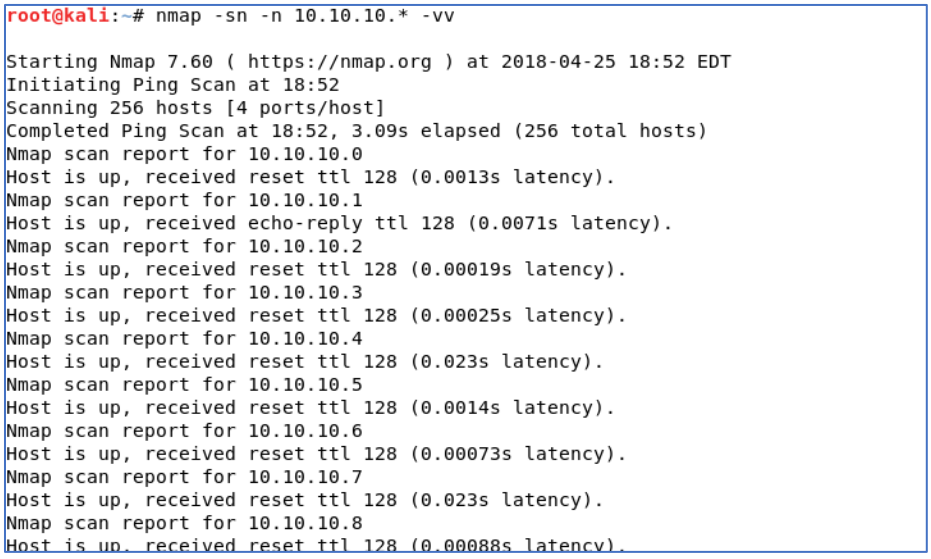

Figura. 4.9 Ejemplo escaneo de dispositivo haciendo uso de Nmap desde comando

En esta tabla se muestra la descripción de cada una de las banderas utilizadas en la herramienta Nmap y su descripción:

Opción	Descripción
-sS	Permite realizar un sondeo sigiloso de puertos debido a que no a completa las conexiones por TCP, no obstante muestra el estado de la conexión.
-Pn	Permite realizar un descubrimiento de sistemas omitiendo las respuestas por paquetes de ICMP
-n	Es utilizado para agilizar el escaneo debido a que omite la resolución inversa por DNS para cada una de las direcciones IP activas.
-vv	Imprime más información acerca de la ejecución de la herramienta, tal como estimación de tiempo

Tabla. 4.1 Descripción de banderas de Nmap

En la figura 4.10 se visualiza información de puertos abiertos en un host con dirección IP 192.168.47.158 que fue escaneado haciendo uso de la herramienta Nmap, cómo se muestra la figura se visualizan puertos activos y no clasificados dentro del rango de los bien conocidos.

