Alaimo Alessandro
23/11/2022

Scansioni con NMAP

Per poter iniziare l'esercizio di oggi, andiamo a configurare i nostri dispositivi in modo tale da essere nella stessa rete, 192.168.50.0, nel seguente modo:

- Kali: 192.168.50.100
- Meta: 192.168.50.101
- Windows7: 192.168.50.102

Fatto ciò iniziamo con le scansioni, tra cui:

- Finger Print Meta:

```
nmap -oN finger_print_meta -f --script smb-os-discovery 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00013s 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:D2:25:45 (Oracle VirtualBox virtual NIC)
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-23T10:41:26-05:00
```

- Syn scan Meta:

```
nmap -oN Syn_meta -sS 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00013s 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:D2:25:45 (Oracle VirtualBox virtual NIC)
```

- TCP scan Meta:

```
nmap -oN TCP_meta -sT 192.168.50.101
Nmap scan report for 192.168.50.101
```

```
Host is up (0.00019s 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
MAC Address: 08:00:27:D2:25:45 (Oracle VirtualBox virtual NIC)
```

- Version scan Meta:

```
nmap -oN Version_meta -sV 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.000073s 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      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?
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:D2:25:45 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:
metasploitable.localdomain,irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel
```

Possiamo notare che la differenza tra TCP e SYN scan sta nel tipo di connessione, nel primo la connessione viene rifiutata mentre l'altro mando una flag RST per terminare il Three-Way Handshake al secondo passaggio. Mentre L'ultimo scan effettuato è nettamente più aggressivo rispetto al TCP scan, riportandoci però tutti i dati delle porte e del target.

- Finger Print Windows:

```
nmap -oN finger_print_windows7 --script smb-os-discovery
192.168.50.102
Nmap scan report for 192.168.50.102
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:88:79:3D (Oracle VirtualBox virtual NIC)
```

Come possiamo vedere il Firewall ci blocca il tentativo di connessione segnandoci tutte le porte come "filtered". Le uniche opzioni per bypassare il Firewall sono:

- Tirandolo giù tramite DoS
- Indurre l'utente a disabilitarlo
- Verificare se impostando il Timing a -T1, riesca ad eludere il firewall. Questo metodo richiede tempo eccessivo.