Raccolta informazioni su macchina metasploitable 192.168.50.100

- **nmap -sn -PE <target>**
  - sn esegue un ping ai vari host nell'intervallo specificato. Se un host risponde, verrà elencato come attivo.

  -PE abilita la rilevazione tramite ICMP Echo Request.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 04:55 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00087s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

- **crackmapexec ssh <target>**
  interroga il servizio ssh sull'ip target

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ssh 192.168.50.100
SSH         192.168.50.100  22     192.168.50.100   [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

- **nmap -sV <target>**

  esegue lo scan delle porte principali e della versione dei servizi attivi su ciasuna porta, analizza il sistema operativo della macchina target in base al Time To Live (banner grabbing)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:42 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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 126.20 seconds
```

Riepilogo informazioni raccolte

- L'host ha IP 192.168.50.100 ed è attivo

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 04:55 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00087s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

- Il servizio ssh è attivo sulla porta 22, la versione utilizzata è relativa ad un sistema operativo Debian-Ubuntu

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ssh 192.168.50.100
SSH         192.168.50.100  22     192.168.50.100   [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

- Si conferma il sistema operativo Unix Linux, basato su kernel Linux, distribuzione Debian Ubuntu.
- Il server web è Apache httpd, attivo sulla porta 80
- Il server web JSP Apache Tomcat/Coyote, attivo sulla porta 8180

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:42 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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 126.20 seconds
```