Report

Scansione Metaesploitable e Windows 7

All'interno di questo report, verranno analizzate le scansioni effettuate sulle macchine target Metaesploitable e Windows 7 tramite la macchina virtuale Kali Linux.

Gli indirizzi IP utilizzati sono sulla stessa rete interna e sono così distribuiti:

- Kali Linux: 192.168.50.100
- Metaesploitable: 192.168.50.101
- Windows 7: 192.168.50.102

Le scansioni fatte sulle macchine target riguardano:

- L'IP delle macchine target;
- I sistemi operativi;
- Le porte aperte;
- I servizi in ascolto;
- Versione dei servizi.

Lo strumento utilizzato per questa scansione è nmap («Network Mapper»), progettato per scansionare rapidamente reti di grandi dimensioni, ma è indicato anche per l'utilizzo verso singoli host.

I comandi principali utilizzati per recuperare le informazioni precedentemente menzionate sono:

- nmap -O 192.168.50.101 (Metaesploitable) / nmap -O 192.168.50.102 (Windows 7); → OS fingerprint.
- nmap -sS 192.168.50.101 (Metaesploitable)→ stealth scan;
- nmap -sT 192.168.50.101 (Metasploitable)→ TCP connect;
- nmap -sV 192.168.50.101 (Metaesploitable)→Version detection;

I risultati ottenuti nel caso della macchina target Kali Linux (192.168.50.101) sono i seguenti:

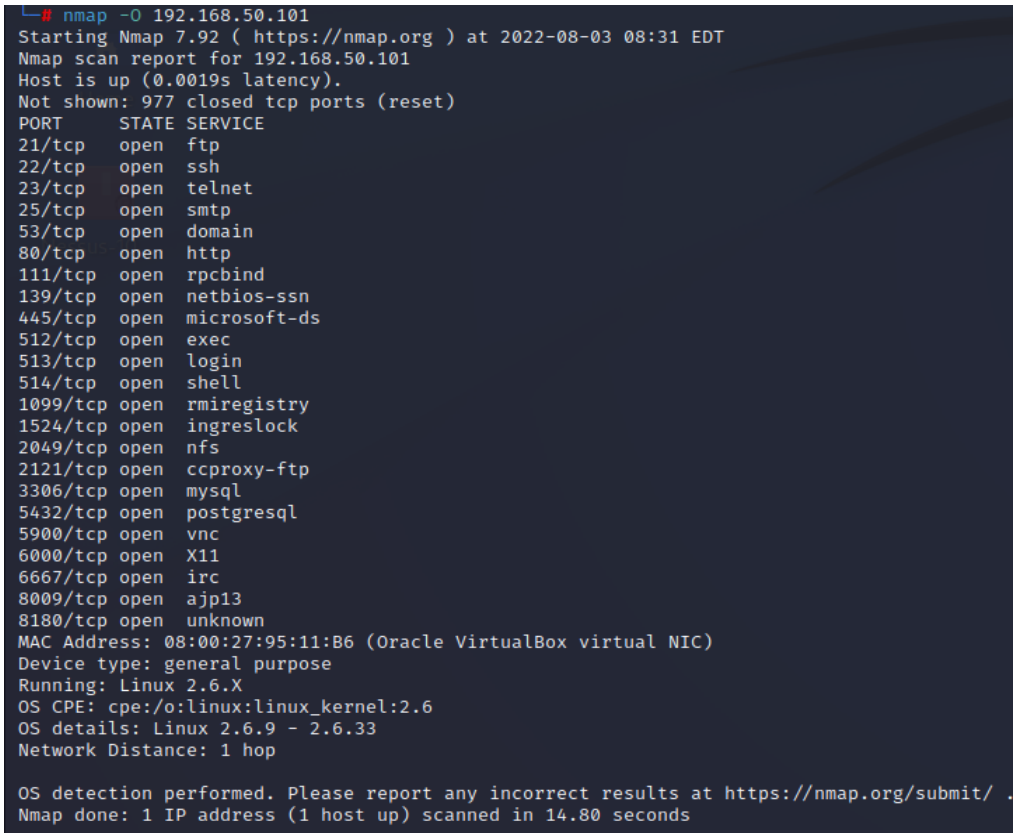
OS FINGERPRINT

è una feature che si utilizza con il comando nmap -O. Questa funzionalità stima il sistema operativo della macchina target ispezionando i pacchetti ricevuti. Questa stima viene fatta attraverso:

- i valori del TTL, **time to live**;
- la grandezza della finestra **TCP** (rappresenta il numero di byte che un dato sistema si aspetta di ricevere in input prima di inviare una conferma di messaggio ricevuto, ACK).

Questo comando, inoltre, ci restituisce il Sistema Operativo della macchina e la sua versione.

