Certificado de Profesionalidad en Seguridad Informática
IronHack - SOC

Módulo 2
Práctica 3 - Nmap

Alumno: Julián Gordon

Indice

Introducción 3

Descarga e Instalación de Nmap 4

Reconocimiento de IPs de nuestra red 5

Escaneo avanzado sobre máquina Metasploitable 7

Escaneo usando módulos de scripts 8

Conclusiones 11

Introducción

En el ámbito de la ciberseguridad, la evaluación de la seguridad de redes y sistemas es una tarea crítica para proteger la integridad y confidencialidad de la información. En este contexto, Nmap (Network Mapper) emerge como una herramienta fundamental y de código abierto utilizada por profesionales de seguridad informática en todo el mundo. Nmap ofrece capacidades avanzadas de exploración de red, permitiendo a los administradores de sistemas identificar dispositivos, servicios y sistemas operativos en una red, así como detectar posibles vulnerabilidades que podrían ser explotadas por atacantes malintencionados.

El objetivo principal de esta actividad es introducirnos en el uso de Nmap mediante la instalación y realización de escaneos básicos en diferentes sistemas operativos, incluyendo Windows, Linux. A través de esta experiencia práctica, podremos adquirir habilidades esenciales para identificar dispositivos activos en una red, explorar los servicios que ofrecen y comprender cómo Nmap puede ser utilizado como una herramienta efectiva en la evaluación de la seguridad de redes.

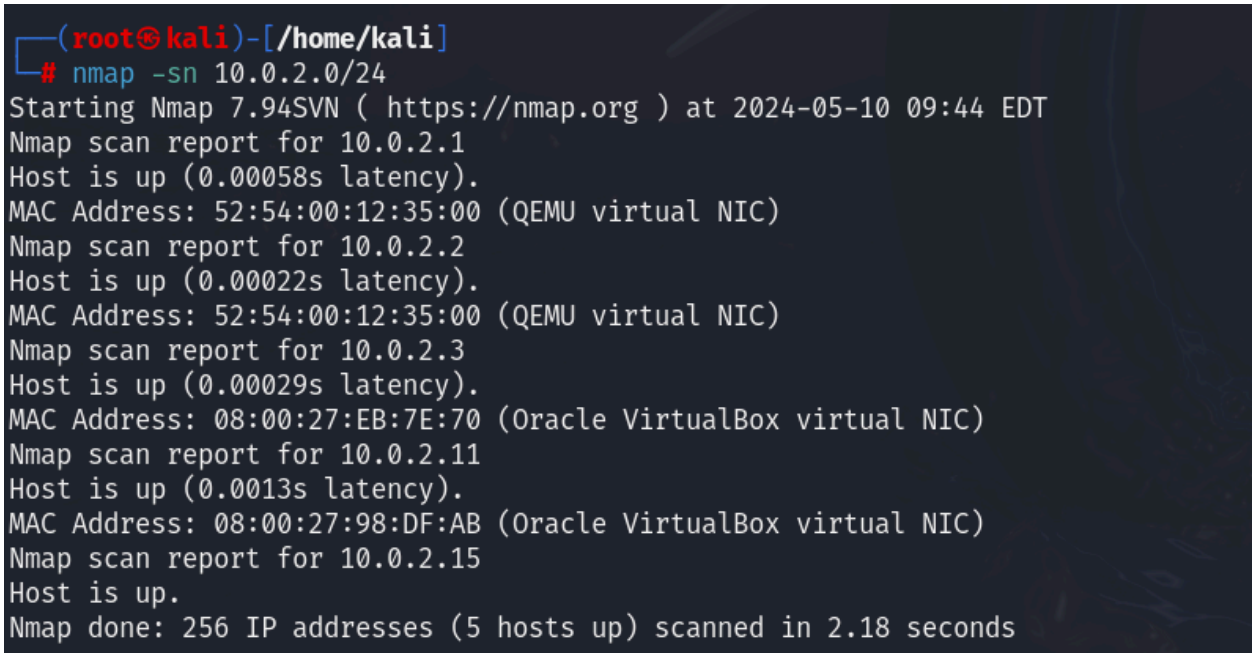
Para llevar a cabo esta práctica, se utilizará un entorno virtualizado donde se simulará una red con el sistema operativo Kali Linux como plataforma de ataque y Metasploitable y Windows 10 como objetivos de prueba. Esta configuración proporcionará un ambiente seguro y controlado para que adquiramos experiencia práctica en el uso de Nmap, explorando sus capacidades básicas y avanzadas en la identificación de dispositivos, servicios y vulnerabilidades en una red simulada.