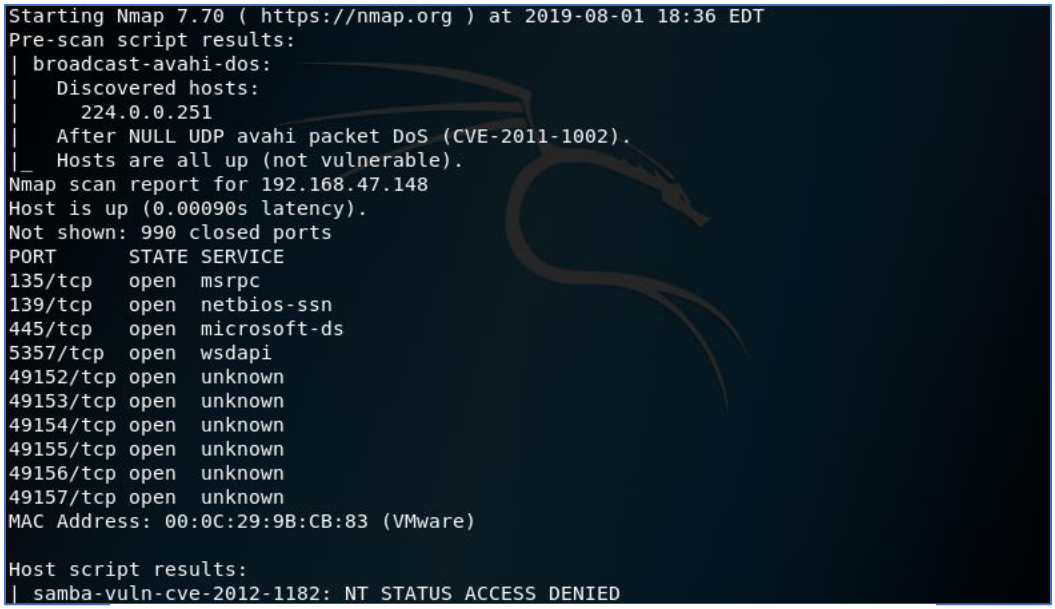

Figura. 4.10 Recolección de información

Una vez recolectada la información, en los equipos de interés se realiza un análisis de vulnerabilidades para determinar cuál sería el mejor vector de ataque posible. Tal y como se muestra en la figura 4.11, tras realizar el análisis de vulnerabilidades el objetivo muestra que tiene la vulnerabilidad MS17-010.

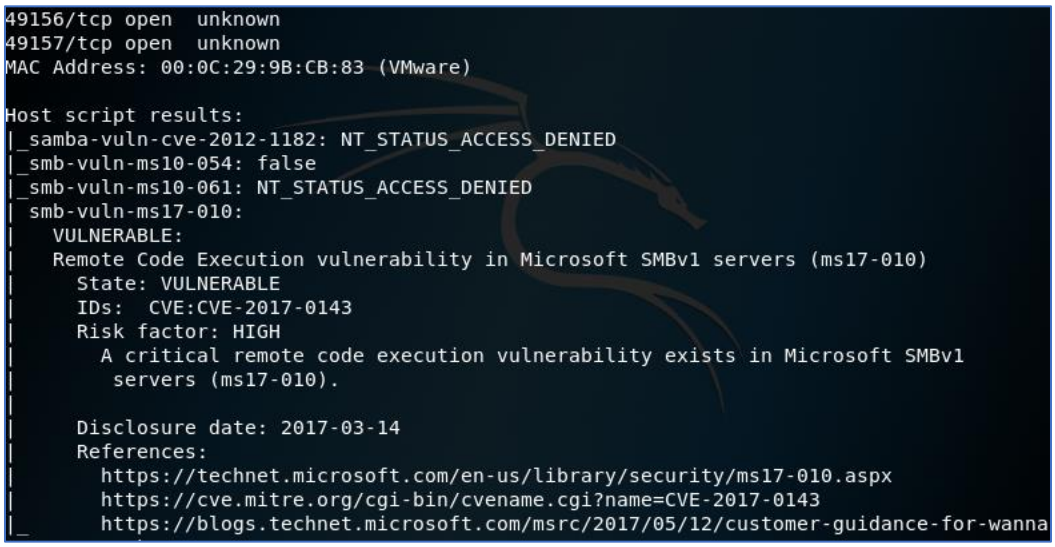

Figura. 4.11 Análisis de vulnerabilidades

Al realizar el análisis de vulnerabilidades se detectó presenté la vulnerabilidad MS17-010 la cual fue un caso relevante en 2017, esta vulnerabilidad se encontró en segmentos de

red pertenecientes a la “Empresa X”, dicha vulnerabilidad fue un caso alarmante durante 2017, la cual fue expuesta por el grupo de cibercriminales ‘The Shadow Brokers’, quienes se encargaron de liberar una serie de exploits públicos permitiendo a cualquier persona con Internet poder explotar estas vulnerabilidades. La vulnerabilidad MS17-010 que permite a los exploits conocidos como EternalBlue, EternalChampion, EternalRomance, EternalSynergy, WannaCry, EternalRocks o Petya, vulnerar sistemas Windows, en tan solo tres días logró afectar a más de 200,000 sistemas en más de 150 países, por ello como parte de la labor del consultor de seguridad es de suma importancia estar en constante actualización acerca de las posibles brechas que surgen día a día.

