Scansione vulnerabilità e risoluzione criticità

SACHELE

SOC analyst: Michele Stella

Corso: Cybersecurity Analyst

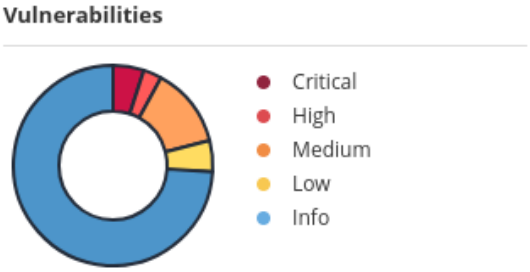
Data: 12/12/2025

Richiesta: Effettuare una scansione completa sul target e risolvere 4 problemi critici

Indice:

Risultato scansione target

Effettuata una scansione della macchina target con **ip 192.168.50.101** con sistema operativo **metasploitable** (ubuntu linux). La scansione è stato eseguita tramite nessus su macchina **Kali Linux.**



Le vulnerabilità scansionate sono moltissime (63), evidenziando che si tratta di una macchina non correttamente protetta.

Si dia precedenza a quelle evidenziate come '**critical**', riportate nella tabella sottostante.

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	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1		
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2		
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1		
CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3		

Il livello di criticità viene espresso seguendo il sistema **CVSS**, così strutturato:

Range **CRITICAL:** 9.0 - 10.0

Range **HIGH:** 8.9 - 7.0

Range **MEDIUM:** 6.9 - 4.0

Range **LOW:** 3.9 - 0.1

INFO: 0.0

Remediations 1

VNC Server ‘password’ Password

Di cosa si tratta:

VNC (Virtual Network Computing) è un servizio che permette il **controllo da remoto dello schermo** . Molto simile alla funzione “desktop remoto”.

Perché è considerata di livello critical:

Il server VNC usa una password **debole** (“password”). Un eventuale attaco di **brute force** (tentare di accedere utilizzando le password più comuni) potrebbe facilmente permettere il controllo remoto del nostro server. Un utente con questo accesso, potrebbe:

- visuallizare file e programmi
- acquisire permessi da admin/root
- installare malware o creare **backdoor** (accessi secondari al nostro server)

Soluzioni pratiche:

Una soluzione ovvia e rapida potrebbe essere quella di disabilitare il servizio. Ma dato che il servizio potrebbe tornare utile ai fini aziendali, procediamo sostituendo la password vulberabile con una più robusta.

-guida step by step per il cambio credenziali-

Per prima cosa, si termini il processo così da poterlo poi modificare, identifichiamo il **PID** (Identificatore di Processo).

```
root@metasploitable:/home/msfadmin# ps aux | grep vnc
root      4659  0.0  2.3  13924 12000 ?        S    06:22   0:00 Xtightvnc :0 -d
esktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -r
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
root      4663  0.0  0.2   2724  1192 ?        S    06:22   0:00 /bin/sh /root/.
vnc/xstartup
root      4804  0.0  0.1   3004   756 tty1     R+   06:31   0:00 grep vnc
```

Si proceda alla chiusura con il comando “**kill**” per poi procedere al cambio password con il comando “**vncpasswd**”.

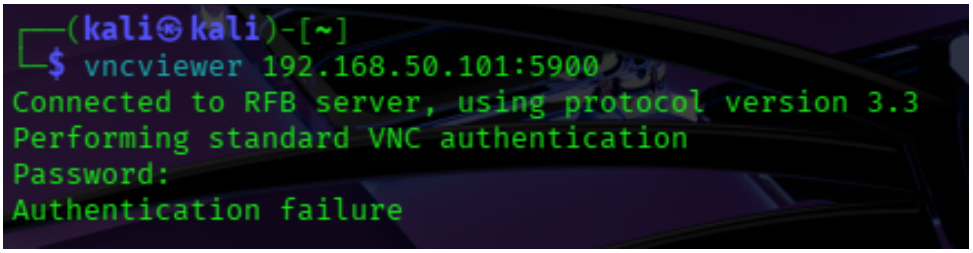
```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# vncserver :0
```

La password è stato sostituita per il test con v0to7dai, si proceda a sostituirla nuovamente una volta terminata la lettura del report.

Suggerimento: utilizzare un password manager come quelli forniti da aziende come proton, nordVPN ecc. così da utilizzarne più complesse, protette, cifrate e non vincolate dalla memoria del singolo utente.

Verifica:

Si utilizzi un'altra macchina (nel caso specifo dello screen **kali**) per controllare che il tutto sia avvenuto con successo. L'estratto di codice mostra un tentativo di accesso al server VNC della macchina con **IP 192.168.50.101 Metasploitable2** utilizzando come password "password".



