

Aplicación de la etapa de Reconocimiento

Sesión 02



Objetivos del módulo

- Familiarizar al estudiante con el ambiente virtualizado.
- Familiarizar al estudiante con los comandos básicos de escaneo y reconocimiento en red.



Requerimientos iniciales

- Se requiere del estudiante comprenda el uso de herramientas como Nmap para el reconocimiento de la red que rodea un sistema autónomo.
- Se requiere que el estudiante trabaje con las máquinas virtuales configuradas en la sesión anterior.
- Se requiere que ambas máquinas virtuales puedan comunicarse en red (comprobación con ping).
- Se requiere que el estudiante detenga cualquier ejecución de Antivirus o Firewall en su computadora anfitrión, para que estos interrumpan la ejecución normal del laboratorio.

Inicio de infraestructura

Encendido de las máquinas virtuales.



Inicio del entorno

- Inicie VirtualBox.
- Inicie su máquina virtual de Metasploitable.
- Las credenciales aparecen en la pantalla de inicio.

```
* Starting deferred execution scheduler atd

* Starting periodic command scheduler crond

* Starting Tomcat servlet engine tomcat5.5

* Starting web server apache2

* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'

* Tok 1

* Warning: Never expose this UM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```



Inicio del entorno

- Inicie su máquina virtual de Kali (la versión de su preferencia).
- Tanto en Kali como en Metasploitable, ejecute el comando ifconfig para que sepa qué IP's tiene cada máquina virtual.

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable: "$ ifconfig
          Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a
          inet addr:10.0.2.129 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3992 (3.8 KB) TX bytes:11630 (11.3 KB)
          Interrupt:19 Base address:0x2000
          Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX butes:44105 (43.0 KB) TX butes:44105 (43.0 KB)
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

```
ali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 10.0.2.128 netmask 255.255.25.0 broadcast 10.0.2.255
       inet6 fe80::20c:29ff:fe55:51d4 prefixlen 64 scopeid 0x20<link>
       ether 00:0c:29:55:51:d4 txqueuelen 1000 (Ethernet)
       RX packets 96 bytes 14078 (13.7 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 92 bytes 9443 (9.2 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,L00PBACK,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 28 bytes 1596 (1.5 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 28 bytes 1596 (1.5 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
oot@kali:~#
```

Explicación del comando ifconfig.





Proceso de reconocimiento

Instrucciones de uso de herramientas básicas en el proceso de reconocimiento de IP's, protocolos y puertos.



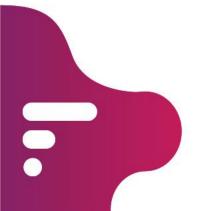
- Durante la etapa de reconocimiento, se suelen realizar pruebas de ping de diferente naturaleza sobre los puertos de los sistemas objetivos. Esta tarea se lleva a cabo para identificar cuales sistemas están activos para luego identificar aquellos puertos abiertos en búsqueda de posibles vulnerabilidades.
- El concepto de escaneo se vincula directamente con el reconocimiento de aplicaciones que pudieran poseer vulnerabilidades que luego serán comprobadas en la etapa de explotación. Sin embargo, si el descubrimiento no se realiza conociendo explícitamente los resultados e interpretándolos correctamente, podría dejarse de lado ciertos sistemas y no contemplarse durante las etapas posteriores.

- Uso del comando: ping <IP a escanear>
- Interpretación del comando ping:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping 10.0.2.129
PING 10.0.2.129 (10.0.2.129) 56(84) bytes of data.
64 bytes from 10.0.2.129: icmp seq=1 ttl=64 time=3.42 ms
64 bytes from 10.0.2.129: icmp seq=2 ttl=64 time=0.918 ms
64 bytes from 10.0.2.129: icmp seq=3 ttl=64 time=0.875 ms
64 bytes from 10.0.2.129: icmp seq=4 ttl=64 time=0.918 ms
64 bytes from 10.0.2.129: icmp seq=5 ttl=64 time=0.876 ms
64 bytes from 10.0.2.129: icmp seq=6 ttl=64 time=0.909 ms
--- 10.0.2.129 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 0.875/1.318/3.416/0.938 ms
root@kali:~#
```

Explicación del comando ping.





- Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich1) y cuyo desarrollo se encuentra hoy a cargo de una comunidad.
- Fue creado originalmente para Linux aunque actualmente es multiplataforma.
- Se usa para detectar aquellos sistemas "vivos", para luego realizar un escaneo más profundo en búsqueda de potenciales servicios u aplicaciones vulnerables.

