

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** 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.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

SVOLGIMENTO:

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.868	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEOL (8.04.x)	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
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1

ho selezionato il tipo di scansione (basic network scan) ho selezionato poi common ports inserito il target della macchina meta ho salvato le modifiche e ho fatto partire la scansione come si vede dallo screenshot.

REPORT VULNERABILITY ASSESSMENT CON NESSUS

OBIETTIVO: scansione della macchina metasploitable e azioni di remediation su alcune vulnerabilità critiche

TITOLO: vulnerability assessment-metaploitable

AUTORE: Emanuela Parisi

DATA SCANSIONE: 27/09/2025

TOOL: Nessus

TARGET: IP 192.168.50.101

SOMMARIO ESECUTIVO

Questa attività di laboratorio come progetto aveva come obiettivo l'utilizzo di Nessus per eseguire un Vulnerability Assessment su una macchina volutamente vulnerabile (*Metasploitable*) e di implementare delle azioni di remediation su alcune vulnerabilità critiche rilevate.

È stata configurata e avviata una scansione di tipo *Basic Network Scan*, limitata alle porte comuni.

La scansione è durata 19 minuti e sono state trovate 122 vulnerabilità di cui diverse classificate come critical high.

INTRODUZIONE:

lo scopo dell'attività era familiarizzazione con le scansioni su nessus e implementazione di azioni di remediation di alcune vulnerabilità critiche

AMBITO: solo le porte comuni

METODOLOGIA DI SCANSIONE:

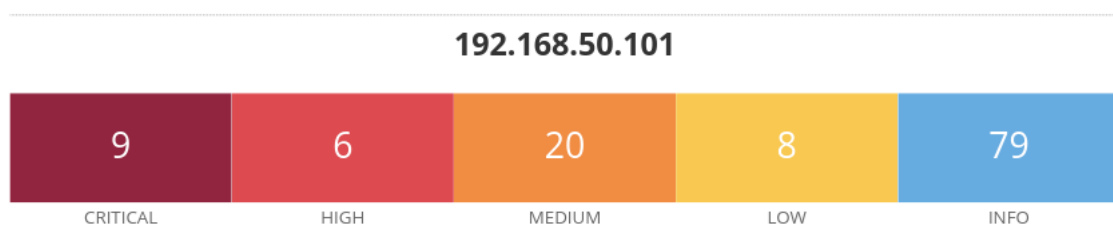
TIPO DI SCAN UTILIZZATO: Basic network scan

TARGET IP: 192.168.50.101

RISULTATI GENERALI

TOTALE VULNERABILITÀ: 122

CLASSIFICAZIONE PER SEVERITÀ:



ANALISI DELLE VULNERABILITÀ PIÙ RILEVANTI

UnrealIRCd Backdoor Detection

- CVE: CVE-2010-2075
- Descrizione: Versioni compromesse di UnrealIRCd contengono una backdoor che consente l'esecuzione di comandi remoti.
- Host/Porta: TCP/6667
- Impatto: Compromissione completa del sistema.
- Mitigazione: Reinstallazione da sorgente sicura, aggiornamento a versione supportata.

VNC Server 'password' Password

- Descrizione: Il servizio VNC consente l'accesso remoto utilizzando la password debole "password".
- Host/Porta: TCP/5900
- Impatto: Accesso remoto non autorizzato.
- Mitigazione: Disabilitare VNC non necessario, impostare password robuste.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

- CVE: CVE-2020-1938
- Descrizione: Questa vulnerabilità, nota come *Ghostcat*, consente a un attaccante remoto di sfruttare il connettore AJP (porta 8009) di Apache Tomcat per leggere file arbitrari o eseguire codice, se combinata con altre condizioni.
- Host/Porta: TCP/8009
Impatto: Possibile lettura di file sensibili e compromissione del sistema.
- Mitigazione: Aggiornare Tomcat a una versione corretta ($\geq 9.0.31$, $8.5.51$, $7.0.100$), disabilitare il connettore AJP se non necessario, o limitare l'accesso.

