Simulazione fase di raccolta

Parte 2

Sommario

Traccia esercizio principale

https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

Traccia esercizio facoltativo

Utilizzare tutti i tool proposti ed approfondire lo studio dei metodi di evasione firewall con Nmap:

https://nmap.org/book/firewall-subversion.html

https://nmap.org/book/man-bypass-firewalls-ids.html

Configurazione ai fini dell'esercizio

Si è configurato due reti nel laboratorio virtuale, collegate tra loro da pfSense. Il collegamento tra Kali Linux e Metasploitable2 sarà pertanto tra due reti diverse. Per quanto riguarda la configurazione vedasi report M3 W9 D5 su pfSense.

A metà esercizio, a causa dei limiti imposti da pfSense, si è riconfigurato Metasploitable2 sulla stessa rete di Kali Linux.

Svolgimento esercizio principale

Punto di partenza

Individuare la rete a cui si è connessi, se la macchina target si trovi nella stessa rete. Ai fini dell'esercizio, l'autore conosce già l'indirizzo IP target, tuttavia si fa una simulazione come se non si conoscesse l'indirizzo IP.

Lanciare il comando **ip a** su terminale Kali.

```
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:88:c5:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 4184sec preferred_lft 4184sec
    inet6 fe80::aadf:3f4f:33a0:c954/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Scansione rete ed individuazione IP target

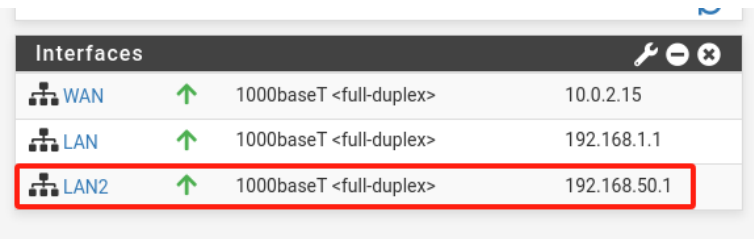
Dall'indirizzo IP 192.168.1.101/24 si deduce che il gateway è 192.168.1.1 e pertanto si può eseguire una scansione della rete 192.168.1.1 con il comando **sudo nmap -A 192.168.1.0/24** o in alternativa utilizzare netdiscover **netdiscover -r 192.168.1.0/24**

```
|   http/1.0
|_  http/0.9
| ssl-cert: Subject: commonName=pfSense-66e2d3e9b1f3c/organizationName=pfSense GUI default Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-66e2d3e9b1f3c
| Not valid before: 2024-09-12T11:43:37
|_Not valid after:  2025-10-15T11:43:37
MAC Address: 08:00:27:35:4E:1A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.11 ms pfSense.home.arpa (192.168.1.1)

Nmap scan report for 192.168.1.101
Host is up (0.000036s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

```
Currently scanning: 192.168.1.0/24   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.1.1     08:00:27:35:4e:1a      1      60  PCS Systemtechnik GmbH
```

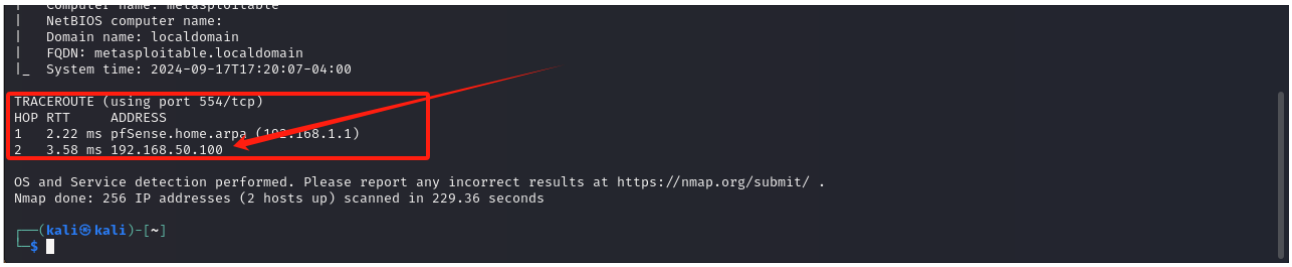
Non ci sono informazioni utili rilevanti, tuttavia tramite questa scansione si scopre che pfSense è il gateway.

