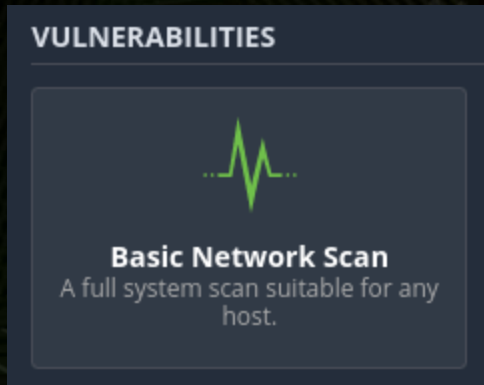


# Compito S5-L5

Scansione completa sul target Metasploitable  
tramite Nessus



Avviata la macchina Kali Linux con Nessus, scegliamo l'opzione "basic network scan" per avviare la scansione.



Ci chiederá adesso tutte le informazioni necessarie per eseguire la scansione. Inseriamo quindi i seguenti paramentri:

192.168.49.101 é l'indirizzo IP della macchina Metasploitable.

A screenshot of the Nessus 'New Scan / Basic Network Scan' configuration window. The 'Settings' tab is active, showing fields for Name, Description, Folder, and Targets. The 'Targets' field contains the IP address 192.168.49.101. The 'Name' field contains 'Metasploitable' and the 'Description' field contains 'Compito S5-L5'. The 'Folder' dropdown is set to 'My Scans'. At the bottom, there are 'Save' and 'Cancel' buttons.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Metasploitable

Description: Compito S5-L5

Folder: My Scans

Targets: 192.168.49.101

Upload Targets [Add File](#)

Save Cancel

Settings Credentials Plugins

BASIC >  
DISCOVERY   
ASSESSMENT >  
REPORT >  
ADVANCED >

Scan Type Port scan (common ports) ▼

**General Settings:**  
Always test the local Nessus host  
Use fast network discovery

**Port Scanner Settings:**  
Scan common ports  
Use netstat if credentials are provided  
Use SYN scanner if necessary

**Ping hosts using:**  
TCP  
ARP  
ICMP (2 retries)

Save ▼ Cancel

Su "discovery" impostiamo l'opzione "port scan (commons port)" in modo da scansionare le sole porte più frequentemente utilizzate.

Andiamo poi ad impostare il tipo di scansione che, in questo caso, sarà quella completa.

New Scan / Basic Network Scan  
[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC >  
DISCOVERY >  
ASSESSMENT   
REPORT >  
ADVANCED >

Scan Type Scan for all web vulnerabilities (complex) ▼

**General Settings:**  
Avoid potential false alarms  
Enable CGI scanning  
Perform thorough tests

**Web Applications:**  
Start crawling from "/"  
Crawl 1000 pages (max)  
Traverse 6 directories (max)  
Test for known vulnerabilities in commonly used web applications  
Perform each generic web app test for 10 minutes (max)  
Try all HTTP methods  
Attempt HTTP Parameter Pollution

Save ▼ Cancel



Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Processing

Output

☐ Override normal verbosity

☒ I have limited disk space. Report as little information as possible

☐ Report as much information as possible

☒ Show missing patches that have been superseded

When enabled, includes superseded patch information in the scan report.

☒ Hide results from plugins initiated as a dependency

When enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.

☒ Allow users to edit scan results

When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.

☐ Designate hosts by their DNS name

Uses the host name rather than IP address for report output.

☐ Display hosts that respond to ping

Reports hosts that successfully respond to a ping.

☐ Display unreachable hosts

When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.

☐ Display Unicode characters

When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Save

Cancel

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Default

Performance options:

30 simultaneous hosts (max)

4 simultaneous checks per host (max)

5 second network read timeout

Save

Cancel























































Lasciamo invece di default le impostazioni sia sulla sezione "report" che su "advcaned". Clicchiamo su "salva" e avviamo la scansione. Potrebbe volerci diverso tempo a seconda della potenza della macchina che abbiamo.


































































Una volta finita la scansione possiamo notare sul pannello di destra diverse informazioni tra cui il tempo della scansione, la policy, il tipo di scanner e la data. In basso invece tutte le varie criticità con i diversi livelli di importanza:

- info: possibili problematiche future;
- mixed: possono essere sia info che low/medium/high/critical;
- low/medium/high/critical: criticità da risolvere.



Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
 <b>critical</b>	10.0 *		NFS Exported Share Information Disclosure	RPC	1		
 <b>critical</b>	10.0		Unix Operating System Unsupported Version Detection	General	1		
 <b>critical</b>	10.0 *		UnrealIRCd Backdoor Detection	Backdoors	1		
 <b>critical</b>	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
 <b>critical</b>	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
 <b>critical</b>	9.8		Bind Shell Backdoor Detection	Backdoors	1		
 <b>mixed</b>	...	...	Phpmysql (Multiple Issues)	CGI abuses	4		
 <b>critical</b>	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
 <b>mixed</b>	...	...	Apache Tomcat (Multiple Issues)	Web Servers	3		
 <b>mixed</b>	...	...	PHP (Multiple Issues)	CGI abuses	3		
 <b>high</b>	7.5		NFS Shares World Readable	RPC	1		
 <b>high</b>	7.5 *		rlogin Service Detection	Service detection	1		
 <b>high</b>	7.5 *		rsh Service Detection	Service detection	1		
 <b>high</b>	7.5		Samba Badlock Vulnerability	General	1		
 <b>mixed</b>	...	...	SSL (Multiple Issues)	General	28		
 <b>mixed</b>	...	...	ISC Bind (Multiple Issues)	DNS	5		
 <b>mixed</b>	...	...	Twiki (Multiple Issues)	CGI abuses	2		
 <b>medium</b>	6.5		TLS Version 1.0 Protocol Detection	Service detection	2		

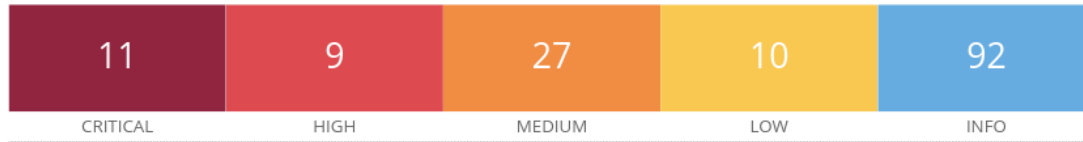
 <b>medium</b>	6.5		Unencrypted Telnet Server	Misc.	1		
 <b>medium</b>	5.9		SSL Anonymous Cipher Suites Supported	Service detection	1		
 <b>medium</b>	5.9		SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption)	Misc.	1		
 <b>medium</b>	5.3		Browsable Web Directories	CGI abuses	1		
 <b>medium</b>	5.3		HTTP TRACE / TRACK Methods Allowed	Web Servers	1		
 <b>medium</b>	5.3		Tomcat Sample App cal2.jsp 'time' Parameter XSS	CGI abuses : XSS	1		
 <b>medium</b>	5.0 *		Backup Files Disclosure	CGI abuses	1		
 <b>medium</b>	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	2		
 <b>mixed</b>	...	...	SSH (Multiple Issues)	Misc.	6		
 <b>mixed</b>	...	...	PHP (Multiple Issues)	Web Servers	3		
 <b>medium</b>	...	...	Phpmysql (Multiple Issues)	CGI abuses : XSS	2		
 <b>mixed</b>	...	...	SMB (Multiple Issues)	Misc.	2		
 <b>mixed</b>	...	...	TLS (Multiple Issues)	Misc.	2		
 <b>mixed</b>	...	...	TLS (Multiple Issues)	SMTP problems	2		
 <b>low</b>	3.7		SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1		
 <b>low</b>	2.6 *		X Server Detection	Service detection	1		
 <b>mixed</b>	...	...	Web Server (Multiple Issues)	Web Servers	11		
 <b>info</b>	...	...	SMB (Multiple Issues)	Windows	7		
 <b>info</b>	...	...	HTTP (Multiple Issues)	Web Servers	6		
 <b>info</b>	...	...	HTTP (Multiple Issues)	CGI abuses	4		
 <b>info</b>	...	...	TLS (Multiple Issues)	General	4		

Ecco alcune delle criticità di Metasploitable con i vari livelli di importanza.