Apache Tomcat SEoL ($\leq 5.5.x$)

- CVE: N/A (problema di End of Life, non più supportato)
- Descrizione: La versione di Apache Tomcat individuata è fuori supporto ($\leq 5.5.x$). Ciò significa che non riceve più aggiornamenti di sicurezza, rendendo il server vulnerabile a molteplici exploit conosciuti e futuri.
- Host/Porta: TCP/8080
- Impatto: Elevato rischio di compromissione, poiché eventuali vulnerabilità non vengono più corrette.
- Mitigazione: Aggiornare Tomcat a una versione supportata ($\geq 9.x$ o $10.x$), rimuovere servizi obsoleti e seguire le linee guida ufficiali di hardening.

SCELTA DELLE VULNERABILITÀ CRITICHE RELATIVI PASSAGGI DELLE REMEDIATION

UnrealIRCd Backdoor Detection

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ps aux | grep unreal  
root      4679  0.0  0.1   8540  2660 ?        S    10:44   0:00 /usr/bin/unreal  
ircd  
msfadmin  6532  0.0  0.0   3008    776 tty1      S+   13:45   0:00 grep unreal  
msfadmin@metasploitable:~$ ps aux | grep [u]nreal  
root      4679  0.0  0.1   8540  2660 ?        S    10:44   0:00 /usr/bin/unreal  
ircd  
msfadmin@metasploitable:~$ sudo su  
[sudo] password for msfadmin:  
root@metasploitable:/home/msfadmin# kill 4679  
root@metasploitable:/home/msfadmin# ps aux | grep unreal  
root      6554  0.0  0.0   3004    772 tty1      S+   13:52   0:00 grep unreal  
root@metasploitable:/home/msfadmin#
```

il servizio unrealircd è un servizio (demone) su un sistema Linux e ascolta tipicamente sulla porta TCP 6667, il servizio riceve connessioni client IRC (da programmi come HexChat, mIRC, Irssi) Permette di creare canali di chat, moderatori, ban, permessi. Può collegarsi ad altri server UnrealIRCd per formare reti IRC distribuite.

UnrealIRCd è un programma server per creare e gestire chat IRC

comandi eseguiti: come da screenshot ho prima individuato il processo da killare dopo averlo individuato l'ho killato con il comando kill seguito dal PID

APACHE TOMCAT

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9446	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SSoL (<= 5.5.x)

```
killall -V, --version

-e,--exact          require exact match for very long names
-l,--ignore-case    case insensitive process name match
-g,--process-group  kill process group instead of process
-i,--interactive    ask for confirmation before killing
-l,--list           list all known signal names
-q,--quiet          don't print complaints
-r,--regex          interpret NAME as an extended regular expression
-s,--signal SIGNAL  send this signal instead of SIGTERM
-u,--user USER      kill only process(es) running as USER
-v,--verbose        report if the signal was successfully sent
-V,--version        display version information
-w,--wait           wait for processes to die

