

Progetto Settimana 5

Report Nessus e azioni di rimedio

Un Vulnerability Scanner è uno strumento per trovare le vulnerabilità di un determinato target; NESSUS (il software che andremo ad utilizzare) identifica le vulnerabilità andandole a confrontare con un database sempre aggiornato e classificandole in base al livello di rischio (critical, high, medium, low e info). Attraverso il software possiamo anche andare ad eseguire degli attacchi veri e proprio di test come la BRUTE FORCE.

Andiamo ora a sviscerare e risolvere le vulnerabilità evidenziate nel report consultabile tramite link https://github.com/Eindr/progetto-settimana-5/blob/main/Meta_vulnerability.pdf:

1. **Bind Shell Backdoor Detection**: è sintomo della creazione di una BACKDOOR che crea un canale di comunicazione tra un sistema remoto e uno compromesso. In questo caso bisogna agire immediatamente effettuando un'analisi e un monitoraggio generale della macchina (porte, file di sistema, account utente, traffico di rete etc..). In questo caso NESSUS ci fornisce la porta interessata nel report e quindi non ci resterà che andarla a chiudere con il comando `'netstat -tulnp'` e terminando il processo:

```
root@metasploitable:~# cd /
root@metasploitable:~# sudo netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4507/xinetd
root@metasploitable:~# sudo kill 4507
root@metasploitable:~#
```

Output

Nessus was able to execute the command "id" using the following request :

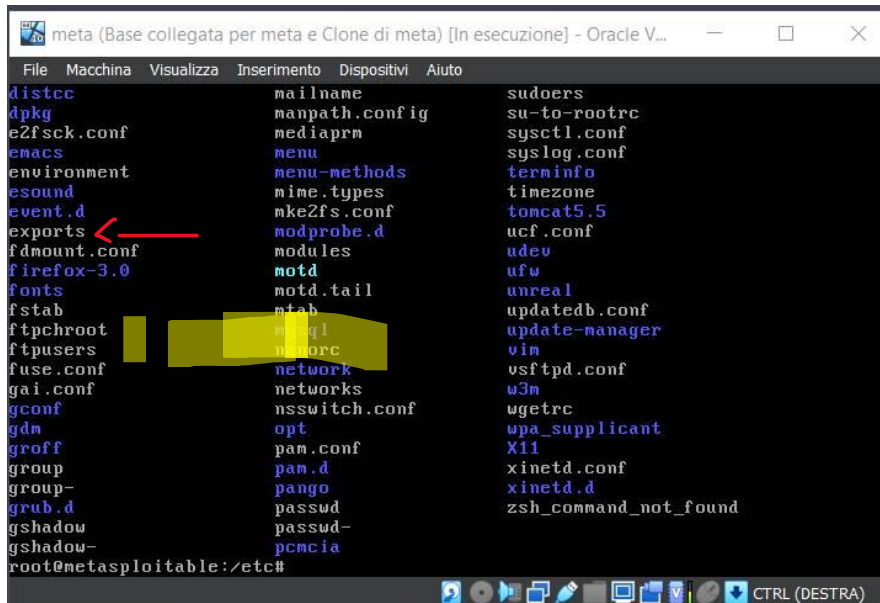
This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:~# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
----- snip -----

To see debug logs, please visit individual host

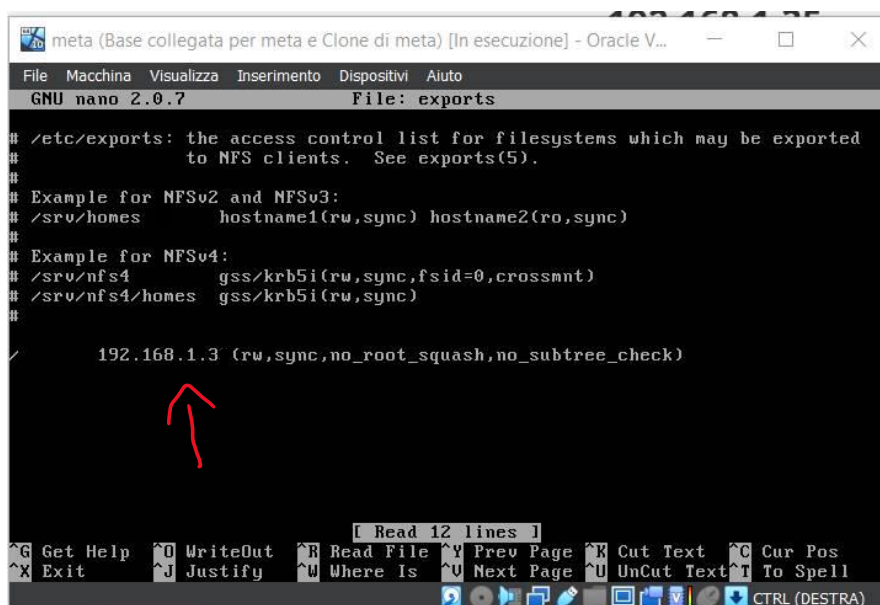
Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.35

