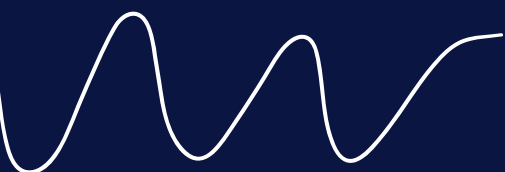


ACTIVITY



PROGETTO S5L5



ha lo scopo di identificare ed assegnare un rischio alle vulnerabilità / configurazioni errate trovate nelle fasi precedenti, e preparare alla fase di exploit.

ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

Mettere in comunicazione le due macchine (Kali Linux e Metasploitable) mettendoli sulla stessa rete.
Accesso Nessus

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche / high** e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Prime 4 vulnerabilità scansionate:

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		Settings	Scan Details
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🔄	✎	Policy: Basic Network Scan Status: Completed Severity Base: CVSS v3.0 ✎ Scanner: Local Scanner Start: Today at 4:16 AM End: Today at 4:38 AM Elapsed: 23 minutes
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄	✎	
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🔄	✎	
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🔄	✎	

PRIMA VULNERABILITÀ

1) NFS Exported Share Information Disclosure:

è una vulnerabilità in cui le informazioni condivise tramite NFS sono diffuse in modo non autorizzato. Questo può accadere se la configurazione del sistema NFS non è adeguatamente protetta.

Soluzioni:

- Impostare i permessi di condivisione in modo che solo gli utenti autorizzati possano accedere ai dati condivisi.
- Limitare l'accesso NFS solo agli host o alle reti autorizzate.
- Mantenere tutti i software di sistema e le implementazioni NFS aggiornate.
- Monitorare e registrare l'accesso NFS per individuare attività sospette o non autorizzate.

Procedura:

- Si apre il terminale;
- Si crea una directory che ti permette di esportare solo i file presenti nella directory. Comando 'mkdir ~/nome directory';
- Si modifica il file exports con il comando 'sudo nano /etc/exports';

VALUTAZIONE DELLA VULNERABILITÀ

```
GNU nano 2.0.7 File: /etc/exports
# /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 hostname1(rw,sync) hostname2(ro,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)
```



```
GNU nano 2.0.7 File: /etc/exports
# /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 hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
# /home/msfadmin/nfs_share metasploitable(rw,sync,no_root_squash,subtree_c$
```

- /home/tuo_utente/nome directory: Il percorso della directory che vuoi condividere.
- *: Indica che qualsiasi host ha accesso (assicurati che il tuo sistema sia configurato per accettare connessioni NFS).
- rw: Consente la scrittura (puoi personalizzare questa opzione).
- sync: Le modifiche vengono sincronizzate subito.
- no_root_squash: Consente all'utente root del client di essere l'utente root sul server NFS.
- no_subtree_check: Migliora le prestazioni, ma riduce la sicurezza. Puoi considerare di rimuoverlo in un ambiente di produzione.

- Con il comando 'sudo exportfs -a' si aggiornano le configurazioni del NFS;
- Si avvia il servizio con il comando 'sudo /etc/init.d/nfs-kernel-server start';

```
msfadmin@metasploitable:~$ sudo exportfs -a
msfadmin@metasploitable:~$ sudo service nfs-kernel-server start
sudo: service: command not found
msfadmin@metasploitable:~$ sudo rpcbind start
sudo: rpcbind: command not found
msfadmin@metasploitable:~$ sudo service nfs-kernel-server status
sudo: service: command not found
msfadmin@metasploitable:~$ sudo systemctl nfs-kernel-server status
sudo: systemctl: command not found
msfadmin@metasploitable:~$ sudo systemctl start nfs-kernel-server
sudo: systemctl: command not found
msfadmin@metasploitable:~$ sudo systemctl start nfs-kernel-server
sudo: systemctl: command not found
msfadmin@metasploitable:~$ sudo systemctl start nfs-kernel-server
sudo: systemctl: command not found
msfadmin@metasploitable:~$ sudo systemctl start nfs-kernel-server
sudo: systemctl: command not found
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server status
nfsd running
```

- Infine si avvia la scansione di Nessus per vedere se la vulnerabilità è diminuita.

