EJERCICIOS ESCÁNER DE RED NMAP

Prerrequisitos

Kali Linux
Metasploitable2

Creación del laboratorio

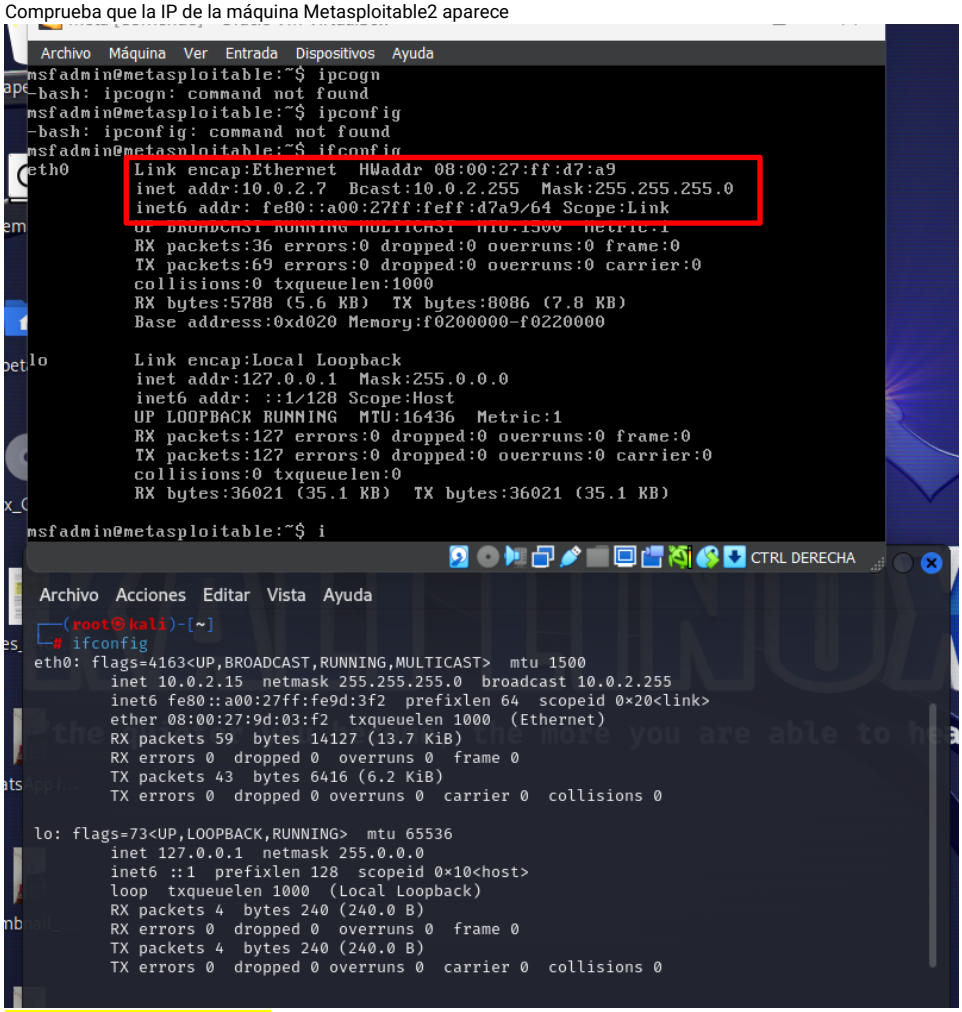
Descarga la imagen de máquina virtual de Metasploitable2:
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
Sigue esta guía de instalación para crear la máquina virtual Metasploitable2:
https://www.hacking-tutorial.com/tips-and-trick/install-metasploitable-on-virtual-box/
Utiliza la siguiente configuración para las máquinas virtuales Metasploitable2 y Kali Linux:
Configuración > Red > Adaptador 1 > Red NAT > NatNetwork > Aceptar
Enciende las máquinas virtuales, Metasploitable2 y Kali Linux, y comprueba:
Dirección IP de Kali Linux
Dirección IP de Metasploitable2
Haz ping para comprobar la conectividad entre ellas
En caso de obtener resultado negativo, revisa todos los pasos comenzando de nuevo desde el principio. En caso de obtener resultado positivo, realiza los siguientes ejercicios