- Existen varias formas de ejecutar Nmap. La más común es iniciar una ventana de comandos y luego escribir el comando:
 - root@kali:~# nmap <número IP> o <rango> o <DNS>
- Este comando escaneará el objetivo y devolverá información relacionada.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap 10.0.2.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-29 22:06 EDT
Nmap scan report for 10.0.2.129
Host is up (0.0028s latency).
Not shown: 977 closed ports
PORT
         STATE SERVICE
21/tcp
         open ftp
22/tcp
         open ssh
23/tcp
         open telnet
25/tcp
         open smtp
         open domain
53/tcp
80/tcp
         open http
111/tcp
         open rpcbind
139/tcp
         open netbios-ssn
        open microsoft-ds
445/tcp
512/tcp
        open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
root@kali:~#
```

Explicación del comando nmap <número IP>



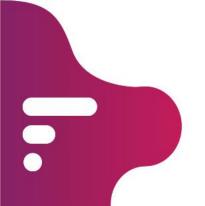


- TCP SYN Ping, este tipo de escaneo es el preferido de muchos hackers debido a que es rápido. Para comprobar si un sistema tiene activa algún tipo de actividad web, Nmap envía un paquete del tipo SYN al puerto 80 por ejemplo.
- Si el servidor responde con un paquete con el flag RST activado significa que el puerto se encuentra cerrado, pero el equipo está activo. Si el sistema responde con un paquete del tipo SYN/ACK, significa que el puerto se encuentra abierto, y naturalmente, el sistema está activo.
- Más adelante se explicará fondo el proceso three-way-handshake.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PS fidevirtual.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-30 00:19 EDT
Nmap scan report for fidevirtual.com (18.213.42.108)
Host is up (0.053s latency).
rDNS record for 18.213.42.108: ec2-18-213-42-108.compute-1.amazonaws.com
Not shown: 984 filtered ports
PORT
          STATE SERVICE
          open ssh
22/tcp
80/tcp open
               http
259/tcp closed esro-gen
264/tcp closed bgmp
443/tcp open
                 https
1594/tcp closed sixtrak
2022/tcp closed down
3517/tcp closed 802-11-iapp
5822/tcp closed unknown
5906/tcp closed unknown
8086/tcp closed d-s-n
9207/tcp closed wap-vcal-s
10082/tcp closed amandaidx
10626/tcp closed unknown
32777/tcp closed sometimes-rpc17
49159/tcp closed unknown
Nmap done: 1 IP address (1 host up) scanned in 72.67 seconds
```

Explicación del comando *nmap -PS < número IP> o < DNS>*





- TCP ACK Ping, en este caso se envía un paquete con el flag TCP ACK activado. Este tipo de paquete se utiliza para generar una conexión previo al envío de un paquete SYN y luego un SYN/ACK.
- De esa manera, el sistema objetivo responderá con un paquete del tipo RST si es que se encuentra activo.
- Esto se debe a que el sistema no espera este tipo de paquete debido a que no se ha generado la conexión de forma correspondiente (three-way-handshake).

```
root@kali:~

File Edit View Search Terminal Help

root@kali:~# nmap -PA fidevirtual.com

Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-30 00:05 EDT

Nmap scan report for fidevirtual.com (18.213.42.108)

Host is up (0.064s latency).

rDNS record for 18.213.42.108: ec2-18-213-42-108.compute-1.amazonaws.com

Not shown: 997 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

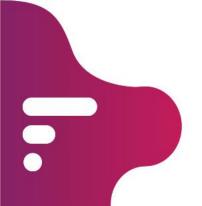
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 61.25 seconds
```



Explicación del comando *nmap -PA < número IP> o <DNS>*





Desactivación del ping

- En ciertos casos, algunos sistemas no responden al ping tradicional debido a una configuración particular o la presencia de algún dispositivo que descarta este tipo de paquetes.
- Para estos casos, es posible configurar Nmap para que deshabilite las pruebas utilizando ping. De esta manera se realiza un escaneo forzado sobre las direcciones IP de los sistemas objetivos más allá de que estos no respondan al ping. Para habilitar esta opción solo basta con incluir -PN en el comando.

Conclusión



Conclusión

- Cada una de estas técnicas amplía las probabilidades de obtener resultados fidedignos frente a diferentes configuraciones en la infraestructura que se está analizando.
- Con esto nos referimos a la presencia de diferentes configuraciones sobre los sistemas objetivos así como también la presencia de Firewalls, IDS/IPS, balanceadores de carga, entre otras alternativas.
- En ciertos casos pueden existir filtros sobre un determinado tipo de paquetes por lo que, utilizar otras técnicas, ayuda a obtener resultados verídicos.

