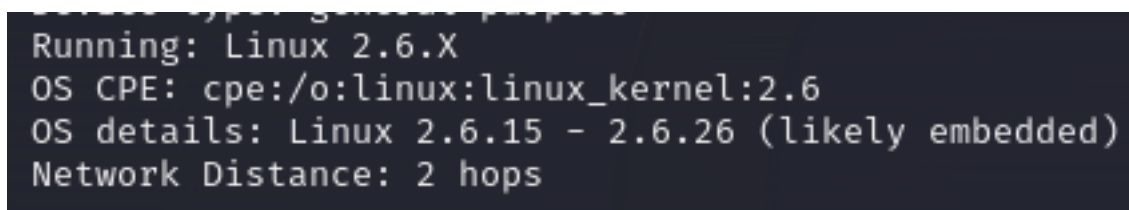


CONSEGNA 21 FEBBRAIO S5L3

Lo scopo di oggi è quello di eseguire delle scansioni sui target Metasploitable e Windows 7, usando Nmap. L'obiettivo è quello di raccogliere informazioni, quali l'indirizzo IP, il sistema operativo, le porte aperte e i servizi in ascolto con versione. Oltretutto ci viene anche chiesto quali sono i risultati ottenuti dalla scansione di Windows 7, che avendo il firewall attivo, presenta una serie di ovvie problematiche.

Cominciamo sul target Metasploitable, per prima cosa andiamo ad effettuare lo Scan OS fingerprint, tramite il flag -O.

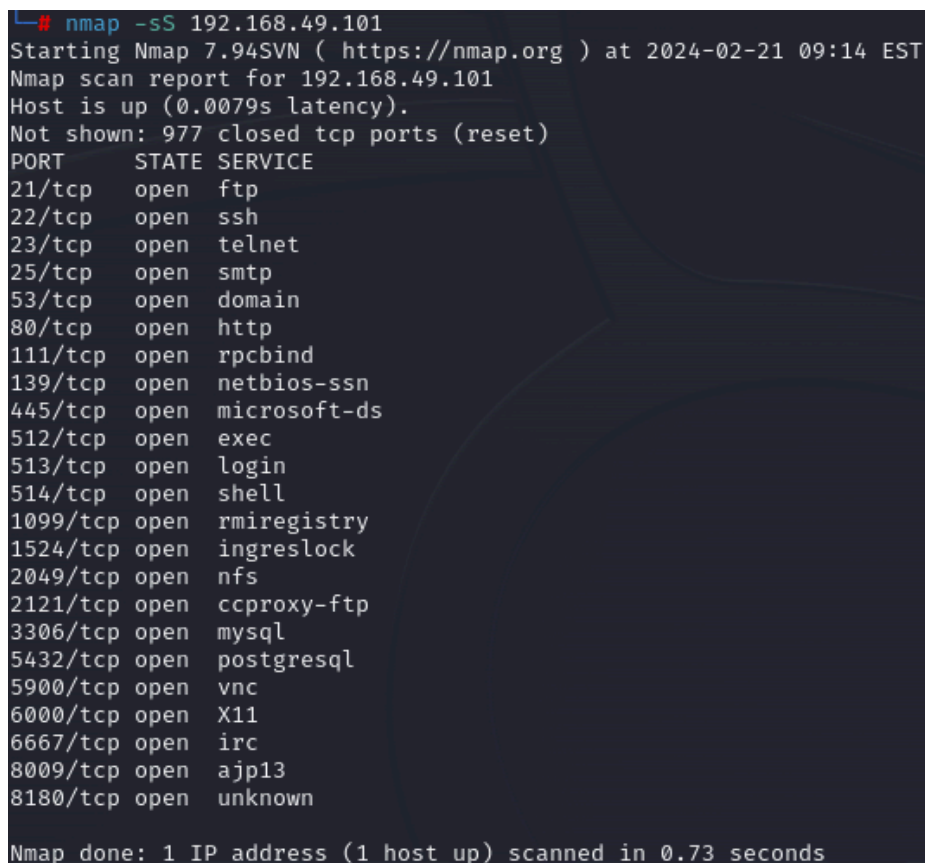


```
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
```

Fig. 1

Come in figura 1, Nmap ci dice che il sistema operativo è Linux, per la versione ci da un range che va da 2.6.15 - 2.6.26: questa incertezza è data dal fatto che il flag -O non è riuscito a scoprire la versione esatta del sistema operativo, quindi ci da un range di possibilità che possiamo ritenere accettabile per i nostri scopi.

Il secondo scan che andremo ad effettuare è il Syn scan, attraverso il flag -sS.



```
└─$ nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:14 EST
Nmap scan report for 192.168.49.101
Host is up (0.0079s 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

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

Fig.2

Come in Fig.2 , il Syn scan ci ha dato tutte le porte TCP aperte, in 0.73 secondi. Il Syn scan è un metodo poco invasivo, in quanto non conclude il 3 way handshake: appurato che la porta è aperta chiude la comunicazione. Se invece andiamo ad usare il flag -sT, il metodo usato sarà molto più invasivo, visto che Nmap andrà a completare tutti i passaggi del 3 day handshake, stabilendo di fatto un canale.

```
└─# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:15 EST
Nmap scan report for 192.168.49.101
Host is up (0.040s latency).
Not shown: 977 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

Fig.3

Come possiamo notare in Fig.3 l'unica differenza tra i due metodi è data dal tempo: il flag -sT richiede meno tempo per la scansione delle porte.

L'ultimo metodo che andremo ad usare su Meta è il Version Detestino, che oltre a dirci quali porte sono in ascolto, rileva i servizi sulla porta stessa. Lo usiamo tramite il flag -sV. Come vediamo in Fig.4 la moltitudine dei servizi attivi ci apre una panoramica su eventuali vulnerabilità, una tra queste si trova sulla porta 21 nel servizio vsftpd 2.3.34.

```

└─# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:25 EST
Nmap scan report for 192.168.49.101
Host is up (0.032s latency).
Not shown: 977 closed tcp ports (reset)
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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.78 seconds

```

Fig.4

Per quanto riguarda il secondo target, Windows 7, andare ad effettuare uno scan OS fingerprint risulta ostico, visto che il target ha un firewall impostato su public network, quindi con molte restrizioni. Ho effettuato molte prove, ad esempio provando a lavorare con il time template, diminuendo il tempo che passa tra l'invio di richieste successive (tramite lo switch T0 / T1), ma con scarsi risultati date le lunghissime tempistiche di attesa. Per ovviare a questo ho provato ad indirizzare la mia ricerca su un'unica porta, ma sempre con scarsi risultati. Un'altro metodo che ho provato, ma sempre con scarsi risultati, è quello di configurare Nmap per inviare pacchetti da una porta nota, come la 80. Generalmente gli IPS/IDP non bloccano i pacchetti provenienti da porte note. Come vediamo in Fig.5, Nmap non riesce a trovare il sistema operativo perché trova troppi fingerprint match. Ne concludo che bisogna ricercare altri metodi o script per cercare di aggirare il firewall.

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.102 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:24 EST
Nmap scan report for 192.168.50.102
Host is up (0.0010s 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:ED:C8:3E (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 24.25 seconds
```

Fig.5