

PROGETTO SETTIMANALE



vulnerability assessment

Vulnerability scanner: Nessus

Target: Metasploitable (192.168.50.101)

In questo esercizio andremo a fare una scansione completa sul target Metasploitable, dopo di che andremo ad analizzare varie vulnerabilità e le andremo a risolvere.

- **Prima scansione.**

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼		⚙
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0	Unix Opera...	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server...	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell ...	Backdoors	1	🕒	✎
<input type="checkbox"/>	CRITICAL	...	 2 SSL (...	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	MIXED	...	 2 SSL (...	Service detection	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General	1	🕒	✎

Come possiamo vedere dalla figura, nella prima scansione si possono vedere varie vulnerabilità, quelle che noi andremo a risolvere sono la “VNC Server 'password' Password” e “Blind Shell Back door detection”.

- **“VNC Server 'password' ”**

Questa vulnerabilità ci avvisa che la nostra macchina target ha una password molto debole, quindi per sistemare questo problema andremo a cambiare la password cercando di aumentarne il livello di sicurezza.

61708 - VNC Server 'password' Password	
Synopsis	A VNC server running on the remote host is secured with a weak password.
Description	The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
Solution	Secure the VNC service with a strong password.
Risk Factor	Critical
CVSS v2.0 Base Score	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
Plugin Information	Published: 2012/08/29, Modified: 2015/09/24
Plugin Output	tcp/5900/vnc

- **Comandi effettuati**

```
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# ls
metasploitable:1.log  metasploitable:1.pid  passwd  xstartup
root@metasploitable:/home/msfadmin/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin/.vnc#
```

Per andare a risolvere questa vulnerabilità non ci resta quindi che andare sulla nostra macchina target e andremo con questi comandi a creare una nuova password, così da evitare l'accesso senza le credenziali.

Sev ▼	Score ▼	Name ▲	Family ▲
<input type="checkbox"/> CRITICAL	10.0 *	Debian Op...	Gain a shell remotely
<input type="checkbox"/> CRITICAL	10.0 *	NFS Export...	RPC
<input type="checkbox"/> CRITICAL	10.0	Unix Opera...	General
<input type="checkbox"/> CRITICAL	9.8	Bind Shell ...	Backdoors

Possiamo infatti vedere nella figura sopra che dopo un'ulteriore scansione la vulnerabilità VNC sia stata neutralizzata.

- **“bind shell”**

Ora invece passiamo alla vulnerabilità del Bind Shell.

```
File Actions Edit View Help
(kali@kali)-[~]
$ netcat 192.168.50.101 1524
^C
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.101 -p 1524
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 10:49 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00031s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:06:9A:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

(root@kali)-[/home/kali]
#
```

```
root@metasploitable:/home/msfadmin# ufw

Usage: ufw COMMAND

Commands:
  enable                Enables the firewall
  disable               Disables the firewall
  default ARG           set default policy to ALLOW or DENY
  logging ARG           set logging to ON or OFF
  allow|deny RULE       allow or deny RULE
  delete allow|deny RULE delete the allow/deny RULE
  status                show firewall status
  version               display version information

root@metasploitable:/home/msfadmin# ufw disable
Firewall stopped and disabled on system startup
root@metasploitable:/home/msfadmin# ufw enable 1524
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
root@metasploitable:/home/msfadmin# _
```

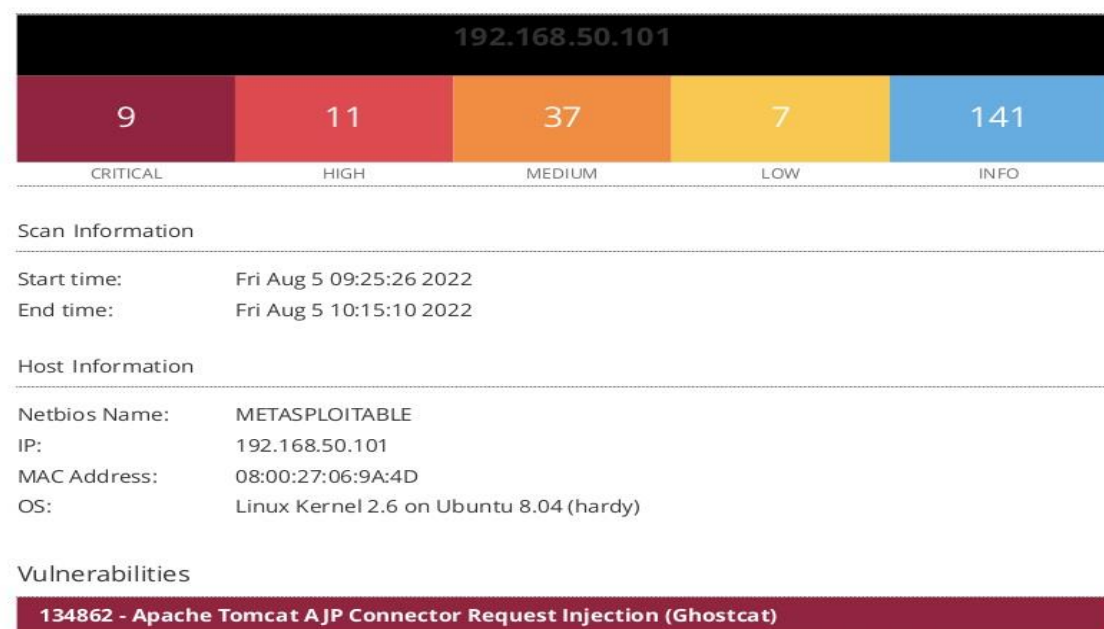
Qui sopra possiamo vedere abbiamo attivato il firewall della porta interessata (1524) sul nostro terminale.

- **ULTIMA SCANSIONE**

Effettuando nuovamente la scansione, si può notare come avendo effettuato le modifiche le vulnerabilità non sono più presenti.

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼		⚙
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0	Unix Opera...	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	...	2 SSL (...)	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	MIXED	...	2 SSL (...)	Service detection	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General	1	🕒	✎
<input type="checkbox"/>	MIXED	...	15 SSL (...)	General	27	🕒	✎
<input type="checkbox"/>	MIXED	...	5 ISC BI...	DNS	5	🕒	✎

• REPORT



Qui sopra il report finale che ci indica le vulnerabilità rimaste.