A lo largo de esta actividad, se enfatizará la importancia de la exploración proactiva de la red y la comprensión de los resultados obtenidos a través de los escaneos realizados con Nmap.

Instalación de la herramienta Nmap

Comenzaremos esta práctica instalando la herramienta Nmap en nuestro sistema Kali Linux. Para ello usaremos el comando sudo apt install nmap.

Ahora realizamos un escaneo simple para verificar los dispositivos en nuestra misma red local. Usamos el comando nmap -sn 10.0.2.0/24



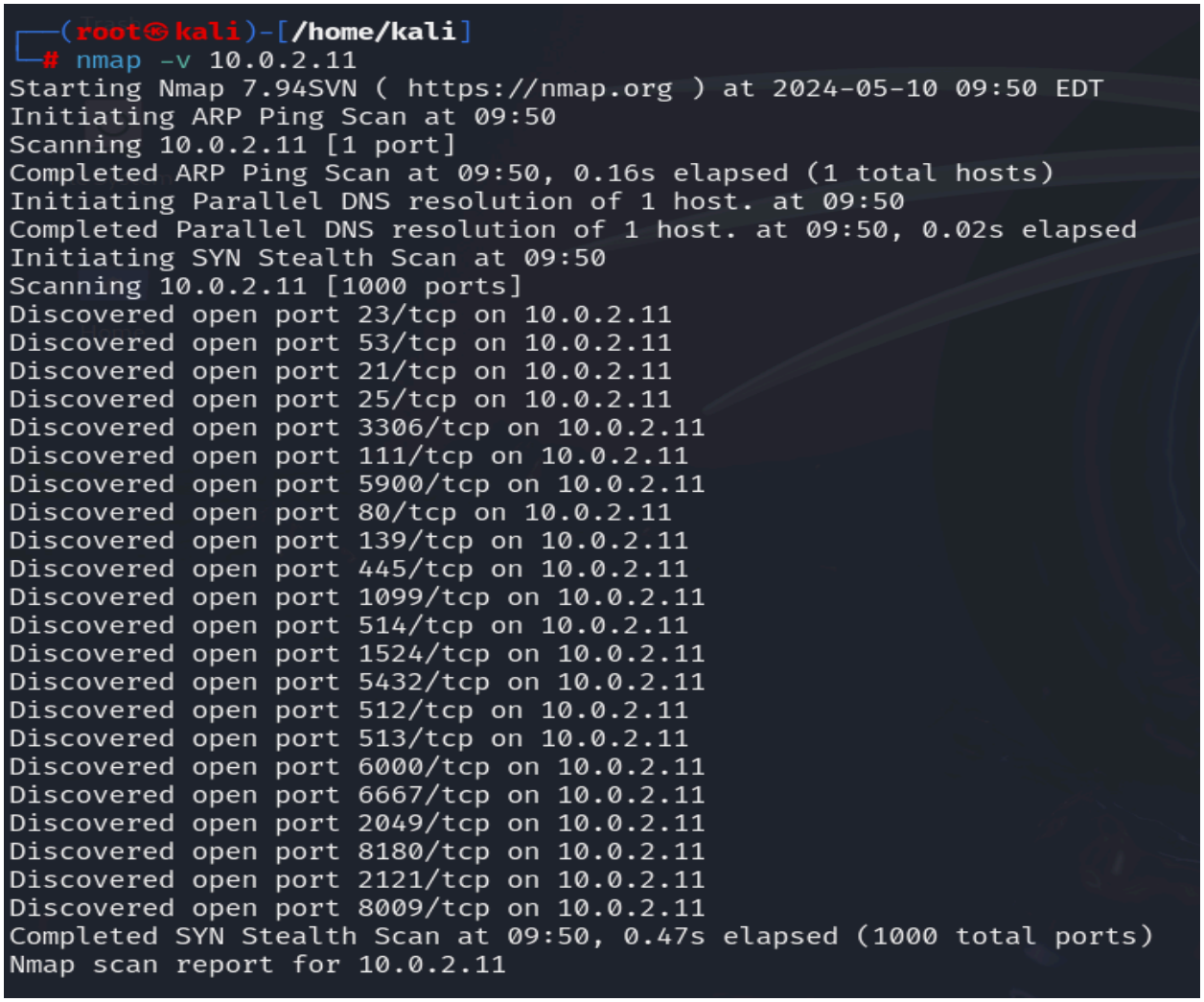
Podemos verificar que encontró 4 IPs dentro de nuestra red, vamos a explicar que es cada una. Las direcciones IP 10.0.2.1, 10.0.2.2 y 10.0.2.3 son direcciones IP asignadas por VirtualBox a diferentes componentes de su entorno virtualizado. Estas direcciones son utilizadas internamente por VirtualBox para la comunicación entre las máquinas virtuales y el host.