Tentativo con nuova password:

Possiamo notare come sia stato possibile accedere alla macchina meta.

Remediations 2

Bind Shell Backdoor Detection

Di cosa si tratta:
Questa vulnerabilità indica la presenza di una **shell remota** (un terminale) in ascolto su una porta di rete. Chiunque riesca a collegarsi a quella porta può inviare comandi al sistema.

Perché è considerata di livello critical:
Non richiede autenticazione: è una **backdoor**. Nessus ha dimostrato l'impatto eseguendo il comando id e ottenendo risposta con **uid=0 (root)**. In pratica: accesso completo al server.

```
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:/#
```

Soluzioni pratiche:
In questa casistica si rende necesssario chiudere la **backdoor.**

-guida step by step per il cambio credenziali-

Si cerchi qual è il servizio in esecuzione su questa porta per terminarlo, è già un inizio.

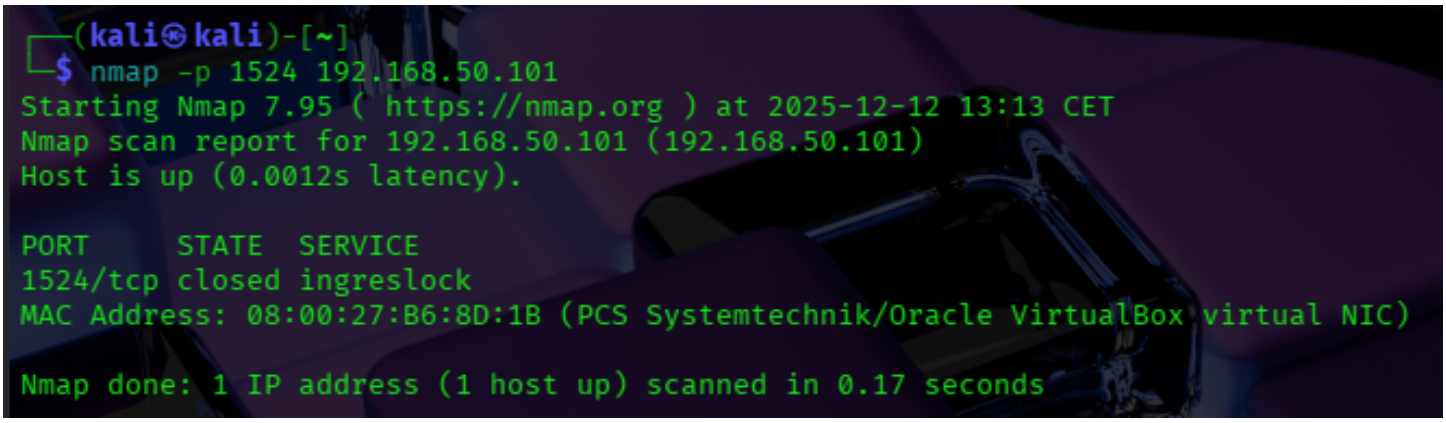
```
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4502 root   12u  IPv4  12159       TCP *:ingreslock (LISTEN)
You have new mail in /var/mail/root
root@metasploitable:/home/msfadmin# _
```

Si termini il processo utilizzando il **PID** (4502) come per la vulnerabilità precedente.

Verifichiamo la porta sia ora inaccessibile:

```
root@metasploitable:/home/msfadmin# kill -9 4502
bash: kill: (4502) - No such process
root@metasploitable:/home/msfadmin# netstat -tln | grep 1524
root@metasploitable:/home/msfadmin# _
```

La porta non mostra più nulla, si effettui usa seconda verifica utilizzando **kali**:



Si utilizzi **nmap** (strumento di scansione porte). La porta **1524/tcp** risulta ora chiusa.

Attenzione, si tratta di una soluzione temporanea. La soluzione definitiva consiste nel disabilitare permanentemente il servizio che riapre la backdoor sulla porta 1524 attraverso il file di configurazione.

Remediations 3

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Di cosa si tratta:
Ghostcat è una problematica che fa riferimento al connettore AJP di **Apache Tomcat**

Perché è considerata di livello critical:
Con Ghostcat un attaccante **senza autenticazione** può sfruttare il connettore AJP, con cui leggere file dell'applicazione web (config, codice, ecc.) o in casi più gravi, arrivare anche ad eseguire codice**.**

Cosa comporta disabilitarlo o limitarlo:

- Se **disabiliti AJP**, chiudi proprio l'ingresso vulnerabile. Possibile effetto collaterale: se Apache stava usando AJP per parlare con Tomcat, alcune pagine/app potrebbero non funzionare.
- Se **lo limiti a localhost (127.0.0.1)**, AJP resta disponibile solo internamente al server, quindi Nessus (che arriva dalla rete) non lo vede più.

