FIDE VIRTUAL

Curso introductorio de Ethical Hacking

Semana 01

Profesor: Randall Barnett Villalobos

Aplicación de la etapa de Reconocimiento

Sesión 02

FIDE VIRTUAL

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.

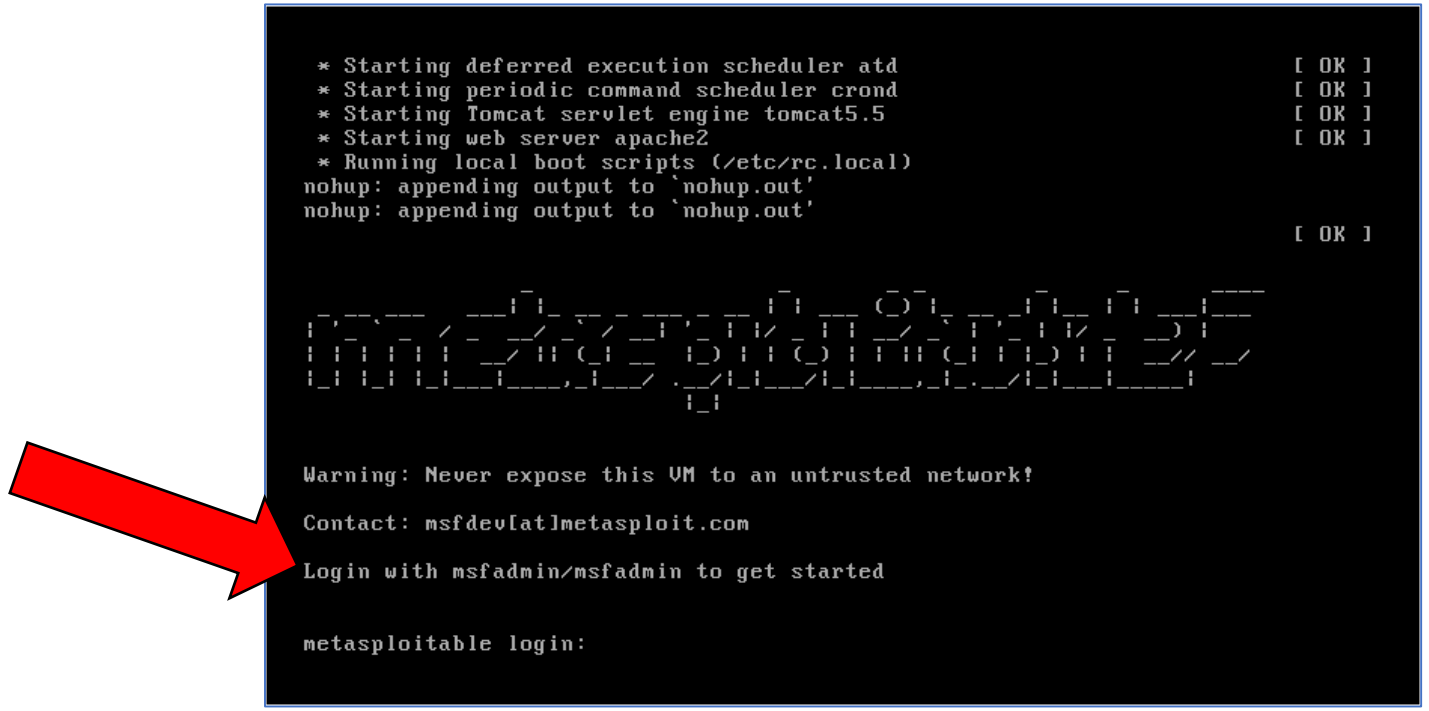
Inicio de infraestructura

Encendido de las máquinas virtuales.