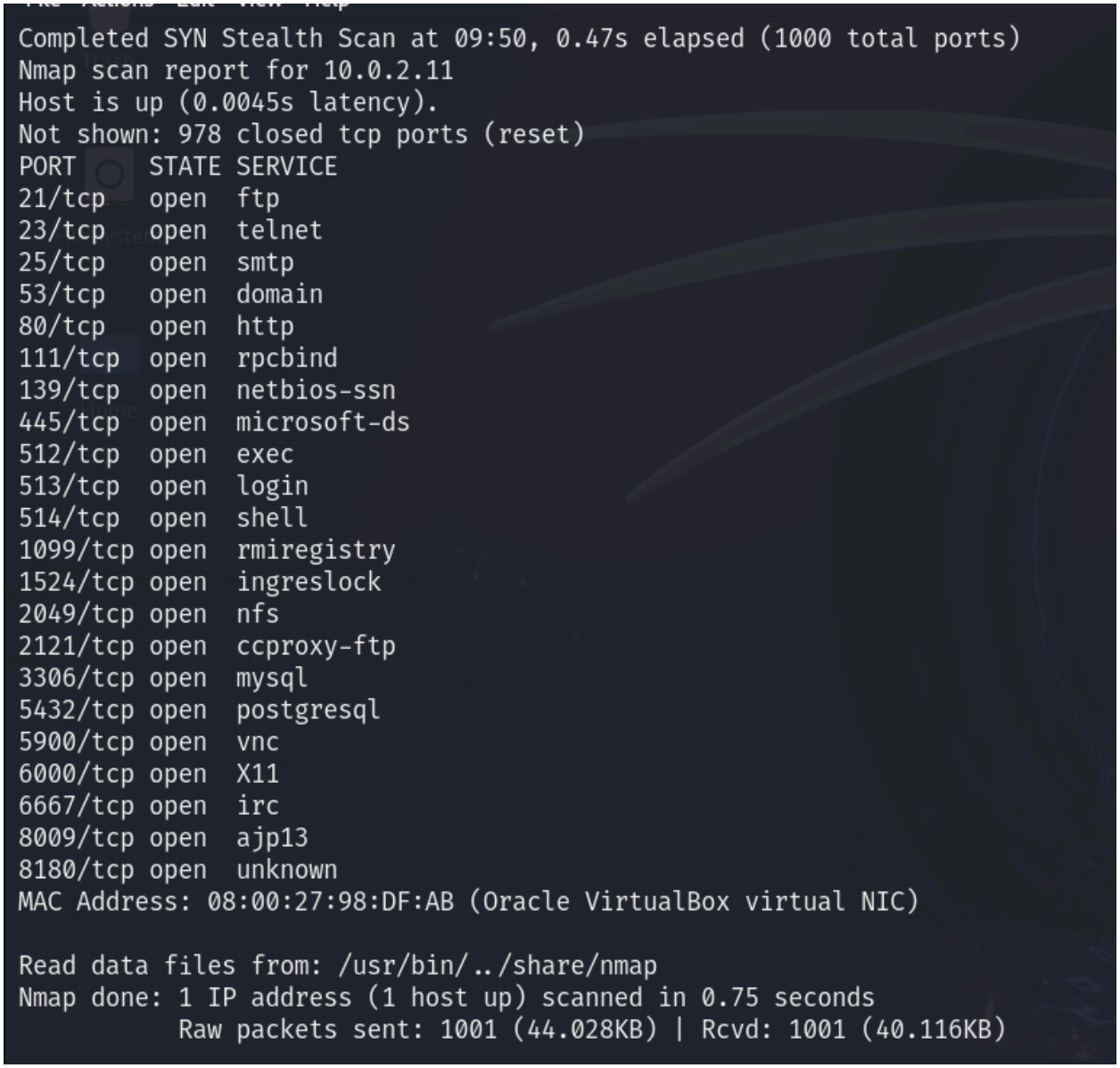
- 10.0.2.1: Esta dirección IP es comúnmente asignada a la puerta de enlace (gateway) virtual de la red NAT en VirtualBox. Funciona como el punto de

entrada y salida para el tráfico de red entre las máquinas virtuales y la red externa.

