M3_W10D4

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

INTRODUZIONE:

I vari tool che visioneremo sono in grado di fornirci informazioni dettagliate per quanto riguarda il bersaglio (rete o OS). Nell specifico andremo a vedere quali porte sono aperte e quali no , che tipo di servizio offrono e la versione del loro software, in oltre andremo a vedere scansioni invasive (operazione facilmente identificabile in quanto sfruttano la connessione a 3 way hand shake) e scansioni passive (difficili da localizzare in quanto sono piu leggere per la dimensione di pacchetti inviati e molto piu rapide ma per questo meno dettagliate).

Capire le parti esposte di un sistemo , il suo OS , le versioni software dei suoi servizi presenti sulle porte , capire anche se le porte sono chiuse o filtrare , sono tutte informazione che aiutano un operatore a localizzare eventuali vulnerabilita .

Scansione:

scansioni NMAP

NMAP e un port scanner molto utilizzato in quanto e capace di eseguire scansioni con un gran numero di variabili.

Scansione 1.

Nmap -sn -PE <target>

Namp = ricchiamo tool

-sn (non scansiona le porte)

-PE(utilizza il protocoll Icmp per la discovery dei host attivi)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 09:32 EST
Nmap scan report for PC192.168.1.8-002 (192.168.1.8)
Host is up (0.00037s latency).
MAC Address: 08:00:27:48:A0:5E (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Vediamo come la scansione e durata 0.07 sec , il host e attivo sulla rete e vediamo anche l indirizzo della scheda di rete del bersaglio (MAC), vediamo anche che la scheda di rete e rilasciata da una virtual box.

Scansione 2

nmap <target> –top-ports 10 –open

-top-port 10 (scansiona le prime N porte che trova)

-open (aperte)

nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.1.17 -top-port 10 -open
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 09:32 EST
Nmap scan report for PC192.168.1.17.homenet.telecomitalia.it (192.168.1.17)
Host is up (0.0013s 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: 08:00:27:48:A0:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

la scansione mostra in output:

-le 7 porte aperte/tcp

-3 porte chiuse

-i servizi abilitati sulle porte scansionate

-l operatore che fornisce la rete

-l indirizzo MAC della scheda di rete del target/ il fatto che la scheda di rete e generata all interno di una VB

-il tempo impiegato 0.15 sec

Scansione 3

Crackmapexec protocollo <target>

```
smb                      own stuff using SMB
rdp                      own stuff using RDP
mssql                    own stuff using MSSQL
winrm                    own stuff using WINRM
ssh                      own stuff using SSH
ldap                     own stuff using LDAP
ftp                      own stuff using FTP
```

Protocollo ( )

Inserendo uno dei seguenti protocolli la scansione andra a localizzare la porta direttamente collegata ed esso e la versione del del software che lo gestisce
ES

```
┌──(root㉿kali)-[/home/kali]
└─# crackmapexec ftp 192.168.1.17
FTP         192.168.1.17    21     192.168.1.17     [*] Banner: (vsFTPd 2.3.4)

┌──(root㉿kali)-[/home/kali]
└─# crackmapexec ssh 192.168.1.17
SSH         192.168.1.17    22     192.168.1.17     [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

┌──(root㉿kali)-[/home/kali]
└─# crackmapexec smb 192.168.1.17
SMB         192.168.1.17    445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:Fal
se) (SMBv1:True)
```

Scansione 4

NetDiscover e uno strumento di ricognizione per gli indirizzi attivo/passivo.

Netdiscover -r

-netdiscover (lancio del tool)

- -r (per usare l intervallo)