FIDE VIRTUAL

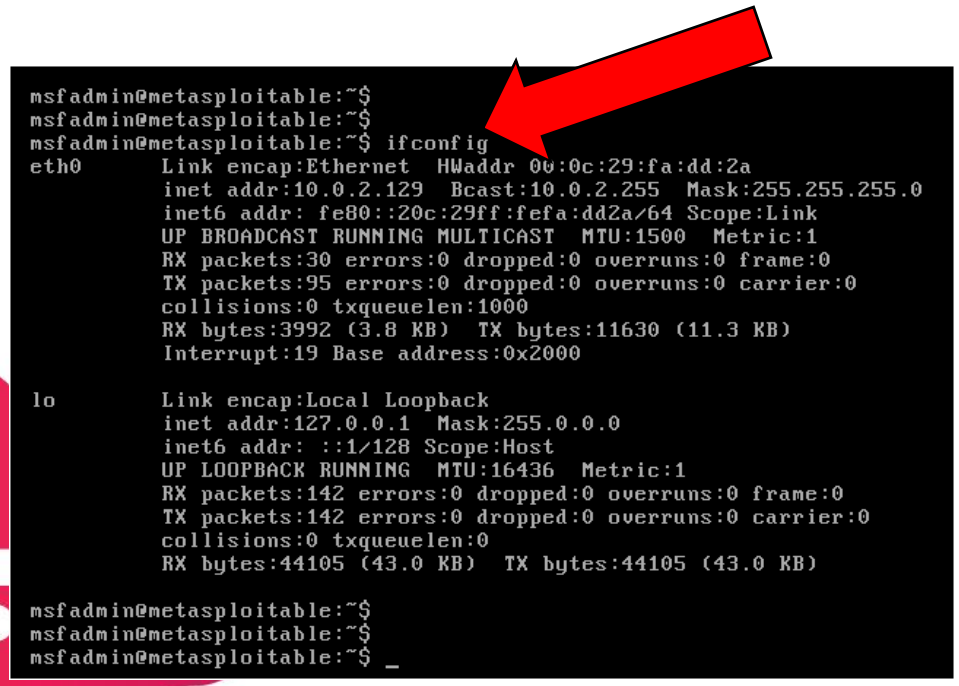
Inicio del entorno

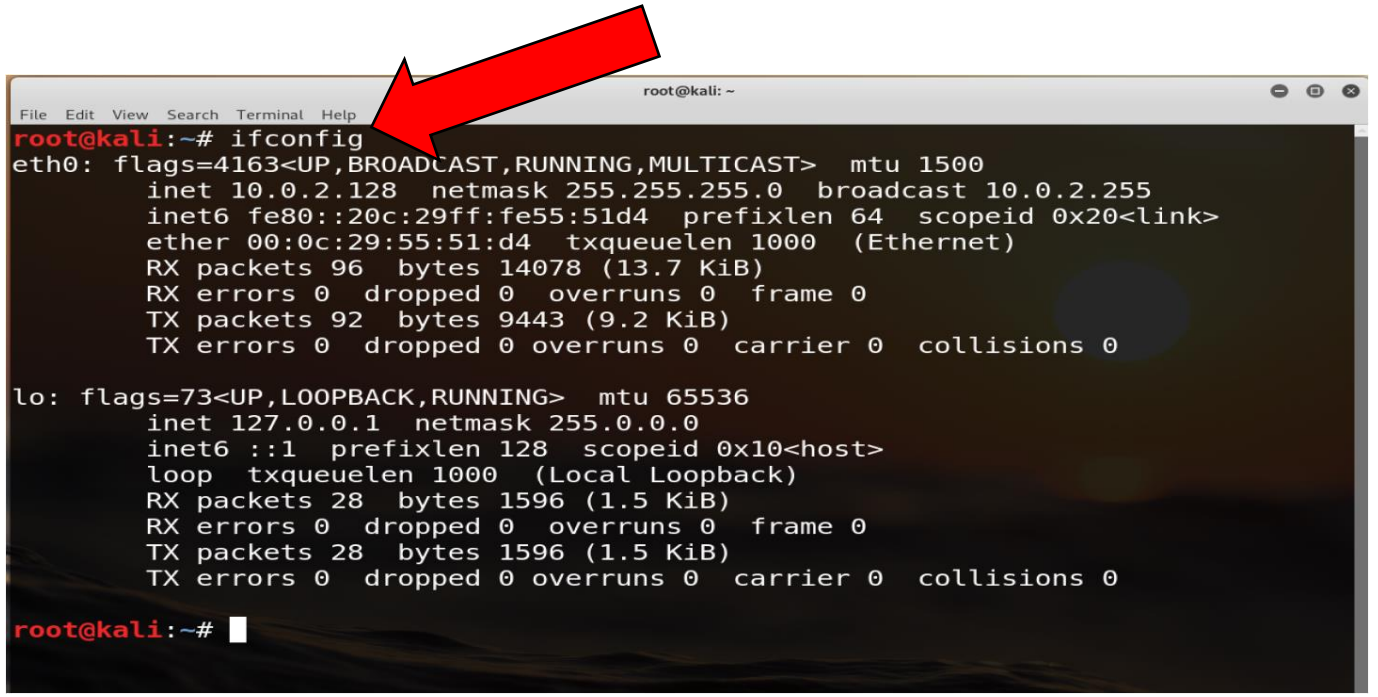
- Inicie VirtualBox.
- Inicie su máquina virtual de Metasploitable.
- Las credenciales aparecen en la pantalla de inicio.



