

PROGETTO W12D4



Esercizio
Traccia e requisiti

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.



Esercizio
Traccia e requisiti

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

SCANSIONE DI NESSUS SU METASPLOITABLE

192.168.1.17

9

3

22

7

78

CRITICAL

HIGH

MEDIUM

LOW

INFO

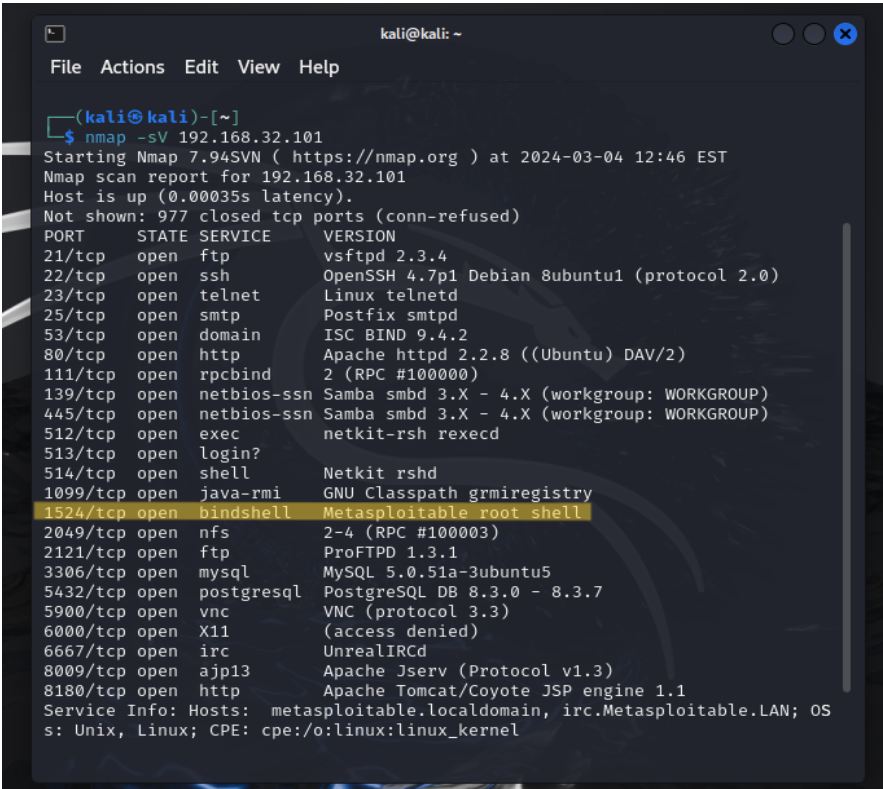
Vulnerabilities

Total: 119

SEVERITY	CVSS V3.0	VPR 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	-	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

Risoluzione vulnerabilità 51988

Quando si esegue una scansione nmap da Kali verso l'indirizzo di Metasploitable, viene individuata una porta con il servizio "bindshell" attivo, che corrisponde alla porta 1524.

