Esercizio Day 4

Information Gathering

Per l'esercizio di oggi ci viene chiesto di usare uno degli strumenti visti a lezione, per trovare informazioni sulla macchina metasploitable che abbiamo nel nostro laboratorio virtuale.

In questo caso utilizzerò NMAP però come tool di information gathering.

Cos'è NMAP ?
Come possiamo leggere dal sito ufficiale : https://nmap.org/ , nmap è un'utility utilizzata per effettuare network discovery e security auditing tra le altre cose.
E' molto utile inloltre per enumerare porte e servizi, grazie ai diversi tipi di scan che può effettuare.

Sintassi :

```
nmap <scan types> <options> <target>
```

Stati delle porte:

Ci sono sei possibili stati per le porte che possiamo ottenere.

Aperta : indica che la connessione con la porta scansita è stata stabilita.

Chiusa : Quando una porta è chiusa il protocollo TCP riceve come risposta il pacchetto RST (Reset).

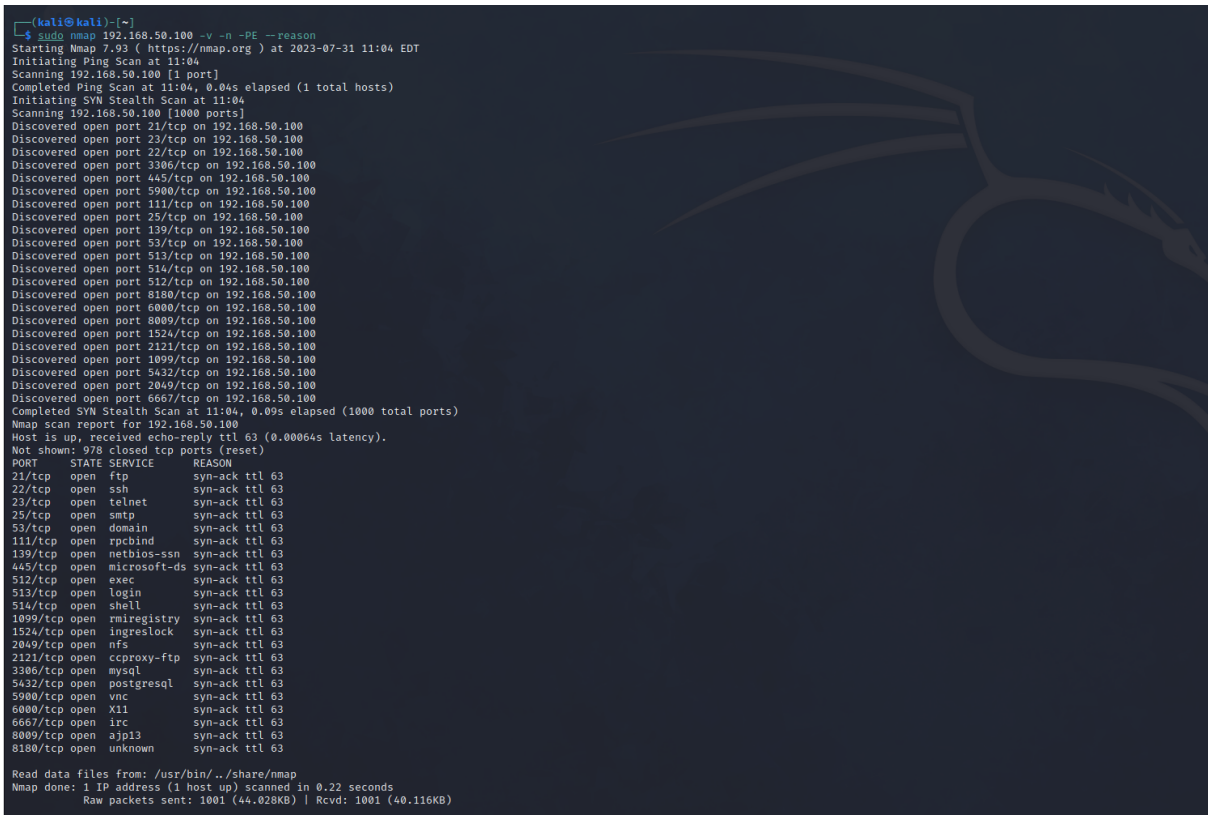
Filtrata : Nmap non può identificare lo stato della porta.

Non filtrata : questo stato si verifica solo quando lo scan TCP-ACK viene effettuato, tuttavia lo scan non riesce a determinare se la porta sia accessibile o meno.

Aperta|Filtrata : questo accade quando non si ottiene una risposta da una porta specifica. Può indicare la presenza di un firewall a protezione della porta.

Chiusa|Filtrata : risultato che si può ottenere soltanto tramite un Idle Scan.

