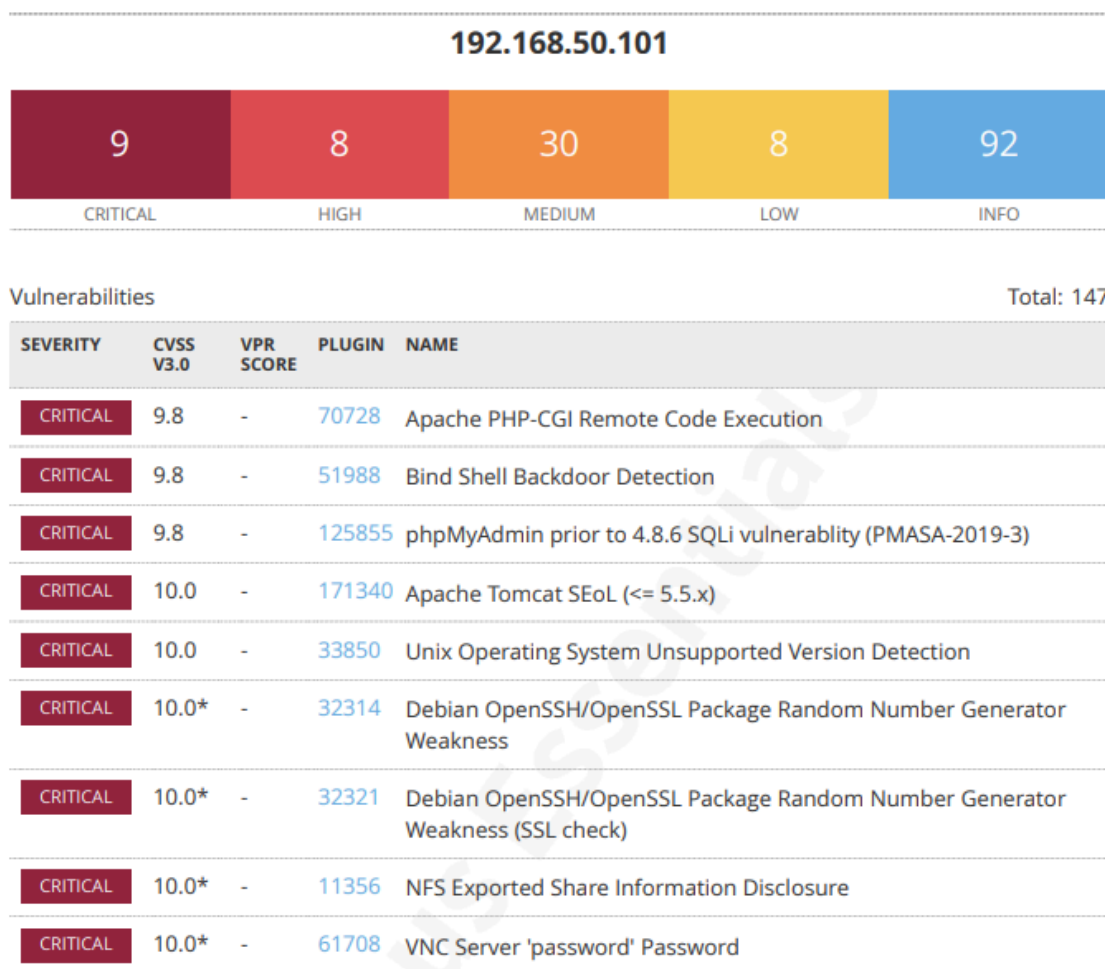


## Consegna S5\_L5

Nell'esercizio di oggi viene richiesto di scansionare con Nessus il target Metasploitable per conoscere le sue vulnerabilità. Successivamente si scelgono tra 2/4 delle vulnerabilità critiche/high per implementare delle azioni di rimedio.



La scansione di Nessus sul target Metasploitable 192.168.50.101, mi mostra diverse vulnerabilità critical le quali verranno prese in esame.

### Bind Shell Backdoor Detection

Una Bind Shell è una backdoor che apre una porta specifica del sistema target e mette in ascolto una shell su questa porta. Quando un attaccante si connette a questa porta, ottiene l'accesso al sistema. Quindi, indica una serie di pratiche e strumenti volti ad individuare e neutralizzare le backdoor, proteggendo così il sistema da accesso non autorizzato.

## SOLUZIONE:

Per risolvere il problema della Bind Shell procedo con l'analisi della porta 1524. Sulla macchina Kali Linux, controllo se ho l'accesso alla porta con il comando:

**nc 192.168.50.101 1524**

```
(kali㉿kali)-[~]  
$ nc 192.168.50.101 1524  
root@metasploitable:/# id  
uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/# whoami  
root  
root@metasploitable:/#  
root@metasploitable:/# ^C
```

Come si può notare kali sta comunica con la porta, confermando che è accessibile.

Procedo a bloccare con la porta 1524 sulla Metasploitable, ma prima ho bisogno del codice pid.

Procedo con il comando:

**sudo fuser 1524/tcp**

per cercare il codice pid (numero univoco assegnato dal sistema operativo ad ogni processo in esecuzione).

```
msfadmin@metasploitable:~$ sudo fuser 1524/tcp  
[sudo] password for msfadmin:  
1524/tcp: 4442 10615  
msfadmin@metasploitable:~$ kill -9 4442  
-bash: kill: (4442) - Operation not permitted  
msfadmin@metasploitable:~$ sudo kill -9 4442  
msfadmin@metasploitable:~$
```

Trovato il pid (4442), procedo con il comando:

**sudo kill -9 4442**

bloccando quindi l'accesso alla porta 1524.