Soluzioni pratiche:

Si disabiliti il servizio, seguendo la guida.

-guida step by step per il cambio credenziali-

Verifichiamo che la porta AJP (8009) sia effettivamente aperta.

```
root@metasploitable:/home/msfadmin# netstat -tnl | grep 8009
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
```

La porta 8009 risulta effettivamente in ascolto. Prima di tutto disabilitiamolo per questa sessione:

```
root@metasploitable:/home/msfadmin# /etc/init.d/tomcat6 stop
bash: /etc/init.d/tomcat6: No such file or directory
root@metasploitable:/home/msfadmin# netstat -tnl | grep 8009
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
root@metasploitable:/home/msfadmin# ls /etc/init.d | grep tomcat
tomcat5.5
root@metasploitable:/home/msfadmin# /etc/init.d/tomcat5.5 stop
 * Stopping Tomcat servlet engine tomcat5.5                             [ OK ]
root@metasploitable:/home/msfadmin# netstat -tnl | grep 8009
root@metasploitable:/home/msfadmin# _
```

Ora disabilitiamo l'avvio automatico per ogni sessione:

```
root@metasploitable:/home/msfadmin# netstat -tnl | grep 8009
root@metasploitable:/home/msfadmin# update-rc.d -f tomcat5.5 remove
 Removing any system startup links for /etc/init.d/tomcat5.5 ...
   /etc/rc0.d/K10tomcat5.5
   /etc/rc1.d/K10tomcat5.5
   /etc/rc2.d/S90tomcat5.5
   /etc/rc3.d/S90tomcat5.5
   /etc/rc4.d/S90tomcat5.5
   /etc/rc5.d/S90tomcat5.5
   /etc/rc6.d/K10tomcat5.5
root@metasploitable:/home/msfadmin# ps aux | grep tomcat
root      7564  0.0  0.1   3004   756 tty1     R+   07:49   0:00 grep tomcat
root@metasploitable:/home/msfadmin#
```

Si utilizzi nuovamente **nmap** su macchina **kali** per verificare che la porta 8009 sia chiusa

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 8009 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-12 13:51 CET
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0013s latency).

PORT     STATE  SERVICE
8009/tcp closed ajp13
MAC Address: 08:00:27:B6:8D:1B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Remediations 4

SSL Version 2 and 3 Protocol Detection

Di cosa si tratta:
SSL/TLS è la “serratura” che protegge le connessioni HTTPS (porta 443). Serve a cifrare i dati tra client e server.

Perché è considerata di livello critical:
Se il server accetta **SSL 2.0 / SSL 3.0**, accetta protocolli vecchi con difetti noti. Un attaccante può provare a forzare il downgrade della connessione o sfruttare debolezze crittografiche per fare attacchi tipo **man-in-the-middle** (introdursi a metà tra le comunicazione per modficare il contenuto inviato o ricevuto) o ridurre la sicurezza della cifratura.

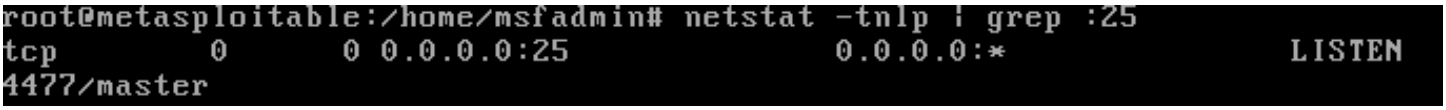
Soluzioni pratiche:

Anche per questa casistica, si provveda a disabilitare i servizi. I client moderni continueranno a funzionare usando TLS. I client molto vecchi potrebbero non riuscire più a collegarsi, ma è un compromesso necessario per la sicurezza dei dati.

Le porte “incriminate” sono la **25/tcp/smtp** e la **5432 / tcp / postgresql**

-guida step by step per il cambio credenziali-

Individuazioni servizi attivi sulle porte:



