

## TRACCIA

Utilizzare alcuni strumenti forniti per raccogliere informazioni sulla macchina metasploitable e produrre un report con l'esecuzione degli strumenti e un riepilogo delle informazioni trovate.

1 In questa prima fase è stato utilizzato il comando netdiscover -r 192.168.50.101. Questo strumento ci ha permesso di identificare gli host attivi nella rete locale inviando richieste ARP. Così è stato trovata la macchina con IP 192.168.50.101(in seguito nell'esercizio cambierà in 10.0.2.15) e il relativo MAC Address. Oltre alla lunghezza del pacchetto c'è anche il tipo di scheda di rete virtuale legata al MAC address, "PCS Systemtechnik GmbH", per via di VirtualBox:

```
Currently scanning: Finished! | 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
192.168.50.101 08:00:27:dc:2c:06 1 60 PCS Systemtechnik GmbH
```

2 Poi è stato lanciato il comando nmap -sn -PE 192.168.50.101. Questo comando esegue un ping scan (-sn) utilizzando specificamente pacchetti ICMP Echo request (opzione -PE) per determinare se l'host è online senza effettuare una scansione delle porte. Il risultato ha confermato che l'host 192.168.50.101 è attivo ("Host is up") con un indicatore di latenza e le altre informazioni trovate prima:

```
[root@kali]# nmap -sn -PE 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 11:37 EST
Nmap scan report for 192.168.50.101
Host is up (0.00081s latency).
MAC Address: 08:00:27:DC:2C:06 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

3 Il terzo step è il comando nmap 192.168.50.101 --top-ports 10 --open. Qui l'obiettivo era scansionare rapidamente le 10 porte più comuni e visualizzando esclusivamente quelle aperte. Questo ha permesso di trovare immediatamente servizi importanti attivi come FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80) e i servizi Microsoft-ds (445). La macchina meta è un server con molti servizi esposti:

```
[root@kali]# nmap 192.168.50.101 --top-ports 10 -open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 12:06 EST
Nmap scan report for 192.168.50.101
Host is up (0.00028s 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:DC:2C:06 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

4 A questo punto è stata eseguita una scansione molto più approfondita, con il comando nmap 192.168.50.101 -p- -sV --reason --dns-server ns. Questo comando ha scansionato l'intero range di porte (-p-), attivato il rilevamento delle versioni dei servizi (-sV) e richiesto la motivazione tecnica dello stato della porta (--reason). La scansione ha restituito un elenco dettagliato di software obsoleti, come vsftpd 2.3.4, Apache 2.2.8 e una bindshell sulla porta 1524, oltre a database come MySQL e PostgreSQL, tutto su porte aperte. Le reasons del perché sono aperte vengono mostrate in base agli scambi syn-ack avvenuti (solo ack se non fossero riusciti):

```
[#] nmap 192.168.50.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.95 ( https://nmap.org ) at 2023-12-01 12:10 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.00% done; ETC: 12:10 (0:00:02 remaining)
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 12:10 (0:00:02 remaining)
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 12:12 (0:00:04 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 12:12 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00014s latency).
Not shown: 65505 closed tcp ports (reset)

```

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	open	ftp	syn-ack ttl 64 vsftpd 2.3.4	
22/tcp	open	ssh	syn-ack ttl 64 OpenSSH 4.7p1 Debian 8Ubuntu1 (protocol 2.0)	
23/tcp	open	telnet	syn-ack ttl 64 Linux telnetd	
25/tcp	open	smtp	syn-ack ttl 64 Postfix smtpd	
53/tcp	open	domain	syn-ack ttl 64 ISC BIND 9.4.2	
80/tcp	open	http	syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV /2)	
111/tcp	open	rpcbind	syn-ack ttl 64 2 (RPC #100000)	
139/tcp	open	netbios-ssn	syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	

```
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec syn-ack ttl 64 netkit-rsh reexec
513/tcp open login? syn-ack ttl 64
514/tcp open shell syn-ack ttl 64 Netkit rshd
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 (Ubuntu 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
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 engine 1.1
8787/tcp open drb syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbs)
37230/tcp open status syn-ack ttl 64 1 (RPC #100024)
44785/tcp open java-rmi syn-ack ttl 64 GNU Classpath grmiregistry
57533/tcp open nlockmgr syn-ack ttl 64 1-4 (RPC #100021)
57928/tcp open mounted syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 08:00:27:DC:B6:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

È stato utilizzato poi il comando "us -mT -lV 192.168.50.101:a -r 300 -R 3 && us -mU -lV 192.168.50.101:a -r 300 -R 3" per una doppia scansione, sia TCP che UDP: && concatena due operazioni, la prima parte (-mT) scansiona le porte TCP, mentre la seconda (-mU) le porte UDP (:a dopo l'IP fa scansionare tutte le porte disponibili). Sono state impostate anche velocità e affidabilità: -r 300 manda 300 pacchetti al secondo (con 3000 essendo una vm creava problemi), mentre -R 3 fa inviare ogni pacchetto per tre volte consecutive, assicurandosi di rilevare le porte anche se dei pacchetti falliscono. L'output mostra il risultato della parte TCP, elencando rapidamente una grande quantità di porte aperte (es. 80, 445, 3306, 6667) con un TTL di 64, e la parte UDP, anche questa con svariate porte aperte ma bloccata per mancanza di tempo:

```
[root@kali㉿kali]# us -mT -Tv 192.168.50.101:a -r 300 -R 3 & us -mU -Tv 192.168.50.101:a -r 300 -R 3
adding 192.168.50.101/32 mode `TCPscan' ports 'a' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer t
han 11 Minutes, 2 Seconds
TCP open 192.168.50.101:80 ttl 64
TCP open 192.168.50.101:445 ttl 64
TCP open 192.168.50.101:514 ttl 64
TCP open 192.168.50.101:21 ttl 64
TCP open 192.168.50.101:6697 ttl 64
TCP open 192.168.50.101:37230 ttl 64
TCP open 192.168.50.101:139 ttl 64
TCP open 192.168.50.101:25 ttl 64
TCP open 192.168.50.101:5900 ttl 64
TCP open 192.168.50.101:8180 ttl 64
TCP open 192.168.50.101:6000 ttl 64
TCP open 192.168.50.101:8787 ttl 64

adding 10.0.2.15/32 mode `UDPscan'
using interface(s) eth0
scanning 1.00e+00 total hosts with
tle longer than 1 Hours, 5 Minutes
UDP open 10.0.2.2:67 ttl 255
UDP open 10.0.2.15:53218 ttl 64
UDP open 10.0.2.15:53 ttl 64
UDP open 10.0.2.15:111 ttl 64
UDP open 10.0.2.15:137 ttl 64
```

6 è stato poi lanciato il comando nmap -sS -sV -T4 10.0.2.15. Questo combina tre opzioni: la scansione SYN "stealth" (-sS) per analizzare le porte senza completare la connessione TCP, la scansione delle versioni (-sV) per trovare i software in esecuzione su ogni porta, e il tempo di scansione, impostato su "Aggressive" (-T4) per velocizzare l'operazione.

L'output è una mappa dettagliata della macchina bersaglio (che ora ha IP 10.0.2.15). Sono stati trovati servizi con versioni note per essere difettose. Il servizio sulla porta 1524 ("Metasploitable root shell") permette l'accesso root diretto senza password. In generale sono stati trovati molti altri servizi aperti, tra cui server web (Apache su 80 e Tomcat su 8180), database (MySQL su 3306) e servizi di accesso remoto:

```
(kali㉿kali)-[~]
$ nmap -sS -sV -T4 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 10:15 EST
Nmap scan report for 10.0.2.15
Host is up (0.00012s 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 rexec
513/tcp   open  login   GNU Classpath grmiregistry
514/tcp   open  tcpwrapped
1099/tcp  open  java-remi  Metasploitable root shell
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)

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: 08:00:27:8E:84:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 12.79 seconds
(kali㉿kali)-[~]
```

7 Il comando sudo hping3 --scan known 10.0.2.15 permette di inviare pacchetti TCP personalizzati; qui è stato usato in modalità "scan" per controllare le porte "known" su Metasploitable. A differenza delle scansioni precedenti con Nmap che hanno avuto successo, l'output di questo comando mostra un risultato strano: la lista finale riporta una lunga serie di "Not responding ports", tra cui quelle dei servizi che sappiamo essere attivi come FTP (21), SSH (22) e HTTP (80). Fortunatamente non è l'unico scanner a disposizione:

```
(kali㉿kali)-[~]
$ sudo hping3 --scan known 10.0.2.15
[sudo] password for kali:
Scanning 10.0.2.15 (10.0.2.15), port known
266 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-ds) (51 2 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)
```

8 Si è proceduto quindi utilizzando netcat con il comando nc -nvz 10.0.2.15 1-1024. Le opzioni -n (niente risoluzione DNS), -v (verbose) e -z (scansione senza invio dati) hanno permesso di verificare rapidamente le porte dalla 1 alla 1024. Questo metodo ha confermato manualmente la disponibilità di servizi essenziali come shell, login, exec e gli altri già visti prima:

```
(kali㉿kali)-[~]
$ nc -nvz 10.0.2.15 1-1024
(UNKNOWN) [10.0.2.15] 514 (shell) open
(UNKNOWN) [10.0.2.15] 513 (login) open
(UNKNOWN) [10.0.2.15] 512 (exec) open
(UNKNOWN) [10.0.2.15] 445 (microsoft-ds) open
(UNKNOWN) [10.0.2.15] 139 (netbios-ssn) open
(UNKNOWN) [10.0.2.15] 111 (sunrpc) open
(UNKNOWN) [10.0.2.15] 80 (http) open
(UNKNOWN) [10.0.2.15] 53 (domain) open
(UNKNOWN) [10.0.2.15] 25 (smtp) open
(UNKNOWN) [10.0.2.15] 23 (telnet) open
(UNKNOWN) [10.0.2.15] 22 (ssh) open
(UNKNOWN) [10.0.2.15] 21 (ftp) open
```

9 Sempre con Netcat è stato usato il comando nc -nv 10.0.2.15 22. per creare questa volta una connessione completa alla porta 22.

Così sono state recuperate informazioni sul server SSH: SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1. che identificano con precisione la versione del sistema operativo (Ubuntu, datata) e del servizio SSH, così da poter ricercare exploit specifici per queste versioni.

```
(kali㉿kali)-[~]
$ nc -nv 10.0.2.15 22
(UNKNOWN) [10.0.2.15] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

10 Il comando nmap -sV 10.0.2.15 trova le versioni dei servizi all'interno di una macchina. L'output elenca non solo le porte aperte, ma chiede anche al servizio qual è la sua versione. In fondo alla scansione si notano informazioni sull'host: "Hosts: metasploitable.localdomain, irc.Metasploitable.LAN", oltre ovviamente all'inventario completo delle versioni vulnerabili dei software, permettendo di mappare le vulnerabilità del sistema operativo con precisione:

```
(kali㉿kali)-[~]
$ nmap -sV 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 10:23 EST
Nmap scan report for 10.0.2.15
Host is up (0.00018s 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  tcpwrapped
1099/tcp  open  java-rmi GNU Classpath grmiregistry

1099/tcp open  java-rmi  GNU Classpath grmiregistry
1524/tcp open  bindshell Metasploitable root shell
2049/tcp open  nfs     ProFTPD 1.3.1
2121/tcp open  ftp     MySQL 5.0.51a-3ubuntu5
3306/tcp open  mysql   PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp open  postgresql VNC (protocol 3.3)
5900/tcp open  vnc     (access denied)
6000/tcp open  X11     UnrealIRCd
6667/tcp open  irc     Apache Jserv (Protocol v1.3)
8009/tcp open  ajp13   Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open  http   MAC Address: 08:00:27:8E:84:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 12.83 seconds
```

11 Infine, è stato eseguito il comando nmap -f --mtu=512 10.0.2.15 per testare le difese; l'opzione -f divide i pacchetti e --mtu=512 è la dimensione dei pacchetti divisi: in questo modo si può provare ad aggirare firewall semplici. Il risultato non è cambiato rispetto ai precedenti, dimostrando che non ci sono filtri che bloccano le richieste di pacchetti frammentati, e confermando l'enorme esposizione della macchina:

```
(kali㉿kali)-[~]
$ nmap -f --mtu=512 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 10:26 EST
Nmap scan report for 10.0.2.15
Host is up (0.00014s 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

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: 08:00:27:8E:84:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

## **CONCLUSIONI E RIEPILOGO**

Dalle scansioni effettuate sulla macchina target (IP 10.0.2.15), queste sono le conclusioni:

### **Identikit della Macchina (Target)**

- L'analisi dei servizi ha identificato il sistema operativo come una versione molto datata di Linux (Ubuntu/Debian).
- Nome Host: La macchina si presenta con il nome "metasploitable".
- Il valore TTL (Time To Live) è sempre 64: i sistemi Linux/Unix lo impostano di default a 64, mentre i sistemi Windows solitamente 128. Anche a livello di rete è confermato che il bersaglio è Linux .

### **Punti di Ingresso "Aperti"**

- Sulla porta 1524 è stato trovato un servizio chiamato "root shell". Questo è un problema grave: significa che esiste una "porta" aperta che permette a chiunque di entrare come amministratore (root).
- Software Compromessi: Sono stati individuati programmi specifici noti per contenere delle backdoor, come vsftpd 2.3.4 (Porta 21) e UnrealIRCd (Porta 6667).

### **Comunicazioni Non Protette**

- La macchina utilizza servizi vecchi come Telnet (Porta 23) e i servizi R-login (Porte 512-514). Questi mettono in chiaro anche le password scritte, diventando molto pericolosi.

### **Esposizione Totale dei Dati**

- Servizi che dovrebbero essere interni e protetti, come i database MySQL (Porta 3306) e PostgreSQL (Porta 5432), sono invece aperti e accessibili dalla rete esterna.
- Sono attivi servizi di condivisione file (NFS sulla porta 2049 e Samba sulle porte 139/445) che espongono i file nel sistema.

### **Assenza di Difese Perimetrali**

- Le scansioni hanno rilevato oltre 20 servizi aperti. Il fatto che ogni singola porta interrogata abbia risposto immediatamente conferma che non esiste alcun firewall o sistema di filtraggio attivo a protezione della macchina.