Ejercicio 1 - Nmap

Descubre los equipos conectados a la Red NAT 10.0.2.X-255 o 10.0.2.X/24

```
┌──(root㉿kali)-[~]
└─# nmap -sn 10.0.2.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 17:52 CEST
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.00085s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00056s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00078s latency).
MAC Address: 08:00:27:E4:C4:F2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7 (10.0.2.7)
Host is up (0.011s latency).
MAC Address: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.13 seconds
```

Comprueba que la IP de la máquina Metasploitable2 aparece



Esta es la IP de Metasploitable2

```
MAC Address: 08:00:27:E4:C4:F2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7 (10.0.2.7)
Host is up (0.011s latency).

┌──(root㉿kali)-[~]
└─# ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=2.44 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=39.7 ms
^C
── 10.0.2.7 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 2.435/21.085/39.735/18.650 ms
```

Ejercicio 2 - Nmap

Escanea los puertos de la máquina Metasploitable2

```
┌──(root㉿kali)-[~]
└─# nmap -sV -p- 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 18:02 CEST
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 18:03 (0:00:01 remaining)
```

```
Nmap scan report for 10.0.2.7 (10.0.2.7)
Host is up (0.0099s latency).
Not shown: 65505 closed tcp ports (reset)
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     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 rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
39870/tcp open  java-rmi    GNU Classpath grmiregistry
44509/tcp open  mountd      1-3 (RPC #100005)
45411/tcp open  nlockmgr    1-4 (RPC #100021)
49975/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe
:/o:linux:linux_kernel
```

Ejercicio 3 - Nmap

Realiza un esquema de la siguiente forma:

PUERTO - ESTADO - SERVICIO - QUE HACE ESTE SERVICIO para todos los puertos del equipo

```
┌──(root㉿kali)-[~]
└─# nmap 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 13:33 CEST
Nmap scan report for 10.0.2.7
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
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: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
```

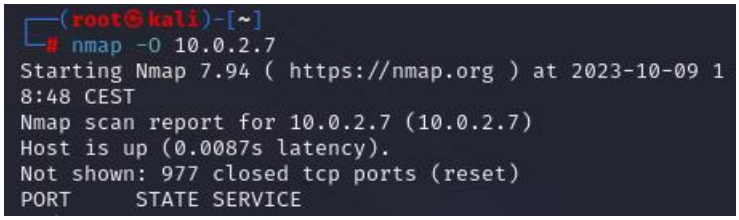
Busca información de los puertos y servicios según el resultado de Nmap en Google

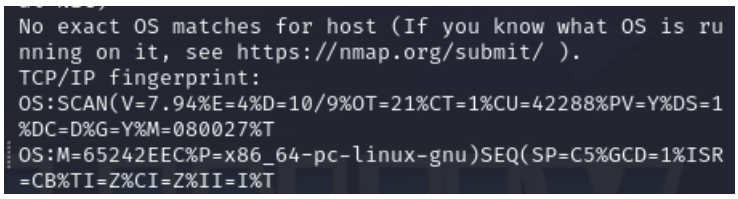
- 21/tcp open ftp: transferencia de archivos entre dispositivos en una red.
- 22/tcp open ssh: facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.
- 23/tcp open telnet: Permite la comunicación de terminal a terminal y se puede utilizar para varios fines.
- 25/tcp open smtp: se encarga del envío de correos electrónicos desde un cliente como Outlook hacia el servidor
- 53/tcp open domain: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados.
- 80/tcp open http: el protocolo de transferencia de hipertexto que se utiliza para acceder a todas las páginas web.
- 111/tcp open rpcbind: se puede utilizar para identificar el sistema operativo Nix y para obtener información sobre los servicios disponibles.
- 139/tcp open netbios-ssn: se utiliza si SMB está configurado para ejecutarse en NetBIOS sobre TCP/IP.
- 445/tcp open microsoft-ds: es un protocolo de red utilizado principalmente en redes Windows para compartir recursos, como archivos o impresoras, a través de una red.
- 512/tcp open exec: Este protocolo permite a los usuarios ejecutar comandos en un host remoto.
- 513/tcp open login: Este protocolo permite a los usuarios iniciar sesión en un host remoto y ejecutar comandos en él.
- 514/tcp open shell: Este protocolo permite a los usuarios ejecutar comandos en un host remoto. El puerto 514 es el puerto predeterminado para el servicio de shell remota rsh
- 1099/tcp open rmiregistry. El registro RMI es un servicio de nombres que se utiliza para registrar objetos remotos y hacerlos accesibles a los clientes que desean invocar métodos en ellos
- 1524/tcp open ingreslock: Ingreslock es un backdoor que se utiliza a menudo como una puerta trasera por programas que explotan servicios RPC (Remote Procedure Call) vulnerables
- 2049/tcp open nfs: es un protocolo de red que permite a los sistemas operativos compartir archivos y directorios a través de una red.
- 2121/tcp open ccproxy-ftp: es un servidor proxy que se utiliza para compartir una conexión a Internet en una red local.
- 3306/tcp open mysql: es un sistema de gestión de bases de datos relacional que se utiliza para almacenar y recuperar datos.
- 5432/tcp open postgresql: es un sistema de gestión de bases de datos relacional que se utiliza para almacenar y recuperar datos.
- 5900/tcp open vnc: es un sistema de control remoto de escritorio que permite a los usuarios conectarse y controlar una computadora de forma remota a través de una red.
- 6000/tcp open X11: es un sistema de ventanas que proporciona una interfaz gráfica de usuario para sistemas operativos basados en Unix y Linux
- 6667/tcp open irc: es un sistema de chat en línea que permite a los usuarios comunicarse en tiempo real a través de una red.
- 8009/tcp open ajp13: es un protocolo binario que se utiliza para la comunicación entre servidores web y servidores de aplicaciones.
- 8180/tcp open unknown: El puerto 8180 es un puerto comúnmente utilizado para servicios web y aplicaciones, pero sin más información, no puedo determinar el propósito exacto del servicio que se ejecuta en este puerto.

