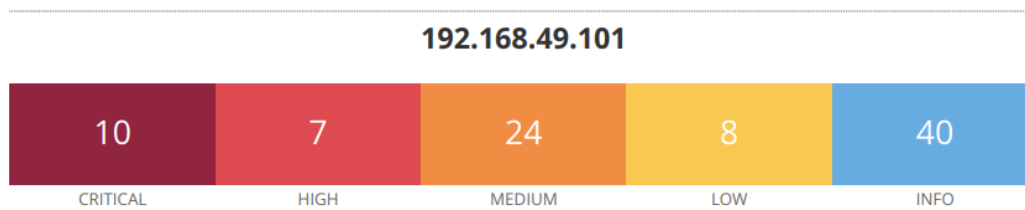


# Scansione tramite Nessus e Risoluzione delle rispettive criticità



## Vulnerabilities

Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

Come possiamo vedere Nessus ha trovato varie criticita', andando ad analizzarle e successivamente a "Fixarle" ossia risolverle:

- VNC Server password

---

CRITICAL	10.0*	-	61708	VNC Server 'password' Password
----------	-------	---	-------	--------------------------------

---

sicuramente una delle problematiche piu' pericolose ...ma anche piu' facile nella risoluzione....ossia una password "debole"

la possiamo facilmente cambiare utilizzando il comando:  
"vncpasswd"

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

andando ad inserire una password piu' sicura .

