lunedì 16 settembre 2024 19:44

Traccia:

Si richiede allo studente di effettuare le scansioni dell'esercizio precedente con Nmap sul target Windows 7.

Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report.

Os Fingerprint

```
C:\home\kali> sudo nmap -Pn -O --osscan-limit 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 09:10 EDT
Nmap scan report for 192.168.50.103
Host is up (0.0070s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:C0:D5:74 (Oracle VirtualBox virtual NIC)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.22 seconds
```

Descrizione del comando:

Nmap: Viene utilizzato per la scanzione delle reti, rilevamento degli host, porte aperte e per determinare informazioni sui sistemi

-Pn: Disabilita il Ping dell'host, in questo caso nmap non tenterà di verificare se l'host è attivo tramite ICMP o altri metodi di ping prima di procedere con la scansione. Comando utle nel caso l'host potrebbe non rispondere al ping (ad esempio a causa dei farewall), ma è comunque raggiungibile e ha porte aperte.

-O: Abilita il rilevamento del sistema operativo basandosi sulle caratteristiche dei pacchetti di rete, come risposte TCP/IP che verranno poi confrontate con un database di impronte digitali note per identificare l'OS

--ooscan-limit: Limita il tentativo di rilevamento solo agli host che hanno delle porte aperte, evitando di cercare di identificare l'OS su host che non hanno porte accessibili, migliorando l'efficienza della scansione.

Syn Scan e Version detection

```
C:\home\kali> sudo nmap -sV -sS 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 09:11 EDT
Nmap scan report for 192.168.50.103
Host is up (0.0046s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:C0:D5:74 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.13 seconds
```

Descrizione del comando:

-sV: Conosciuta come Version detection, è a tutti gli effetti una scansione TCP connect con l'aggiunta di specifici test per la rilevazione dei servizi in ascolto su una porta. Così come la scansione TCP connect è piuttosto facile da rilevare in quanto genera molto traffico di rete.

-sS: Anche detta Stealth scan o half-open non completa il processo three-way handshake come la scanzione TPC ma, appurato che la porta è aperta chiude la comunicazione restituendo un RST. Questa è un tipo di scansione più veloce e meno invasiva rispetto alla TCP.

Tpc connect e Version detection

```
C:\home\kali> sudo nmap -sV -sT 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 09:13 EDT
Nmap scan report for 192.168.50.103
Host is up (0.0035s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:C0:D5:74 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.73 seconds
```

Descrizione del comando:

-sT: Esegue una scanzione full TCP connect utilizzando il metodo three-way handshake e tenta di stabilire una connessione su ciascuna delle porte specificate. Rispetto alla SYN è più lenta e più invasiva, quindi più facilmente rilevabile.

Di seguito alle scansioni effettuate sul nostro target (Metasploitable) abbiamo appreso:

- Indirizzo IP: 192.168.50.103
- Sistema Operativo: Windows 7
- Porte Aperte con Servizi in Ascolto e relative versioni:
  135/tcp:
  - **Servizio**: msrpc

- **Versione**: Microsoft Windows RPC

139/tcp:

- **Servizio**: netbios-ssn
- **Versione**: Microsoft Windows netbios-ssn

445/tcp:

- **Servizio**: microsoft-ds
- **Versione**: Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

49152/tcp:

- **Servizio**: msrpc
- **Versione**: Microsoft Windows RPC

49153/tcp:

- **Servizio**: msrpc
- **Versione**: Microsoft Windows RPC

49154/tcp:

- **Servizio**: msrpc
- **Versione**: Microsoft Windows RPC

49155/tcp:

- **Servizio**: msrpc
- **Versione**: Microsoft Windows RPC

49156/tcp:

- **Servizio**: msrpc
- **Versione**: Microsoft Windows RPC

```
C:\home\kali> sudo nmap -sV -sS -T3 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 13:41 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0095s 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:EF:90:CD (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linu
x_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.17 seconds
```