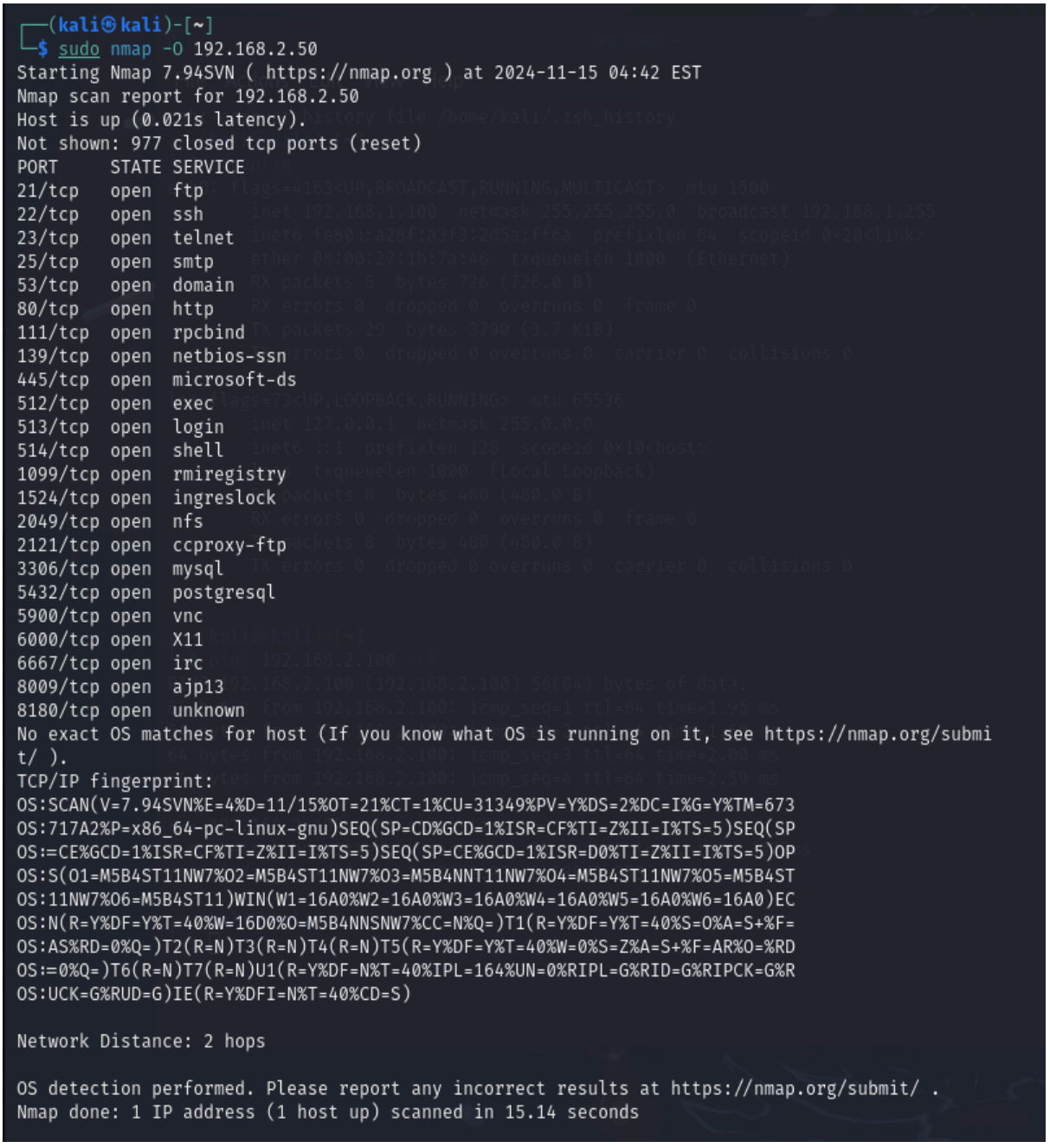
Esercizio W11D1 di Pandolfi Luciano - Scansione dei servizi in ascolto

Traccia: Tecniche di scansione con Nmap

Si richiede di effettuare le seguenti scansioni sul target Metasploitable (target e attaccante devono essere su due reti diverse):
ATTACCANTE: Kali Linux ip 192.168.1.100
TARGET: Metasploitable_2 ip 192.168.2.50

● **OS fingerprint**



- **Syn Scan**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.2.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 04:44 EST
Nmap scan report for 192.168.2.50
Host is up (0.045s 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 3.09 seconds
```

- **TCP connect**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.2.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 04:48 EST
Nmap scan report for 192.168.2.50
Host is up (0.067s 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 2.92 seconds
```

● **Version detection**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.2.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 04:49 EST
Nmap scan report for 192.168.2.50
Host is up (0.039s 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       OpenBSD or Solaris rlogind
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       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:lin
ux: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 18.41 seconds
```

1. **IP del Target:**

   Indirizzo IP del target Metasploitable (`192.168.2.50`).

2. **Sistema Operativo:**

   I risultati del rilevamento del sistema operativo non sono presenti a causa di un errore (non identificato “ No exact OS matches for host”).

3. **Porte Aperte:**

   Alcune delle porte aperte scoperte durante le scansioni (sia con `-sS`, `-sT`, e `-sV`) sono ad esempio:

   - Porta 22 (SSH)
   - Porta 23 (Telnet)
   - Porta 80 (HTTP)
   - Porta 445 (SMB)

4. **Servizi in Ascolto con Versione:**

La scansione con `-sV` mi ha fornito informazioni sui servizi e le versioni specifiche in esecuzione su ciascuna porta aperta, ad esempio:

- Porta 22: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- Porta 23: Linux telnetd
- Porta 80: Apache httpd 2.2.8 ((Ubuntu) DAV/2)
- Porta 445: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

5. **Descrizione dei Servizi:**

- **SSH (Porta 22)**: Il servizio SSH permette l'accesso remoto sicuro a una macchina tramite una connessione criptata. Viene utilizzato per amministrare server e sistemi in modo sicuro.
- **Telnet (Porta 23)**: Telnet è un protocollo di rete per la comunicazione remota, ma è considerato obsoleto e insicuro poiché trasmette i dati in chiaro.
- **HTTP (Porta 80)**: HTTP è il protocollo principale per il trasferimento di pagine web e viene utilizzato dai browser per caricare siti web.
  Non è criptato, infatti si preferisce l'uso di HTTPS che è la versione sicura di HTTP.
- **SMB (Porta 445)**: il servizio SMB serve per la condivisione di file e stampanti in una rete locale, tipicamente tra dispositivi Windows.