Pertanto si può procedere alla pagina di configurazione di pfSense per scoprire quali reti sono state configurare e/o collegate. Sempre ai fini didattici dell'esercizio, si è a conoscenza delle credenziali di accesso alla pagina di configurazione dei pfSense all'indirizzo IP **192.168.1.1** avviandolo da browser da Kali.



Si scopre che c'è un'altra rete collegata **192.168.50.1** con subnet **/24**.

Pertanto si prosegue con il comando per la scansione di nmap sul nuovo indirizzo IP **sudo nmap -A 192.168.50.0/24**



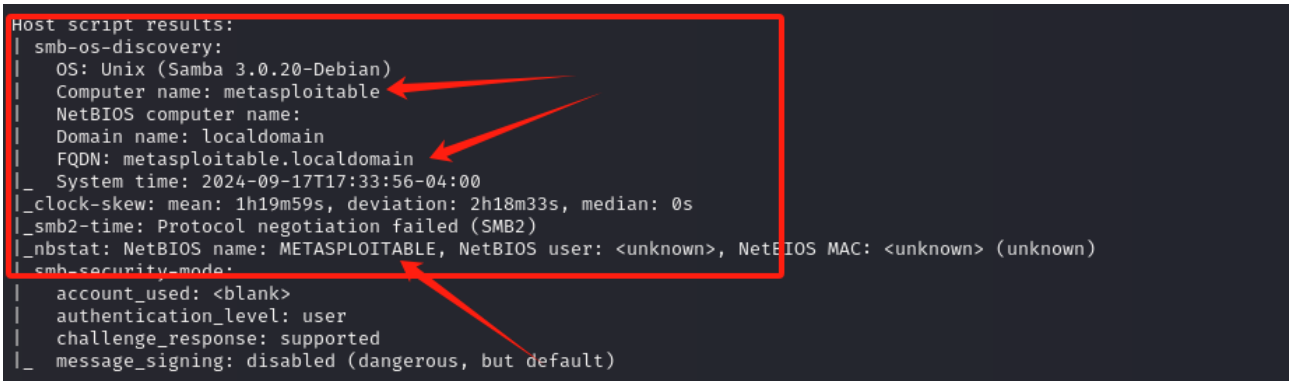
Individuato una macchina con indirizzo ip **192.168.50.100** che è l'unica macchina collegata alla rete.

Conferma IP target appartenga a Metasploitable2

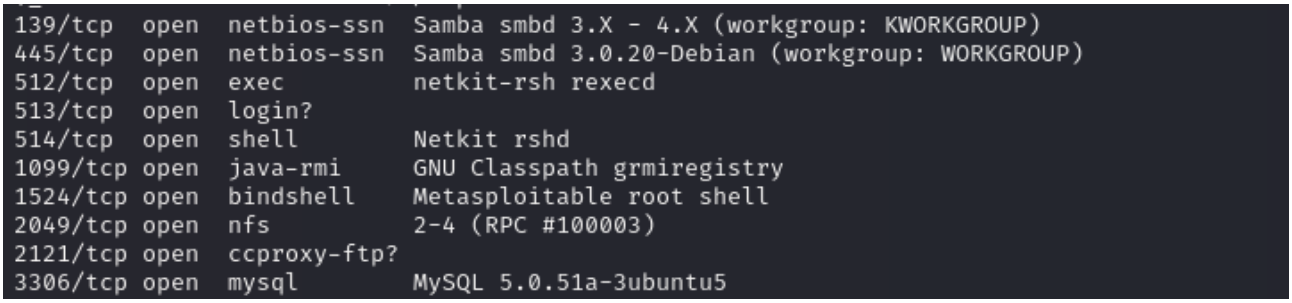
Per accertare che sia l'indirizzo IP di Metasploitable2 utilizzare **sudo nmap -A 192.168.50.100**