- 10.0.2.2: Esta dirección IP es asignada al propio host de VirtualBox, es decir, la máquina física donde se ejecuta VirtualBox. Se utiliza para la comunicación entre las máquinas virtuales y el sistema operativo anfitrión.
- 10.0.2.3: Esta dirección IP puede ser asignada a la interfaz de red del sistema operativo invitado (guest) en VirtualBox. En este caso, la dirección IP está asociada a una interfaz de red virtual proporcionada por Oracle VirtualBox.
- 10.0.2.11: Es la dirección IP asignada a la máquina virtual Metasploitable, una distribución vulnerable diseñada para propósitos de entrenamiento y pruebas de seguridad.
- 10.0.2.15: Es la dirección IP asignada a nuestra máquina virtual Kali Linux

Ahora vamos a realizar un escaneo de puertos en un host específico, en este caso la máquina de Metasploitable, utilizando: nmap -v - 10.0.2.11

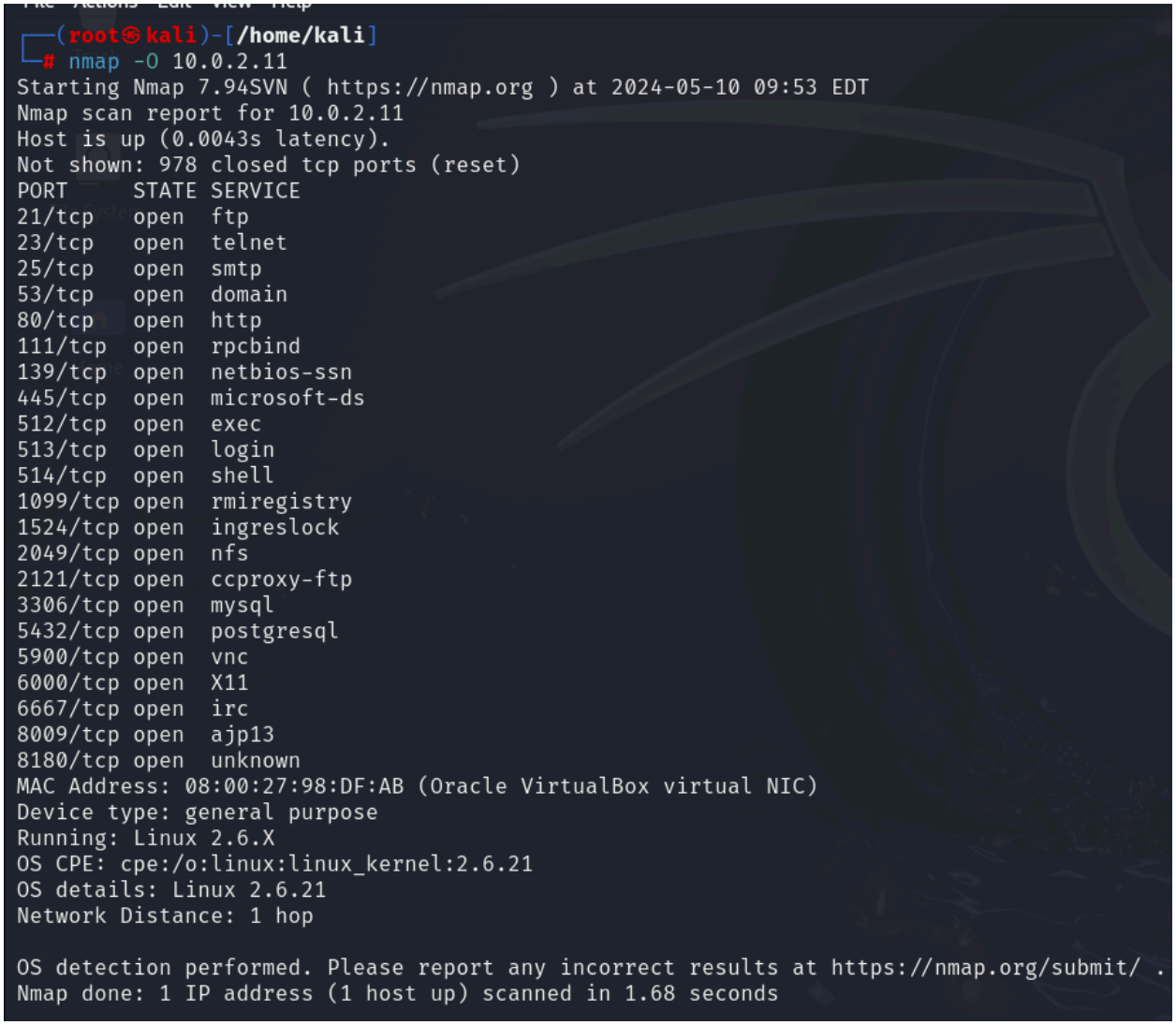




```
Completed SYN Stealth Scan at 09:50, 0.47s elapsed (1000 total ports)
Nmap scan report for 10.0.2.11
Host is up (0.0045s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
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: 08:00:27:98:DF:AB (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.116KB)
```