Ejercicio 4 - Nmap

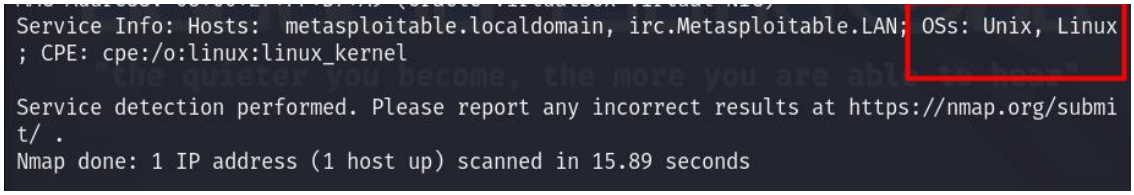
¿Qué versión de sistema operativo utiliza?

No especifica el sistema operativo al ejecutar el comando





Al hacer un comando más especifico sí determina el OS



```
┌──(root㉿kali)-[/etc]
└─# nmap -sV 10.0.2.7 -T 3 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 05:47 EDT
Nmap scan report for 10.0.2.7 (10.0.2.7)
Host is up (0.013s latency).
```

```
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
Device type: general purpose|router|media device|WAP|switch
Running (JUST GUESSING): Linux 2.6.X|2.4.X (97%), Linksys embedded (96%), Osmosys embedded (
96%), Extreme Networks ExtremeXOS 15.X|16.X (93%), AVM embedded (93%), ZyXEL embedded (93%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:linksys:rv042 cpe:/h:linksys:wrv54g cpe:/o:linu
x:linux_kernel:2.4.32 cpe:/o:extremenetworks:extremexos:15 cpe:/o:extremenetworks:extremexos
:16 cpe:/o:linux:linux_kernel:2.4.18 cpe:/h:avm:fritz%21box_fon_wlan_7240
```

Ejercicio 5 - Nmap

Completa el esquema del ejercicio 3 con la versión de los servicios desplegados.

PUERTO - ESTADO - SERVICIO - VERSION DEL SERVICIO

```
┌──(root㉿kali)-[~]
└─# nmap -sV 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 13:31 CEST
Nmap scan report for 10.0.2.7
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
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     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 rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         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 (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linu
x; CPE: cpe:/o:linux:linux_kernel
```

Ejercicio 6 - Nmap, Http, Netcat y Telnet

Comprueba manualmente la versión de dos de los servicios levantados utilizando nc, telnet y navegador web

Escogí el servicio SSH y HTTP servicios prestados en los puertos 22,80 respectivamente

NC:

```
┌──(root㉿kali)-[~]
└─# nc 10.0.2.7 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

```
┌──(root㉿kali)-[~]
└─# nc 10.0.2.7 80
```

Telnet:

```
┌──(root㉿kali)-[~]
└─# telnet 10.0.2.7 22
Trying 10.0.2.7 ...
Connected to 10.0.2.7.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

```
┌──(root㉿kali)-[~]
└─# telnet 10.0.2.7 80
Trying 10.0.2.7 ...
Connected to 10.0.2.7.
Escape character is '^]'.
```