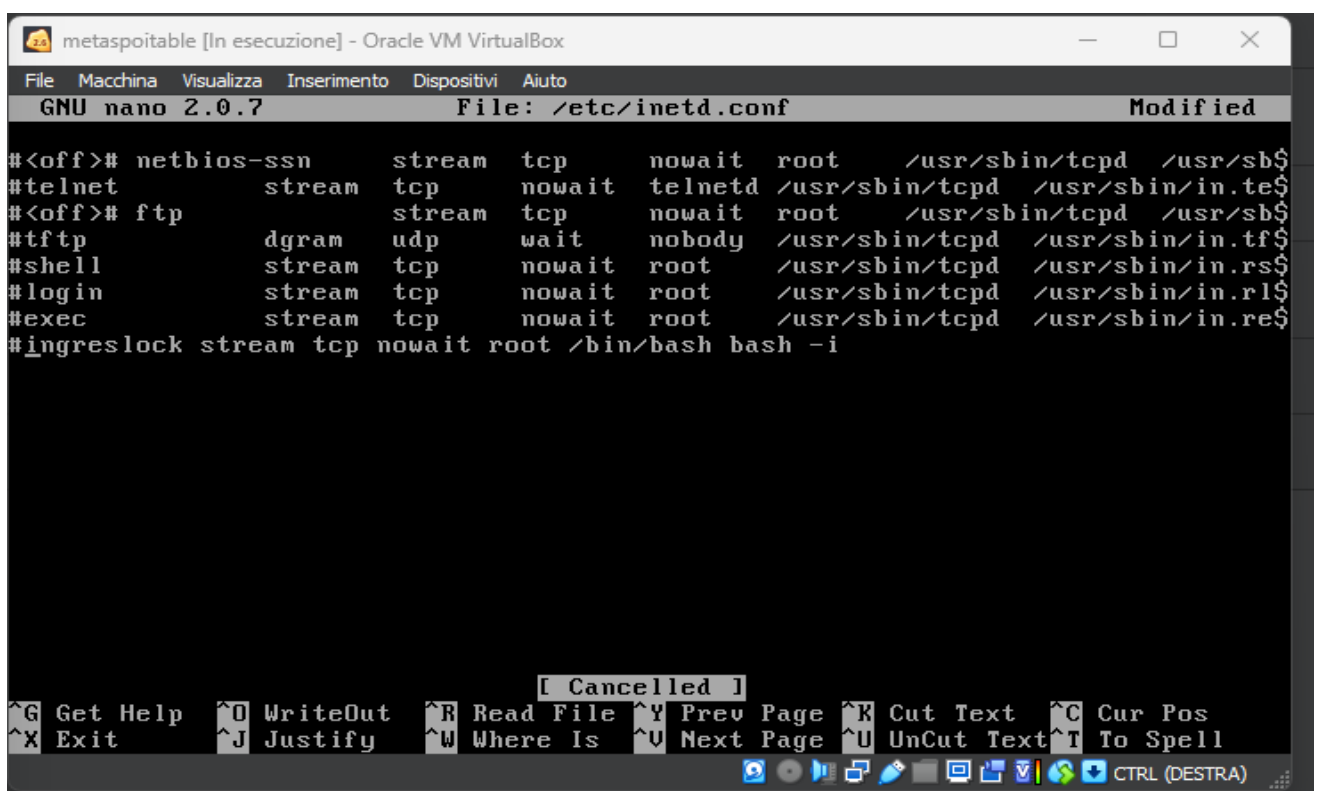


Successivamente provo a usare il servizio Netcat per connettermi a Metasploitable, sfruttando la porta aperta.

```
(kali㉿kali)-[~]  
$ netcat 192.168.32.101 1524  
root@metasploitable:/# uname  
Linux  
root@metasploitable:/# hostname  
metasploitable  
root@metasploitable:/# echo $$  
4922  
root@metasploitable:/# whoami  
root  
root@metasploitable:/#
```

La connessione è riuscita, verifico eseguendo anche qualche comando.

Passo al terminale di Metasploitable, mi sposto nella cartella /etc per cercare la backdoor, utilizzo il comando `sudo nano inetd.conf`. Individuo la backdoor e commento le righe di codice pertinenti, rendendola "vuota".



```
metasploitable [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
GNU nano 2.0.7 File: /etc/inetd.conf Modified  
#<off># netbios-ssn stream tcp nowait root /usr/sbin/tcpd /usr/sbin/$  
#telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd  
#<off># ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.ftpd  
#tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd  
#shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rsh  
#login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogin  
#exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd  
#ingreslock stream tcp nowait root /bin/bash bash -i  
[ Cancelled ]  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell  
CTRL (DESTRA)
```

Ritento la connessione con Netcat su Kali:

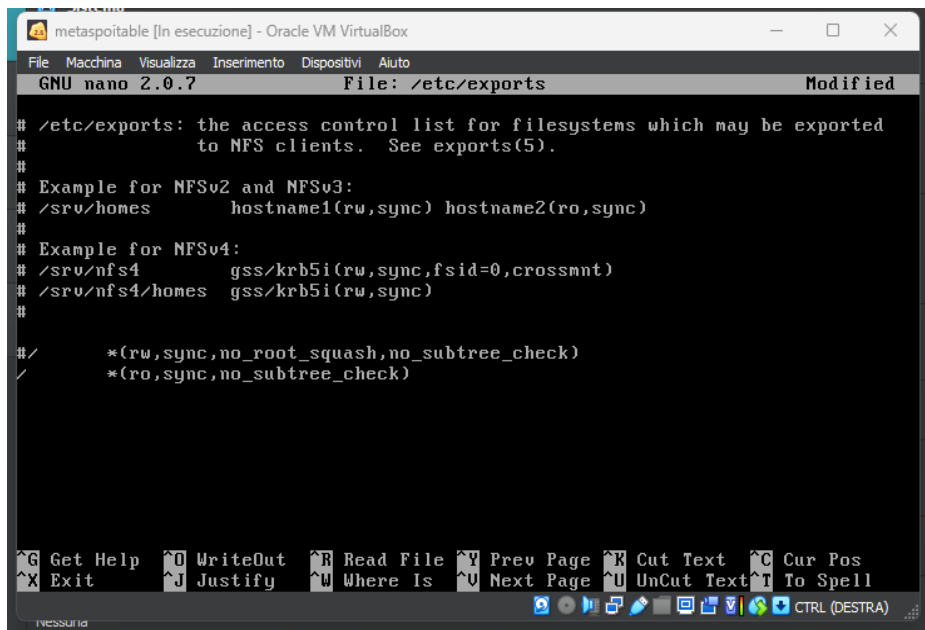
```
kali@kali: ~  
File Actions Edit View Help  
└─$ netcat 192.168.32.101 1524  
(UNKNOWN) [192.168.32.101] 1524 (ingreslock) : Connection refused  
  
└─(kali@kali)-[~]  
└─$ nmap -sV 192.168.32.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 12:29 EST  
Nmap scan report for 192.168.32.101  
Host is up (0.00014s latency).  
Not shown: 982 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
25/tcp    open  smtp        Postfix smtpd  
53/tcp    open  domain      ISC BIND 9.4.2  
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind     2 (RPC #100000)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
1099/tcp  open  java-rmi    GNU Classpath grmiregistry  
2049/tcp  open  nfs         2-4 (RPC #100003)  
2121/tcp  open  ftp         ProFTPD 1.3.1  
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc         VNC (protocol 3.3)  
6000/tcp  open  X11         (access denied)  
6667/tcp  open  irc         UnrealIRCd  
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)  
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS  
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://  
nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 35.13 seconds
```

La connessione è stata rifiutata, si può vedere anche dalla scansione di Nmap che la porta 1524 non è più aperta.

Risoluzione vulnerabilità 11356

Dal terminale di Metasploitable mi sposto nel file `"/etc/exports"`, successivamente commento la penultima riga che concede l'accesso da qualunque directory con i privilegi di lettura e scrittura.

Una volta commentata la riga, aggiungo una nuova riga che concede solo privilegi di lettura agli utenti che vi accedono.



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/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      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)
/      *(ro, sync, no_subtree_check)
```

Risoluzione vulnerabilità [61708](#)

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito 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.

Quindi, procedo alla prova di accesso da Kali utilizzando il servizio VNCviewer, inserendo la password "password". Dopo aver inserito le credenziali, l'accesso è stato completato con successo.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ vncviewer 192.168.32.101  
Connected to RFB server, using protocol version 3.3  
Performing standard VNC authentication  
Password:  
Authentication successful  
Desktop name "root's X desktop (metasploitable:0)"  
VNC server default format:  
  32 bits per pixel.  
  Least significant byte first in each pixel.  
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0  
Using default colormap which is TrueColor. Pixel format:  
  32 bits per pixel.  
  Least significant byte first in each pixel.  
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0  
  
root@metasploitable: /  
root@metasploitable:/# uname  
Linux  
root@metasploitable:/# hostname  
metasploitable  
root@metasploitable:/# whoami  
root  
root@metasploitable:/#  
root@metasploitable:/# psswd  
-bash: psswd: command not found  
root@metasploitable:/# passwd  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@metasploitable:/#
```

Sostituisco la password "password" con una più complessa, utilizzando anche numeri, maiuscole e caratteri speciali.

SECONDA SCANSIONE DI NESSUS SU METASPLOITABLE

192.168.1.17



Vulnerabilities

Total: 116

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
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*	-	46882	UnrealIRCd Backdoor Detection