Ora si proceda con la chiusura servizio e disabilitiamo l’avvio automatico, segue un check da **metasploitable** e da **kali**.

```
root@metasploitable:/home/msfadmin# /etc/init.d/postfix stop
 * Stopping Postfix Mail Transport Agent postfix
root@metasploitable:/home/msfadmin# update-rc.d -f postfix remove
 Removing any system startup links for /etc/init.d/postfix ...
   /etc/rc0.d/K20postfix
   /etc/rc1.d/K20postfix
   /etc/rc2.d/S20postfix
   /etc/rc3.d/S20postfix
   /etc/rc4.d/S20postfix
   /etc/rc5.d/S20postfix
   /etc/rc6.d/K20postfix
root@metasploitable:/home/msfadmin# netsta -tnlp | grep :25
bash: netsta: command not found
root@metasploitable:/home/msfadmin# netstat -tnlp | grep :25
root@metasploitable:/home/msfadmin# _
```

```
root@metasploitable:/home/msfadmin# ls /etc/init.d | grep postgres
postgresql-8.3
root@metasploitable:/home/msfadmin# /etc/init.d/postgresql-8.3 stop
 * Stopping PostgreSQL 8.3 database server                              [ OK ]
root@metasploitable:/home/msfadmin# update-rc.d -f postgresql-8.3 remove
 Removing any system startup links for /etc/init.d/postgresql-8.3 ...
   /etc/rc0.d/K21postgresql-8.3
   /etc/rc1.d/K21postgresql-8.3
   /etc/rc2.d/S19postgresql-8.3
   /etc/rc3.d/S19postgresql-8.3
   /etc/rc4.d/S19postgresql-8.3
   /etc/rc5.d/S19postgresql-8.3
   /etc/rc6.d/K21postgresql-8.3
root@metasploitable:/home/msfadmin# netsta -tnlp | grep :5432
bash: netsta: command not found
root@metasploitable:/home/msfadmin# netstat -tnlp | grep :5432
root@metasploitable:/home/msfadmin# _
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 443,5432 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-12 14:31 CET
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0019s latency).

PORT     STATE  SERVICE
443/tcp  closed https
5432/tcp closed postgresql
MAC Address: 08:00:27:B6:8D:1B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Remediations 5 opzionale

NFS Shares World Readable

Di cosa si tratta:
NFS (Network File System) serve a condividere cartelle in rete: altri host possono avere accesso a directory del server.

Perché è considerata di livello high:
Il server non sta limitando gli accessi. Questo significa che chiungue nella rete può leggere quei contenuti. Può esporre file di configurazione, dati sensibili o informazioni utili per attacchi successivi.

Soluzioni pratiche:
Si modifica la configurazione NFS per permettere accesso **solo a host/subnet autorizzati** (ad esempio solo alla macchina **Kali**).

-guida step by step per il cambio credenziali-

Si verifichi cosa la macchina esporta

```
/       *(rw,sync,no_root_squash,no_subtree_check)
```

Il server NFS esporta la directory **/** senza restrizioni di accesso (*****) e con permessi di scrittura (**rw**). Questo consente a qualunque host in rete di leggere o modificare file del sistema. Inoltre l'opzione **no_root_squash** permette al root del client di mantenere privilegi elevati lato server, aumentando l'impatto. La remediation consiste nel limitare gli host autorizzati e applicare opzioni più sicure.

Si utilizzi il comando **sudo nano /etc/exports** per effettuare le modifiche necessarie al file

```
/       192.168.50.0/24(ro,sync,root_squash,no_subtree_check)
```

Cosa abbiamo modificato

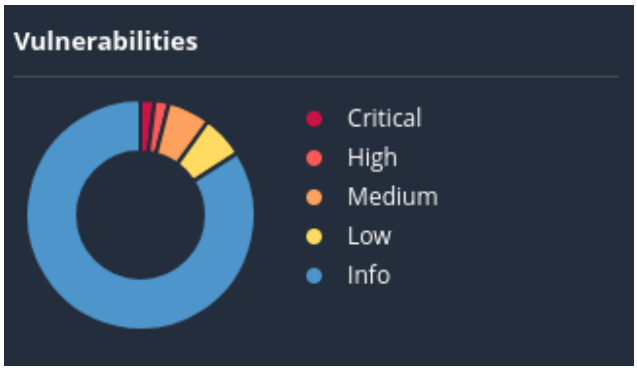
* → solo 192.168.50.0/24 (solo la tua rete)

rw → ro (solo lettura)

no_root_squash → root_squash (root del client non è "root" sul server)

Scannerizzazione finale con nessus

Si presti attenzione a come la fetta che rappresenta la parte '**critical**' del nostro grafico sia diminuita.



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	5.1	0.0165	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	3
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2
LOW	2.6 *			X Server Detection	Service detection	1
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1

Ulteriore verifica, l'elenco delle vulnerabilità, dove non sono più presenti quelle trattate nelle pagine seguenti.

192.168.50.101	Fail	2	2	5	5	73

Possiamo notare come le vulnerabilità **CRITICAL** siano passete da **9** a **2**, le **HIGH** da **5** a **2**, le **MEDIUM** da **22** a **5** e le **LOW** da **8** a **5**. Anche le **INFO** calate moltissimo passando da **127** a **73**.

In conclusione, la macchina "**meta"** è ora molto più sicura, ma necessita ancora di moltissimi inteventi.