En las pruebas realizadas como análisis interno, se llevó a cabo la validación de esta vulnerabilidad haciendo uso de la herramienta Metasploit, la cual en la figura 4.12 se muestra el cómo se realizó la validación de la vulnerabilidad MS17-010 haciendo uso de la herramienta Metasploit y se visualiza que el equipo cuenta con dicha vulnerabilidad presente.

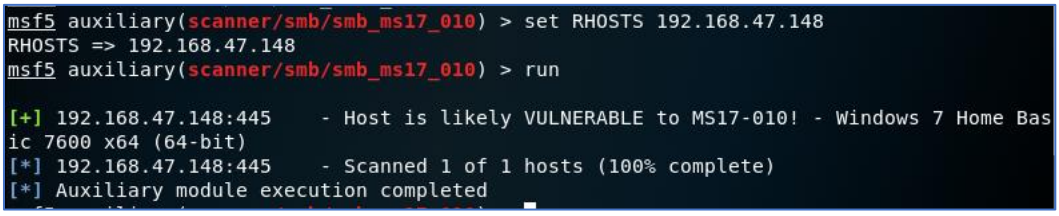

Figura. 4.12 Validación de MS17-010 con herramienta Metasploit

Haciendo uso de esta se compromete el equipo con la vulnerabilidad MS17-010 con el afán de obtener un acceso y posteriormente hacerlo persistente.

En la figura 4.13 podemos visualizar como en uno de los equipos se logra acceder a la terminal de Windows haciendo uso de Metasploit para obtener acceso haciendo uso de la vulnerabilidad presente.