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

103 Captured ARP Req/Rep packets, from 11 hosts.   Total size: 6180

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.1.4     06:21:92:0c:a9:1f      9     540  Unknown vendor
192.168.1.14    d8:bb:c1:b4:05:c4      6     360  Micro-Star INTL CO., LTD.
192.168.1.2     d0:50:99:7b:07:54     66    3960  ASRock Incorporation
192.168.1.1     3c:98:72:40:e2:b0      5     300  Sercomm Corporation.
192.168.1.6     d2:fa:2b:d5:a0:2b      1      60  Unknown vendor
192.168.1.7     d8:aa:59:13:20:85      1      60  Tonly Technology Co. Ltd
192.168.1.9     06:31:92:b3:81:ae      8     480  Unknown vendor
192.168.1.17    08:00:27:48:a0:5e      4     240  PCS Systemtechnik GmbH
192.168.1.102   06:31:92:b3:81:ae      1      60  Unknown vendor
192.168.1.103   06:31:92:b3:81:ae      1      60  Unknown vendor
192.168.1.104   06:31:92:b3:81:ae      1      60  Unknown vendor
```

Vediamo che la scansione si esegue tracciando i host attivi sulla rete determinando i loro MAC/ host name . questa e una scansione di invio pacchetti in tempo reale , se un altro host si connette alla sotto rete in esame verra subito scansionato e aggiunto alla lista.

Scansione 5

Unicornscan esegue una scansione SYN.

In questa scansione analizzeremo tutte le porte del nostro target inviandogli 3000 pacchetti per sec.

`us -mT -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3`

