SCANSIONE DEI SERVIZI CON NMAP W11D1

TRACCIA:

Effettuare queste scansioni sul target Metasploitable 2:

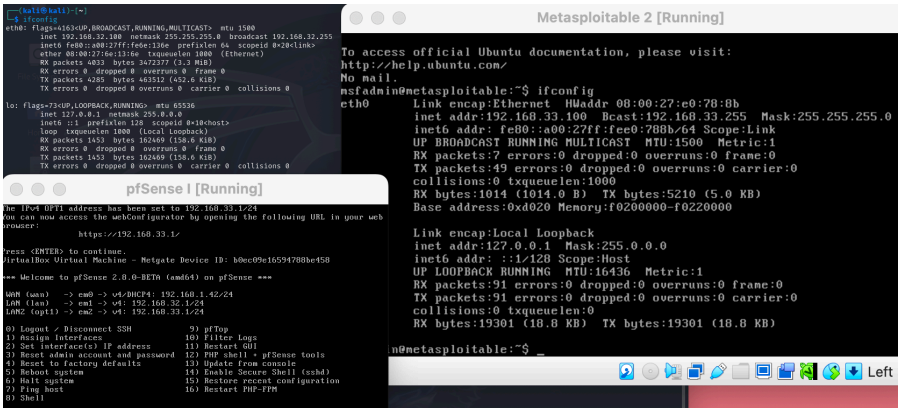
1. OS Fingerprint
2. Syn Scan
3. TCP Connect
4. Version Detection

Riportare le seguenti informazioni:

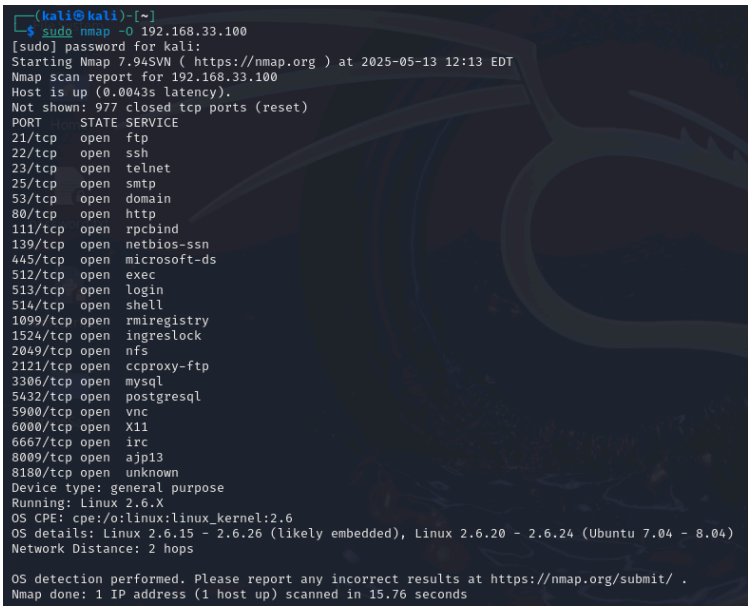
- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

SOLUZIONE:

Configurare Kali, Metasploitable 2 e Pfsense come segue



1. OS Fingerprint: scan per trovare dettagli sul sistema operativo del target



2. Syn Scan: esegue una scansione SYN sul target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.33.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:15 EDT
Nmap scan report for 192.168.33.100
Host is up (0.036s 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

Nmap done: 1 IP address (1 host up) scanned in 13.75 seconds
```

3. TCP Connect: esegue una scansione TCP sul target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.33.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:17 EDT
Nmap scan report for 192.168.33.100
Host is up (0.060s 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

Nmap done: 1 IP address (1 host up) scanned in 13.94 seconds
```

4. Version Detection: esegue una scansione TCP sul target, specificando la versione dei servizi

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.33.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:19 EDT
Nmap scan report for 192.168.33.100
Host is up (0.054s 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  ccproxy-ftp?
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
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 187.44 seconds
```