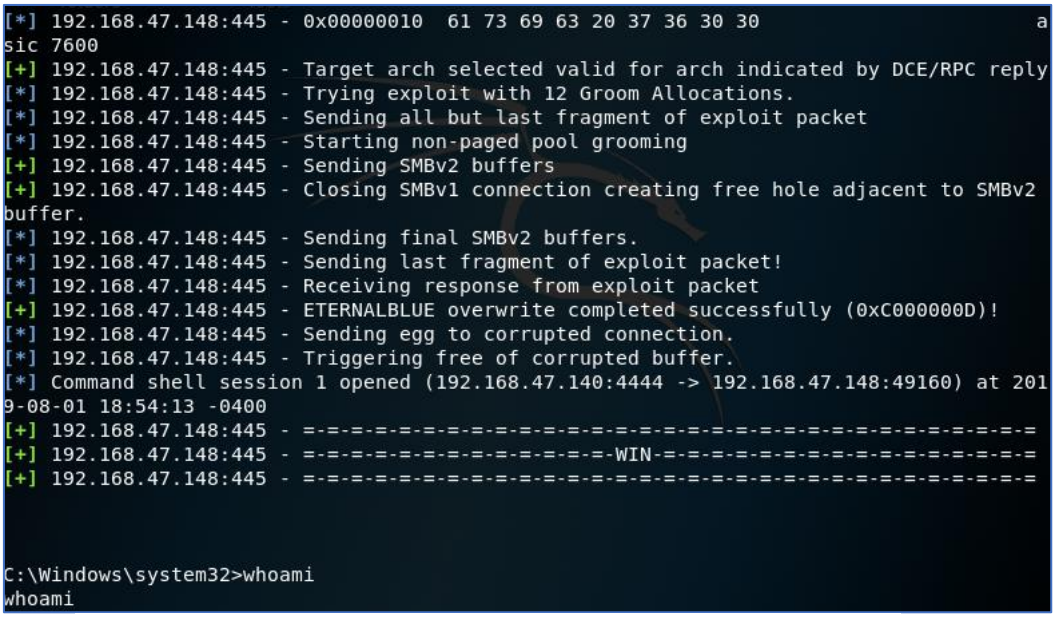

Figura. 4.13 Obteniendo acceso al sistema vulnerable

Una de las principales actividades es encontrar información dentro de los equipos para determinar el impacto del ataque, como se muestra en la figura 4.14 en la carpeta de documentos del usuario “Prueba” se muestra el listado de archivos, entre ellos un | con contraseñas y que no se encuentra cifrado, brindando información de servicios y usuarios dentro de posibles servidores.

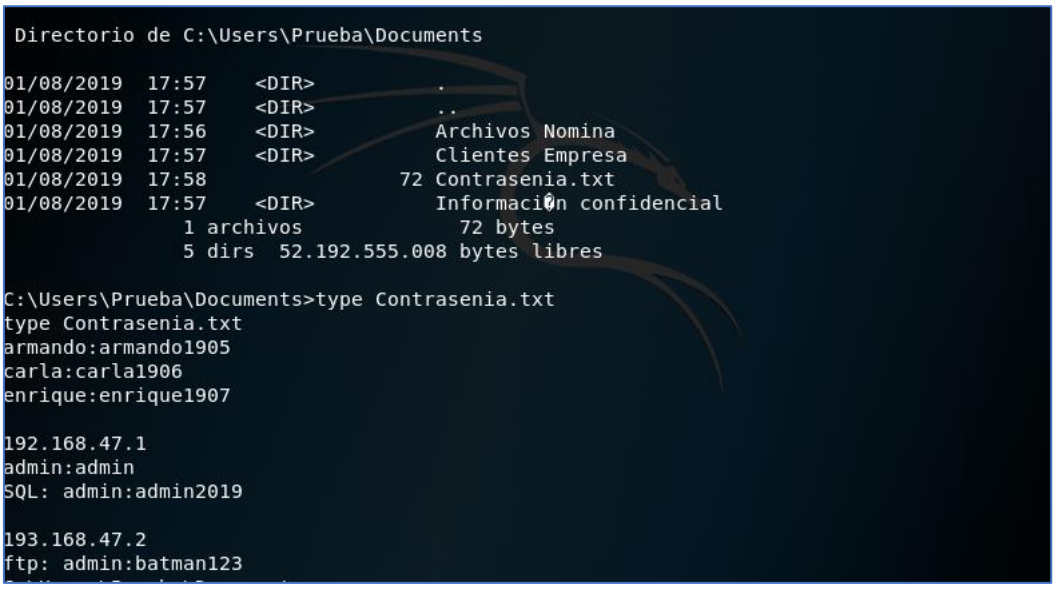

Figura. 4.14 Información sensible recabada

En este ejercicio de simulación se muestran solo algunas de las fases de la metodología que se utilizan con meros objetivos demostrativos, debido a que un ejercicio de pentest es más complejo y depende mucho del análisis del consultor, así como de la dificultad que posea la infraestructura de red.

5. Resultados

Actualmente México necesita crear una estrategia de ciberseguridad para hacer frente a cada uno de los incidentes que podrían presentarse y la labor de un consultor de seguridad informática permite a las empresas encontrar las posibles brechas de seguridad que podrían ser utilizadas por un atacante para afectar la imagen y credibilidad de una empresa. Es responsabilidad de un consultor de seguridad estar en constante actualización acerca del desarrollo de las tecnologías.

Como parte de las pruebas realizadas en los sectores públicos y privados es posible detectar que la mayoría de los casos el contar con expertos en materia de seguridad expone a los usuarios y a las operaciones del negocio, teniendo como principal reto el incorporar el servicio de seguridad tanto de forma interna y externa (auditorías) para estar a la vanguardia. Si bien es cierto que no es posible contar con cien por ciento de seguridad es importante para el consultor tratar de cubrir la mayoría de los escenarios o al menos los más críticos en la infraestructura de alguna empresa.