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.





Mira el video

Explicación del comando *ifconfig*.

Proceso de reconocimiento

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

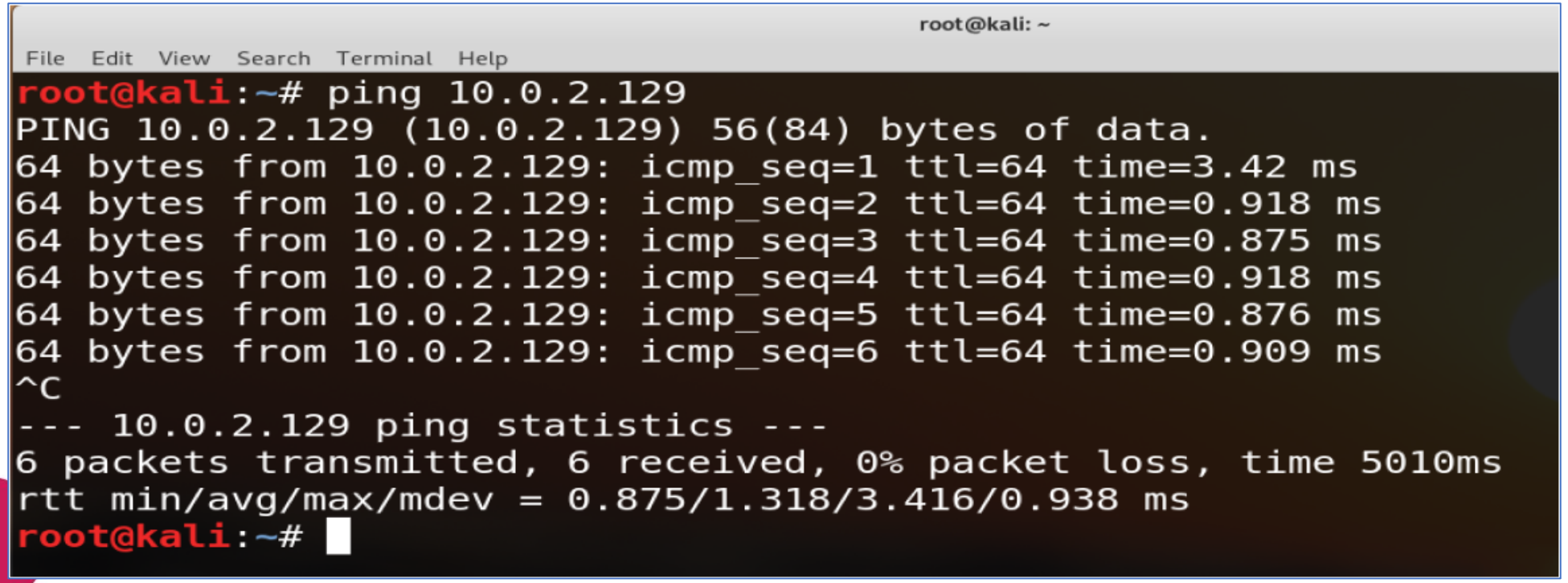
FIDE VIRTUAL

Uso de herramientas de escaneo

- 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 de herramientas de escaneo

