- **Primo scan**

13	12	35	8	163
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Aug 5 05:05:51 2022
End time: Fri Aug 5 05:30:36 2022

Host Information

DNS Name: ISLAM-KHALIL.station
Netbios Name: METASPLOITABLE
IP: 192.168.1.5
MAC Address: 08:00:27:39:6D:CD
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

- **Secondo Scan**

4	8	12	5	114
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Aug 5 10:01:01 2022
End time: Fri Aug 5 10:20:00 2022

Host Information

DNS Name: ISLAM-KHALIL.station
Netbios Name: METASPLOITABLE
IP: 192.168.1.5
MAC Address: 08:00:27:39:6D:CD
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

1- **VNC Password** → Risolta

Gravita	Punto	Plugin	Nome
CRITICAL	**10.0**	**61708**	VNC Server 'password' Password

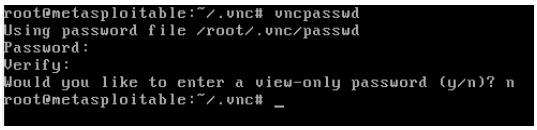
Descrizione
Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione
Proteggi il servizio VNC con una **password complessa**.

Porta	Hosts
5900 / tcp / vnc	192.168.1.5

Soluzione:
Su Metasploitable ho aperto il percorso del file della password vnc tramite root al seguente percorso /root/.vnc/passwd
nano passwd → password **cifrato**

Per cambiare la password ho eseguito il comando: **vncpasswd**
** la password deve essere di 6-8 caratteri
Ho cambiato la password a: **P@s$w0rd**



nano passwd → La nuova cifratura di password

2- Backdoor → Risolta

Gravita	Punto	Plugin	Nome
CRITICAL	**9.8**	**51988**	Bind Shell Backdoor Detection

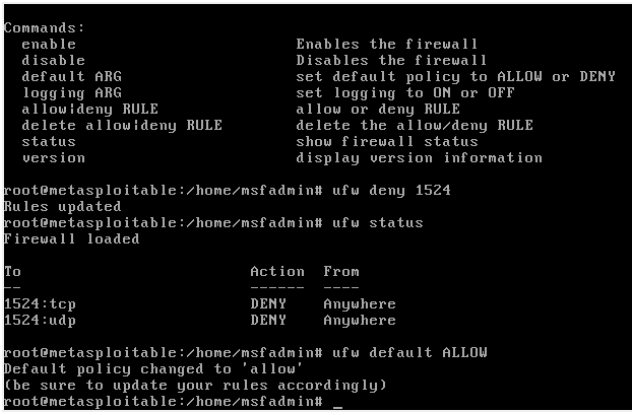
Descrizione
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Porta	Hosts
1524 / tcp / wild_shell	192.168.1.5

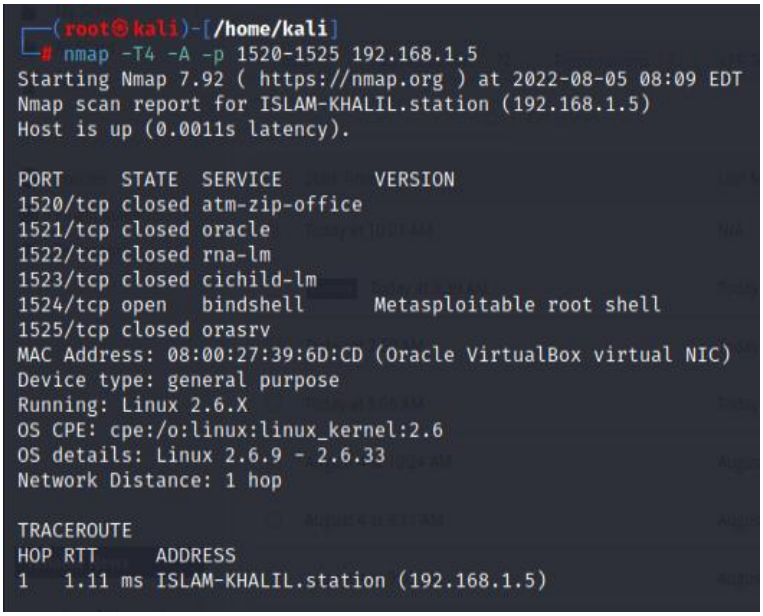
Ho scoperto che esiste una backdoor sulla porta 1524, quindi ho aperto Metasploitable come root,

