

- **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                           |
|-----------------|-------------|--------------|--------------------------------|
| <b>CRITICAL</b> | <b>10.0</b> | <b>61708</b> | 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**

```
GNU nano 2.0.7      File: passwd
^@<^rz^TX
```

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**

```
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# _
```

nano passwd → La nuova cifratura di password

```
GNU nano 2.0.7      File: passwd
^Y^k^R^G:
```

## 2- Backdoor → Risolta

| Gravita         | Punto      | Plugin       | Nome                          |
|-----------------|------------|--------------|-------------------------------|
| <b>CRITICAL</b> | <b>9.8</b> | <b>51988</b> | 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 comando: **ufw default ALLOW**
- Ho chiuso la porta 1524 con il comando: **ufw deny 1524**.

```
Commands:
  enable           Enables the firewall
  disable          Disables the firewall
  default ARG      set default policy to ALLOW or DENY
  logging ARG      set logging to ON or OFF
  allow/deny RULE  allow or deny RULE
  delete allow/deny RULE  delete the allow/deny RULE
  status           show firewall status
  version          display version information

root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To Action From
-----
1524/tcp DENY Anywhere
1524/udp DENY Anywhere

root@metasploitable:/home/msfadmin# ufw default ALLOW
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin#
```

Per confermare le configurazioni su kali provato a fare scansione nmap

### 1. Prima di attivare firewall

```
(root@kali)-[/home/kali]
# nmap -T4 -A -p 1520-1525 192.168.1.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 08:09 EDT
Nmap scan report for ISLAM-KHALIL.station (192.168.1.5)
Host is up (0.0011s latency).

PORT      STATE SERVICE      VERSION
1520/tcp  closed atm-zip-office
1521/tcp  closed oracle
1522/tcp  closed rna-lm
1523/tcp  closed cichild-lm
1524/tcp  open  bindshell    Metasploitable root shell
1525/tcp  closed orasrv
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 1.11 ms ISLAM-KHALIL.station (192.168.1.5)
```

### 2. Dopo attivare il firewall

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.1.5 -p 1-5000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 09:38 EDT
Nmap scan report for ISLAM-KHALIL.station (192.168.1.5)
Host is up (0.0025s latency).
Not shown: 4983 closed tcp ports (reset)

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3632/tcp  open  distccd
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)
```

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

### 3- NFS → Risolta

| Gravita         | Punto       | Plugin       | Nome                                      |
|-----------------|-------------|--------------|---|
| <b>CRITICAL</b> | <b>10.0</b> | <b>11356</b> | 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

```
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)
#
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

- La configurazione modificata

```
GNU nano 2.0.7      File: 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    192.168.1.5(rw,sync,no_subtree_check)
```