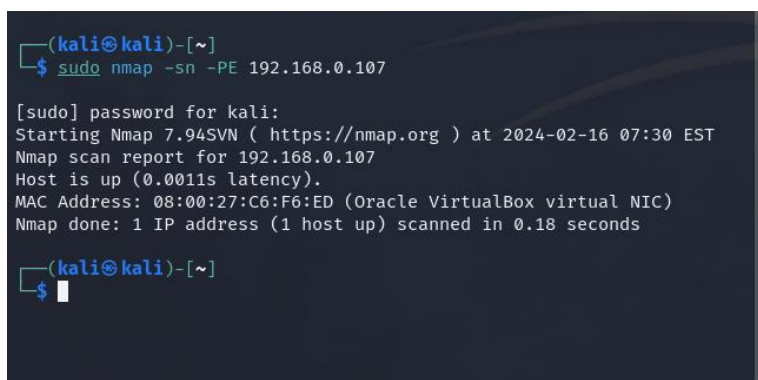


ESERCIZIO W10D4

Tramite alcuni strumenti forniti nel link di epicode, cercherò di ottenere informazioni sulla macchina Metasploitable.

Il primo comando che ho eseguito è stato: **sudo nmap -sn -PE 192.168.0.107** con l'indirizzo IP di Meta, e con le macchine Kali e Meta sulla stessa rete. Questo comando utilizza Nmap per eseguire una scansione di discovery di host nella rete specificata senza effettuare una scansione delle porte. nmap è il comando principale, -sn indica di non eseguire la scansione delle porte, -PE specifica di utilizzare il protocollo ICMP Echo Request per scoprire gli host.



```
(kali㉿kali)-[~]  
$ sudo nmap -sn -PE 192.168.0.107  
  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 07:30 EST  
Nmap scan report for 192.168.0.107  
Host is up (0.0011s latency).  
MAC Address: 08:00:27:C6:F6:ED (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds  
  
(kali㉿kali)-[~]  
$
```

"Nmap scan report for 192.168.0.107": Indica che è stato trovato un host con indirizzo IP 192.168.0.107.

"Host is up": Questo indica che l'host è online e accessibile sulla rete.

"MAC Address: 08:00:27:C6:F6:ED (Oracle VirtualBox virtual NIC)": Viene fornito l'indirizzo MAC dell'host, che è associato a una scheda di rete virtuale Oracle VirtualBox.

"Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds": Questo è un messaggio di completamento che indica che la scansione è stata completata in 0.18 secondi e che un solo host è stato analizzato.

Questo risultato mostra che la macchina con indirizzo IP 192.168.0.107 è attiva sulla rete e utilizza una scheda di rete virtuale Oracle VirtualBox.

SECONDO COMANDO

Procedo con il comando: **netdiscover -r 192.168.0.107**. Netdiscover è un altro strumento di discovery di rete. Netdiscover viene utilizzato per rilevare dispositivi nella rete locale. L'opzione -r specifica l'intervallo di indirizzi IP da esaminare.

```
kali@kali: ~  
File Actions Edit View Help  
Currently scanning: Finished! | Screen View: Unique Hosts  
393 Captured ARP Req/Rep packets, from 5 hosts. Total size: 23580  


| IP            | At MAC Address    | Count | Len   | MAC Vendor / Hostn |
|---------------|-------------------|-------|-------|--------------------|
| ame           | At MAC Address    | Count | Len   | MAC Vendor / Hostn |
| 0.100         | 9c:53:22:e3:ea:4a | 257   | 15420 | TP-Link Corporatio |
| 0.105         | f8:54:f6:bf:17:c3 | 1     | 60    | Unknown vendor     |
| 192.168.0.100 | 9c:53:22:e3:ea:4a | 290   | 17400 | TP-Link Corporati  |
| 192.168.0.1   | d4:72:26:c3:9f:41 | 96    | 5760  | zte corporation    |
| 192.168.0.105 | f8:54:f6:bf:17:c3 | 1     | 60    | Unknown vendor     |
| 192.168.0.107 | 08:00:27:c6:f6:ed | 1     | 60    | PCS Systemtechnik  |
| 192.168.0.101 | 60:ab:14:47:be:ce | 5     | 300   | LG Innotek         |