Navegador:

Ejercicio 7 - Nmap NSE

Realizar un análisis de vulnerabilidades sobre el servicio SSH de Metasploitable2 utilizando los scripts Nmap NSE vulscan y vulners, de forma que la información quede almacenada en un archivo.txt

```
┌──(root㉿kali)-[/home/ginner]
└─# nmap -vv -sV --script=vulners.nse 10.0.2.7 > archivonmap.txt

┌──(root㉿kali)-[/home/ginner]
└─# cat archivonmap.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 15:09 CEST
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:09
Completed NSE at 15:09, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:09
Completed NSE at 15:09, 0.00s elapsed
Initiating ARP Ping Scan at 15:09
Scanning 10.0.2.7 [1 port]
Completed ARP Ping Scan at 15:09, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:09
Completed Parallel DNS resolution of 1 host. at 15:09, 0.01s elapsed
Initiating SYN Stealth Scan at 15:09
Scanning 10.0.2.7 [1000 ports]
```

```
|_      PACKETSTORM:127092      5.9     https://vulners.com/packetstorm/PACKETSTORM:127092      *EX
PLOIT*
|_      CVE-2010-0733   3.5     https://vulners.com/cve/CVE-2010-0733
5900/tcp open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp open  X11         syn-ack ttl 64 (access denied)
6667/tcp open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| vulners:
|   cpe:/a:apache:coyote_http_connector:1.1:
|       PRION:CVE-2023-26044    5.0     https://vulners.com/prion/PRION:CVE-2023-26044
|_      PRION:CVE-2022-36032    5.0     https://vulners.com/prion/PRION:CVE-2022-36032
MAC Address: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cp
e:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:09
Completed NSE at 15:09, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:09
Completed NSE at 15:09, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.61 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

Vulscan

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# mkdir Vulscan

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# cd vulscan
cd: no existe el fichero o el directorio: vulscan

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# cd Vulscan

┌──(root㉿kali)-[/usr/share/nmap/scripts/Vulscan]
└─# git clone https://github.com/scipag/vulscan scipag_vulscan
Clonando en 'scipag_vulscan' ...
remote: Enumerating objects: 297, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 297 (delta 12), reused 16 (delta 4), pack-reused 264
Recibiendo objetos: 100% (297/297), 17.69 MiB | 1.68 MiB/s, listo.
Resolviendo deltas: 100% (175/175), listo.

┌──(root㉿kali)-[/usr/share/nmap/scripts/Vulscan]
└─# ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

```
┌──(root㉿kali)-[/usr/share/nmap/scripts/Vulscan]
└─# ls -la
total 108
drwxr-xr-x 3 root root  4096 oct 16 16:01 .
drwxr-xr-x 4 root root 98304 oct 16 16:02 ..
drwxr-xr-x 4 root root  4096 oct 16 16:01 scipag_vulscan

┌──(root㉿kali)-[/usr/share/nmap/scripts/Vulscan]
└─# cd scipag_vulscan

┌──(root㉿kali)-[/usr/…/nmap/scripts/Vulscan/scipag_vulscan]
└─# ls
_config.yml  exploitdb.csv  osvdb.csv      securityfocus.csv  update.sh    xforce.csv
COPYING.TXT  logo.png       README.md      securitytracker.csv  utilities
cve.csv      openvas.csv    scipvuldb.csv  update.ps1         vulscan.nse

┌──(root㉿kali)-[/usr/…/nmap/scripts/Vulscan/scipag_vulscan]
└─# nmap -sV --script vulscan.nse 10.0.2.24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-16 16:02 CEST
Nmap scan report for 10.0.2.24
Host is up (0.00079s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2006-0883] OpenSSH on FreeBSD 5.3 and 5.4, when used with OpenPAM, does not properly handle when a forked
child process terminates during PAM authentication, which allows remote attackers to cause a denial of service (c
lient connection refusal) by connecting multiple times to the SSH server, waiting for the password prompt, then d
isconnecting.
```

```
| [504] OpenSSH SSHV2 Public Key Authentication Bypass
| [341] OpenSSH UseLogin Local Privilege Escalation
|_
MAC Address: 08:00:27:42:DC:55 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.83 seconds
```

```
┌──(root㉿kali)-[/usr/share/nmap/scripts/vulscan]
└─# nmap -sV --script vulscan.nse 10.0.2.7 > informevulscan.txt
```