Corso Epicode
SIMULAZIONE FASE DI RACCOLTA pt2

Report a cura di Valentino Pizzi
17 settembre, 2025

Obbiettivo:
- metasploitable 192.168.50.101

Contenuti:
- nmap -sn -PE
- netdiscover -r
- nmap -top-ports 10 -open
- nmap -p- -sV -reason -dns-server ns
- nmap -sS -sV -T4
- nc -nvz 1-1024
- nc -nv 22
- nmap -sV

Obbiettivo:

Utilizzare gli strumenti visti a lezione per scansire in diversi modi la macchina metasploitable2 di “IP 192.168.50.101” per raccogliere informazioni e testare differenti strumenti e differenti comandi.

Nmap -sn -Pe:

Abbiamo utilizzato il comando nmap con i flag ***“-sn”***(ping scan) e ***“-PE”***(ICMP echo)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:13 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0085s latency).
MAC Address: 08:00:27:3D:02:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

Netdiscover -r:

Utilizziamo il comando ***"netdiscover"*** per fare un ARP scan della rete, il flag ***"-r"*** serve per scansire un range di indirizzi, in questo caso non ci serviva perché abbiamo scansionato un solo indirizzo.

```
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  08:00:27:3d:02:94      1      60  PCS Systemtechnik GmbH
```

Nmap -top-ports 10 -open:

Utilizziamo nmap con i flag ***"-top-ports 10"*** (serve per scansionare le prime 10 porte piu' conosciute) e ***"-open"***(per mostrare solo quelle aperte)

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 -top-ports 10 -open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:17 CEST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.101
Host is up (0.0067s 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: 08:00:27:3D:02:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

Nmap -p- -sV -reason -dns-server ns:

Usiamo nmap con i flag ***"-p-"***(per scansionare tutte le porte), ***"-sV"***(per conoscere la versione dei servizi attivi), ***"-reason"***(per sapere perche' quella porta e' in quel preciso stato), ***"-dns-server"***(per specificare un preciso server DNS)

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 -p- -sV -reason -dns-server 192.168.50.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:19 CEST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.15% done; ETC: 08:19 (0:00:01 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:20 (0:00:01 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:21 (0:00:04 remaining)
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.0017s 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 rexecd
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 (Admin email admin@Metasploitable.LAN)
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/drb)
39262/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
39955/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
46224/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
46518/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 08:00:27:3D:02:94 (PCS Systemtechnik/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 181.53 seconds
```

Nmap -sS -sV -T4:

Usiamo nmap con i flag ***"-sS"***(per fare una SYN scan), ***"-sV"***(per sapere la versione del servizio attivo), ***"-T4"***(per settare un timing per i pacchetti, in questo caso e' poco piu' veloce di una scansione normale)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:22 CEST
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 08:23 (0:00:01 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0089s 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: 08:00:27:3D:02:94 (PCS Systemtechnik/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 65.88 seconds
```

---

nc -nvz 1-1024:

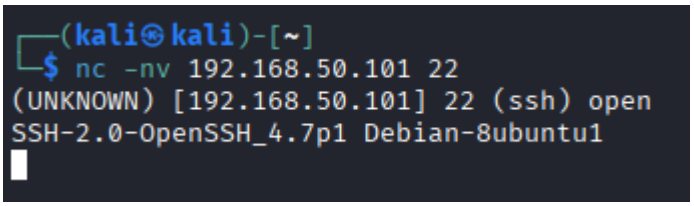
Usiamo netcat con i flag ***"-nvz"***(-n serve per indicare solo l'IP e non il DNS, -v per la ripetitivita' e -z per lo scanning) sulle porte dalla 1 alla 1024.

```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

---

nc -nv 22:

Usiamo netcat ***"-nv"***(-n serve per indicare solo l'IP e non il DNS, -v per la ripetitivita') solo sulla porta 22



Nmap -sV:

Usiamo nmap con il flag ***"-sV"*** per sapere la versione dei servizi attivi nella macchina target