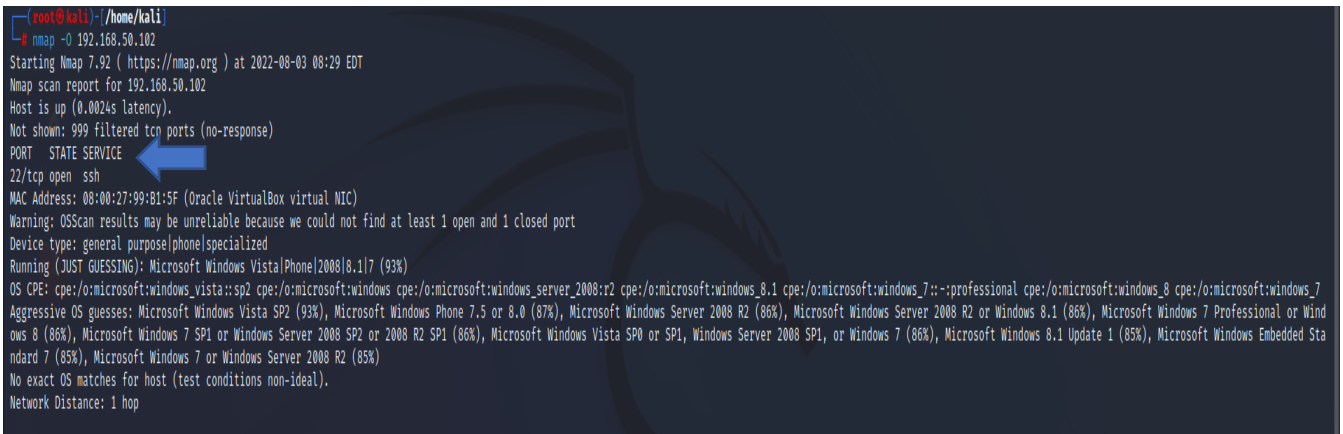
Di seguito viene riportato il comando -O sul target 192.168.50.101 (**Kali Linux).**



Il target 192.168.50.102 (**Windows 7**) non ha riportato risultati soddisfacenti in quanto i dati sono protetti da firewall o IPS/IDS.

Pertanto, l'unica informazione disponibile è la porta 22 (SSH) con stato open.

Di seguito il comando eseguito:



SYN SCAN

Per quanto riguarda il Syn scan verso la macchina target Metaesploitable possiamo recuperare le seguenti informazioni:

```
└─# nmap -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:34 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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: 08:00:27:95:11:B6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

Qui vengono rinvenute tutte le porte aperte della macchina con relativo servizio svolto da ognuna di esse. Ovviamente le porte chiuse (977) non vengono mostrate per facilitare l'analisi.

TCP CONNECT

Con il comando -sT andiamo a fare una scansione completa della rete, in cui le due macchine stringono un "three-way-handshake".

Questo comando è più invasivo rispetto agli altri poiché va a stabilire una connessione vera e propria.

I risultati però sono gli stessi dello stealth scan.

Di seguito il comando eseguito:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:35 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0044s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:95:11:B6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

VERSION DETECTION

Per quanto riguarda la version detection, il comando -sV restituisce le versioni di tutti i servizi in ascolto sulle porte aperte della macchina target Metaesploitable.

Di seguito il comando eseguito:

```
# nmap -sV 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:37 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00059s 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?
514/tcp  open  shell       Netkit rshd
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       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:95:11:B6 (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 66.33 seconds
```

Nella tabella sono registrati tutti i dati appresi dalla scansione effettuata con il tool nmap.

IP	SISTEMA OPERATIVO	PORTE APERTE	SERVIZI IN ASCOLTO	VERSIONE
192.168.50.101	Metasploitable	21/TCP	ftp	vsftpd 2.3.4
		22/TCP	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
		23/TCP	telnet	Linux telnetd
		25/TCP	smtp	Postfix smtpd
		53/TCP	domain	ISC BIND 9.4.2
		80/TCP	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
		111/TCP	rpcbind	2 (RPC #100000)
		139/TCP	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
		445/TCP	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
		512/TCP	exec	netkit-rsh rexecd
		513/TCP	login	
		514/TCP	shell	Netkit rshd
		1099/TCP	java-rmi	GNU Classpath grmiregistry
		1524/TCP	bindshell	Metasploitable root shell
		2049/TCP	nfs	2-4 (RPC #100003)
		2112/TCP	ftp	ProFTPD 1.3.1
		3306/TCP	mysql	MySQL 5.0.51a-3ubuntu5
		5432/TCP	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
		5490/TCP	vnc	VNC (protocol 3.3)
		6000/TCP	X11	(ACCESS DENIED)
		6667/TCP	irc	UnrealIRCd

		8009/TCP	ajp13	Apache Jserv (Protocol v1.3)
		8180/TCP	http	Apache Tomcat/Coyote JSP engine 1.1
192.168.50.102	Windows 7	22/TCP	SSH	OpenSSH 6.7 (protocol 2.0)

Windows 7 case

Nel caso della scansione effettuata sulla macchina con sistema operativo Windows 7 sono stati rinvenute pochissime informazioni.

L'unica porta disponibile e aperta è la porta 22/TCP (SSH), trovata con il comando -O.

La ragione plausibile per cui la macchina non risponde ai ping effettuati con il tool nmap è la presenza di firewall attivi o IPS/IDS.

POSSIBILI SOLUZIONI:

Una delle possibili soluzioni da me sperimentate per ricevere qualche informazione in più è attraverso il comando "nmap -sV -sS 192.168.50.102", che mi ha restituito la versione del servizio SSH utilizzato su quella porta (OpenSSH 6.7 (protocol 2.0)).

Di seguito il comando utilizzato su nmap:

```
└─# nmap -sV -sS 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 10:23 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.7 (protocol 2.0)
MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

Un'altra possibilità sarebbe quella di frammentare la rete con il comando "-f ip target" ma non ha prodotto alcun risultato.