Il flag -A in nmap è considerato invasivo. Attivando -A, nmap esegue una scansione approfondita che include:

- Rilevamento del sistema operativo: Prova a determinare il sistema operativo del target.
- Rilevamento delle versioni dei servizi: Identifica le versioni dei servizi in esecuzione.
- Rilevamento degli script: Esegue vari script di scansione per raccogliere informazioni aggiuntive.
- Rilevamento degli host: Scansiona per identificare gli host attivi nella rete.



Confermato il sistema operativo e rilevato inoltre le porte aperte.



Raccolta dati con gli strumenti consigliati dalla traccia

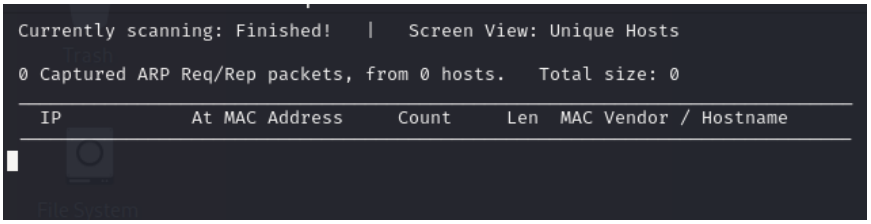
1. nmap -sn -PE <target>

Esegue una scansione di tipo ping per verificare se l'host è online usando pacchetti ICMP Echo Request. **nmap -sn -PE 192.168.50.100**

- **-sn**: Questo flag sta per "Scan No Port". Indica a nmap di eseguire una scansione di tipo "Ping" senza eseguire una scansione delle porte. Questo comando è utile per determinare se un host è attivo o meno senza esaminare le porte aperte.
- **-PE**: Questo flag specifica che nmap deve utilizzare i pacchetti ICMP Echo Request (i classici "ping") per verificare se l'host è raggiungibile. È uno dei metodi che nmap utilizza per effettuare un ping agli host.
-

2. netdiscover -r <target>

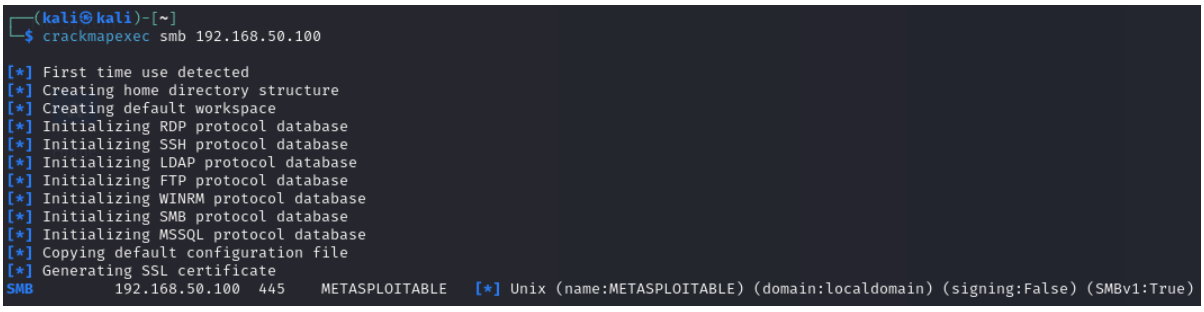
Scansiona la rete 192.168.50.0/24 per scoprire dispositivi attivi. **sudo netdiscover -r 192.168.50.0/24**



-r 192.168.50.0/24: Specifica l'intervallo di indirizzi IP da scansionare. In questo caso, 192.168.50.0/24 indica una rete con maschera di sottorete 255.255.255.0, che include tutti gli indirizzi IP da 192.168.50.1 a 192.168.50.254.

