Mapping Windows7

Il mapping di una rete a monte di un penetration testing serve principalmente a comprendere la topologia della rete, identificare i suoi componenti e le relative interconnessioni. Questa fase è cruciale perché fornisce una panoramica dettagliata dell'ambiente di rete, consentendo ai tester di identificare potenziali vulnerabilità e punti di ingresso per un attacco. Alcuni dei principali obiettivi e benefici del mapping di una rete prima di un penetration testing sono:

1-Identificazione delle risorse: Consente di individuare tutti i dispositivi presenti nella rete, come server, router, switch, firewall, e dispositivi IoT. Questo aiuta a comprendere la superficie di attacco potenziale.

2-Mappatura delle interconnessioni: Permette di capire come i dispositivi sono collegati tra loro e quali sono i flussi di traffico predominanti. Questo aiuta a individuare punti di accesso critici o nodi centrali che potrebbero essere bersagli appetibili per un attacco.

3-Rilevamento delle vulnerabilità: Identifica eventuali vulnerabilità presenti nei dispositivi o nelle configurazioni di rete. Questo può includere versioni obsolete del software, password deboli, servizi non necessari esposti e così via.

4-Valutazione della sicurezza: Fornisce una base per valutare la robustezza delle misure di sicurezza esistenti, come le politiche di accesso, i controlli dei firewall e la gestione delle patch.

5-Pianificazione delle strategie di attacco: Aiuta a pianificare e dirigere gli sforzi di penetration testing concentrandosi sui punti critici identificati durante il mapping della rete.

Esecuzione degli Strumenti

nmap -sn -PE <target>

netdiscover -r <target>

nmap -sP Ip <target>

nmap -sP <target>

nmap -sS -O <target>

nmap -p 135,139,455 <target>

nmap <target> -top-ports 20 -open

nmap <target>-p- -sV --reason --dns-server ns

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

58 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 3480

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
192.168.1.1     fc:40:09:dd:71:25     53    3180  zte corporation
192.168.1.9     40:80:e1:14:33:57      1      60  Unknown vendor
192.168.1.15    08:00:27:d8:c3:d7      1      60  PCS Systemtechnik GmbH
192.168.1.21    64:1c:ae:cf:2a:65      1      60  Samsung Electronics Co.,Ltd
192.168.1.2     cc:2d:21:3e:99:78      2     120  Tenda Technology Co.,Ltd.Donggu
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -O 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:15 CEST
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D8:C3:D7 (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: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8
.0
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP Ip 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:13 CEST
Failed to resolve "Ip".
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0019s latency).
MAC Address: 08:00:27:D8:C3:D7 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:15 CEST
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0029s latency).
MAC Address: 08:00:27:D8:C3:D7 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.1.15/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:18 CEST
Nmap scan report for wind3.hub.wind3.hub (192.168.1.1)
Host is up (0.014s latency).
MAC Address: FC:40:09:DD:71:25 (zte)
Nmap scan report for 192.168.1.2 (192.168.1.2)
Host is up (0.21s latency).
MAC Address: CC:2D:21:3E:99:78 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.0018s latency).
MAC Address: 40:80:E1:14:33:57 (Unknown)
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.059s latency).
MAC Address: C0:23:8D:69:1D:0C (Samsung Electronics)
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0023s latency).
MAC Address: 08:00:27:D8:C3:D7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.21 (192.168.1.21)
Host is up (0.0090s latency).
MAC Address: 64:1C:AE:CF:2A:65 (Samsung Electronics)
Nmap scan report for 192.168.1.24 (192.168.1.24)
Host is up (0.25s latency).
MAC Address: CC:2D:21:3E:99:78 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for 192.168.1.100 (192.168.1.100)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 5.39 seconds
```

Riepilogo delle informazioni trovate

Il risultato dello scanning ha riportato gli indirizzi i MAC address dei dispositivi associati al target, oltre che il MAC address del target stesso.

Sono state rilevate vulnerabilità alle porte 135,139,455.

139 3 455 sono associate al SMB, sta per "Server Message Block", ed è un protocollo di rete utilizzato principalmente per condividere risorse, come file, stampanti e porte seriali, tra computer su una rete locale. È il protocollo di condivisione file primario utilizzato nei sistemi operativi Windows.

La porta TCP 135 è comunemente associata al servizio Microsoft RPC (Remote Procedure Call), che è un protocollo utilizzato per la comunicazione tra processi su computer in una rete. Tuttavia, la porta 135 può essere utilizzata anche da altri servizi e applicazioni.