Ahora haremos un escaneo un poco más avanzado sobre nuestro mismo objetivo con el comando nmap -O y nos dará el sistema operativo de esta máquina.

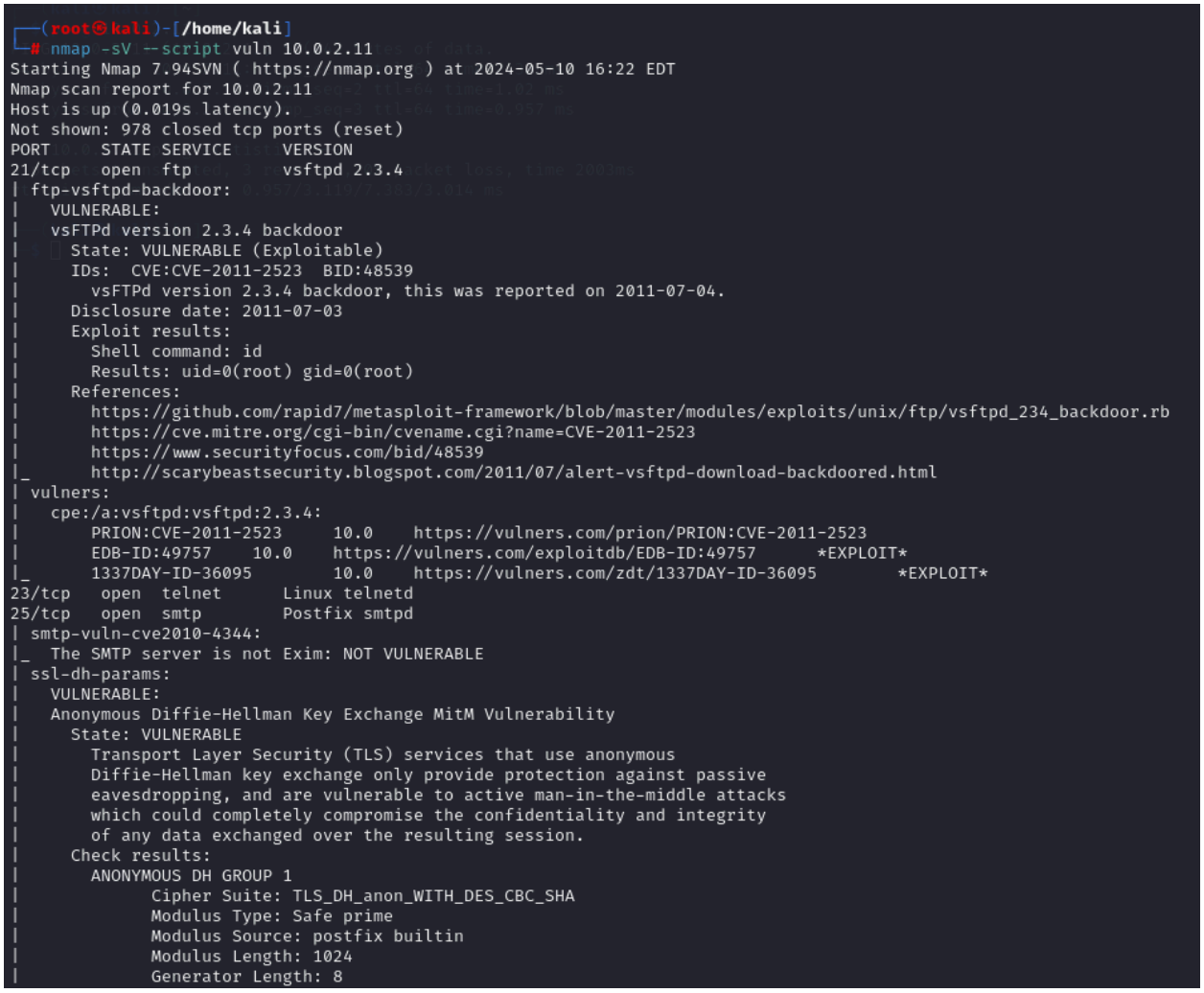


Podemos observar que el sistema operativo detectado por nmap es un Linux 2.6.21. Esto es correcto ya que sabemos que Metasploitable corre en un Linux.

Ahora vamos a realizar un escaneo detallado utilizando scripts de Nmap para obtener información adicional sobre servicios específicos corriendo en la máquina de Metasploitable, para ello usaremos los siguientes comandos:

Para un Escaneo de vulnerabilidades con el script vuln:

nmap -sV --script vuln 10.0.2.11



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --script vuln 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 16:22 EDT
Nmap scan report for 10.0.2.11
Host is up (0.019s latency).
Not shown: 978 closed tcp ports (reset)
PORT   STATE SERVICE     VERSION
21/tcp open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       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:
|       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
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| vulners:
|   cpe:/a:vsftpd:vsftpd:2.3.4:
|       PRION:CVE-2011-2523     10.0    https://vulners.com/prion/PRION:CVE-2011-2523
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|_      1337DAY-ID-36095        10.0    https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
23/tcp open  telnet      Linux telnetd
25/tcp open  smtp        Postfix smtpd
| 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
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
```

```
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       SSV:2853        10.0    https://vulners.com/seebug/SSV:2853     *EXPLOIT*
|       PRION:CVE-2008-0122     10.0    https://vulners.com/prion/PRION:CVE-2008-0122
|       SSV:60184       8.5     https://vulners.com/seebug/SSV:60184    *EXPLOIT*
|       PRION:CVE-2012-1667     8.5     https://vulners.com/prion/PRION:CVE-2012-1667
|       CVE-2012-1667   8.5     https://vulners.com/cve/CVE-2012-1667
|       SSV:60292       7.8     https://vulners.com/seebug/SSV:60292    *EXPLOIT*
|       PRION:CVE-2014-8500     7.8     https://vulners.com/prion/PRION:CVE-2014-8500
|       PRION:CVE-2012-5166     7.8     https://vulners.com/prion/PRION:CVE-2012-5166
|       PRION:CVE-2012-4244     7.8     https://vulners.com/prion/PRION:CVE-2012-4244
|       PRION:CVE-2012-3817     7.8     https://vulners.com/prion/PRION:CVE-2012-3817