```

netdiscover ha terminato la scansione e ha trovato cinque host nella rete. Ecco una breve analisi del risultato:

192.168.0.100 - Indirizzo IP associato a un dispositivo con indirizzo MAC 9c:53:22:e3:ea:4a, che appartiene a TP-Link Corporation Limited.

192.168.0.1 - Indirizzo IP associato a un dispositivo con indirizzo MAC d4:72:26:c3:9f:41, che appartiene a ZTE Corporation.

192.168.0.105 - Indirizzo IP associato a un dispositivo con indirizzo MAC f8:54:f6:bf:17:c3. Il produttore del dispositivo è sconosciuto.

192.168.0.107 - Questo è l'indirizzo IP della macchina Metasploitable, che abbiamo già identificato in precedenza, con indirizzo MAC 08:00:27:c6:f6:ed, associato a PCS Systemtechnik GmbH.

192.168.0.101 - Indirizzo IP associato a un dispositivo con indirizzo MAC 60:ab:14:47:be:ce, che appartiene a LG Innotek.

TERZO COMANDO

crackmapexec 192.168.0.107 e indico poi un protocollo a mia scelta

CrackMapExec è uno strumento avanzato per testare la sicurezza dei sistemi di rete. Si concentra sulla scansione e sfrutta le vulnerabilità nei sistemi Windows. Questo strumento può essere utilizzato per eseguire varie operazioni, inclusa la raccolta di informazioni sulle risorse condivise, gli account utente e le password.

```
(kali㉿kali)-[~]  
$ sudo crackmapexec smb 192.168.0.107  
  
SMB          192.168.0.107    445      METASPLOITABLE  [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)  
  
(kali㉿kali)-[~]  
$
```

Ecco il risultato della scansione SMB sulla macchina Metasploitable utilizzando crackmapexec:

SMB: Il protocollo SMB è stato identificato.

192.168.0.107: Indirizzo IP della macchina Metasploitable.

445: La porta TCP 445 è utilizzata dal protocollo SMB per la comunicazione.

METASPLOITABLE: Nome del sistema.

Unix: Il sistema operativo è stato identificato come Unix.

(name: METASPLOITABLE): Nome della macchina.

(domain: localdomain): Dominio della macchina.

(signing: False): La firma dei messaggi SMB non è abilitata.

(SMBv1: True): Il supporto per SMB versione 1 è attivo sulla macchina.

Questo risultato fornisce informazioni utili sulla configurazione SMB della macchina Metasploitable.

QUARTO COMANDO

nmap 192.168.0.107 -top-ports 10 -open

Qui, utilizziamo di nuovo Nmap, ma questa volta specifichiamo di scansionare solo le prime 10 porte più comuni. L'opzione --open indica di mostrare solo le porte aperte.

```
(kali㉿kali)-[~]  
$ sudo nmap 192.168.0.107 --top-ports 10 --open  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 07:52 EST  
Nmap scan report for 192.168.0.107  
Host is up (0.00072s latency).  
Not shown: 3 closed tcp ports (reset)  
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  
MAC Address: 08:00:27:C6:F6:ED (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds  
  
(kali㉿kali)-[~]  
$
```

Il comando è stato eseguito con successo. Ecco una breve analisi del risultato:

21/tcp: La porta 21 è aperta e indica che il servizio FTP è in esecuzione sulla macchina Metasploitable.

22/tcp: La porta 22 è aperta e indica che il servizio SSH (Secure Shell) è in esecuzione sulla macchina Metasploitable.

23/tcp: La porta 23 è aperta e indica che il servizio Telnet è in esecuzione sulla macchina Metasploitable.