- NFS Exported Share Information Disclosure

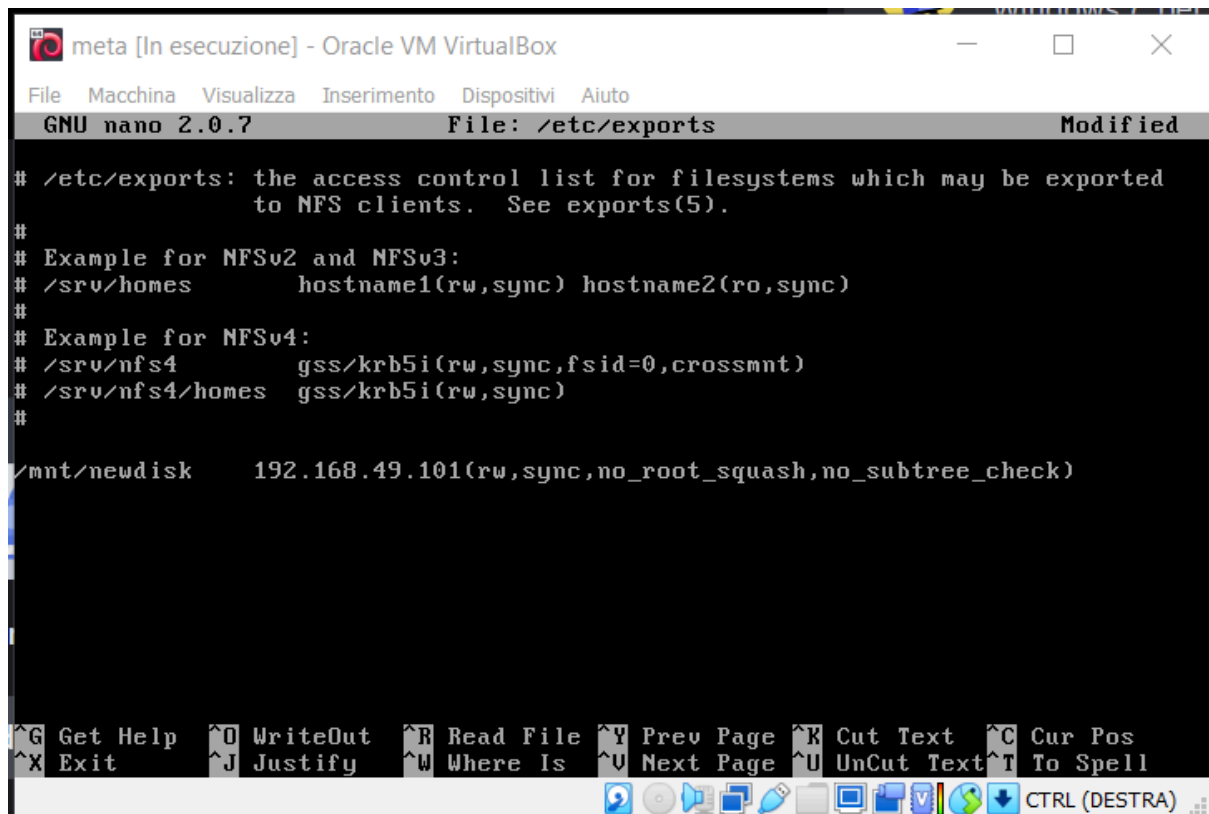
---

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
----------	-------	-----	-------	---

---

qui la criticita' è relativa alla condivisione NFT e alla sua sicurezza e configurazione

si puo' risolvere andando a configurare i suoi parametri  
aprendo il file "export" dentro la directory /etc  
andando a modificare il parametro che regola l'accessibilità agli host selezionando  
un solo ip che puo' accedere al servizio ossia della nostra macchina.



```
meta [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)
#
/mnt/newdisk      192.168.49.101(rw,sync,no_root_squash,no_subtree_check)

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

e successivamente alla modifica salviamo il file.

- BACK DOOR

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
----------	-----	---	-------	-------------------------------

troviamo come critica' la presenza di una backdoor aperta e accessibile, senza alcuna protezione; andiamo dunque a chiudere la porta

CRITICAL

Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```

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

----- 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	192.168.49.101

dalla immagine di Nessus soprastante vediamo in basso a sinistra il numero della porta

```

msfadmin@metasploitable:/etc$ sudo netstat -tulpn | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4623/xinetd
msfadmin@metasploitable:/etc$

```

```

msfadmin@metasploitable:/etc$ sudo netstat -tulpn | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4623/xinetd
msfadmin@metasploitable:/etc$ sudo kill 4623
msfadmin@metasploitable:/etc$

```

Dal terminale di meta verifichiamo lo stato della porta tramite il comando netsat ed i parametri “-tulpn” (-t tcp; -u udp; -l le porte in ascolto; -p program mostra il nome del programma che la sta utilizzando; -n numeric). L’output sarà una lista di tutte le porte in ascolto, lo andiamo a filtrare tramite il comando grep “port\_id”. poi andremo a killare il processo con “sudo kill numero\_processo”.

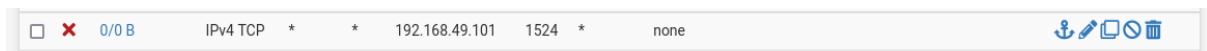
Dal terminale di kali possiamo verificare che la porta sia effettivamente chiusa con il comando nmap inserendo ip e numero porta

```
(kali㉿kali)-[~]
$ sudo nmap -sS -p 1524 192.168.49.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 06:39 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
tem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.49.101
Host is up (0.0019s latency).

PORT      STATE SERVICE
1524/tcp  closed ingreslock

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

ovviamente al riavvio della macchina il processo riprendera'.  
per una soluzione piu' definitiva si propone di inserire una regola del firewall che blocchi sull IP 192.168.49.101 la porta 1524.



- Apache Tomcat AJP Connector Request Injection

**CRITICAL** 9.8 9.0 134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Essendo un servizio non utilizzato sulla macchina, invece di aggiornarlo, si è preferito disabilitare la porta “8009”, utilizzata dal servizio TomCat, inserendo un “!” all’inizio della sintassi.

