

Escanear puertos con nmap

Carlos Vicent Arnau Chuquispuma

Spain-cs-pt-11

Índice

1. Objetivo de la auditoria	3
2. Alcance de la auditoria	3
3. Herramientas y técnicas utilizadas	3
4. Enumeración de puertos y servicios.....	3
5. Documentar Vulnerabilidades Asociadas a los Servicios.....	4
5.1. Sistema operativo del target	6
5.2. Vulnerabilidades reportadas del target.....	7

Escanear puertos con nmap

1. Objetivo de la auditoria

Se ha realizado una auditoria sobre la máquina virtual Metasploit con el fin de identificar los puertos que se encuentran abiertos, y los programas que se ejecutan a través de ellos.

2. Alcance de la auditoria

El 22 de enero del 2026 se han realizado acciones de pentesting, de la cual tenemos la siguiente información:

IP	192.168.1.43 (DHCP)
Usuario	msfadmin
Contraseña	Conocida por el equipo auditor

3. Herramientas y técnicas utilizadas

Se han utilizado la herramienta Nmap para realizar el escaneo de puertos.

4. Enumeración de puertos y servicios

```
nmap -sV <IP >
```

```
kali@kali: ~  
$ nmap -sV 192.168.1.43  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 01:25 +0100  
Nmap scan report for 192.168.1.43  
Host is up (0.00074s 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:DB:2E:D3 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 12.94 seconds  
  
kali@kali: ~
```

5. Documentar Vulnerabilidades Asociadas a los Servicios

Se han encontrado varias vulnerabilidades. De las cuales se han seleccionado las siguientes:

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
21	FTP	Vsftpd 2.3.4	CVE-2011-2523	La versión instalada de vsftpd contiene una puerta trasera, que permite al atacante abrir una terminal de comandos en el puerto 6200. Lo que permite el acceso remoto sin necesidad de una autenticación adecuada.	Enlace
22	SSH	OpenSSH 4.7	CVE-2023-38408	OpenSSH presenta una vulnerabilidad en la función de reenvío del agente (ssh-agent). Si un usuario se conecta a un servidor malicioso con esta función activada, puede provocar que el atacante cargue módulos inseguros, permitiendo la ejecución de código en el equipo del usuario.	Enlace
80	HTTP	Apache 2.2.8	CVE2017-1001000	Esta versión de Apache contiene una vulnerabilidad en que permite a un atacante provocar un fallo en el servidor al manipular nombres de directorios de usuarios. Esto puede generar una denegación de servicio (DoS), haciendo que el servidor web deje de responder o se bloquee cuando procesa solicitudes especialmente diseñadas.	Enlace
3306	MYSQL	MySQL 5.0.51	CVE-2017-15945	MySQL tiene una vulnerabilidad que permite a un atacante ejecutar consultas especialmente manipuladas que pueden provocar un fallo en el servidor o una condición de denegación de servicio. Versiones antiguas como la 5.0.51 son especialmente sensibles, ya que no incluyen las protecciones actuales frente a consultas malformadas o	Enlace