|       CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
|       CVE-2012-5166   7.8     https://vulners.com/cve/CVE-2012-5166
|       CVE-2012-4244   7.8     https://vulners.com/cve/CVE-2012-4244
|       CVE-2012-3817   7.8     https://vulners.com/cve/CVE-2012-3817
|       CVE-2008-4163   7.8     https://vulners.com/cve/CVE-2008-4163
|       PRION:CVE-2010-0382     7.6     https://vulners.com/prion/PRION:CVE-2010-0382
|       CVE-2010-0382   7.6     https://vulners.com/cve/CVE-2010-0382
|       EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    7.2     https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    *EXPLOIT*
|       EDB-ID:42121    7.2     https://vulners.com/exploitdb/EDB-ID:42121      *EXPLOIT*
|       CVE-2017-3141   7.2     https://vulners.com/cve/CVE-2017-3141
|       PRION:CVE-2015-8461     7.1     https://vulners.com/prion/PRION:CVE-2015-8461
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|       PRION:CVE-2015-8704     6.8     https://vulners.com/prion/PRION:CVE-2015-8704
|       PRION:CVE-2009-0025     6.8     https://vulners.com/prion/PRION:CVE-2009-0025
|       CVE-2021-25216  6.8     https://vulners.com/cve/CVE-2021-25216
|       CVE-2015-8704   6.8     https://vulners.com/cve/CVE-2015-8704
|       CVE-2009-0025   6.8     https://vulners.com/cve/CVE-2009-0025
|       PRION:CVE-2015-8705     6.6     https://vulners.com/prion/PRION:CVE-2015-8705
|       CVE-2015-8705   6.6     https://vulners.com/cve/CVE-2015-8705
|       PRION:CVE-2010-3614     6.4     https://vulners.com/prion/PRION:CVE-2010-3614
|       CVE-2010-3614   6.4     https://vulners.com/cve/CVE-2010-3614
|       SSV:4636        5.8     https://vulners.com/seebug/SSV:4636     *EXPLOIT*
|       SSV:30099       5.0     https://vulners.com/seebug/SSV:30099    *EXPLOIT*
|       SSV:20595       5.0     https://vulners.com/seebug/SSV:20595    *EXPLOIT*
|       PRION:CVE-2016-9444     5.0     https://vulners.com/prion/PRION:CVE-2016-9444
|       PRION:CVE-2016-2848     5.0     https://vulners.com/prion/PRION:CVE-2016-2848
|       PRION:CVE-2015-8000     5.0     https://vulners.com/prion/PRION:CVE-2015-8000
|       PRION:CVE-2012-1033     5.0     https://vulners.com/prion/PRION:CVE-2012-1033
```

Podemos observar que este script además de decirnos las vulnerabilidades de los puertos y servicios que encuentra, también nos da información sobre dónde encontrar los exploits para vulnerarlas.

Escaneo utilizando scripts para la detección de servicios de bases de datos:

nmap -sV --script=db* 10.0.2.11