Andremo adesso a scegliere delle vulnerabilità di livello "critical" e ne troveremo le soluzioni.

Queste, sono già consigliate da Nessus per ogni vulnerabilità, spesso seguite anche da link esterni.

192.168.49.101



#### Vulnerabilities

Total: 149

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	-	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	-	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS

Scarichiamo infine il report in PDF con in dettaglio tutti i dati della scansione, i vari livelli di vulnerabilità e le informazioni relative ad essa.



# NFS Exported Share Information Disclosure

La maggior parte delle implementazioni NFS ha modelli specifici nei filehandle che possono essere indovinati. La maggior parte delle implementazioni NFS si basa sulla segretezza dei filehandle per la sicurezza effettiva dei file. Un utente malintenzionato può indovinare i filehandle per bypassare la sicurezza e ottenere l'accesso non autorizzato alle risorse NFS.

Soluzione: applicare la patch jumbo NFS (patch-ID# 100173). Disponibile sul sito Web Sun Microsystems.

Dopo aver installato la patch, eseguire "fsirand" sull'intero file system. Questo renderà difficile per un utente remoto indovinare i filehandle NFS, impedendo all'utente di condurre montaggi non autorizzati e accedere ai file system NFS

CRITICAL

## NFS Exported Share Information Disclosure

### Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

### Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

### Output

The following NFS shares could be mounted :

```
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz
less...
```

To see debug logs, please visit individual host

Port ▼

Hosts

2049 / udp / rpc-nfs

192.168.49.101



# VNC Server 'password' Password

Questo report ci avvisa che il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito infatti ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

La soluzione che ci consiglia é quindi di cambiare password inserendone una piú complessa, preferibilmente composta da numeri, maiuscole e minuscole, punteggiatura e caratteri speciali.

Per aggiornare o modificare la password VNC bisognerà utilizzare il comando `vncpasswd`. `vncpasswd` ti chiederà due volte di inserire la nuova password:

```
$ vncpasswd
Parola d'ordine:
Verificare:
```

Il `vncpasswd` accetta anche l'immissione di una password da STDIN che consente anche di archiviare il file della password in una posizione diversa. L'esempio seguente modificherà la password VNC `MYVNCPASSWORD` e la memorizzerà in `~/.secret/vncpassdato` che la `.secret`:

```
$ echo MYVNCPASSWORD | vncpasswd -f > ~/.secret/passvnc
```

