



SCANSIONE VULNERABILITÀ CON NESSUS

report di **MORGAN PETRELLI S5/L5**



INDICE

VULNERABILITÀ TROVATE
VNC SERVER PASSWORD
BIND SHELL BACKDOOR DETECTION
RISULTATO AZIONI DI RIMEDIO



| <input type="checkbox"/> Sev ▼ | CVSS ▼ | VPR ▼ | Name ▲ | Family ▲ | Count ▼ | ⚙ |
|-----------------------------------|--------|-------|----------------------------------------------------------|-----------------------|---------|-----|
| <input type="checkbox"/> CRITICAL | 10.0 * | 5.9 | NFS Exported Share Information Disclosure | RPC | 1 | 🕒 ✎ |
| <input type="checkbox"/> CRITICAL | 10.0 | | Unix Operating System Unsupported Version Detection | General | 1 | 🕒 ✎ |
| <input type="checkbox"/> CRITICAL | 10.0 * | | VNC Server 'password' Password | Gain a shell remotely | 1 | 🕒 ✎ |
| <input type="checkbox"/> CRITICAL | 9.8 | 9.0 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | 1 | 🕒 ✎ |
| <input type="checkbox"/> CRITICAL | 9.8 | | Bind Shell Backdoor Detection | Backdoors | 1 | 🕒 ✎ |
| <input type="checkbox"/> CRITICAL | 9.8 | | SSL Version 2 and 3 Protocol Detection | Service detection | 1 | 🕒 ✎ |

Traccia:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.



CRITICAL 10.0 * VNC Server 'password' Password Gain a shell remotely 1

La vulnerabilità evidenziata indica che la password predefinita del server VNC è troppo debole o non è stata cambiata dalla configurazione predefinita.

Con il comando `vncpasswd` ho modificato la password con una più complicata così da evitare possibili attacchi di brute force.

Ho messo una password di accesso completo e una di solo lettura per rendere ancora più sicuro il server


```
$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 14:40 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0045s latency).

PORT      STATE SERVICE      VERSION
1524/tcp  open  bindshell    Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds
```

```
$ nc 192.168.50.101 1524
root@metasploitable:/# netstat -tuln | grep 1524
tcp        0      0 0.0.0.0:1524          0.0.0.0:*          LISTEN
root@metasploitable:/# sudo lsof -i :1524
COMMAND  PID USER  FD   TYPE DEVICE SIZE NODE NAME
bash     3106 root   0u    IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
bash     3106 root   1u    IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
bash     3106 root   2u    IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
bash     3106 root  255u  IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
lsof     3117 root   0u    IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
lsof     3117 root   1u    IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
lsof     3117 root   2u    IPv4 156852      TCP 192.168.50.101:ingreslock→192.168.50.100:45828 (ESTABLISHED)
xinetd   4525 root  12u   IPv4 12198      TCP *:ingreslock (LISTEN)
root@metasploitable:/# sudo kill 4525
root@metasploitable:/# ^C

(kali@kali)-[~]
$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```



CRITICAL

9.8

Bind Shell Backdoor Detection

Backdoors

1






Nessus ci segnala che è presente una backdoor sulla porta 1524.

Per risolvere questa vulnerabilità ho innanzitutto, con il comando Nmap `-sV -p 1524 IP TARGET`, scansionato la porta specifica 1524 per vedere se effettivamente la backdoor fosse presente.

Con il comando `nc 192,168,50,101 1524` mi sono connesso alla porta 1524. Ho utilizzato prima il comando `netstat -tuln | grep 1524` non per errore, ma per vedere il pid della porta in ascolto 1524; come risultato però ho avuto soltanto la possibilità di vedere il processo attivo sulla porta in ascolto. Utilizzando invece il comando esatto, `sudo lsof -i :1524`, ho avuto come risultato il pid che mi è servito per interrompere il processo con il comando `sudo kill 4525 (pid)`

Ho verificato che effettivamente la connessione si interrompe e come si può vedere non è più possibile accedere alla backdoor.

| Sev ▼ | CVSS ▼ | VPR ▼ | Name ▲ | Family ▲ | Count ▼ |
|-----------------------------------|--------|-------|----------------------------------------------------------------------------------------------------------------|-----------------------|---------|
| <input type="checkbox"/> CRITICAL | 10.0 * | | NFS Exported Share Information Disclosure | RPC | 1 |
| <input type="checkbox"/> CRITICAL | 10.0 | | Unix Operating System Unsupported Version Detection | General | 1 |
| <input type="checkbox"/> CRITICAL | 9.8 | | SSL Version 2 and 3 Protocol Detection | Service detection | 2 |
| <input type="checkbox"/> CRITICAL | 9.8 | | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | 1 |
| <input type="checkbox"/> MIXED | ... | ... |  Phpmyadmin (Multiple Issues) | CGI abuses | 4 |
| <input type="checkbox"/> CRITICAL | ... | ... |  SSL (Multiple Issues) | Gain a shell remotely | 3 |
| <input type="checkbox"/> MIXED | ... | ... |  PHP (Multiple Issues) | CGI abuses | 3 |
| <input type="checkbox"/> HIGH | 7.5 * | | CGI Generic Remote File Inclusion | CGI abuses | 1 |

Dopo aver effettuato le azioni di rimedio ho nuovamente scansionato con nessus per verificare che effettivamente le azioni di rimedio effettuate sono andate a buon fine. Come possiamo vedere non sono più presenti fra le vulnerabilità critiche il che ci fa capire che le azioni apportate sono state efficaci.