3. crackmapexec <target>

Esegue una scansione SMB per raccogliere informazioni sul target. **crackmapexec smb 192.168.50.100**



crackmapexec: È uno strumento di post-exploitation e di gestione della rete utilizzato per eseguire vari tipi di scansioni e test di penetrazione su reti e servizi.

SMB 192.168.50.100 445 METASPLOITABLE: Indica che è stato rilevato un servizio SMB in esecuzione sull'indirizzo IP 192.168.50.100 sulla porta 445, e il nome del computer è METASPLOITABLE.

4. nmap <target> –top-ports 10 –open

Scansiona le 10 porte più comuni sul target e mostra solo quelle aperte: **nmap 192.168.50.100 --top-ports 10 –open**

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.100 --top-ports 10 --open

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 18:38 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0040s latency).
Not shown: 3 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

5. nmap <target> -p- -sV –reason –dns-server ns

Nota: per continuare con questo comando, a causa dei limiti imposti da pfSense, da questo punto in poi, le due macchine saranno configurate nella stessa rete interna. Meta 192.168.1.100

Scansionare tutte le porte e identificare i servizi e le versioni. Mostrare il motivo per cui una porta è in uno stato particolare. Utilizzare un server DNS specifico: **nmap 192.168.1.100 -p- -sV --reason --dns-servers 192.168.1.1** in questo caso si è utilizzato il DNS di pfSense.

- **-p-**: Scansiona tutte le porte (da 1 a 65535).
- **-sV**: Rileva le versioni dei servizi in esecuzione sulle porte aperte.
- **--reason**: Mostra il motivo per cui Nmap ha classificato una porta come aperta, chiusa o filtrata.
- **--dns-servers <DNS_SERVER>**: Specifica quali server DNS utilizzare per la risoluzione dei nomi durante la scansione.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.100 -p- -sV --reason --dns-servers 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:04 EDT
Nmap scan report for 192.168.1.100
Host is up, received syn-ack (0.0025s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     REASON  VERSION
21/tcp    open  ftp         syn-ack vsftpd 2.3.4
22/tcp    open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack Linux telnetd
25/tcp    open  smtp        syn-ack Postfix smtpd
53/tcp    open  domain      syn-ack ISC BIND 9.4.2
80/tcp    open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack netkit-rsh rexecd
513/tcp   open  login       syn-ack OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped  syn-ack
1099/tcp  open  java-rmi    syn-ack GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack Metasploitable root shell
2049/tcp  open  rpcbind     syn-ack
2121/tcp  open  ftp         syn-ack ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack (access denied)
6667/tcp  open  irc         syn-ack UnrealIRCd
6697/tcp  open  irc         syn-ack UnrealIRCd
8009/tcp  open  ajp13       syn-ack Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34265/tcp open  rpcbind     syn-ack
40311/tcp open  unknown     syn-ack
58541/tcp open  rpcbind     syn-ack
59440/tcp open  rpcbind     syn-ack
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

6. us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3

Nota: dopo il punto precedente la configurazione di Meta mantiene IP a 192.168.1.100

us -mT -Iv 192.168.1.100:a -r 3000 -R 3 && us -mU -Iv 192.168.1.100:a -r 3000 -R 3

Questo comando esegue due scansioni separate sul target con l'indirizzo IP 192.168.1.100 utilizzando lo strumento us. Di seguito è fornita una spiegazione dettagliata di ciascun flag e parametro utilizzato:

I. **us**: Il nome dello strumento di scansione utilizzato. Non è uno strumento standard, quindi il suo comportamento specifico dipende dalla sua implementazione.

II. **-mT**:
   a. **-m**: Indica il tipo di scansione o protocollo da utilizzare.
   b. **T**: Specifica che la scansione deve essere eseguita utilizzando il protocollo TCP.