VALUTAZIONE DELLA VULNERABILITÀ

SECONDA VULNERABILITÀ

2) VNC Server 'password' Password:

VNC (Virtual Network Computing) è un sistema di controllo remoto che consente agli utenti di accedere e controllare un computer da un'altra posizione tramite una connessione di rete.

Soluzioni:

- Password forte: Questa password dovrebbe essere complessa e difficile da indovinare contenente almeno 8 caratteri tra lettere maiuscole e minuscole, alfanumerici e speciali.
- Crittografia: È consigliabile utilizzare una connessione VNC cifrata per proteggere i dati scambiati tra il client e il server.
- Autenticazione a due fattori: Se possibile, utilizzare l'autenticazione a due fattori per il server VNC. Questo aggiunge un ulteriore livello di sicurezza richiedendo un secondo metodo di autenticazione oltre alla password.
- Firewall e filtraggio degli indirizzi IP: Limitare l'accesso al server VNC utilizzando un firewall o il filtraggio degli indirizzi IP.
- Aggiornamenti: Assicurarsi che il software VNC e il sistema operativo siano aggiornati

Procedura:

- Aprire il terminale;
- Cambio di privilegi da guest a root con il comando 'sudo su';
- Avviare il server di VNC con il comando 'vncserver';
- Cambio password con il comando 'vncpasswd';
- Infine si fa la scansione per vedere se la vulnerabilità è diminuita.

```
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
msfadmin 10776 0.0 0.0 3004 752 tty1 R+ 06:21 0:00 grep Xtightvnc
msfadmin@metasploitable:~$ cd /home/uncuser
-bash: cd: /home/uncuser: No such file or directory
msfadmin@metasploitable:~$ cd root/home/uncuser
-bash: cd: root/home/uncuser: No such file or directory
msfadmin@metasploitable:~$ cd /root/home/uncuser
-bash: cd: /root/home/uncuser: No such file or directory
msfadmin@metasploitable:~$ cd root
-bash: cd: root: No such file or directory
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:~$ cd /home/uncuser
bash: cd: /home/uncuser: No such file or directory
root@metasploitable:~$ cd /home/msfadmin
bash: cd: /uncuser: No such file or directory
root@metasploitable:~$ cd /home/msfadmin
root@metasploitable:~$ vncpasswd
Using passwd file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~$
```

VNC



<input type="checkbox"/>	VNC (Multiple Issues)	Service detection	3	0	✓
<input type="checkbox"/>	Apache HTTP Server (Multiple Issues)	Web Servers	2	0	✓
<input type="checkbox"/>	PHP (Multiple Issues)	Web Servers	2	0	✓
<input type="checkbox"/>	RPC (Multiple Issues)	RPC	2	0	✓
<input type="checkbox"/>	XSH (Multiple Issues)	General	2	0	✓
<input type="checkbox"/>	XSH (Multiple Issues)	Service detection	2	0	✓
<input type="checkbox"/>	Web Server (Multiple Issues)	Web Servers	2	0	✓
<input type="checkbox"/>	Nessus SYN scanner	Port scanners	25	0	✓
<input type="checkbox"/>	RPC Services Enumeration	Service detection	10	0	✓
<input type="checkbox"/>	Service Detection	Service detection	10	0	✓
<input type="checkbox"/>	OpenSSL Detection	Service detection	2	0	✓
<input type="checkbox"/>	RMI Registry Detection	Service detection	2	0	✓
<input type="checkbox"/>	API Connector Detection	Service detection	1	0	✓
<input type="checkbox"/>	Backported Security Patch Detection (FTP)	General	1	0	✓
<input type="checkbox"/>	Backported Security Patch Detection (WWW)	General	1	0	✓
<input type="checkbox"/>	Common Platform Enumeration (CPE)	General	1	0	✓
<input type="checkbox"/>	Device Type	General	1	0	✓
<input type="checkbox"/>	Ethernet Card Manufacturer Detection	Misc.	1	0	✓
<input type="checkbox"/>	Ethernet MAC Addresses	General	1	0	✓
<input type="checkbox"/>	ICMP Timestamp Request Remote Date Disclosure	General	1	0	✓
<input type="checkbox"/>	IRC Daemon Version Detection	Service detection	1	0	✓
<input type="checkbox"/>	Nessus Scan Information	Settings	1	0	✓
<input type="checkbox"/>	NFS Share Export List	RPC	1	0	✓

