MATTIA PASTORELLI

SCANSIONE DEI SERVIZI CON NMAP

1

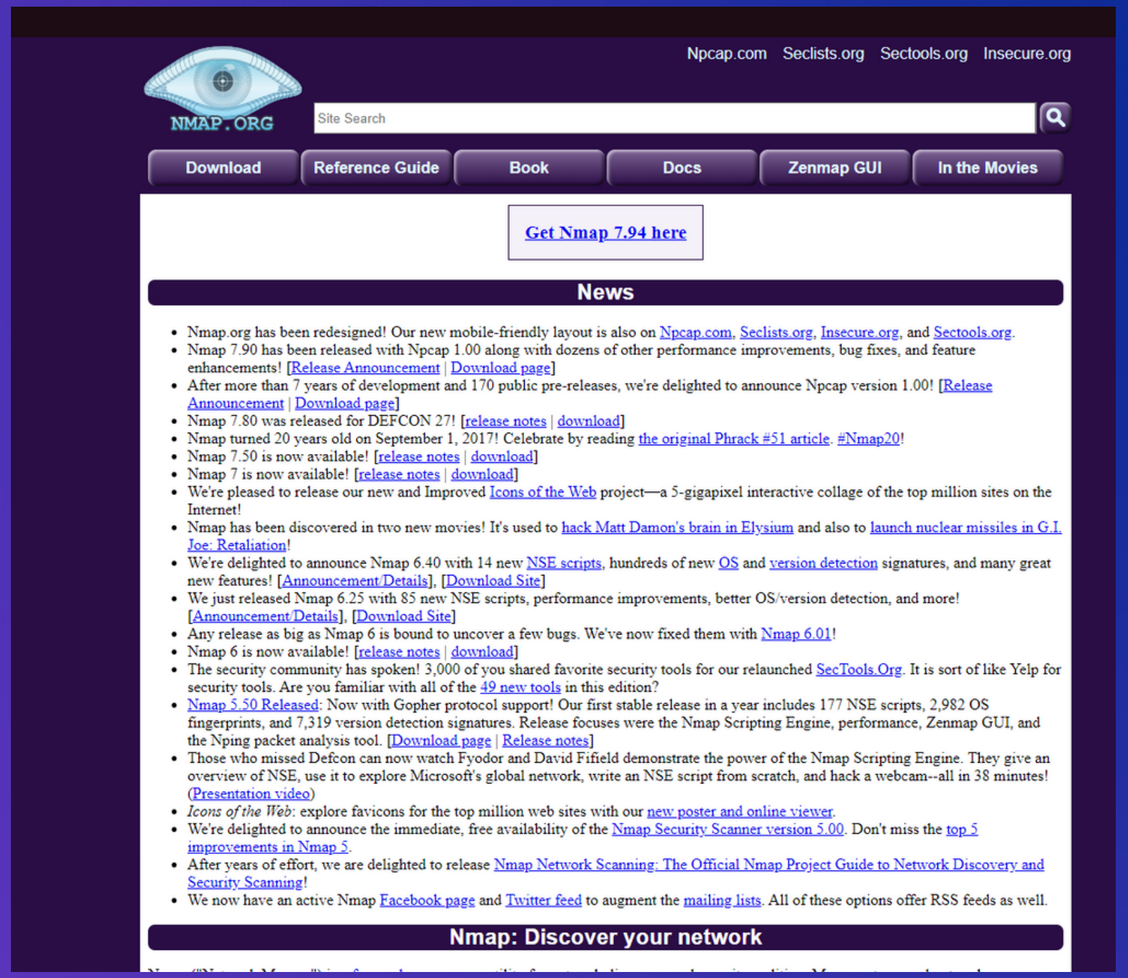
COMANDA:

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.

COS'È NMAP?

Nmap, acronimo di "Network Mapper", è uno strumento di scansione di rete open source utilizzato per esaminare e mappare dispositivi su una rete, rilevendo porte aperte, servizi in esecuzione, e altre informazioni rilevanti sulla sicurezza



OS FINGER PRINT

Un OS fingerprint, o "fingerprinting" dell'OS, si riferisce al processo di identificazione del sistema operativo in esecuzione su un determinato host in una rete.

In figura possiamo vedere il comando nmap (ip) --script smb-os-discovery, il quale effettua uno script dell'ip al fine di individuare le porte presenti sulla rete e l'OS dell'Host analizzato (in questo caso Meta)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.100 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:46 EST
Nmap scan report for 192.168.50.100
Host is up (0.012s 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: 08:00:27:7B:7F:8E (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: 2024-01-10T09:42:34-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.77 seconds
```

SYN SCAN

Lo "SYN SCAN" è una tecnica di scansione di porte attraverso l'invio di un solo pacchetto, il quale non comporta il completamento della 3 way - handshake (mancano SYN/ACK e ACK).

Viene utilizzato principalmente per analizzare le porte disponibili e aperte su un determinato indirizzo IP

Questo scan è meno intrusivo rispetto ad una scansione completa, di conseguenza è più rapida e fa "meno rumore"

Comando : nmap -sS (IP destinatario META)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:45 EST
Nmap scan report for 192.168.50.100
Host is up (0.0017s 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: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

TCP CONNECT

Il TCP CONNECT è sempre una scansione di porte utilizzata per verificare l'apertura o la chiusura di porte su un host, ma a differenza dalla SYN SCAN, questa completa la 3 way - handshake

Questa scansione è più completa ed utile se stiamo effettuando un controllo di rete o un PT, per quanto riguarda un attaccante questa è una soluzione poco adottata perché genera parecchio “rumore”.

Comando: nmap -sT (IP destinatario META)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:58 EST
Nmap scan report for 192.168.50.100
Host is up (0.0031s 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: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

VERSION DETECTION

La VERSION DETECTION o anche detto “Banner Grabbing”, consiste nel recupero delle informazioni esposte da un determinato software o demone di un servizio (Es: Versione e nome del softwere/servizio)

Può essere utilizzato per verificare eventuali vulnerabilità su alcuni servizi.

Comando: nmap -sV (IP destinatario META)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 09:19 EST
Nmap scan report for 192.168.50.100
Host is up (0.00051s 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  unknown
MAC Address: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

OS FINGER PRINT

WINDOWS 7

Questa volta è stato effettuato L'OS fingerprinting sulla macchina di Windows 7 al fine di scoprire la versione dell'OS.

E' stato possibile disattivando il Firewall di Windows. Altrimenti non ci sarebbe stato nessun riscontro e nessun risultato.

Possiamo notare che a differenza di Meta, windows non mostra tutte le porte (ES. 21,22 ecc..), questo può essere successo per diversi motivi:
1) Diversità di sistema operativo
2) Il firewall di windows blocca determinati accessi, bisogna inserire una regola all'interno che lasci passare il segnale da Kali verso windows. Quindi Problemi di Autorizzazione e Sicurezza per firewall e scansione porte

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:53 EST
Nmap scan report for 192.168.50.102
Host is up (0.00097s latency).
Not shown: 991 closed tcp ports (reset)
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
49157/tcp open  unknown
MAC Address: 08:00:27:DA:A2:FD (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2024-01-10T14:53:15+01:00
```