

M/C

# Progetto S5L5

S5L5 Nessus

01

# 02

Nel progetto odierno andiamo ad utilizzare  
nessus un potente  
vulnerability scanner. Questo tool  
professionale e preciso è tra i migliori in  
circolazione e ci permette di rilevare le  
vulnerabilità dei vari componenti di una  
rete.

Nelle prossime slide andremo a visualizzare  
un report  
sulla nostra macchina meta e a risolvere  
alcune  
vulnerabilità critiche

Andando ad effettuare il primo basic network scan questi sono i risultati ottenuti, nelle prossime slide andremo a vedere nello specifico alcune delle criticità trovate e le andremo a risolvere

Scan S5L5

ConfigureAudit Trail

Back to My Scans

Hosts 1Vulnerabilities 27History 2

FilterSearch Vulnerabilities27 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	3	
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	...	...	2 SMB (Multiple Issues)	Misc.	2	
<input type="checkbox"/>	INFO	...	...	3 VNC (Multiple Issues)	Service detection	9	
<input type="checkbox"/>	INFO	...	...	6 SMB (Multiple Issues)	Windows	7	
<input type="checkbox"/>	INFO	...	...	2 RPC (Multiple Issues)	RPC	2	
<input type="checkbox"/>	INFO			Nessus SYN scanner	Port scanners	28	
<input type="checkbox"/>	INFO			Service Detection	Service detection	12	

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	192.168.1.14

# Bind Shell Backdoor

Una "bind backdoor" è un tipo specifico di backdoor che consente a un attaccante remoto di stabilire una connessione di rete a una macchina compromessa. Questo tipo di backdoor può essere utilizzato per aprire una "shell" di comando remota, consentendo all'attaccante di eseguire comandi sul sistema remoto senza autenticazione.

# Risoluzione bind shell backdoor

```
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw default ALLOW
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$
```

Come si evince dalla slide precedente, Nessus ci segnala che sulla porta 1524 c'è una bind shell backdoor andiamo quindi a lavorare sulla porta in questione. Ho risolto questa vulnerabilità abilitando il Firewall di meta e andando a negare l'accesso alla porta in questione, che adesso è protetta dal firewall. Potenzialmente questo discorso va esteso a tutte le porte aperte e inutilizzate, le quali vanno chiuse o gestite con determinate politiche di sicurezza

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

more...

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.1.14

**NFS Exported Share Information Disclosure**

Si riferisce a una vulnerabilità nella configurazione di un server NFS (Network File System) che potrebbe consentire a utenti non autorizzati di ottenere informazioni sensibili sulle condivisioni NFS esistenti. Questa vulnerabilità può rivelare dettagli sulla configurazione del server NFS, inclusi i percorsi di condivisione, le autorizzazioni e le risorse disponibili.

# Risoluzione NFS Exported Share Information Disclosure

```
GNU nano 2.0.7      File: exports      Modified
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      kali(rw,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

Questo è come si presentava il file di configurazione in `/etc/exports` che come possiamo vedere nella foto affianco, nel ultimo rigo consente azioni a chiunque in quanto presente quel asterisco. Come risoluzione ho pensato di commentare questa riga eliminando così il libero accesso.

Sarebbe stato comunque possibile rimuovere

l'asterisco e andare a indicare l'hostname degli host autorizzati, in modo da implementare una nuova regola di sicurezza

Qui sotto possiamo vedere la modifica apportata:

```
#_ *(rw,sync,no_root_squash,no_subtree_check)
```

Hosts1

Vulnerabilities27

History2

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	192.168.1.14
5901 / tcp / vnc	192.168.1.14
5902 / tcp / vnc	192.168.1.14

# VNC Server ‘password’ Password

Questa vulnerabilità fa riferimento alla password per accedere al server in questione, ci segnala che abbiamo impostato una password debole, per l’appunto “password”. Nessus è riuscito a rilevare la password simulando un attacco brute force, questa una delle tantissime funzionalità del nostro tool.



## Risoluzione VNC server password 'password'