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



Mira el video

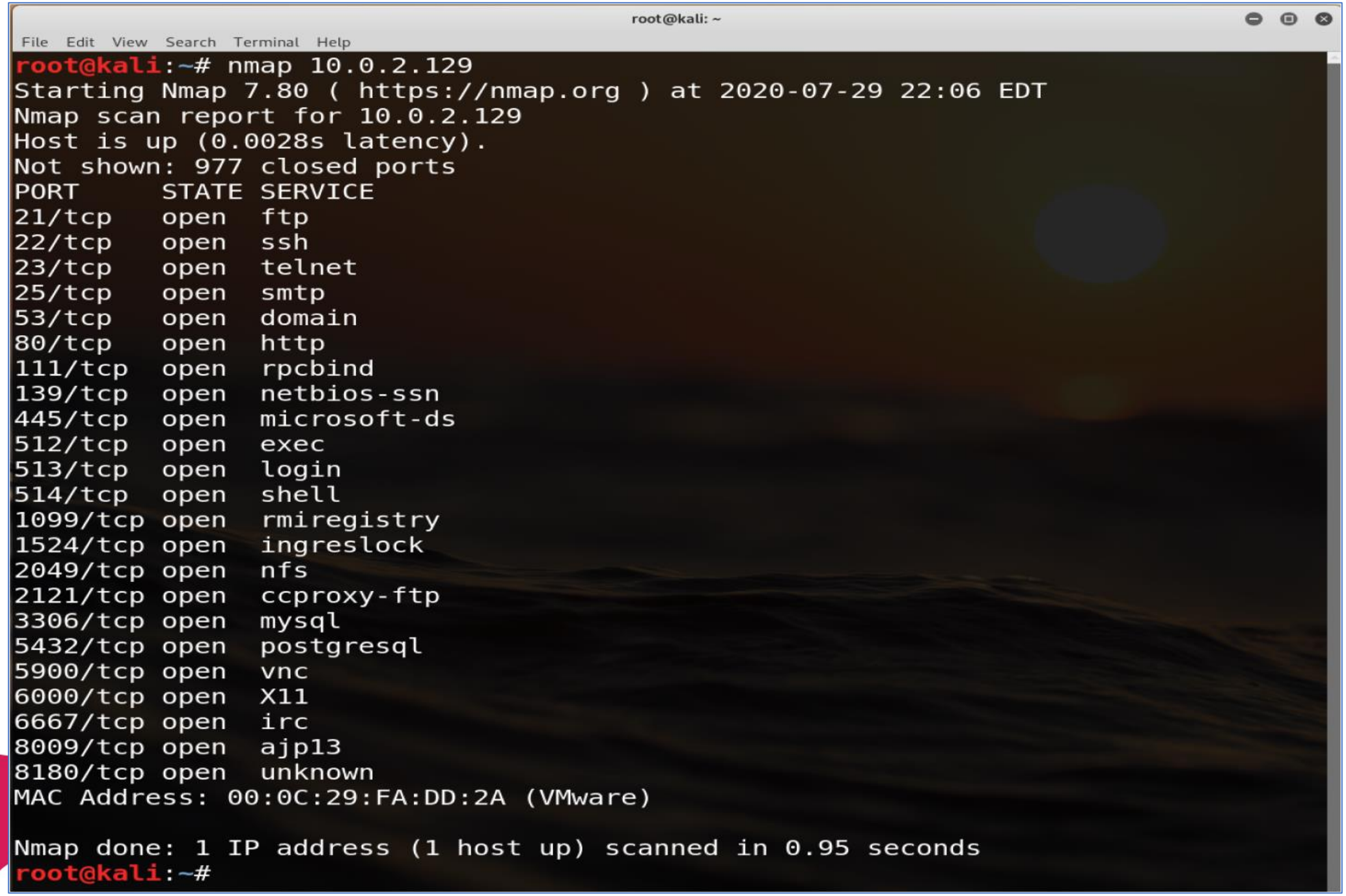
Explicación del comando *ping*.