root@metasploitable:/home/msfadmin# killall -r 'tomcat'
tomcat: no process killed
root@metasploitable:/home/msfadmin# pkill -h
pkill: invalid option -- h
Usage: pkill [-SIGNAL] [-fvx] [-n|-o] [-P PPIDLIST] [-g PGRPLIST] [-s SIDLIST]
        [-u EUIDLIST] [-U UIDLIST] [-G GIDLIST] [-t TERMLIST] [PATTERN]
root@metasploitable:/home/msfadmin# pkill -f tomcat
root@metasploitable:/home/msfadmin# ps aux | grep tomcat
root      4844  0.0  0.0   3004   768 tty1      S+   16:26   0:00 grep tomcat
root@metasploitable:/home/msfadmin#
```

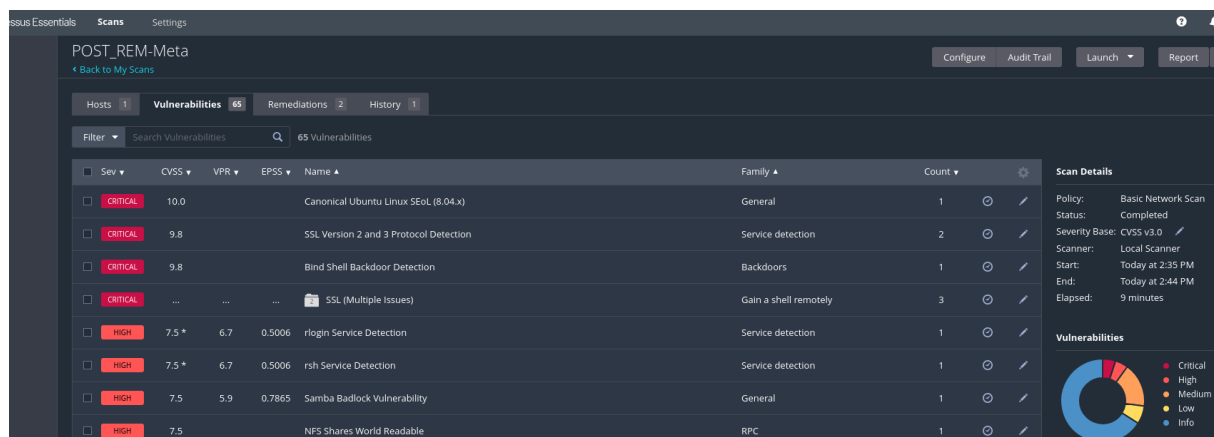
per risolvere le 2 vulnerabilità critiche di apache ho dovuto cercare il comando giusto dopo vari tentativi falliti alla fine ho usato il comando pkill -f che mi permette di terminare i processi in linux e mi permette di specificare una stringa di ricerca.

VNC 'PASSWORD' PASSWORD

```
root@metasploitable:/home/msfadmin# killall -r 'tomcat'
tomcat: no process killed
root@metasploitable:/home/msfadmin# pkill -h
pkill: invalid option -- h
Usage: pkill [-SIGNAL] [-fux] [-n!-o] [-P PPIDLIST] [-g PGRPLIST] [-s SIDLIST]
        [-u EUIDLIST] [-U UIDLIST] [-G GIDLIST] [-t TERMLIST] [PATTERN]
root@metasploitable:/home/msfadmin# pkill -f tomcat
root@metasploitable:/home/msfadmin# ps aux | grep tomcat
root      4844  0.0  0.0   3004   768 tty1      S+   16:26   0:00 grep tomcat
root@metasploitable:/home/msfadmin# vnc -h
bash: vnc: command not found
root@metasploitable:/home/msfadmin# vnc
vncconnect vncpasswd vncserver
root@metasploitable:/home/msfadmin# vncpasswd -h
Password:
Password too short
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

per questa vulnerabilità che comportava l'utilizzo e l'accesso da remoto attraverso l'utilizzo di una password debole che era appunto la parola password, per risolvere questa vulnerabilità critica non ho fatto altro che scegliere una password più robusta.

SCANSIONE DOPO LE AZIONI DI REMEDIATION



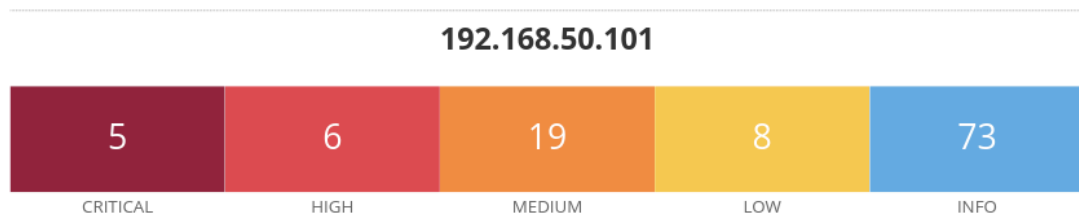
Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 2:35 PM
- End: Today at 2:44 PM
- Elapsed: 9 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info



Vulnerabilities Total: 111

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
HIGH	8.6	5.2	0.0334	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	0.3085	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

come possiamo vedere la scansione dopo le azioni di remediation sono diminuite le vulnerabilità critiche da 9 a 5.