

PROGETTO SETTIMANALE

Vulnerability Assessment

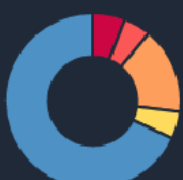
Vulnerability scanner: Nessus
Target: Metasploitable - 192.168.50.101

Spett.le Azienda,
a seguito vostra richiesta d'intervento sulla verifica di eventuali vulnerabilità sulla vostra rete, abbiamo riscontrato diverse criticità. Qui di seguito un report della scansione effettuata sull'ip in intestazione.

- 1) Il primo passo è stato di effettuare una scansione sulle tutte le porte della rete target. Così facendo, applicando un **“basic network Scan”** abbiamo effettivamente riscontrato diverse vulnerabilità. D'importante evidenza sono quelle “critiche” rappresentati nel grafico sotto riportato.

<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	...	SSL (...)	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	MIXED	...	SSL (...)	Service detection	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General	1	🕒	✎

- 2) Abbiamo dunque attuato delle contromisure per la vulnerabilità **VNC Server**, andando a creare una nuova password in modo tale da non permettere l'accesso senza credenziali. Qui di seguito il risultato ottenuto (come si può evincere non risulta più la vulnerabilità relativa al VNC)

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼	Modify	Scan Details	
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	🕒 ✎	Policy:	Basic Network Scan
<input type="checkbox"/>	CRITICAL	10.0	Unix Opera...	General	1	🕒 ✎	Status:	Completed
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell ...	Backdoors	1	🕒 ✎	Severity Base:	CVSS v3.0 ✎
<input type="checkbox"/>	CRITICAL	...	SSL (...)	Gain a shell remotely	3	🕒 ✎	Scanner:	Local Scanner
<input type="checkbox"/>	MIXED	...	SSL (...)	Service detection	3	🕒 ✎	Start:	Today at 4:33 PM
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC	1	🕒 ✎	End:	Today at 5:00 PM
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General	1	🕒 ✎	Elapsed:	27 minutes
<input type="checkbox"/>	MIXED	...	SSL (...)	General	27	🕒 ✎	Vulnerabilities	
								
							<ul style="list-style-type: none">● Critical● High● Medium● Low● Info	

Questi i comandi effettuati per poter cambiare la password:

```
Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log

msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin/.vnc# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# lx
bash: lx: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpassword
bash: vncpassword: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpass
bash: vncpass: command not found
root@metasploitable:/home/msfadmin/.vnc# ls
metasploitable:1.log metasploitable:1.pid passwd xstartup
root@metasploitable:/home/msfadmin/.vnc# psswd
bash: psswd: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpsswd
bash: vncpsswd: command not found
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#
```

- 3) Risolta la prima problematica, ci siamo concentrati sulla vulnerabilità relativa alla **Bind Shell**. In questo caso, abbiamo provveduto ad attivare il **Firewall** relativo alla porta interessata (p:1524). Di seguito i passaggi effettuati sul terminale di Metasploit.

```
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# _
```

```

(massi87@kali)-[~]
$ netcat 192.168.50.101 1524
^C

(massi87@kali)-[~]
$ sudo su
[sudo] password di massi87:
(root@kali)-[/home/massi87]
# nmap -sS 192.168.50.101 -p 1524
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 17:18 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00064s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock
MAC Address: AA:89:7B:0A:6F:25 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

(root@kali)-[/home/massi87]
# _

```

4) Effettuate le modifiche, abbiamo dunque eseguito una nuova scansione, ottenendo quindi il risultato cercato. Come si evince dalla figura sottostante, la vulnerabilità relativa alla backdoor non risulta più essere presente.

Hosts 1
Vulnerabilities 59
Remediations 2
Notes 2
VPR Top Threats
History 9

Filter
Search Vulnerabilities
59 Vulnerabilities


<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	...	SSL (...)	Gain a shell remotely	3	
<input type="checkbox"/>	MIXED	...	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	...	SSL (...)	General	27	
<input type="checkbox"/>	MIXED	...	ISC Bi...	DNS	5	

Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:26 PM
End: Today at 5:53 PM
Elapsed: 28 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

5) Qui di seguito il report finale con le vulnerabilità rimaste attive. Le presenti verranno risolte in seguito, dopo un’attenta valutazione della gestione del rischio residuo.



Report generated by Nessus™

Basic scan progetto settimanale

Fri, 05 Aug 2022 17:53:55 CEST

TABLE OF CONTENTS

[Vulnerabilities by Host](#)

- [192.168.50.101](#)

Vulnerabilities by Host

Collapse All | Expand All

192.168.50.101

7	6	23	5	128
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Fri Aug 5 17:26:16 2022
End time:	Fri Aug 5 17:53:55 2022

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	AA:89:7B:0A:6F:25
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	+
32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	+
32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	+
11356 - NFS Exported Share Information Disclosure	+
20007 - SSL Version 2 and 3 Protocol Detection	+
20007 - SSL Version 2 and 3 Protocol Detection	+
33850 - Unix Operating System Unsupported Version Detection	+