```
└─# nmap -sV --script=db* 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 10:03 EDT
Nmap scan report for 10.0.2.11
Host is up (0.0089s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      38738/udp   mountd
|   100005  1,2,3      44188/tcp   mountd
|   100021  1,3,4      33056/tcp   nlockmgr
|   100021  1,3,4      59932/udp   nlockmgr
|   100024  1          41532/udp   status
|_  100024  1          59746/tcp   status
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 rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```

Escaneo utilizando un script específico para detectar servicios FTP.

nmap -sV --script ftp* 10.0.2.11

Escaneo detallado utilizando scripts de detección de servicios HTTP:

nmap -sV --script=default,http* 10.0.2.11

Hay una gran variedad de scripts para explotar vulnerabilidades con Nmap, en su página web https://nmap.org/ , podemos encontrar una guia donde nos explica detalles sobre los puertos utilizados por distintos servicios, que comandos utilizar y cómo funciona en profundidad la herramienta.

Conclusiones

Hemos abordado varios aspectos clave relacionados con Nmap y su papel en la ciberseguridad:

- Importancia de la evaluación de seguridad de redes: resaltamos la necesidad de evaluar la seguridad de redes y sistemas para salvaguardar la integridad y confidencialidad de la información en entornos digitales.
- Funcionalidades de Nmap: explicamos cómo Nmap, herramienta de código abierto, ofrece capacidades avanzadas para la exploración de redes, permitiendo a los administradores de sistemas identificar dispositivos, servicios y sistemas operativos, así como detectar vulnerabilidades potenciales.
- Experiencia práctica con Nmap: Se ha proporcionado una visión detallada de la experiencia práctica adquirida al utilizar Nmap para llevar a cabo escaneos básicos y avanzados en una variedad de sistemas operativos, incluyendo Windows y Linux, dentro de un entorno virtualizado.
- Comprensión de los resultados de los escaneos: Se ha enfatizado la importancia de comprender los resultados obtenidos a través de los escaneos realizados con Nmap, lo que incluye la identificación de dispositivos activos, la exploración de servicios ofrecidos y la detección de posibles vulnerabilidades.
- Uso de scripts de Nmap: Se ha explorado el uso de scripts de Nmap para obtener información adicional sobre servicios específicos y para detectar vulnerabilidades en la red, destacando la versatilidad de la herramienta en la detección y explotación de vulnerabilidades.

Este trabajo ha demostrado una comprensión sólida de Nmap como una herramienta integral en la evaluación de la seguridad de redes, destacando su importancia, funcionalidades, aplicación práctica y recursos disponibles para un análisis más profundo.