```
└─#  us -mT -Iv 192.168.1.17:a -r 3000
adding 192.168.1.17/32 mode `TCPscan'
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97
TCP open 192.168.1.17:43447  ttl 64
TCP open 192.168.1.17:60847  ttl 64
TCP open 192.168.1.17:80  ttl 64
TCP open 192.168.1.17:512  ttl 64
TCP open 192.168.1.17:1099  ttl 64
TCP open 192.168.1.17:5900  ttl 64
TCP open 192.168.1.17:139  ttl 64
TCP open 192.168.1.17:514  ttl 64
TCP open 192.168.1.17:513  ttl 64
TCP open 192.168.1.17:25  ttl 64
TCP open 192.168.1.17:2049  ttl 64
TCP open 192.168.1.17:43667  ttl 64
TCP open 192.168.1.17:445  ttl 64
TCP open 192.168.1.17:8009  ttl 64
TCP open 192.168.1.17:21  ttl 64
TCP open 192.168.1.17:23  ttl 64
TCP open 192.168.1.17:1524  ttl 64
TCP open 192.168.1.17:5432  ttl 64
TCP open 192.168.1.17:2121  ttl 64
TCP open 192.168.1.17:111  ttl 64
TCP open 192.168.1.17:22  ttl 64
TCP open 192.168.1.17:33035  ttl 64
TCP open 192.168.1.17:6697  ttl 64
TCP open 192.168.1.17:8180  ttl 64
TCP open 192.168.1.17:8787  ttl 64
TCP open 192.168.1.17:3632  ttl 64
TCP open 192.168.1.17:3306  ttl 64
TCP open 192.168.1.17:6667  ttl 64
TCP open 192.168.1.17:53  ttl 64
TCP open 192.168.1.17:6000  ttl 64
listener statistics 196589 packets recieved 0 packets droped and 0 interfa
TCP open                    ftp[   21]          from 192.168.1.17  ttl 64
TCP open                    ssh[   22]          from 192.168.1.17  ttl 64
TCP open                 telnet[   23]          from 192.168.1.17  ttl 64
TCP open                   smtp[   25]          from 192.168.1.17  ttl 64
TCP open                 domain[   53]          from 192.168.1.17  ttl 64
TCP open                   http[   80]          from 192.168.1.17  ttl 64
TCP open                 sunrpc[  111]          from 192.168.1.17  ttl 64
TCP open             netbios-ssn[  139]          from 192.168.1.17  ttl 64
TCP open            microsoft-ds[  445]          from 192.168.1.17  ttl 64
TCP open                    exec[  512]          from 192.168.1.17  ttl 64
TCP open                   login[  513]          from 192.168.1.17  ttl 64
TCP open                   shell[  514]          from 192.168.1.17  ttl 64
TCP open             rmiregistry[ 1099]          from 192.168.1.17  ttl 64
TCP open              ingreslock[ 1524]          from 192.168.1.17  ttl 64
TCP open                   shilp[ 2049]          from 192.168.1.17  ttl 64
TCP open          scientia-ssdb[ 2121]          from 192.168.1.17  ttl 64
TCP open                   mysql[ 3306]          from 192.168.1.17  ttl 64
TCP open                  distcc[ 3632]          from 192.168.1.17  ttl 64
TCP open              postgresql[ 5432]          from 192.168.1.17  ttl 64
TCP open                  winvnc[ 5900]          from 192.168.1.17  ttl 64
TCP open                     x11[ 6000]          from 192.168.1.17  ttl 64
TCP open                     irc[ 6667]          from 192.168.1.17  ttl 64
TCP open                 unknown[ 6697]          from 192.168.1.17  ttl 64
TCP open                 unknown[ 8009]          from 192.168.1.17  ttl 64
TCP open                 unknown[ 8180]          from 192.168.1.17  ttl 64
TCP open                 msgsrvr[ 8787]          from 192.168.1.17  ttl 64
TCP open                 unknown[33035]          from 192.168.1.17  ttl 64
TCP open                 unknown[43447]          from 192.168.1.17  ttl 64
TCP open                 unknown[43667]          from 192.168.1.17  ttl 64
TCP open                 unknown[60847]          from 192.168.1.17  ttl 64
```

come output ci comparira prima la colonna con tutte le porte aperte

in seguito ogni porta sara messa in ordine numerico crescente con affianco il servizio attivo

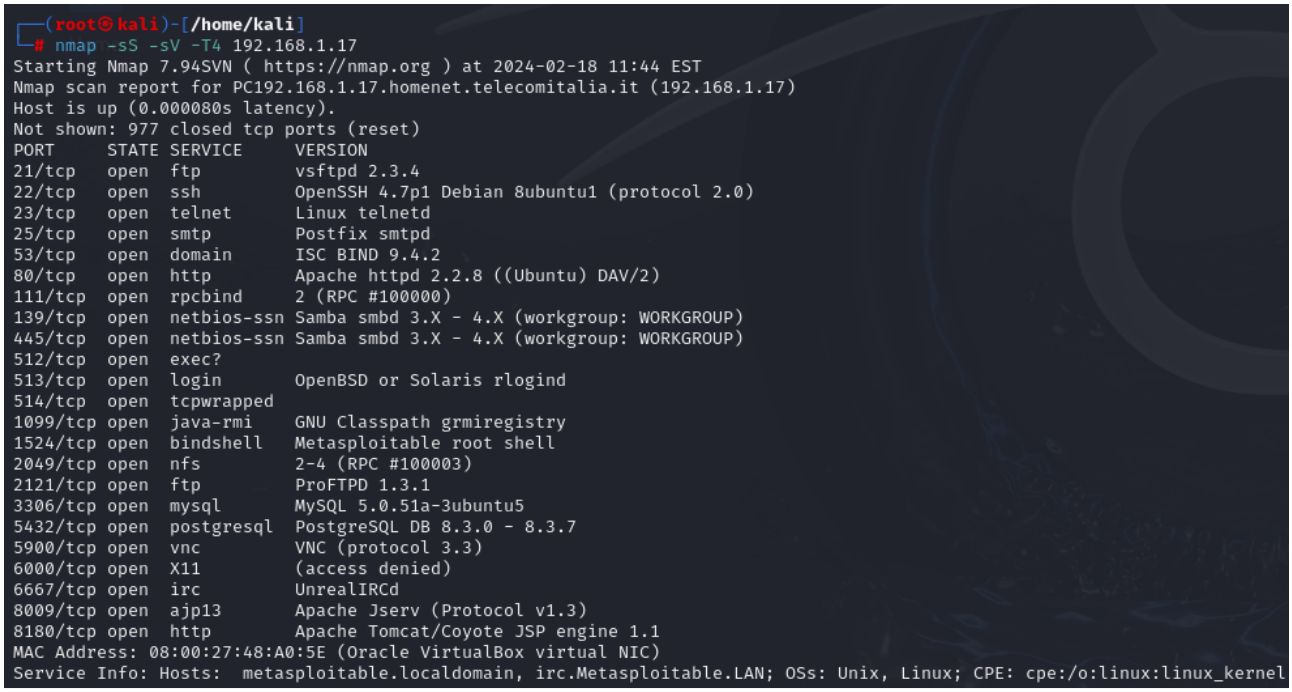
Scansione 7

`nmap -sS -sV -T4 <target>`

`-sS (verifica solo le porte aperte)`

`-sV ( esprime il servizio delle porte)`

`-T4 ( indica il tempo che dovra impiegare la scansione)`



Scansione approfondita i dati ricavati sono:

numero porta, stato, servizio presente sulla determinata porta, versione del software che gestisce la porta.

In fondo alla lista troviamo anche l indirizzo MAC del bersaglio e il OS utilizzato .