<input type="checkbox"/>	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 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghos...	Web Servers	1	
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	

2. **NFS Exported Share Information Disclosure:** questa criticità indica che abbiamo una vulnerabilità inerente al protocollo NFS utilizzato per la condivisione di file e risorse di archiviazione su una rete. In questo caso Metasploitable è il nostro server e dobbiamo restringere gli IP che possono accedervi, così da non rendere i nostri dati aziendali accessibili a tutti. Per fare ciò dobbiamo arrivare al file dove si trovano le configurazioni NFS: sempre a seguito di una ricerca, nella directory 'etc' troviamo il file 'exports' con all'interno le configurazioni da modificare. Basterà sostituire il "*" che indica l'accesso a tutti con solo l'indirizzo IP che vogliamo sia autorizzato:



```
meta (Base collegata per meta e Clone di meta) [In esecuzione] - Oracle V...
File Macchina Visualizza Inserimento Dispositivi Aiuto
distcc mailname sudoers
dpkg manpath.config su-to-rootrc
e2fsck.conf mediaprm sysctl.conf
emacs menu syslog.conf
environment menu-methods terminfo
esound mime.types timezone
event.d nke2fs.conf tomcat5.5
exports ← modprobe.d ucf.conf
fdmount.conf modules udev
firefox-3.0 motd ufw
fonts motd.tail unreal
fstab ntab updatedb.conf
ftphroot nls_q1 update-manager
ftpusers nls_norc vim
fuse.conf network vsftpd.conf
gai.conf networks w3m
gconf nsswitch.conf wgetrc
gdm opt wpa_supplicant
groff pam.conf X11
group pam.d xinetd.conf
group- pango xinetd.d
grub.d passwd zsh_command_not_found
gshadow passwd-
gshadow- pemcia
root@metasploitable:/etc#
```

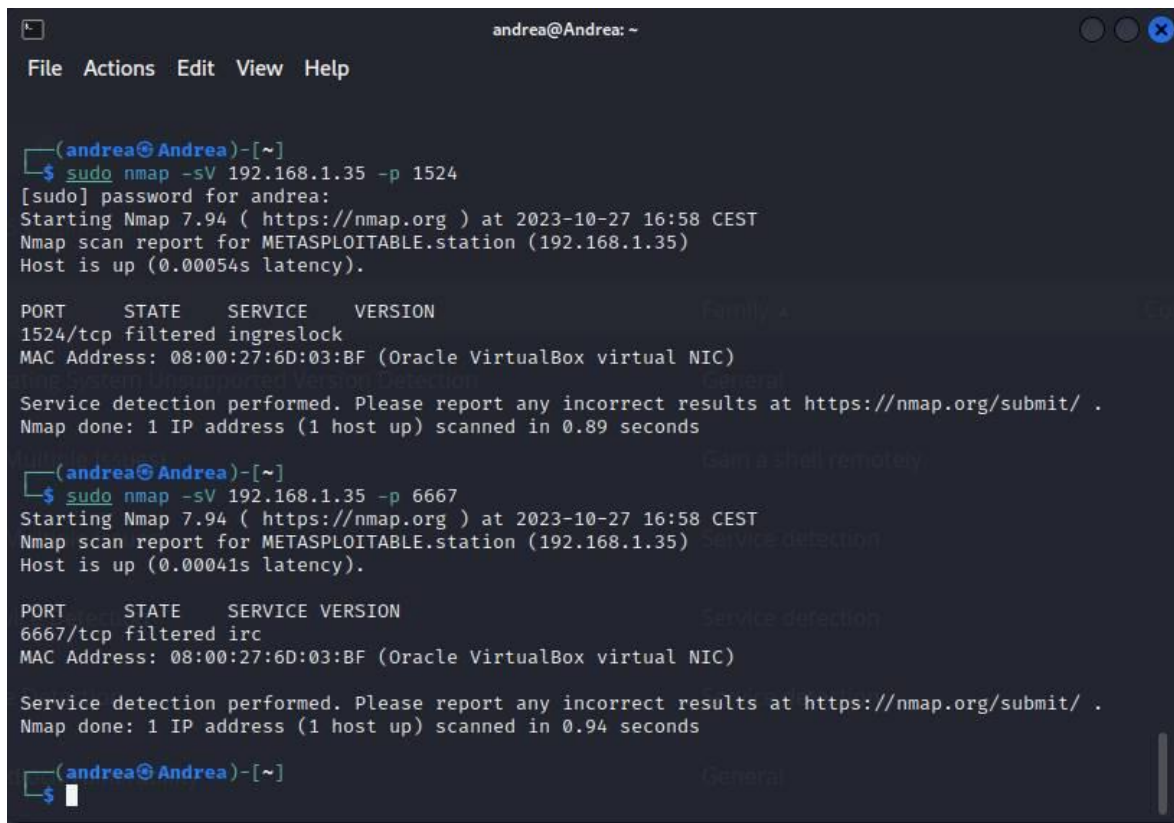


```
meta (Base collegata per meta e Clone di meta) [In esecuzione] - Oracle V...
GNU nano 2.0.7 File: exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
192.168.1.3 (rw,sync,no_root_squash,no_subtree_check)
/

[ Read 12 lines ]
^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)
```