III. **-mU**:
   a. **-m**: Come sopra, indica il tipo di scansione o protocollo.
   b. **U**: Specifica che la scansione deve essere eseguita utilizzando il protocollo UDP.

IV. **-Iv**:
   a. **-I**: Richiede che lo strumento fornisca informazioni dettagliate o approfondite durante la scansione.
   b. **-v**: Abilita la modalità verbose, che fornisce informazioni aggiuntive sullo stato e sui risultati della scansione.

V. **192.168.1.100:a**:
   a. **192.168.1.100**: L'indirizzo IP del target della scansione.
   b. **:a**: Indica che devono essere scansionate tutte le porte disponibili sul target.

VI. **-r 3000**:
   a. **-r**: Specifica un parametro aggiuntivo che potrebbe essere un intervallo di porte, un timeout, o una configurazione di scansione. Il valore 3000 rappresenta il parametro assegnato, il cui significato preciso dipende dalle specifiche dello strumento.

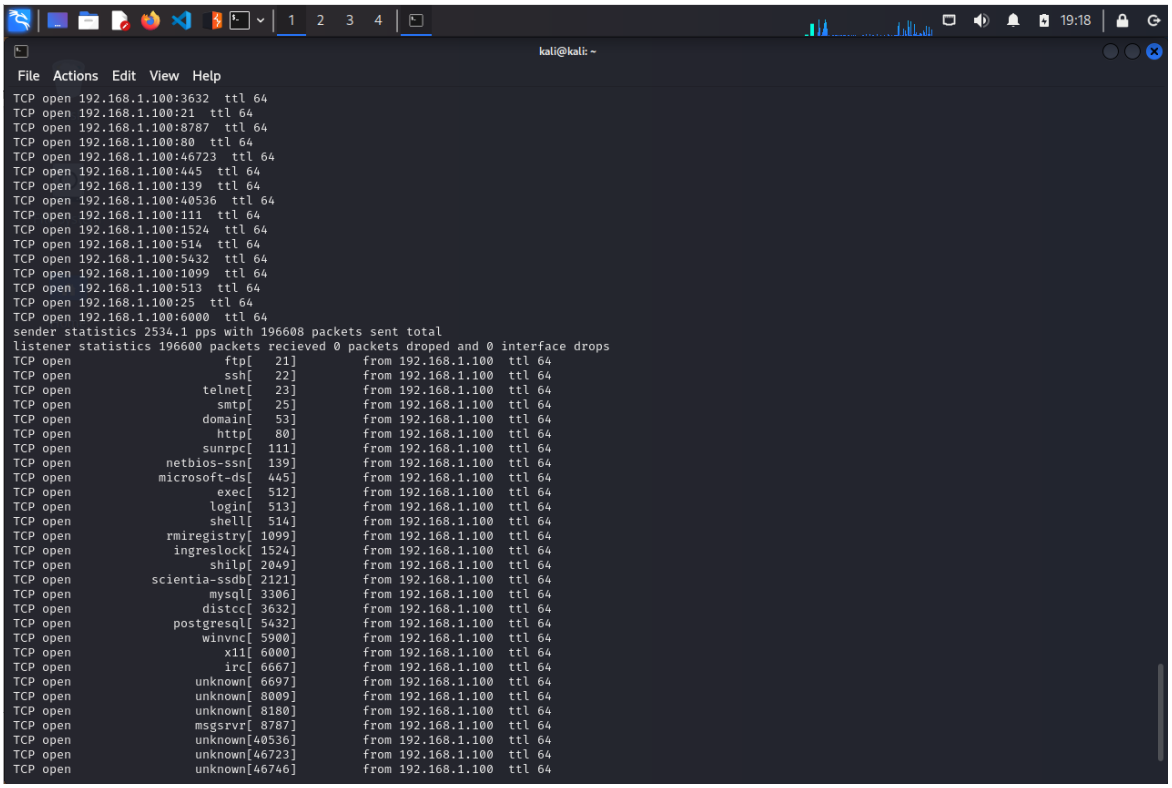
VII. **-R 3**:
   a. **-R**: Definisce un ulteriore parametro configurabile. Potrebbe rappresentare il numero di tentativi, un livello di dettaglio, o un altro valore specifico.
   b. **3**: Il valore assegnato a questo parametro, che indica il numero di tentativi o un altro aspetto della configurazione della scansione.