NFS



VALUTAZIONE DELLA VULNERABILITÀ

SCANSIONE

Tenable Nessus Essentials Scans Settings lyductin

Metasploitable 1 [Back to My Scans](#) [Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrscan

Tenable News

Authentication Bypass in D-Link D-View 8 [Read More](#)

Hosts 1 **Vulnerabilities** 67 **Remediations** 2 **History** 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.9	12 Critical, 7 High, 25 Medium, 7 Low, 133 Info

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:08 AM
End: Today at 7:30 AM
Elapsed: 22 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Tenable Nessus Essentials Scans Settings lyductin

Metasploitable 1 [Back to My Scans](#) [Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrscan

Tenable News

PaperCut NG Unauthenticated XMLRPC Functionality [Read More](#)

Hosts 1 **Vulnerabilities** 67 **Remediations** 2 **History** 1

Filter Search Vulnerabilities 67 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 *		VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
MIXED	DNS (Multiple Issues)	DNS	4	
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
MIXED	SSL (Multiple Issues)	Service detection	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	

Scan Details

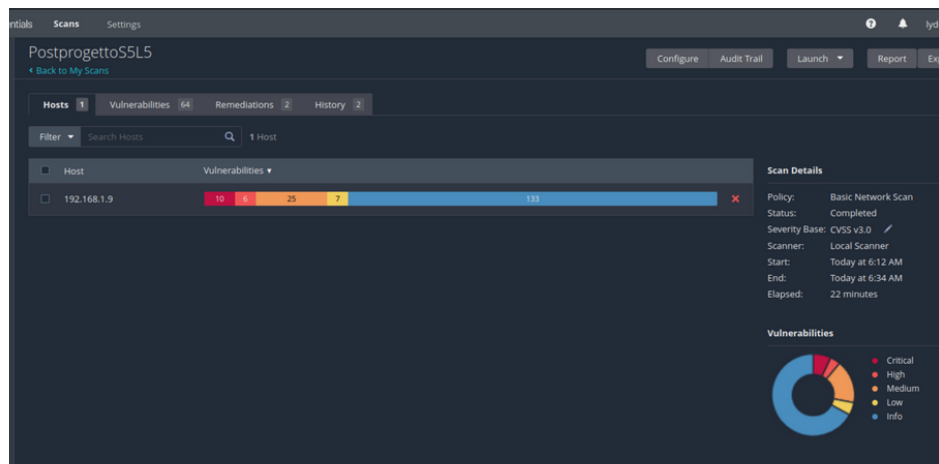
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:08 AM
End: Today at 7:30 AM
Elapsed: 22 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