Come riportato nell'ultima immagine, la kali non riuscirà più a comunicare attraverso quella porta, perchè è stato "killato" il processo.

```
(kali㉿kali)-[~] Operating System Unsupported Version Detection  
$ nc 192.168.50.101 1524  
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```

Un'ulteriore soluzione alla Bind Shell sarebbe quella di aggiungere una regola di firewall per rifiutare il traffico.

## VNC Server 'password' Password

Questa vulnerabilità si riferisce alla password utilizzata per autenticarsi ed accedere ad un server VNC, che consente di controllare un computer a distanza da un altro computer, utilizzando la rete. Questa è una misura di sicurezza per garantire che solo gli utenti autorizzati possano accedere al desktop remoto.

SOLUZIONE:

Sulla macchina metasploitable procedo con il comando:

**vncpasswd**

che consente di impostare o cambiare la password di accesso per un server VNC. La password può essere lunga massimo di 8 caratteri e, per far sì che la macchina sia più in sicurezza, si aggiunge una password complessa, in modo tale da renderla più difficile da indovinare con possibile attacco bruteforce.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
```

Dopo aver cambiato o inserito la password nuova, si verifica che il file di configurazione e i permessi siano corretti.

E nel caso in cui il problema persiste, si può aggiornare il software VNC con il comando:

**sudo apt-get install tightvncserver**

## NFS Exported Share Information Disclosure

Questo è un protocollo di rete che consente agli utenti di accedere ai file su un server remoto come se fossero su un'unità locale.

La vulnerabilità si manifesta quando le informazioni sulle condivisioni NFS esportate, i permessi di accesso e gli indirizzi IP autorizzati, sono accessibili ad utenti non autorizzati. Questo può avvenire se le configurazioni sono impostate in modo insicuro.

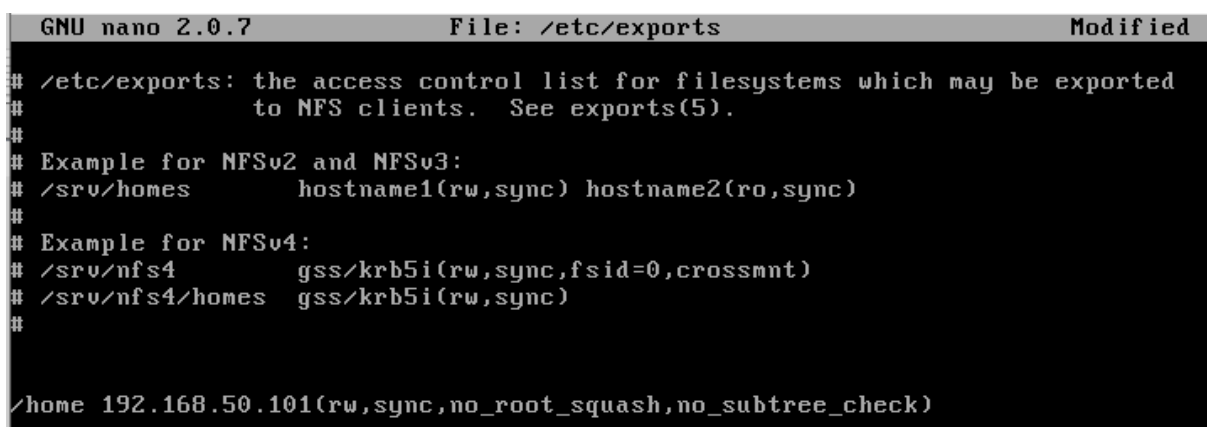
SOLUZIONE:

Inizialmente si verifica che la directory esista, tramite il comando:

```
ls /home
```

Successivamente si apre il file /etc/exports:

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



```
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)
#
/home 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```

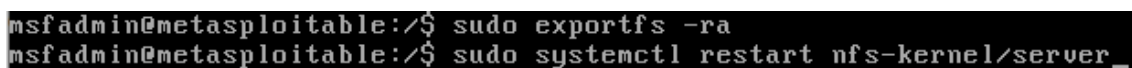
per poi aggiungere una configurazione di condivisione per una directory esistente:

```
/home 192.168.50.101 (rw,sync,no_root_squash,no_subtree_check)
```

Successivamente si applicano le modifiche salvando con il comando:

```
sudo exportfs -ra
```

Per poi riavviare il servizio NFS



```
msfadmin@metasploitable:/$ sudo exportfs -ra
msfadmin@metasploitable:/$ sudo systemctl restart nfs-kernel/server_
```

Infine si verifica che le esportazioni siano configurate correttamente:

**sudo exportfs -v**

```
msfadmin@metasploitable:/$ sudo exportfs -v
/home          192.168.50.101(rw,wdelay,no_root_squash,no_subtree_check)
msfadmin@metasploitable:/$ _
```

## CONCLUSIONI

Sono state risolte 3 vulnerabilità. Per altre presenti nel report di Nessus basterà (come nel caso di Debian OpenSSH/OpenSSL, Apache Tomcat SEoL, phpMyAdmin e Unix Operating System Unsupported Version Detection) eseguire gli aggiornamenti in quanto privo delle ultime versioni.