VIII. **&&**: Operatore di concatenamento di comandi che esegue il secondo comando solo se il primo comando è completato con successo.

Sintesi: Il comando esegue due scansioni sul target 192.168.1.100:

- La prima scansione utilizza il protocollo TCP (-mT), mostrando informazioni dettagliate e verbose (-Iv), e scansiona tutte le porte (:a), con un intervallo o timeout di 3000 (-r 3000) e un parametro di configurazione 3 (-R 3).
- La seconda scansione utilizza il protocollo UDP (-mU), con le stesse opzioni di verbose e dettagli, e gli stessi parametri di intervallo e configurazione.

Si ottengono le seguenti informazioni: Lista delle porte TCP e UDP aperte, Versioni dei servizi e Stato delle porte.



7. nmap -sS -sV -T4 <target>

nmap -sS -sV -T4 192.168.1.100

- La **scansione SYN** (-sS) scopre quali porte TCP sono aperte sul target senza completare il processo di handshake TCP completo, rendendo la scansione relativamente discreta.
- Il flag **version detection** (-sV) fornisce informazioni dettagliate sui servizi attivi su ciascuna porta aperta, inclusa la loro versione.
- Il flag **-T4** velocizza la scansione (più basso è e più stealth)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.1.100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:21 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00043s 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:77:37:E6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.97 seconds
```

8. hping3 –scan known <target>

Comando **hping3 --scan known 192.168.1.100**

hping3 è uno strumento di rete avanzato usato per generare pacchetti TCP/IP personalizzati e condurre varie operazioni di scansione e test di rete. È comunemente usato per eseguire scansioni di porte, test di connettività e verificare la risposta dei sistemi target a specifici pacchetti.

--scan: Il flag --scan indica che si vuole eseguire una scansione delle porte sul target. hping3 supporta diversi tipi di scansione, come la scansione di porte specifiche o intervalli di porte.

known: Questo parametro, quando associato al flag --scan, specifica che la scansione deve essere limitata alle **porte conosciute** (well-known ports), che sono le porte numerate da 0 a 1023. Queste porte sono comunemente assegnate a servizi standard (ad esempio, HTTP sulla porta 80, SSH sulla porta 22, etc.).

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.1.100

Scanning 192.168.1.100 (192.168.1.100), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login)
(514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)
```

Il risultato mostra le porte conosciute che **non hanno risposto** durante la scansione.

9. nc -nvz <target> 1-1024

Utilizzo di Netcat per scansionare le porte 1-1024 e verificare quali sono aperte: **nc -nvz 192.168.1.100 1-1024**

- **-n**: Evita la risoluzione DNS, lavorando direttamente con gli indirizzi IP.
- **-v**: Attiva la modalità **verbose**, fornendo informazioni dettagliate sullo stato di ciascuna porta.
- **-z**: Abilita la modalità **zero-I/O**, controllando semplicemente se le porte sono aperte o chiuse senza trasferire dati.

```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.1.100 1-1024

(UNKNOWN) [192.168.1.100] 514 (shell) open
(UNKNOWN) [192.168.1.100] 513 (login) open
(UNKNOWN) [192.168.1.100] 512 (exec) open
(UNKNOWN) [192.168.1.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.100] 111 (sunrpc) open
(UNKNOWN) [192.168.1.100] 80 (http) open
(UNKNOWN) [192.168.1.100] 53 (domain) open
(UNKNOWN) [192.168.1.100] 25 (smtp) open
(UNKNOWN) [192.168.1.100] 23 (telnet) open
(UNKNOWN) [192.168.1.100] 22 (ssh) open
(UNKNOWN) [192.168.1.100] 21 (ftp) open
```

