



Esercizio S5 L5

Hosts	1	Vulnerabilities	65	Remediations	2	Notes	2	History	1
Filter	Search Vulnerabilities		65 Vulnerabilities						
Sev	CVSS	VPR	Name	Family	Count				
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1			
<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		SSL Version 2 and 3 Protocol Detection	Service detection	2			
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1			
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1			
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3			
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1			
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1			
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	28			
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5			
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2			
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1			
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1			

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 2:27 PM

End: Today at 2:52 PM


Elapsed: 26 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

La richiesta dell'esercizio era di risolvere almeno due delle problematiche di livello High o più alto riscontrate durante lo scan di Nessus.

Seguito verranno mostrati i passaggi per risolvere le seguenti vulnerabilità: NFS Exported Share Information Disclosure, VNC Server 'password' Password, Bind Shell Backdoor Detection ed infine Samba Badlock Vulnerability.



Risoluzione della vulnerabilità VNC Server 'password' Password:

Questa vulnerabilità ci indica che la password del server VNC è letteralmente 'password' che oltre a non essere una password sicura è probabilmente quella predefinita ed è quindi molto facile da bypassare.

Per risolvere questa vulnerabilità è sufficiente eseguire i seguenti comandi da terminale:

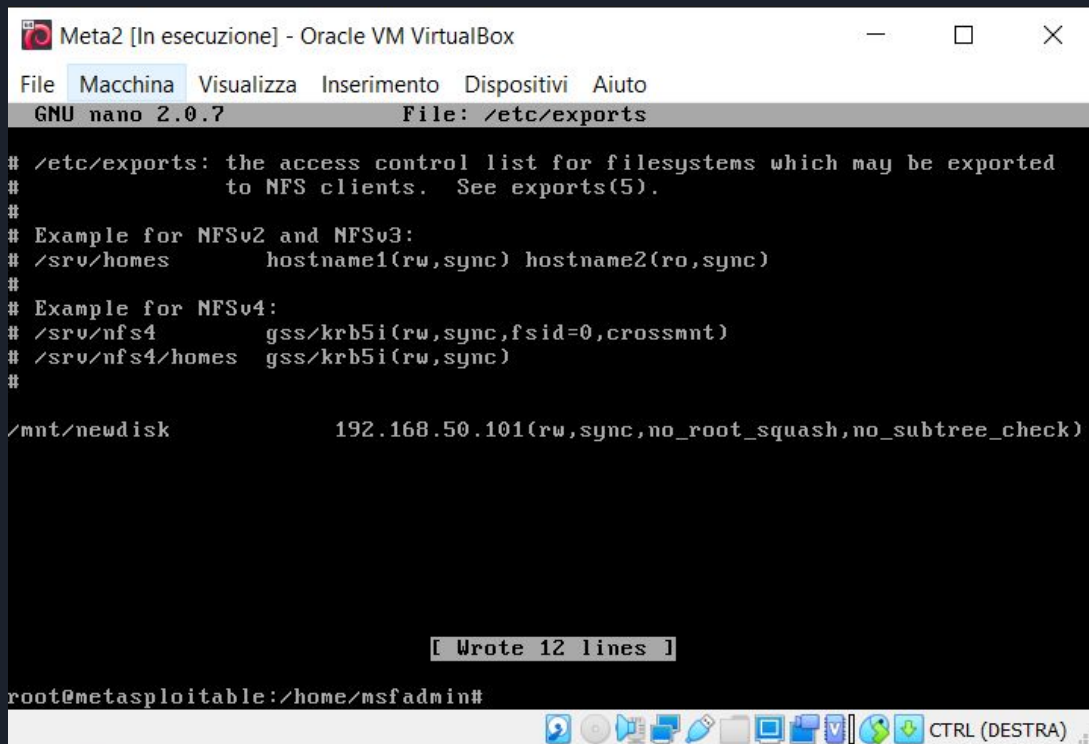
- `sudo su` (per ottenere permessi da amministratore)
- `cd .vnc` (per entrare nella directory nascosta .vnc)
- `vncpasswd` (comando per effettuare il cambio di password)
- `sudo reboot` (per riavviare la macchina e salvare le modifiche effettuate)

Risoluzione della vulnerabilità NFS Exported Share Information Disclosure:

Eseguiamo il comando:

```
sudo nano /etc/exports
```

e sostituiamo l'asterisco nell'ultima riga con l'indirizzo IP di Meta in modo da impedire l'accesso da utenti esterni.



```
Meta2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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)
#
/mnt/newdisk      192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

[ Wrote 12 lines ]

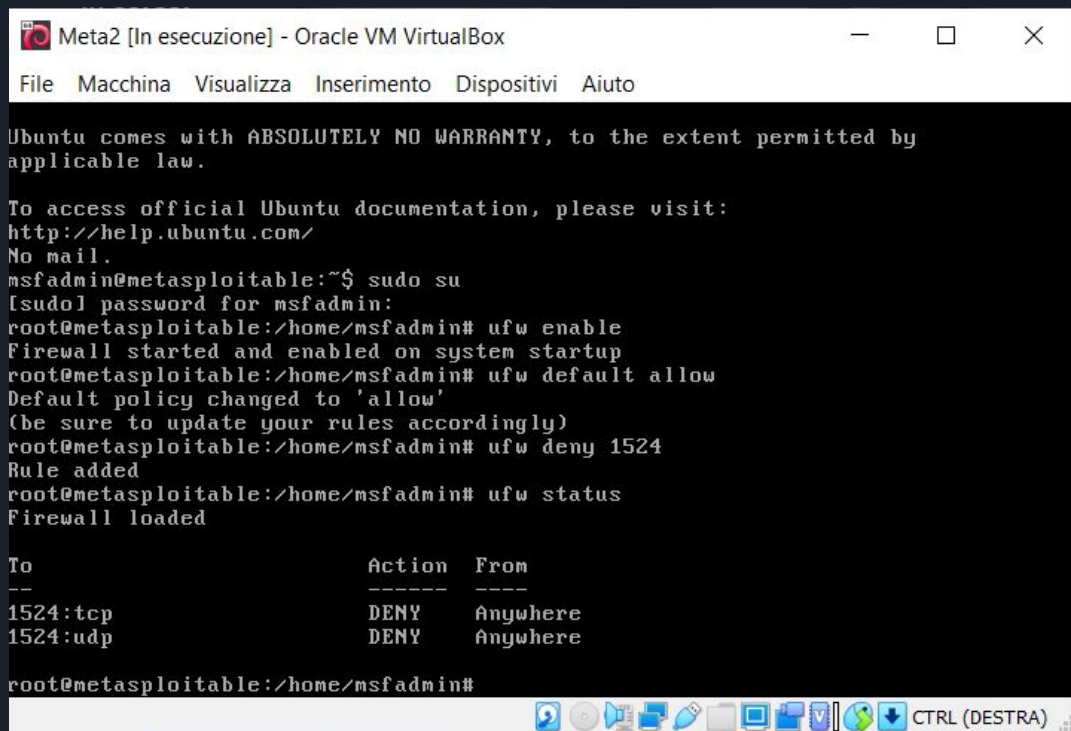
root@metasploitable:/home/msfadmin#
```

Risoluzione della vulnerabilità Bind Shell Backdoor Detection:

Eeguire i seguenti comandi:

- sudo su
- ufw enable
- ufw default allow
- deny 1524

in questo modo avremo creato
una regola firewall che blocca la
connessione sulla porta 1524
dove è in ascolto la backdoor.



```
Meta2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

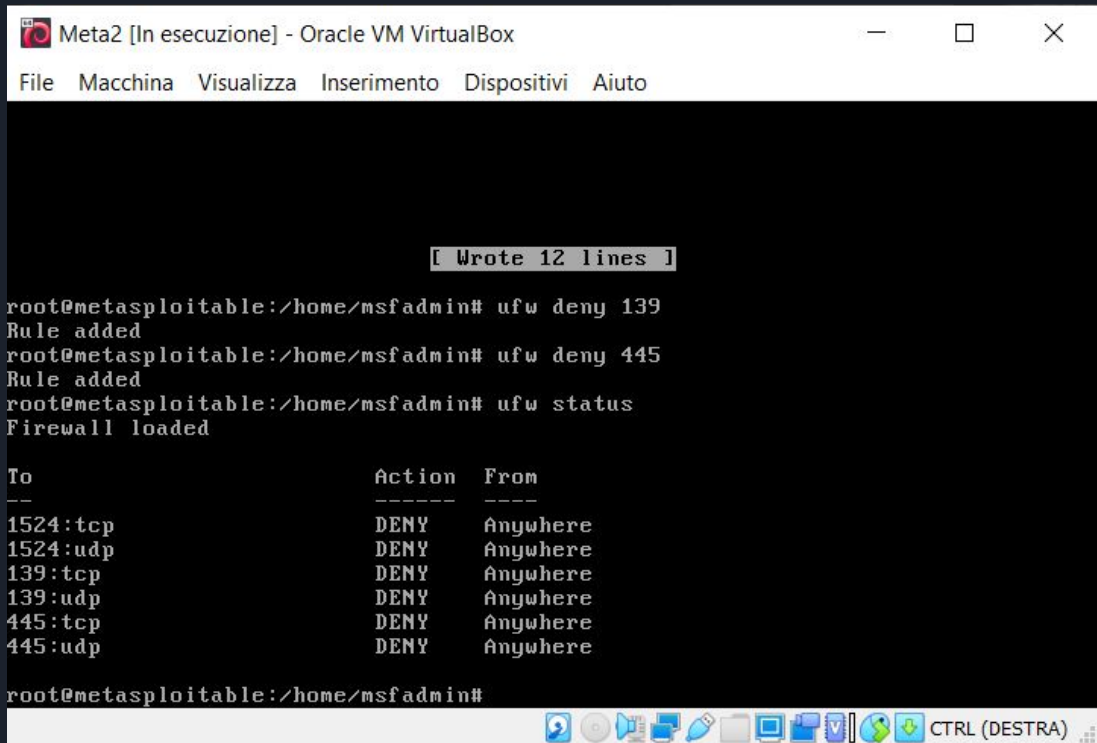
To                Action From
--                -
1524:tcp          DENY  Anywhere
1524:udp          DENY  Anywhere

root@metasploitable:/home/msfadmin#
```

Risoluzione della vulnerabilità Samba Badlock Vulnerability.

In maniera simile alla vulnerabilità precedente, per risolvere questa vulnerabilità andremo a filtrare le porte su cui agisce Samba con lo stesso comando:

- ufw deny 139
- ufw deny 445




```
Meta2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

[ Wrote 12 lines ]

root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To          Action From
--          -
1524:tcp    DENY  Anywhere
1524:udp    DENY  Anywhere
139:tcp     DENY  Anywhere
139:udp     DENY  Anywhere
445:tcp     DENY  Anywhere
445:udp     DENY  Anywhere

root@metasploitable:/home/msfadmin#
```



Ecco uno scan di nmap che mostra le porte aperte su Meta prima di aver inserito le regole firewall.

```
(kali@kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:29 CET
Nmap scan report for 192.168.50.101
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
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)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
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
MAC Address: 08:00:27:E4:38:89 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: 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 65.91 seconds
```

Ecco lo stesso scan ripetuto dopo aver inserito le regole firewall che bloccano le porte indesiderate.

Notare come la porta 139, 445 e 1524 appaiono come 'filtered'

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-22 17:06 CET
Nmap scan report for 192.168.50.101
Host is up (0.00037s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
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   filtered netbios-ssn
445/tcp   filtered microsoft-ds
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
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
8180/tcp  open  unknown
MAC Address: 08:00:27:E4:38:89 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: 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 187.42 seconds
```


Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄	✎
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🔄	✎
<input type="checkbox"/> CRITICAL	📁 SSL (Multiple Issues)	Gain a shell remotely	3	🔄	✎
<input type="checkbox"/> MIXED	📁 SSL (Multiple Issues)	General	24	🔄	✎
<input type="checkbox"/> MIXED	📁 ISC Bind (Multiple Issues)	DNS	5	🔄	✎
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/> MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄	✎
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	🔄	✎
<input type="checkbox"/> MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	🔄	✎
<input type="checkbox"/> MIXED	📁 SSH (Multiple Issues)	Misc.	6	🔄	✎
<input type="checkbox"/> MIXED	📁 TLS (Multiple Issues)	Misc.	2	🔄	✎
<input type="checkbox"/> MIXED	📁 TLS (Multiple Issues)	SMTP problems	2	🔄	✎
<input type="checkbox"/> LOW	2.6 *		X Server Detection	Service detection	1	🔄	✎

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0 ✎
 Scanner: Local Scanner
 Start: Today at 6:07 PM
 End: Today at 6:33 PM
 Elapsed: 26 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

al termine di tutto è stata effettuata una nuova scansione di Nessus e possiamo vedere come non siano più presenti le vulnerabilità di cui ci siamo occupati.