L’esercizio prevede di risolvere almeno 2 vulnerabilità con il programma di scan Nessus di livello High o più alto.

In questo caso verranno visualizzati i passaggi per rimediare alle vulnerabilità: NFS EXPORTED SHARE INFORMATION DISCLOSURE, VNC SERVER ‘PASSWORD’ PASSWORD, BILL SHELL BACKDOOR DETECTION.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
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	9.0	Apache Tomcat AJP Connector Request Injection (Ghos...	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	...	...	SSL (Multiple Issues)	Gain a shell remotely	3

Vulnerabilità VNC SERVER ‘PASSWORD’ PASSWORD: in questo caso ci indica in chiaro che la password è PASSWORD. Questo significa inoltre che molto probabilmente è una psw di default e non è sicura ed è facile da intercettare.

SOLUZIONE: Aprendo la macchina di META ho avviato i permessi di amministratore con il comando SUDO SU, successivamente ho effettuato il comando VNCTPASSWD dandoci la possibilità di cambiare la password. In fine ho effettuato il comando SUDO REBOOT per il riavvio della macchina con le modifiche.

Vulnerabilità NFS ECXPORTED SHARE INFORMATION DISCLOSURE: in questo caso la condivisione NFS potrebbero essere acquisita dall’host in scansione, un utente malintenzionato potrebbe sfruttarlo per leggere o scrivere sull’host remoto. Soluzione: Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

```
  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)
```

Eseguo il comando SUDO nano /etc/exports e andiamo a sostituire * con l’IP di meta. Questa modifica andrà ad impedire l’accesso ad utenti esterni.

```
 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)
#

/       192.168.49.101(rw,sync,no_root_squash,no_subtree_check)
```

Vulnerabilità BIND SHELL BACKDOOR DETECTION: In questo caso un host remoto potrebbe essere compromesso, è in ascolto una shell senza nessuna autenticazione favorendo un attaccante collegandosi ad una porta e inviando direttamente i comandi.

Soluzione: Bisogna verificare se l'host remoto è compromesso e se necessario reinstallare il sistema.

```
root@metasploitable:/home/msfadmin# sudo netstat /tulpn | grep 1524
root@metasploitable:/home/msfadmin# sudo netstat -tulpn | grep 1524
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4653/xinetd
root@metasploitable:/home/msfadmin# sudo kill 4653
root@metasploitable:/home/msfadmin#
```

Con il seguente comando andiamo a verificare che la modifica è andata correttamente e la porta 1424 è stata chiusa.

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sS -p 1524 192.168.49.101ù
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 12:36 CET
Nmap scan report for 192.168.49.101ù (127.0.0.1)
Host is up (0.000028s latency).
rDNS record for 127.0.0.1: localhost

PORT     STATE  SERVICE
1524/tcp closed ingreslock

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(davide㉿kali)-[~]
└─$
```

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.49.101
[sudo] password for davide:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 12:30 CET
Nmap scan report for 192.168.49.101
Host is up (0.0012s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
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; OSs: Linux, Unix; CPE: cpe:/o:l
inux: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 11.52 seconds
```

In fine come vediamo dalla scansione effettuata le vulnerabilità che avevamo evidenziato non ci sono più.