VALUTAZIONE DELLA VULNERABILITÀ

SCANSIONE FINALE



Severity	Vulnerability	CVE	CVSS	Category	Count	Details
Critical	Linux Operating System Unsupported Version Detection	10.0	10.0	General	1	ⓘ ✓
Critical	Bind Shell Backdoor Detection	9.8	9.8	Backdoors	1	ⓘ ✓
High	DNS (Multiple Issues)	—	—	DNS	4	ⓘ ✓
High	Apache Tomcat (Multiple Issues)	—	—	Web Servers	4	ⓘ ✓
Critical	SSL (Multiple Issues)	—	—	Gain a shell remotely	3	ⓘ ✓
High	SSL (Multiple Issues)	—	—	Service detection	3	ⓘ ✓
High	nginx Service Detection	7.5 *	6.7	Service detection	1	ⓘ ✓
High	rsh Service Detection	7.5 *	6.7	Service detection	1	ⓘ ✓
High	Samba Smbd Vulnerability	7.5	6.7	General	1	ⓘ ✓
High	SSL (Multiple Issues)	—	—	General	28	ⓘ ✓
High	ISC Bind (Multiple Issues)	—	—	DNS	5	ⓘ ✓
High	TLS Version 1.0 Protocol Detection	6.5	6.5	Service detection	2	ⓘ ✓
High	Unencrypted Telnet Server	6.5	6.5	Misc.	1	ⓘ ✓
High	SSL DROWN Attack Vulnerability (Decrypting RSA with Disclosed and Weakened Encryptions)	5.9	4.4	Misc.	1	ⓘ ✓
High	SSH (Multiple Issues)	—	—	Misc.	6	ⓘ ✓
High	HTTP (Multiple Issues)	—	—	Web Servers	5	ⓘ ✓
High	SMB (Multiple Issues)	—	—	Misc.	2	ⓘ ✓
High	TLS (Multiple Issues)	—	—	Misc.	2	ⓘ ✓
High	TLS (Multiple Issues)	—	—	SMTP problems	2	ⓘ ✓
Low	X Server Detection	2.6 *	2.6 *	Service detection	1	ⓘ ✓
High	SMB (Multiple Issues)	—	—	Windows	7	ⓘ ✓
High	TLS (Multiple Issues)	—	—	General	4	ⓘ ✓
High	FTP (Multiple Issues)	—	—	Service detection	3	ⓘ ✓

Severity	Vulnerability	CVE	CVSS	Category	Count	Details
High	SSH (Multiple Issues)	—	—	General	2	ⓘ ✓
High	SSH (Multiple Issues)	—	—	Service detection	2	ⓘ ✓
High	Web Server (Multiple Issues)	—	—	Web Servers	2	ⓘ ✓
High	Nessus VPN scanner	—	—	Port scanners	25	ⓘ ✓
High	RPC Services Enumeration	—	—	Service detection	10	ⓘ ✓
High	Service Detection	—	—	Service detection	10	ⓘ ✓
High	OpenSSL Detection	—	—	Service detection	2	ⓘ ✓
High	RMI Registry Detection	—	—	Service detection	2	ⓘ ✓
High	AJP Connector Detection	—	—	Service detection	1	ⓘ ✓
High	Backported Security Patch Detection (FTP)	—	—	General	1	ⓘ ✓
High	Backported Security Patch Detection (WWW)	—	—	General	1	ⓘ ✓
High	Common Platform Enumeration (CPE)	—	—	General	1	ⓘ ✓
High	Device Type	—	—	General	1	ⓘ ✓
High	Ethernet Card Manufacturer Detection	—	—	Misc.	1	ⓘ ✓
High	Ethernet MAC Addresses	—	—	General	1	ⓘ ✓
High	ICMP Timestamp Request Remote Date Disclosure	—	—	General	1	ⓘ ✓
High	IRC Daemon Version Detection	—	—	Service detection	1	ⓘ ✓
High	Nessus Scan Information	—	—	Settings	1	ⓘ ✓
High	NFS Share Export List	—	—	RPC	1	ⓘ ✓
High	OpenSSH Detection	—	—	Misc.	1	ⓘ ✓
High	OS Identification	—	—	General	1	ⓘ ✓
High	OS Security Patch Assessment Not Available	—	—	Settings	1	ⓘ ✓
High	Patch Report	—	—	General	1	ⓘ ✓