lunedì 16 settembre 2024 19:44

Traccia: Tecniche di scansione con Nmap
Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable** (target e attaccante devono essere su due reti diverse):

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

A valle delle scansioni, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

Os Fingerprint

```
C:\home\kali> sudo nmap -Pn -O --osscan-limit 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:18 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0086s 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
Device type: general purpose
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.11 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 -T5 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:20 EDT
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 13:23 (0:00:14 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.044s 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  ccproxy-ftp?
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  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.18 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 -T5 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 10:53 EDT
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 10:55 (0:00:05 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 10:55 (0:00:07 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.024s latency).
Not shown: 978 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?
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  ccproxy-ftp?
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
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.04 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: 192.168.50.101
- Sistema Operativo: Linux 2.6.X un range che va tra 2.6.15 a 2.6.26
- Porte Aperte con Servizi in Ascolto e relative versioni:
  21/tcp (ftp) **Versione:** vsftpd 2.3.4
  22/tcp (ssh) **Versione:** OpenSSH 4.7p1 Debian 8ubuntu1
  23/tcp (telnet) **Versione:** Linux telnetd
  25/tcp (smtp) **Versione**: Postfix smtpd
  53/tcp (domain) **Versione:** ISC BIND 9.4.2
  80/tcp (http) **Versione**: Apache httpd 2.2.8 (Ubuntu) DAV/2
  111/tcp (rpcbind) **Versione**: 2 (RPC #100000)
  139/tcp (netbios-ssn) **Versione:** Samba smbd 3.X
  445/tcp (microsoft-ds) **Versione:** Samba smbd 3.X
  512/tcp (exec) Versioni: netkit-rsh rexecd
  513/tcp (login)
  514/tcp (shell) **Versioni:** Netkit rshd
  1099/tcp (java-rmi) **Versione:** GNU Classpath grmiregistry
  1524/tcp (bindshell) **Versione:** Metasploitable root shell
  2049/tcp (nfs) **Versione:** 2-4 (RPC #100003)
  2121/tcp (ccproxy-ftp)
  3306/tcp (mysql) **Versione:** MySQL 5.0.51a-3ubuntu5
  5432/tcp (postgresql) **Versione**: PostgreSQL DB 8.3.0 - 8.3.7
  5900/tcp (vnc) **Versione:** VNC (protocol 3.3)
  6000/tcp (X11)

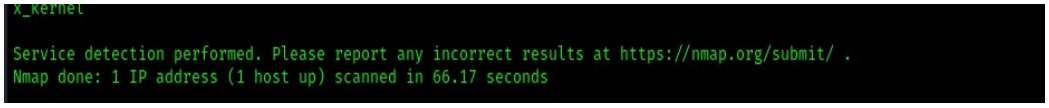
6667/tcp (irc) V**ersione:** UnrealIRCd
8009/tcp (ajp13) **Versione:** Apache Jserv (protocol v1.3)
8180/tcp (unknown**)**

Facoltativo: Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete.
Estendere il report con le nuove informazioni ed evidenziare le differenze.

```
C:\home\kali> sudo nmap -Pn -O --osscan-limit 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 13:26 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0071s latency).
Not shown: 978 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
8180/tcp open  unknown
MAC Address: 08:00:27:EF:90: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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds
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
```



Qui sopra sono riportate due scansioni con target sulla stessa rete: l'OS Fingerprint e il SYN scan. Andandole a confrontare con le immagini sopra possiamo notare che le uniche differenze sono la presenza del **MAC Address 08:00:27:EF:90:CD** che appare scritto solo quando le due macchine si trovano sulla stessa rete e la distanza.
Come possiamo leggere dalle immagini abbiamo:
Network Distance: 1 hope - quando kali e meta si trovano sulla stessa rete
Network Distance: 2 hope - quando kali e meta si trovano su reti diverse (avendo PfSense di mezzo che fornisce la rete alle due macchie)