- Ho abilitato il firewall con il consenso predefinito con commando: **ufw default ALLOW**
- Ho chiuso la porta 1524 con il comando: **ufw deny 1524**.

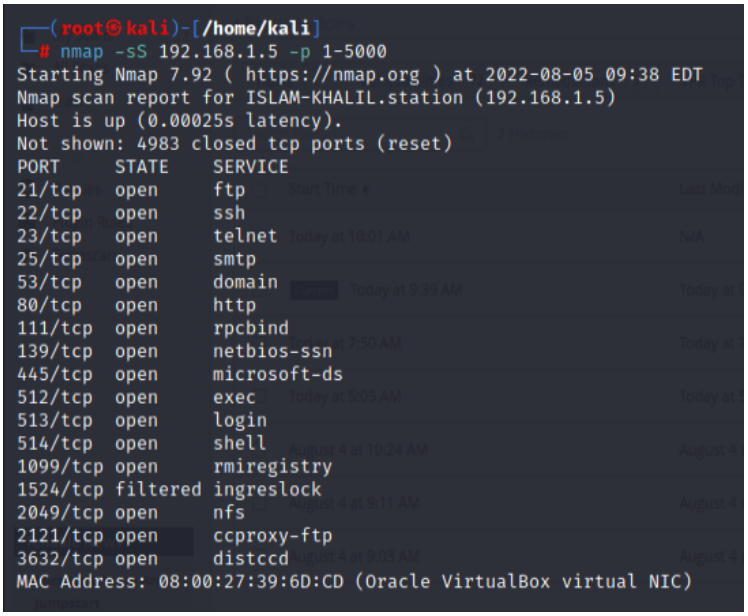


Per confermare le configurazioni su kali provato a fare scansione nmap

1. Prima di attivare firewall



2. Dopo attivare il firwall



Dall'immagine si vede che dopo attivare il firewall la porta 1524 risulta filtered(Filtrata)

3- NFS → Risolta

Gravita	Punto	Plugin	Nome
CRITICAL	**10.0**	**11356**	NFS Exported Share Information Disclosure

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttarlo per leggere (e possibilmente scrivere) file sull'host remoto.

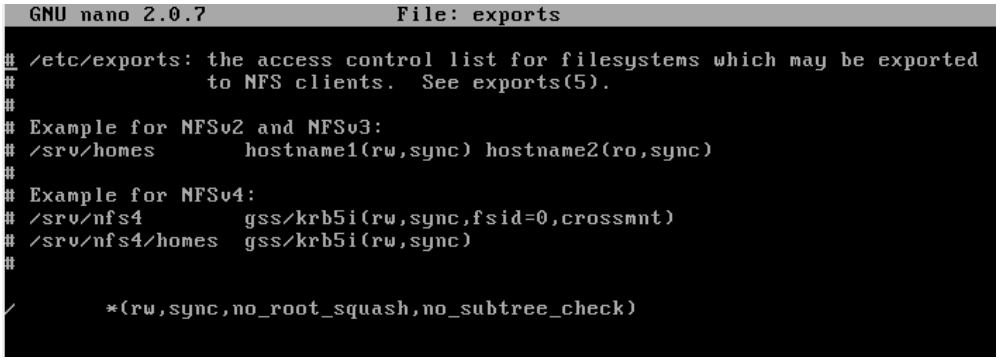
Soluzione

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Porta	Hosts
2049 / udp / rpc-nfs	192.168.1.5

- La configurazione predefinita

  Il path



- La configurazione modificata