25/tcp: La porta 25 è aperta e indica che il servizio SMTP (Simple Mail Transfer Protocol) è in esecuzione sulla macchina Metasploitable.

80/tcp: La porta 80 è aperta e indica che il servizio HTTP è in esecuzione sulla macchina Metasploitable, probabilmente un server web.

139/tcp: La porta 139 è aperta e indica che il servizio NetBIOS-SSN (NetBIOS Session Service) è in esecuzione sulla macchina Metasploitable.

445/tcp: La porta 445 è aperta e indica che il servizio Microsoft-DS (Directory Services) è in esecuzione sulla macchina Metasploitable.

Questo risultato fornisce un'idea delle porte aperte e dei servizi in esecuzione sulla macchina Metasploitable.

QUINTO COMANDO

nmap 192.168.0.107 -p- -sV --reason --system-dns

Questo è un comando Nmap più dettagliato. -p- indica di scansionare tutte le porte, -sV specifica di effettuare una scansione dei servizi/versioni, --reason mostra il motivo per cui Nmap ha

raggiunto una determinata conclusione, e `--dns-server ns` specifica il server DNS da utilizzare per le query DNS.

```
File Actions Edit View Help
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (work
group: WORKGROUP)
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (work
group: WORKGROUP)
512/tcp open exec syn-ack ttl 64 netkit-rsh rexecd
513/tcp open login syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp open tcpwrapped syn-ack ttl 64
1099/tcp open java-rmi syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp open bindshell syn-ack ttl 64 Metasploitable root shell
2049/tcp open nfs syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp open ftp syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp open mysql syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp open distccd syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (U
buntu 4.2.4-1ubuntu4))
5432/tcp open postgresql syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.
7
5900/tcp open vnc syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp open X11 syn-ack ttl 64 (access denied)
6667/tcp open irc syn-ack ttl 64 UnrealIRCd
6697/tcp open irc syn-ack ttl 64 UnrealIRCd (Admin email ad
min@Metasploitable.LAN)
8009/tcp open ajp13 syn-ack ttl 64 Apache Jserv (Protocol v1.
3)
8180/tcp open http syn-ack ttl 64 Apache Tomcat/Coyote JSP e
ngine 1.1
8787/tcp open drb syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; pa
th /usr/lib/ruby/1.8/drbc)
35361/tcp open nlockmgr syn-ack ttl 64 1-4 (RPC #100021)
43747/tcp open mountd syn-ack ttl 64 1-3 (RPC #100005)
50812/tcp open java-rmi syn-ack ttl 64 GNU Classpath grmiregistry
58166/tcp open status syn-ack ttl 64 1 (RPC #100024)
MAC Address: 08:00:27:C6:F6:ED (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 h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.55 seconds

(kali@kali)-[~]
$
```

Il comando `nmap` è stato eseguito con successo e ha fornito un output dettagliato sulla macchina Metasploitable. Ecco una breve analisi del risultato:

21/tcp: Porta aperta, servizio FTP (vsftpd 2.3.4).

22/tcp: Porta aperta, servizio SSH (OpenSSH 4.7p1 Debian 8ubuntu1).

23/tcp: Porta aperta, servizio Telnet (Linux telnetd).

25/tcp: Porta aperta, servizio SMTP (Postfix smtpd).

53/tcp: Porta aperta, servizio DNS (ISC BIND 9.4.2).

80/tcp: Porta aperta, servizio HTTP (Apache httpd 2.2.8).

111/tcp: Porta aperta, servizio RPC (RPCbind 2).

139/tcp e 445/tcp: Porte aperte, servizi NetBIOS-SSN (Samba smbd 3.X - 4.X).

Altre porte aperte includono servizi come RPC, FTP (ProFTPD 1.3.1), MySQL, PostgreSQL, VNC, UnrealIRCd, Apache Tomcat, e altri.