Uso de herramientas de escaneo

- 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.

Uso de herramientas de escaneo

- 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.

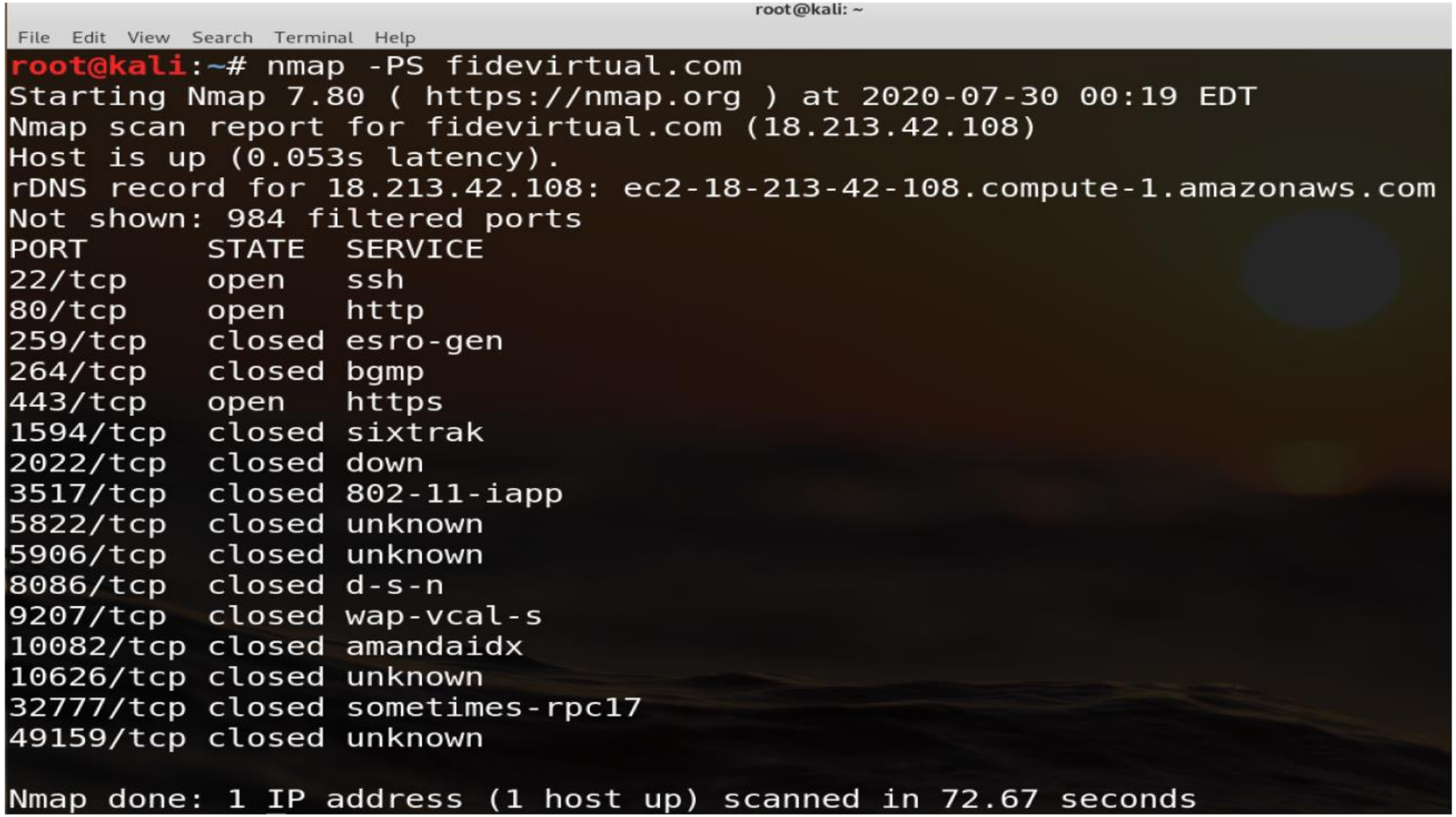

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap 10.0.2.129
Starting Nmap 7.80 (https://nmap.org) at 2020-07-29 22:06 EDT
Nmap scan report for 10.0.2.129
Host is up (0.0028s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
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:~#

Mira el video

Explicación del comando *nmap <número IP>*

Uso de herramientas de escaneo

- 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.

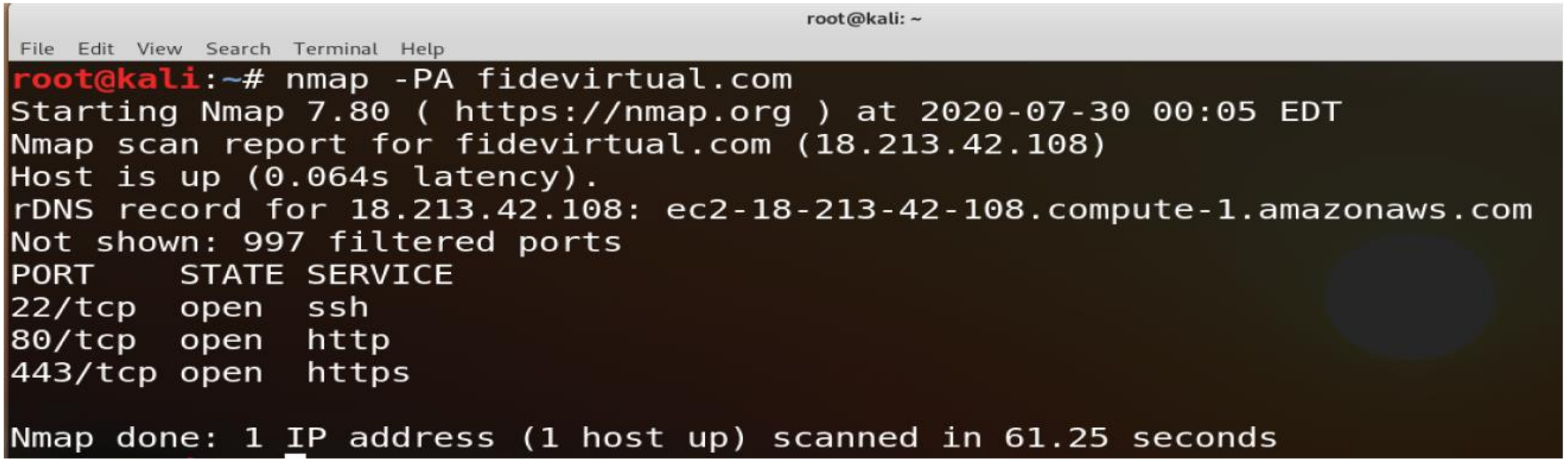

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PS fidevirtual.com
Starting Nmap 7.80 (https://nmap.org) at 2020-07-30 00:19 EDT
Nmap scan report for fidevirtual.com (18.213.42.108)
Host is up (0.053s latency).
rDNS record for 18.213.42.108: ec2-18-213-42-108.compute-1.amazonaws.com
Not shown: 984 filtered ports
PORT STATE SERVICE
22/tcp open ssh
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

Mira el video

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

Uso de herramientas de escaneo

- 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

Mira el video

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

FIDE VIRTUAL

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.

Gracias