SIMULAZIONE FASE DI RACCOLTA INFORMAZIONI W10D4

TRACCIA:

Utilizzare gli strumenti su “https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/” per raccogliere informazioni sulla macchina Metasploitable 2:

1. nmap -sn -PE <target>
2. netdiscover -r <target>
3. crackmapexec <target>
4. nmap <target> --top-ports 10 --aperto
5. nmap <target> -p- -sV --reason --dns-server ns
6. nmap -sS -sV -T4 <target>
7. hping3 --scansione conosciuta <target>
8. nc -nvz <target> 1-1024
9. nc -nv <target> 22
10. nmap -sV <target>
11. nmap -f --mtu=512 <target>

SOLUZIONE:

1. nmap -sn -PE <target>: per fare ricognizione attiva contro qualsiasi bersaglio

```
┌──(kali㉿kali)-[~]
└─$ nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 14:01 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.32.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 14:02 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0014s latency).
MAC Address: 08:00:27:E0:78:8B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

Ha confermato che il target è acceso e raggiungibile.

2. netdiscover -r <target>: per trovare host su reti wireless

```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -r 192.168.32.101
[sudo] password for kali:
```

```
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
_____________________________________________________________________________
192.168.32.101  08:00:27:e0:78:8b      1      60  PCS Systemtechnik GmbH
```

Ha identificato .101

3. crackmapexec <target>: aiuta ad automatizzare la valutazione della sicurezza delle grandi reti Active Directory

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install crackmapexec
[sudo] password for kali:
crackmapexec is already the newest version (5.4.0-0kali6).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1691

┌──(kali㉿kali)-[~]
└─$ crackmapexec 192.168.32.101
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {ssh,mssql,smb,winrm,ldap,ftp,rdp} ...
crackmapexec: error: argument protocol: invalid choice: '192.168.32.101' (choose from ssh, mssql, smb, winrm, ldap, ftp, rdp)

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.32.101
SMB         192.168.32.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
```

Ha rilevato la vulnerabilità Samba

4. nmap <target> --top-ports 10 --aperto: identifica le prime 10 porte aperte in qualsiasi rete

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.101 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 14:12 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0036s 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:E0:78:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

Ha identificato le porte 21, 22, 23, 25, 80, 139 e 445 aperte

5. nmap <target> -p- -sV --reason --dns-server ns: per capire il motivo per cui una porta è contrassegnata come aperta, chiusa o filtrata

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 14:54 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up, received arp-response (0.00080s 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
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)
47172/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
53146/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
56469/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
60043/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 08:00:27:E0:78:8B (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 207.15 seconds
```

Ha identificato diverse porte aperte con versioni

6. nmap -sS -sV -T4 <target>: determina se la porta è in ascolto

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -T4 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-07 09:44 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00067s latency).
Not shown: 978 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
8180/tcp open  unknown
MAC Address: 08:00:27:E0:78:8B (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 194.31 seconds
```

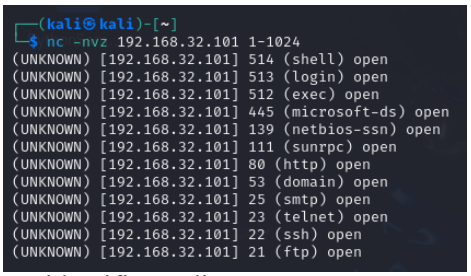
Ha identificato diverse porte comuni

7. hping3 --scan know <target>: assemblatore/analizzatore di pacchetti TCP/IP

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.32.101
[sudo] password for kali:
Scanning 192.168.32.101 (192.168.32.101), port known
264 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-d) (512 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)
```

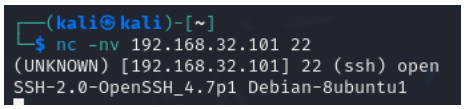
Conferma servizi TCP aperti

8. nc -nvz <target> 1-1024: legge e scrive dati attraverso le connessioni di rete, utilizzando il protocollo TCP/IP



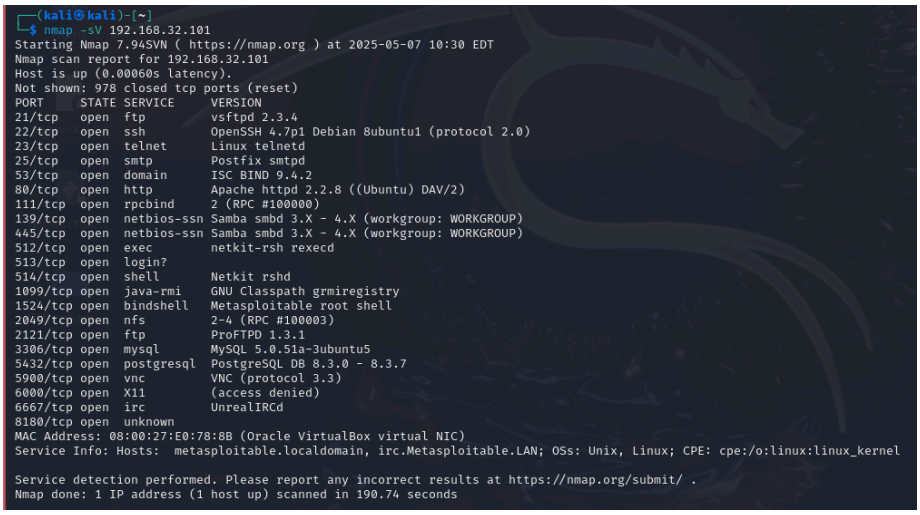
Ha identificato diverse porte aperte

9. nc -nv <target> 22: per scansionare un particolare numero di porta rispetto a qualsiasi obiettivo



SSH attivo con info banner utili

10. nmap -sV <target>: fa una valutazione dettagliata di ciò che è realmente in esecuzione



11. nmap -f --mtu=512 <target>: per aggirare le restrizioni del firewall mediante la frammentazione dei pacchetti