

# Progetto

Eseguiamo tramite il tool “Nessus” una scansione sulla macchina macchina metasploitable (192.168.178.63)

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area displays a table of vulnerabilities. The table has columns for Severity, CVSS, VPR, Name, Family, and Count. The vulnerabilities listed include NFS Exported Share Information Disclosure, Unix Operating System Unsupported Version Detection, UnrealIRCd Backdoor Detection, VNC Server 'password' Password, SSL Version 2 and 3 Protocol Detection, Apache Tomcat AJP Connector Request Injection (Ghostcat), Bind Shell Backdoor Detection, DNS (Multiple Issues), SSL (Multiple Issues), NFS Shares World Readable, rlogin Service Detection, rsh Service Detection, Samba Badlock Vulnerability, and SSL (Multiple Issues). On the right, there's a 'Host Details' section showing IP, MAC, OS, Start, End, Elapsed, and KB. Below that is a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	DNS (Multiple Issues)	DNS	5
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28

come possiamo notare, abbiamo molte vulnerabilita' critiche. Quindi procediamo per risolverne qualcuna.

The screenshot shows the Nessus interface for a specific vulnerability. The top bar indicates 'gerardo / Plugin #61708' and 'Back to Vulnerabilities'. The main section is titled 'Vulnerabilities 71'. The selected vulnerability is 'VNC Server 'password' Password', which is marked as 'CRITICAL'. The 'Description' section states: '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.' The 'Solution' section suggests: 'Secure the VNC service with a strong password.' The 'Output' section shows a log entry: 'Nessus logged in using a password of "password".' Below the output, there's a table with columns 'Port' and 'Hosts'. The table shows a single entry: '5900 / tcp / vnc' on host '192.168.178.63'.

Port	Hosts
5900 / tcp / vnc	192.168.178.63

(VNC "password"Password ) questa è una vulnerabilità, la quale indica che la password impostata sul server VNV è molto debole e può essere scoperta facilmente.

Come seconda vulnerabilità troviamo la seguente:

gerardo / Plugin #51988

Configure Audit Tr

Back to Vulnerabilities

Vulnerabilities 71

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	192.168.178.63

Questa invece ci indica che sulla porta 1524 si trova una backdoor che può essere sfruttata per connettersi al server ed eseguire comandi da remoto.

## SOLUZIONE

Sono andato ad impostare le rules nel firewall della macchina metasploitable (iptables), limitando il traffico sulle porte 1524 e 5900.

**sudo iptables -A INPUT -p tcp --dport 1524 -j DROP**

**sudo iptables -A INPUT -p tcp --dport 5900 -j DROP**

questo comando spiegato brevemente, aggiunge una regola per il protocollo tcp sulla porta 1524 istruendo il firewall a scartare tutti i pacchetti che arrivano su quella porta

```

Try 'iptables -h' or 'iptables --help' for more information.
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:5900
DROP       tcp  --  anywhere              anywhere             tcp dpt:ingreslock
DROP       tcp  --  anywhere              anywhere             tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin#

```

## Scansione finale

gerardo

← Back to All Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 68 Remediations 3 Notes 3 History 1

Filter Search Vulnerabilities 68 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
MIXED	...	...	DNS (Multiple Issues)	DNS	5	
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5		NFS Shares World Readable	RPC	1	
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	
MIXED	...	...	SSL (Multiple Issues)	General	28	

**Scan Details**

Policy: Basic Network Scan  
 Status: Completed  
 Severity Base: CVSS v3.0  
 Scanner: Local Scanner  
 Start: Today at 3:44 PM  
 End: Today at 4:03 PM  
 Elapsed: 19 minutes

**Vulnerabilities**

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

come possiamo notare le due vulnerabilità non vengono riscontrate dal programma