```
msfadmin@metasploitable:/etc$ sudo vncpassword
sudo: vncpassword: command not found
msfadmin@metasploitable:/etc$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:/etc$
```

**Con i comandi sopraindicati siamo andati a impostare una nuova password più sicura per il nostro server VNC, risolvendo così la bassa sicurezza relativa alla password precedentemente usata. Siamo andati a impostare una password così composta : 3 lettere maiuscole, 3 lettere minuscole, 1 numero e 2 caratteri speciali.**

# Scansione post risoluzione delle vulnerabilità

Vulnerabilities49

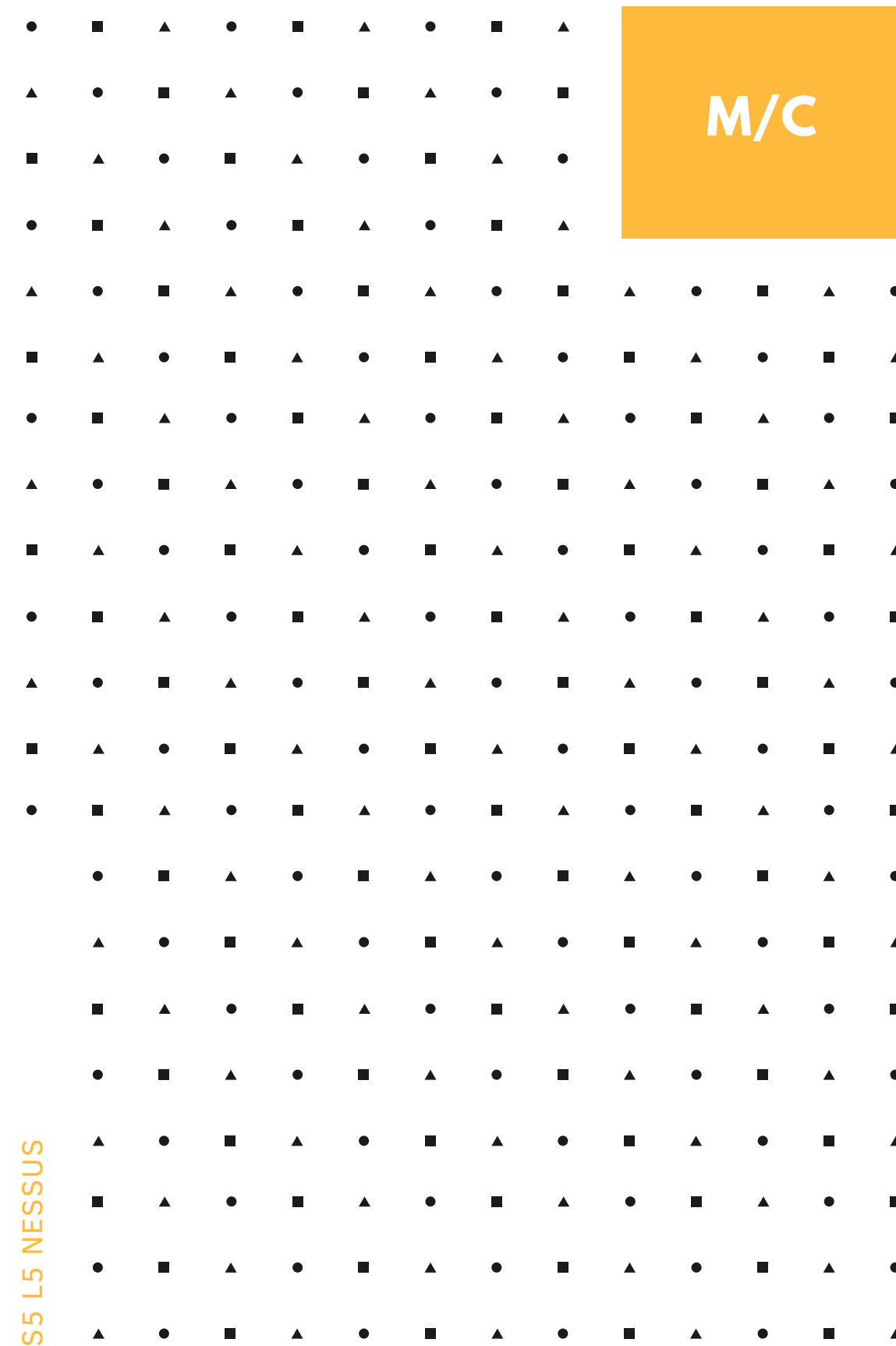
Filter

Search Vulnerabilities

49 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁5 ISC Bind (Multiple Issues)	DNS	5	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁6 SSH (Multiple Issues)	Misc.	6	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁3 HTTP (Multiple Issues)	Web Servers	3	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁2 SMB (Multiple Issues)	Misc.	2	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁2 TLS (Multiple Issues)	SMTP problems	2	🕒	✎
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection	2	🕒	✎
<input type="checkbox"/>	INFO	...	...	📁6 SMB (Multiple Issues)	Windows	7	🕒	✎
<input type="checkbox"/>	INFO	...	...	📁3 VNC (Multiple Issues)	Service detection	6	🕒	✎

Come possiamo vedere dopo il nostro intervento le 3 vulnerabilità non sono più presenti tra quelle critiche



Grazie !

Massimo Cinquegrana