Tramite il test sulle porte del target NMAP ci fornisce quindi alcune informazioni utili.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.100 -v -n -PE --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 11:04 EDT
Initiating Ping Scan at 11:04
Scanning 192.168.50.100 [1 port]
Completed Ping Scan at 11:04, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:04
Scanning 192.168.50.100 [1000 ports]
Discovered open port 21/tcp on 192.168.50.100
Discovered open port 23/tcp on 192.168.50.100
Discovered open port 22/tcp on 192.168.50.100
Discovered open port 3306/tcp on 192.168.50.100
Discovered open port 445/tcp on 192.168.50.100
Discovered open port 5900/tcp on 192.168.50.100
Discovered open port 111/tcp on 192.168.50.100
Discovered open port 25/tcp on 192.168.50.100
Discovered open port 139/tcp on 192.168.50.100
Discovered open port 53/tcp on 192.168.50.100
Discovered open port 513/tcp on 192.168.50.100
Discovered open port 514/tcp on 192.168.50.100
Discovered open port 512/tcp on 192.168.50.100
Discovered open port 8180/tcp on 192.168.50.100
Discovered open port 6000/tcp on 192.168.50.100
Discovered open port 8009/tcp on 192.168.50.100
Discovered open port 1524/tcp on 192.168.50.100
Discovered open port 2121/tcp on 192.168.50.100
Discovered open port 1099/tcp on 192.168.50.100
Discovered open port 5432/tcp on 192.168.50.100
Discovered open port 2049/tcp on 192.168.50.100
Discovered open port 6667/tcp on 192.168.50.100
Completed SYN Stealth Scan at 11:04, 0.09s elapsed (1000 total ports)
Nmap scan report for 192.168.50.100
Host is up, received echo-reply ttl 63 (0.00064s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 63
22/tcp   open  ssh          syn-ack ttl 63
23/tcp   open  telnet       syn-ack ttl 63
25/tcp   open  smtp         syn-ack ttl 63
53/tcp   open  domain       syn-ack ttl 63
111/tcp  open  rpcbind      syn-ack ttl 63
139/tcp  open  netbios-ssn  syn-ack ttl 63
445/tcp  open  microsoft-ds syn-ack ttl 63
512/tcp  open  exec         syn-ack ttl 63
513/tcp  open  login        syn-ack ttl 63
514/tcp  open  shell        syn-ack ttl 63
1099/tcp open  rmiregistry  syn-ack ttl 63
1524/tcp open  ingreslock   syn-ack ttl 63
2049/tcp open  nfs          syn-ack ttl 63
2121/tcp open  ccproxy-ftp  syn-ack ttl 63
3306/tcp open  mysql        syn-ack ttl 63
5432/tcp open  postgresql   syn-ack ttl 63
5900/tcp open  vnc          syn-ack ttl 63
6000/tcp open  X11          syn-ack ttl 63
6667/tcp open  irc          syn-ack ttl 63
8009/tcp open  ajp13        syn-ack ttl 63
8180/tcp open  unknown      syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.116KB)
```

Spiegazione del comando :

sudo : non sempre necessario, ma quando si effettuano alcune richieste nmap ha bisogno dei privilegi di root.

nmap 192.168.50.100 : richiamiamo nmap per eseguire una scansione sull'ip target

switch eventuali :

Di seguito elencati gli switch (opzioni) utilizzati nell'esempio.
-v : Verbose mode -> si utilizza per avere informazioni dettagliate nell'output del comando

-n : Indica a Nmap di non effettuare mai una risoluzione inversa del nome mediante DNS sugli indirizzi IP rilevati. Poiché il DNS è spesso lento anche con il risolutore parallelo integrato di Nmap, questa opzione rende l'intero processo di scansione più veloce.

-PE : usato per ricevere un ICMP echo, timestamp, and netmask request discovery probes

–reason : mostra il perché lo stato della porta è in un particolar modo.

Un altro switch molto utile per esempio è il **-O :**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.100 -O
[sudo] password di kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 11:30 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00066s 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
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 1.71 seconds
```

Come possiamo vedere infatti l'opzione -O permette a Nmap di investigare sul sistema operativo della macchina target.

*Se si usa lo switch **-A** invece si effettua una scansione più aggressiva, il che può addirittura mostrarci come nella schermata successiva, tra le altre cose, l'hostname del target.*

```
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-07-31T11:33:44-04:00

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
1   0.33 ms 192.168.1.1
2   0.71 ms 192.168.50.100

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.92 seconds
```

Considerazioni :

nel corso delle diverse scansioni abbiamo ottenuto diverse informazioni importanti. Partendo per esempio dalle diverse porte aperte, 22 .
Grazie ai vari switch ci vengono fornite altre importanti informazioni quali il servizio, il protocollo con le quali sono state testate, fino ad arrrivare all sistema operativo e l'hostname del target.
E' buona prassi chiudere le porte non utilizzate riducendo così la superficie d'attacco, diminuendo al minimo la possibilità di subire una violazione da parte di malintenzionati.