3. **UnrealIRCd Backdoor Detection:** anche in questo caso andiamo a chiudere la porta con gli stessi comandi del punto 1 oppure possiamo anche andare ad utilizzare il firewall IPTABLES tramite comando `'sudo iptables -A INPUT -p tcp --dport 6667 -j DROP'` per bloccare una porta in ingresso. Con NMAP possiamo vedere le porte "filtered" a causa del firewall.

```
root@metasploitable:/etc# sudo netstat -tulnp | grep 6667
tcp        0      0 0.0.0.0:6667        0.0.0.0:*          LISTEN
4659/unrealircd
root@metasploitable:/etc# sudo kill 4659
root@metasploitable:/etc# _
```



```
andrea@Andrea: ~
File Actions Edit View Help

(andrea@Andrea)-[~]
$ sudo nmap -sV 192.168.1.35 -p 1524
[sudo] password for andrea:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 16:58 CEST
Nmap scan report for METASPLOITABLE.station (192.168.1.35)
Host is up (0.00054s latency).

PORT      STATE      SERVICE      VERSION
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:6D:03:BF (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds

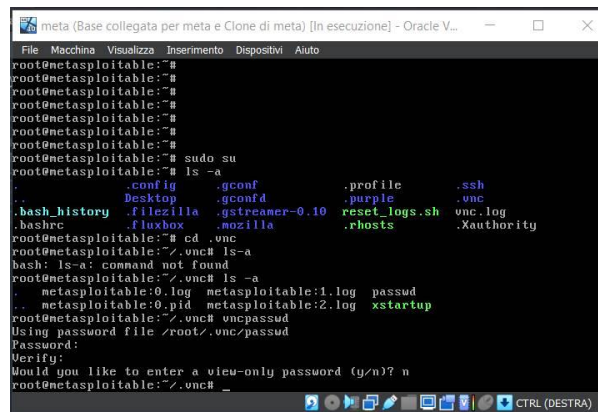
(andrea@Andrea)-[~]
$ sudo nmap -sV 192.168.1.35 -p 6667
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 16:58 CEST
Nmap scan report for METASPLOITABLE.station (192.168.1.35)
Host is up (0.00041s latency).

PORT      STATE      SERVICE      VERSION
6667/tcp  filtered  irc
MAC Address: 08:00:27:6D:03:BF (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds

(andrea@Andrea)-[~]
$
```

4. **VNC Server 'password' Password:** In questo caso **NESSUS** ci fa sapere che il problema principale è la password troppo “debole” del server VNC, tecnologia che consente di controllare un computer in remoto da un altro dispositivo attraverso una connessione di rete. Tramite una ricerca di informazioni in merito, andiamo ad impostare una password più “forte” direttamente da riga di comando su Metasploitable (privilegi da amministratore). Abbiamo utilizzato il comando `'vncpasswd'` per andare a modificare la password (nuova 12345678). Si noti che con la nuova scansione la vulnerabilità è scomparsa:



```
meta (Base collegata per meta e Clone di meta) [In esecuzione] - Oracle V...
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~# sudo su
root@metasploitable:~# ls -la
.          .config      .gconf       .profile     .ssh
Desktop    .gconfd      .purple      .vnc
.bash_history .filezilla  .gstreamer-0.10 reset_logs.sh vnc.log
.bashrc     .fluxbox    .mozilla     .rhosts      .Xauthority
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls -la
.  metasploitable:0.log  metasploitable:1.log  passwd
.. metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc#
```

<input type="checkbox"/>	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 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghos...	Web Servers	1	
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	

Di seguito ,quindi, possiamo vedere il nuovo report di NESSUS senza più le vulnerabilità che siamo andati ad arginare.

itials

Scans

Settings

?

🔔

Eindr4

👤

pass, 2 backdoor, nfs

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 61

Remediations 2

History 1

Filter

Search Vulnerabilities

61 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	MIXED	...	2 SSL (Multiple Issues)	Service detection	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5 *	6.7 rlogin Service Detection	Service detection	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5 *	6.7 rsh Service Detection	Service detection	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	6.7 Samba Badlock Vulnerability	General	1	🕒	✎
<input type="checkbox"/>	MIXED	...	15 SSL (Multiple Issues)	General	28	🕒	✎
<input type="checkbox"/>	MIXED	...	5 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	6.5	Unencrypted Telnet Server	Misc.	1	🕒	✎

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 4:49 PM

End: Today at 4:59 PM

Elapsed: 10 minutes

Vulnerabilities

Critical

High

Medium

Low

Info