

consegna S5 L5

vulnerability assessment

primo report

VS

report finale

Hosts1

Vulnerabilities19

Remediations2

Notes2

History9

Filter

Search Vulnerabilities

59 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
<div><div></div><div>CRITICAL</div></div>	10.0 *		NFS Exported Share Information Disclosure	RPC	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	10.0		Unix Operating System Unsupported Version Detection	General	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	9.8		Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	9.8		Bind Shell Backdoor Detection	Backdoors	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	<div><div></div>SSL (Multiple Issues)</div>	Gain a shell remotely	3	<div><div></div><div></div><div></div></div>
<div><div></div><div>MEDIUM</div></div>	<div><div></div>SSL (Multiple Issues)</div>	Service detection	3	<div><div></div><div></div><div></div></div>
<div><div></div><div>HIGH</div></div>	7.5		NFS Shares World Readable	RPC	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>HIGH</div></div>	7.5		Samba Badlock Vulnerability	General	1	<div><div></div><div></div><div></div></div>
<div><div></div><div>MEDIUM</div></div>	<div><div></div>SSL (Multiple Issues)</div>	General	28	<div><div></div><div></div><div></div></div>
<div><div></div><div>MEDIUM</div></div>	<div><div></div>ISC Bind (Multiple Issues)</div>	DNS	5	<div><div></div><div></div><div></div></div>
<div><div></div><div>MEDIUM</div></div>	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	<div><div></div><div></div><div></div></div>

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 10:47 AM

End:

Today at 11:16 AM

Elapsed:

29 minutes

Vulnerabilities

CRITICAL

HIGH

MEDIUM

LOW

INFO



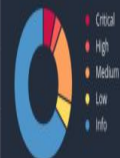
Hosts 1 Vulnerabilities 49 Notes 7 History 9						
Filter	Search Vulnerabilities		49 Vulnerabilities			
Sev	CVSS	VPR	Name	Family	Count	Scan Details
CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1	Policy: Basic Network Scan Status: Running Severity Base: CVSS v3.0 Scanner: Local Scanner Start: Today at 4:07 PM
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
MILD	SSL (Multiple Issues)	Service detection	3	
HIGH	7.5		NFS Shares World Readable	RPC	1	
HIGH	7.5		Samba Badlock Vulnerability	General	1	
MILD	SSL (Multiple Issues)	General	25	
MILD	ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	5.9		SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eEncryption)	Misc.	1	
MILD	SSH (Multiple Issues)	Misc.	6	

Vulnerabilities

Legend:

- Critical
- High
- Medium
- Low
- Info

Vulnerabilities



per arrivare a quel risultato abbiamo risolto alcune vulnerabilità critiche

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :

```
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
```

```
..... snip .....
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.101

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

questa vulnerabilità permetteva di inserire una backdoor sulla porta 1524, per risolverlo e' bastato implementare una regola firewall per chiudere la porta in questione usando ufw che ci permette di accedere al firewall di metasploitable

infine eseguiamo un cambio password in quanto un'altra vulnerabilita' critica

CRITICAL VNC Server 'password' 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.

Output
Nessus logged in using a password of "password".
To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# 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# _
```

per fare ciò' abbiamo usato il comando "vncpasswd" per impostare una password diversa del virtual network computing da quella precedente in quanto molto comune e poco sicura e avrebbe permesso il controllo da remoto della macchina