# Progetto S5/L5

Davide Diglio

# Obiettivi

Effettuare una scansione completa sul target Metasploitable, scegliere un minimo di 2 ad un massimo di 4 vulnerabilità critiche / high risolvendo i problemi.

# Specifiche

- Metasploitable
- Nessus

## Nessus

Nessus è un programma che utilizziamo per scansionare il target, vedendo i tipi di vulnerabilità.

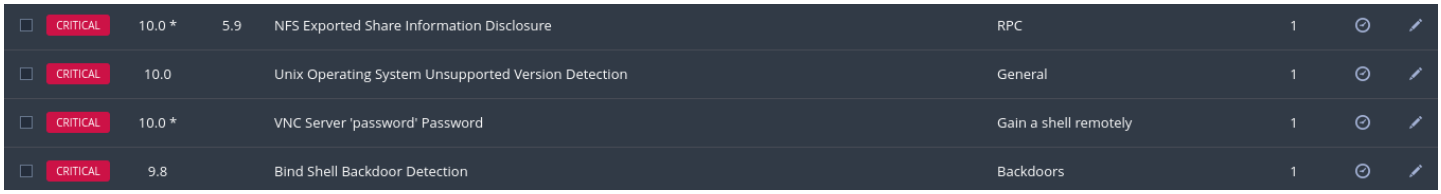
# Svolgimento

## I. Scansione Iniziale

In questa fase vediamo tutti i tipi di vulnerabilità e quali risolvere.


## II. Remediation

In questa fase iniziamo a risolvere le varie vulnerabilità, nel compito dobbiamo risolvere 4 vulnerabilità critiche che possiamo vedere nell'immagine qui sotto.




***Vulnerabilità VNC Server:*** Nessus ci avvisa che la password del server è molto debole e ci suggerisce di cambiarla con una password più forte.

Come fare: per cambiare la password possiamo andare nella root con il comando sudo su, poi con il comando vcnpasswd cambiamo la password.

```
bash: vncservice: command not found
root@metasploitable:/home/msfadmin# vncserver

New 'X' desktop is metasploitable:1

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:1.log

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#
```

***Vulnerabilità Bind Shell Backdoor Detection:*** qui invece Nessus ci avvisa che ci avvisa che un malintenzionato potrebbe collegarsi alla porta remota senza alcuna autenticazione. Un modo di impedire questo è impostando un firewall.

```
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw allow 12345
Rule added
msfadmin@metasploitable:~$ sudo ufw allow from 192.168.1.8
Rule added
msfadmin@metasploitable:~$ sudo ufw reload
```

***Vulnerabilità Unix Operating System Unsupported Version Detection:*** Nessus ci avvisa che la versione di Unix non è più supportata, di conseguenza potrebbe non rilevare delle minacce. Quindi conviene aggiornare il sistema, usando i comandi sudo apt-get update/upgrade.