



CONSEGNA S5/L3

N M A P



Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
 - Syn Scan.
 - TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
 - Version detection.
- E la seguente sul target Windows 7:
- OS fingerprint.

Nell'esercitazione di oggi ci viene richiesto di utilizzare nmap per andare ad effettuare delle scansioni sui target Metasploitable e windows 7, per prima cosa ci viene richiesto di identificare il sistema operativo del nostro bersaglio, per fare questo andremo ad utilizzare da nmap su terminali kali lo switch -O e lo switch -sS, tramite questi switch posso effettuare una scansione che mi restituisca se il sistema operativo in uso sull'indirizzo ip target, ma non andando a creare un traffico di rete intenso, in quanto con lo switch -sS andrò ad inviare un pacchetto SYN, ma qualunque sia la risposta del server non andremo a stabilire una connessione TCP, ovvero il completamento della stretta di mano a tre vie.

```
(root㉿kali)-[~/home/kali]
# nmap -sS -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 10:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.00040s latency).
Not shown: 977 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  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:40:5F:3D (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
```

```
(root㉿kali)-[~/home/kali]
└─# nmap -sV -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 10:19 EST
Nmap scan report for 192.168.50.101
Host is up (0.00070s latency).

Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:40:5F:3D (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.74 seconds
```

In questo secondo esempio possiamo notare l'utilizzo degli switch `-sV`, il quale mi permette di recuperare le informazioni esposte da un determinato software di un servizio abilitato attraverso il banner, e `-sT`, il quale invece mi permette di andare a stabilire una connessione TCP completa andando di fatto a creare un canale, quindi completando la stretta di mano a tre vie.

Nell'ultimo esempio ci viene richiesto di eseguire un test per vedere che versione del sistema operativo si trova su un altro host, in questo caso una macchina Windows 7, a differenza di Metasploitable il firewall di Windows proverà a ostacolare i nostri tentativi di scansione, per evitare problemi potremmo disattivare il firewall su windows, infatti come possiamo evincere dall'immagine sotto riportata sono presenti meno informazioni rispetto a prima.

```
(root㉿kali)-[~/home/kali]
# nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 10:33 EST
Nmap scan report for 192.168.50.102
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:87:45:EB (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8 .1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 Vo IP module, VMware Player virtual NAT device
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.52 seconds
```



THANK YOU