Inoltre, sono state fornite informazioni sul sistema operativo (OSs: Unix, Linux) e sugli host (Hosts: metasploitable.localdomain, irc.Metasploitable.LAN).

Questo output fornisce un'ampia panoramica dei servizi in esecuzione sulla macchina Metasploitable e può essere utilizzato per identificare potenziali vulnerabilità o aree di interesse per ulteriori analisi di sicurezza.

SESTO COMANDO

nc -nvz <target> 1-1024

Questo comando utilizza netcat per testare la connettività alle porte TCP sulla macchina Metasploitable nell'intervallo da 1 a 1024.

```
(kali㉿kali)-[~]
$ sudo nc -nvz 192.168.0.107 1-1024

(UNKNOWN) [192.168.0.107] 514 (shell) open
(UNKNOWN) [192.168.0.107] 513 (login) open
(UNKNOWN) [192.168.0.107] 512 (exec) open
(UNKNOWN) [192.168.0.107] 445 (microsoft-ds) open
(UNKNOWN) [192.168.0.107] 139 (netbios-ssn) open
(UNKNOWN) [192.168.0.107] 111 (sunrpc) open
(UNKNOWN) [192.168.0.107] 80 (http) open
(UNKNOWN) [192.168.0.107] 53 (domain) open
(UNKNOWN) [192.168.0.107] 25 (smtp) open
(UNKNOWN) [192.168.0.107] 23 (telnet) open
(UNKNOWN) [192.168.0.107] 22 (ssh) open
(UNKNOWN) [192.168.0.107] 21 (ftp) open

(kali㉿kali)-[~]
$
```

Ecco un breve riassunto dei servizi associati alle porte aperte:

Porta 514 (shell): Questa porta è associata al servizio di shell remota. Potrebbe indicare la presenza di un servizio di shell remota attivo sulla macchina Metasploitable.

Porta 513 (login): Questa porta è associata al servizio di accesso remoto. Potrebbe indicare la presenza di un servizio di login remoto attivo sulla macchina Metasploitable.

Porta 512 (exec): Questa porta è associata al servizio di esecuzione remota. Potrebbe indicare la presenza di un servizio di esecuzione remota attivo sulla macchina Metasploitable.

Porta 445 (microsoft-ds): Questa porta è associata al servizio di condivisione di file e stampanti di Microsoft Windows (SMB). Potrebbe indicare la presenza di condivisioni SMB attive sulla macchina Metasploitable.

Porta 139 (netbios-ssn): Questa porta è associata al servizio di sessione NetBIOS. Potrebbe indicare la presenza di servizi NetBIOS attivi sulla macchina Metasploitable.

Porta 111 (sunrpc): Questa porta è associata al servizio RPC (Remote Procedure Call). Potrebbe indicare la presenza di servizi RPC attivi sulla macchina Metasploitable.

Porta 80 (http): Questa porta è associata al servizio HTTP. Potrebbe indicare la presenza di un server web attivo sulla macchina Metasploitable.

Porta 53 (domain): Questa porta è associata al servizio DNS (Domain Name System). Potrebbe indicare la presenza di un server DNS attivo sulla macchina Metasploitable.

Porta 25 (smtp): Questa porta è associata al servizio SMTP (Simple Mail Transfer Protocol). Potrebbe indicare la presenza di un server di posta SMTP attivo sulla macchina Metasploitable.

Porta 23 (telnet): Questa porta è associata al servizio Telnet. Potrebbe indicare la presenza di un server Telnet attivo sulla macchina Metasploitable.

Porta 22 (ssh): Questa porta è associata al servizio SSH (Secure Shell). Potrebbe indicare la presenza di un server SSH attivo sulla macchina Metasploitable.

Porta 21 (ftp): Questa porta è associata al servizio FTP (File Transfer Protocol). Potrebbe indicare la presenza di un server FTP attivo sulla macchina Metasploitable.