10. nc -nv <target> 22

Verificare se la porta 22 è aperta su un target specifico: **nc -nv 192.168.1.100 22**

```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.1.100 22

(UNKNOWN) [192.168.1.100] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

11. nmap -sV <target>

Rilevare i servizi in esecuzione su un target specifico: **nmap -sV 192.168.1.100**

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:38 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0021s latency).
Not shown: 977 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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?
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_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.17 seconds
```

12. db_import <file.xml> (For Metasploit Framework)

Per testare questo comando, bisogna salvare su file una precedente scansione, che potrebbe eseguire con **nmap -sV -oX nmap_results.xml 192.168.1.100** il quale salva in xml la scansione del punto 11.
-oX nmap_results.xml: Salva i risultati della scansione in formato XML con il nome nmap_results.xml.

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  gameshell  gameshell.1  gameshell-save.sh  gameshell.sh  Music  nmap_results.xml  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$
```

Con il comando **ls** si ritrova il file generato che bisogna importarlo nel framework di Meta.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_import nmap_results.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 192.168.1.100
[*] Successfully imported /home/kali/nmap_results.xml
msf6 >
```

Avviare la modalità di super utente con **sudo su** e avviare il database PostgreSQL **sudo service postgresql start** e per la configurazione **msfdb init**
Avviare il framework Metasploit con **msfconsole**
Importare il file xml **db_import nmap_results.xml**
Una volta importato si possono cercare vulnerabilità e/o consultare il documento, che in questo report non si analizzerà.

13. nmap -f –mtu=512 <target>

Questo comando è utilizzato per mascherare le scansioni e superare le restrizioni basate sulla dimensione dei pacchetti. **nmap -f --mtu=512 192.168.1.100**

- **-f**: Frammenta i pacchetti IP inviati, utile per eludere IDS e firewall.
- **--mtu=512**: Imposta la dimensione massima dei pacchetti a 512 byte.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -f --mtu=512 192.168.1.100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 20:10 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00040s 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: 08:00:27:77:37:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

14. masscan <network> -p80 –banners –source-ip <target>

Questo comando è utilizzato per scoprire server HTTP su una rete e raccogliere informazioni sui banner dei servizi, con un IP di origine specifico: **masscan 192.168.1.0/24 -p80 --banners --source-ip 192.168.1.100**

- **-p80**: Scansiona solo la porta 80 (HTTP).
- **--banners**: Rileva e mostra banner dei servizi sui target.

```
┌──(root㉿kali)-[/home/kali]
└─# masscan 192.168.1.0/24 -p80 --banners --source-ip 192.168.1.100
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-09-18 00:13:43 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.1.1
^Cwaiting several seconds to exit...
Banner on port 80/tcp on 192.168.1.1: [http.server] nginx
Banner on port 80/tcp on 192.168.1.1: [title] 301 Moved Permanently
Banner on port 80/tcp on 192.168.1.1: [http] HTTP/1.1 301 Moved Permanently\x0d\x0aServer: nginx\x0d\x0aDate: Wed, 18 Sep 2024 00:13:49 GMT\x0d
Type: text/html\x0d\x0aContent-Length: 162\x0d\x0aConnection: close\x0d\x0aLocation: https:///\x0d\x0aX-Frame-Options: SAMEORIGIN\x0d\x0a\x0d
```

Svolgimento esercizio facoltativo

Visitare i siti web

https://nmap.org/book/firewall-subversion.html

https://nmap.org/book/man-bypass-firewalls-ids.html