## 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	192.168.49.101

# Bind Shell Backdoor Detection

## 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
--------	-------

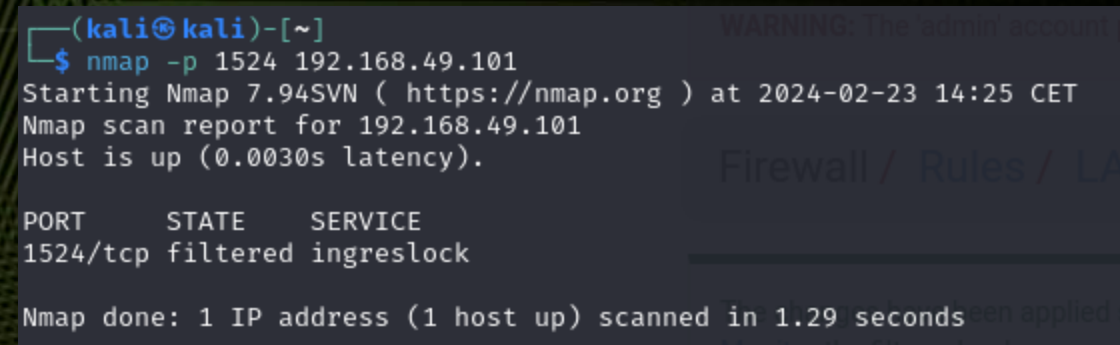
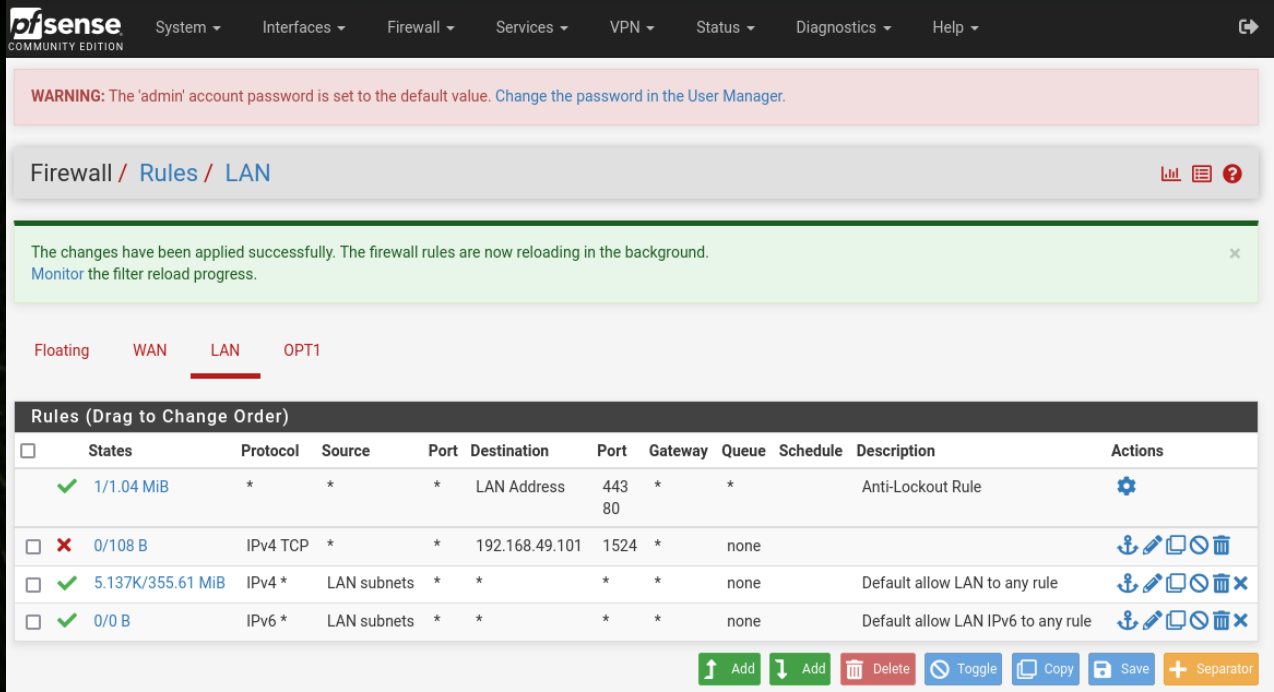
1524 / tcp / wild_shell	192.168.49.101
-------------------------	----------------

Una shell é in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Una possibile soluzione sarebbe quella di controllare se l'host remoto é stato compromesso ed eventualmente reinstallare il sistema.



# Bind Shell Backdoor Detection



La soluzione applicata é stata quella di impostare una regola sul firewall in modo da andare a bloccare il traffico sulla porta 1524 andandola a impostare su uno stato "filtered".

Stato filtered: Nmap non può determinare con esattezza se la porta sia aperta o meno, perché un filtro di pacchetti impedisce ai pacchetti di raggiungere la porta.

Eseguendo nuovamente la scansione su Nessus possiamo notare come sia scomparsa la vulnerabilità

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 *		VNC Server 'password' Password	Gain a shell remotely	1	🔍 🛠️
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔍 🛠️
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	🔍 🛠️
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	🔍 🛠️