Escanear puertos con nmap

				comportamiento inesperado en la gestión de datos.	
--	--	--	--	---	--

Escanear puertos con nmap

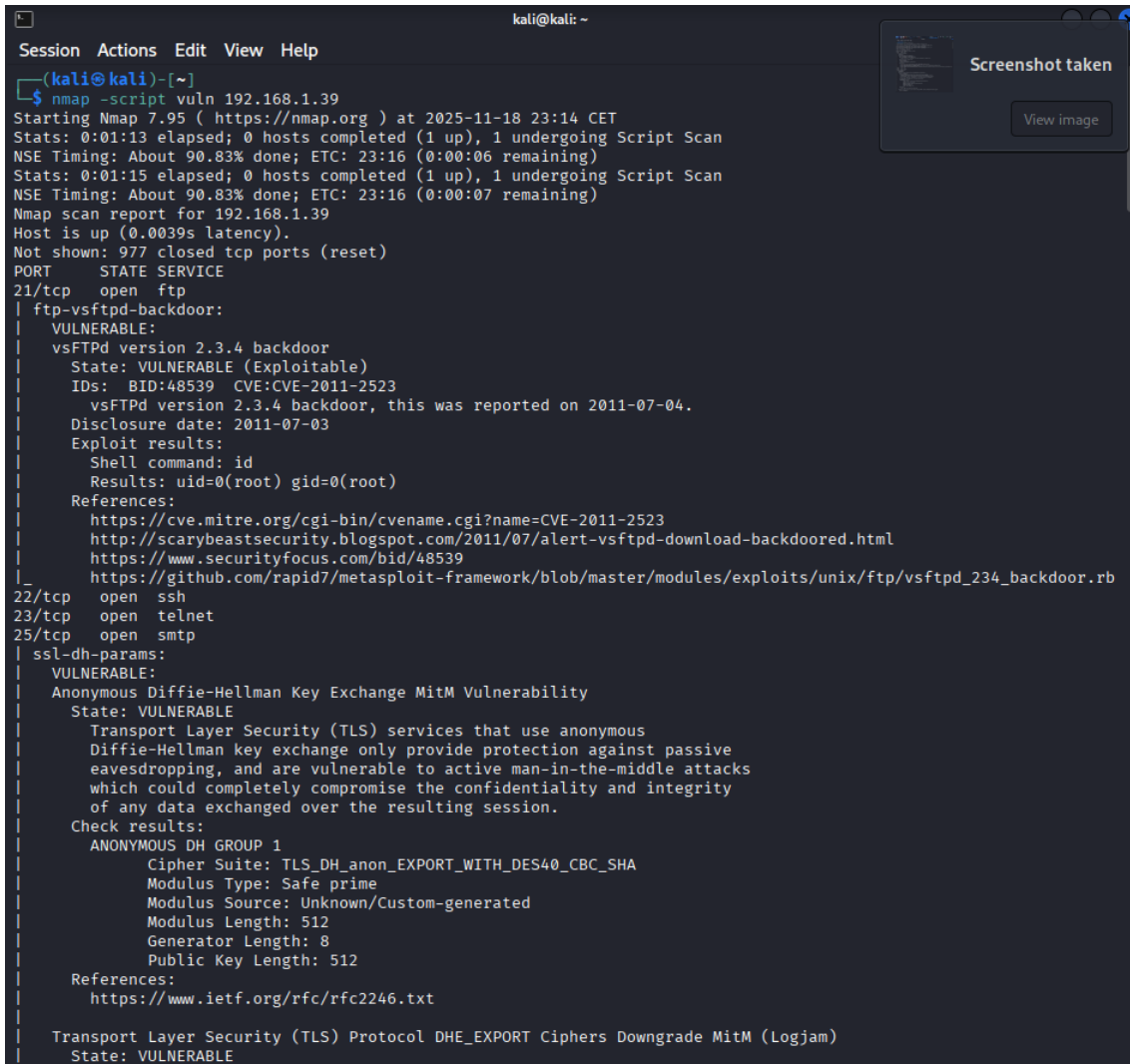
5.1. Sistema operativo del target

Se ha realizado el comando “nmap -A -v 192.168.1.39” para obtener información del target como el sistema operativo.

```
kali@kali: ~  
Session Actions Edit View Help  
|_ http-favicon: Apache Tomcat  
|_ http-methods:  
|_ Supported Methods: GET HEAD POST OPTIONS  
|_ http-title: Apache Tomcat/5.5  
MAC Address: 08:00:27:DB:2E:D3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Uptime guess: 0.020 days (since Tue Nov 18 22:23:48 2025)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=204 (Good luck!)  
IP ID Sequence Generation: All zeros  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_ smb-os-discovery:  
|_ OS: Unix (Samba 3.0.20-Debian)  
|_ Computer name: metasploitable  
|_ NetBIOS computer name:  
|_ Domain name: localdomain  
|_ FQDN: metasploitable.localdomain  
|_ System time: 2025-11-18T16:52:10-05:00  
|_ smb2-time: Protocol negotiation failed (SMB2)  
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
|_ Names:  
|_ METASPLOITABLE<00> Flags: <unique><active>  
|_ METASPLOITABLE<03> Flags: <unique><active>  
|_ METASPLOITABLE<20> Flags: <unique><active>  
|_ \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>  
|_ WORKGROUP<00> Flags: <group><active>  
|_ WORKGROUP<1d> Flags: <unique><active>  
|_ WORKGROUP<1e> Flags: <group><active>  
|_ clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s  
|_ smb-security-mode:  
|_ account_used: guest  
|_ authentication_level: user  
|_ challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 4.09 ms 192.168.1.39  
  
NSE: Script Post-scanning.  
Initiating NSE at 22:52  
Completed NSE at 22:52, 0.00s elapsed  
Initiating NSE at 22:52  
Completed NSE at 22:52, 0.00s elapsed  
Initiating NSE at 22:52  
Completed NSE at 22:52, 0.00s elapsed
```

5.2. Vulnerabilidades reportadas del target

Se ha realizado el comando “nmap –script vuln 192.168.1.39” para obtener las vulnerabilidades reportadas del sistema.



```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ nmap -script vuln 192.168.1.39
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 23:14 CET
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.83% done; ETC: 23:16 (0:00:06 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.83% done; ETC: 23:16 (0:00:07 remaining)
Nmap scan report for 192.168.1.39
Host is up (0.0039s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:  BID:48539  CVE:CVE-2011-2523
|   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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| 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_EXPORT_WITH_DES40_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: Unknown/Custom-generated
|   Modulus Length: 512
|   Generator Length: 8
|   Public Key Length: 512
|   References:
|   https://www.ietf.org/rfc/rfc2246.txt
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|   State: VULNERABLE

```