6. Conclusiones

Durante el desarrollo del presente documento se dio a conocer acerca de las actividades desempeñadas en una institución orientada a brindar servicios de seguridad informática, así cómo las actividades a realizar por parte de un consultor de seguridad informática.

En el desarrollo del proyecto se utilizó la metodología PTES orientada a describir los pasos necesarios para realizar una prueba de penetración que permita plasmar los hallazgos en un informe en dónde se debe dar relevancia a los hallazgos de seguridad a los cuales se encuentra expuesta una institución, definiéndolos con base a una evaluación posibles riesgos y uso de métricas utilizadas para hacer frente a las deficiencias de seguridad con las que se cuente dentro de una institución.

En el ámbito de seguridad se requieren personas que su conocimiento sea trasversal en todas las áreas tales como sistemas operativos, bases de datos, lenguajes de programación, redes de datos, normativas, leyes, lo cual le permitirá brindar soluciones integrales de aporte real y tangible, además de tener un dominio integral en cual sea el enfoque de seguridad que se asuma. Debido a que hablar de seguridad es transversal, la carrera brinda una capacitación en diversos ámbitos de tecnología brindando al alumno las bases

necesarias para ejercer su profesión en cualquiera de las áreas de tecnología que se desempeñe.

En el caso de un consultor de Seguridad Informática, las actividades realizadas que se expresan en el presente escrito plasman que es necesario contar con una serie de conocimientos que no se limitan únicamente a un área de tecnología, sino que requiere de una formación sólida en diversas áreas. El haberme desempeñado durante una temporada realizando estas actividades, me brindó un panorama general de las necesidades actuales enfocadas a la seguridad informática, así como las diversas líneas que se pueden seguir para estar en constante capacitación. Descubrí que uno de los principales retos es la constante actualización debido a que el surgimiento de nuevas vulnerabilidades es al día lo cual conlleva a tener un pensamiento analítico y crítico para poder encontrar una posible solución a las brechas detectadas.

Es importante señalar que actualmente se cuenta con una deficiencia de personas expertas en materia de seguridad, así como una cultura de concientización a los usuarios, pues en gran parte de los casos los usuarios suelen ser el eslabón más débil dentro de la cadena, debilitando así los esfuerzos que se hagan por parte del área de seguridad de cada empresa.

7. Anexos

7.1 Glosario

- ***Backdoor***: Por su traducción en inglés se define como puerta trasera. Permite el acceso a un sistema a un atacante, brindando la posibilidad de manipular el equipo en su totalidad.
- ***Exploit***: Es un software malicioso que hace uso de las vulnerabilidades presentes en un equipo para controlar o infectar un sistema.
- ***Command and control***: Mediante el uso de un servidor central es utilizado para controlar otros dispositivos, en la mayoría de estos casos es utilizado por malware.
- ***Rootkit***: Herramientas de malware que tienen como principal objetivo brindar el control de forma remoto a un dispositivo.

7.2 .Diccionario

- MBR: Master Boot Record
- TI: Tecnologías de la información
- PTES: Penetration Testing Execution Standard
- WAF: Web Applcation Firewall
- IP: Internet Protocol

8 Referencias

Institute, S. (s.f.). *Information Security Training* . Obtenido de https://www.sans.org/

Lyon, G. (s.f.). *NMAP.org*. Obtenido de https://Nmap.org/man/es/index.html

Standard, T. P. (s.f.). *The Penetration Testing Execution Standard*. Obtenido de http://www.pentest-standard.org/index.php/Main_Page

Walker, M. (2016). *CEH Certified Ethical Hacker All-In-One Exam Guide*. McGraw-Hill Education.