Il file da modificare si trova all’interno del percorso /etc/tomcat5.5/server.xml  
il comando sara’: “sudo nano /etc/tomcat5.5/server.xml

```
GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml

        noCompressionUserAgents="gozilla, traviata"
        compressableMimeType="text/html,text/xml"

-->

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS" />

-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
        enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

e con l'opportuna modifica diventera' :

```
GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml

        noCompressionUserAgents="gozilla, traviata"
        compressableMimeType="text/html,text/xml"

-->

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS" />

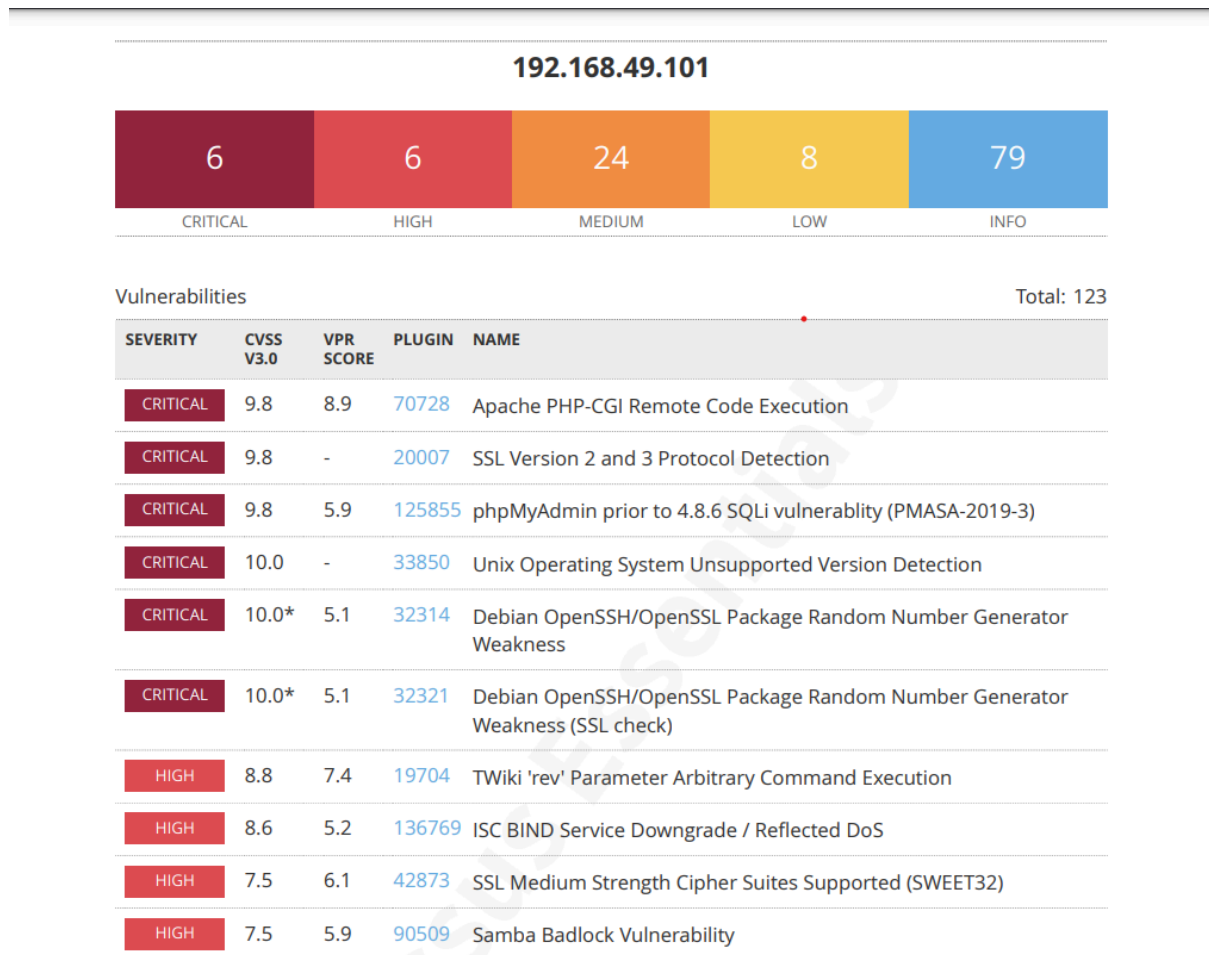
-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!--<Connector port="8009"
        enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--

[ Wrote 384 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  ^V Next Page ^U UnCut Text ^T To Spell
```

facendo una nuova scansione vedremo che le criticita' sono state eliminate:



Grazie per l'attenzione