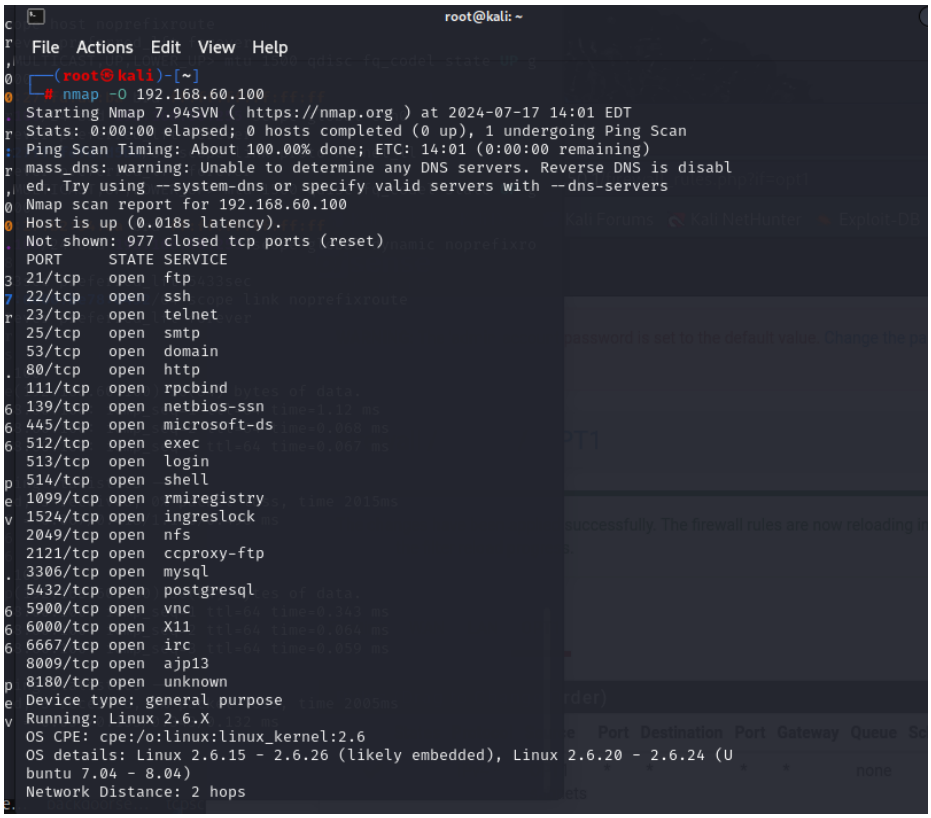
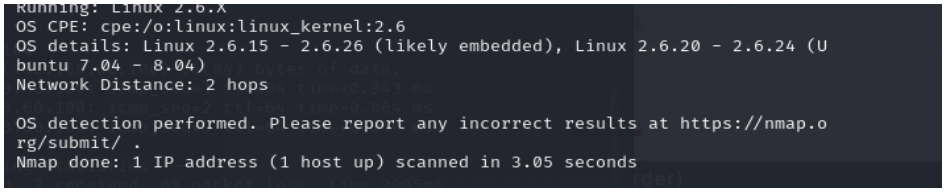
W11D1 – Scansioni con Nmap su reti diverse

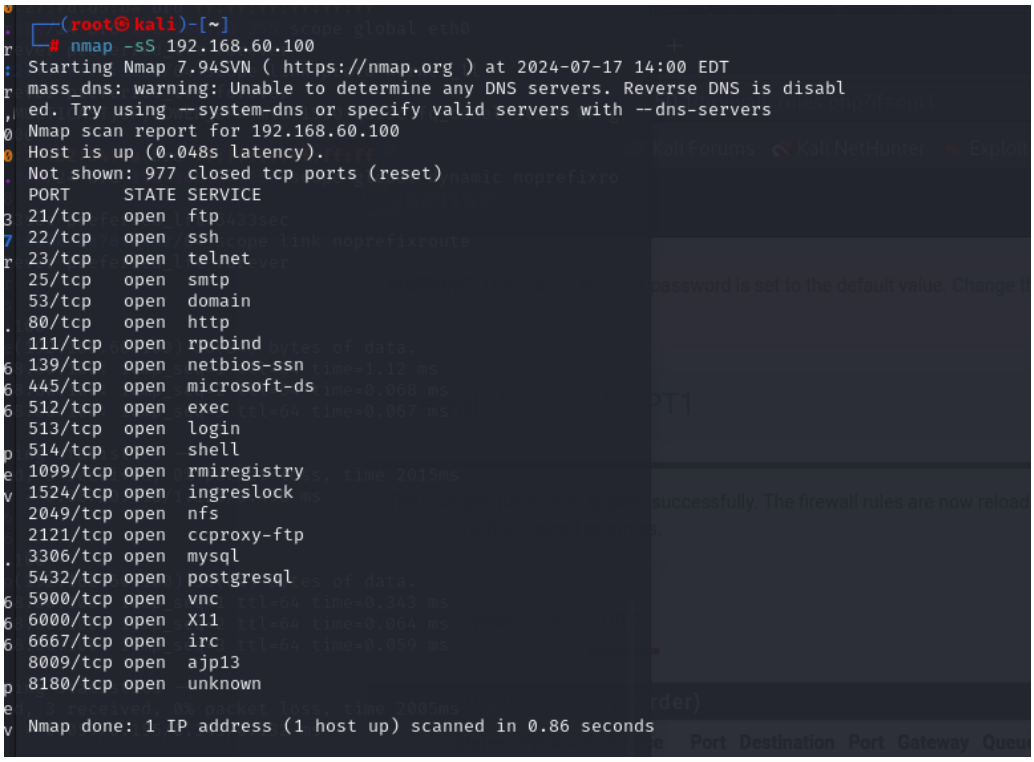
Esercizio obbligatorio ed esercizio facoltativo

OS fingerprint con le macchine su reti diverse.



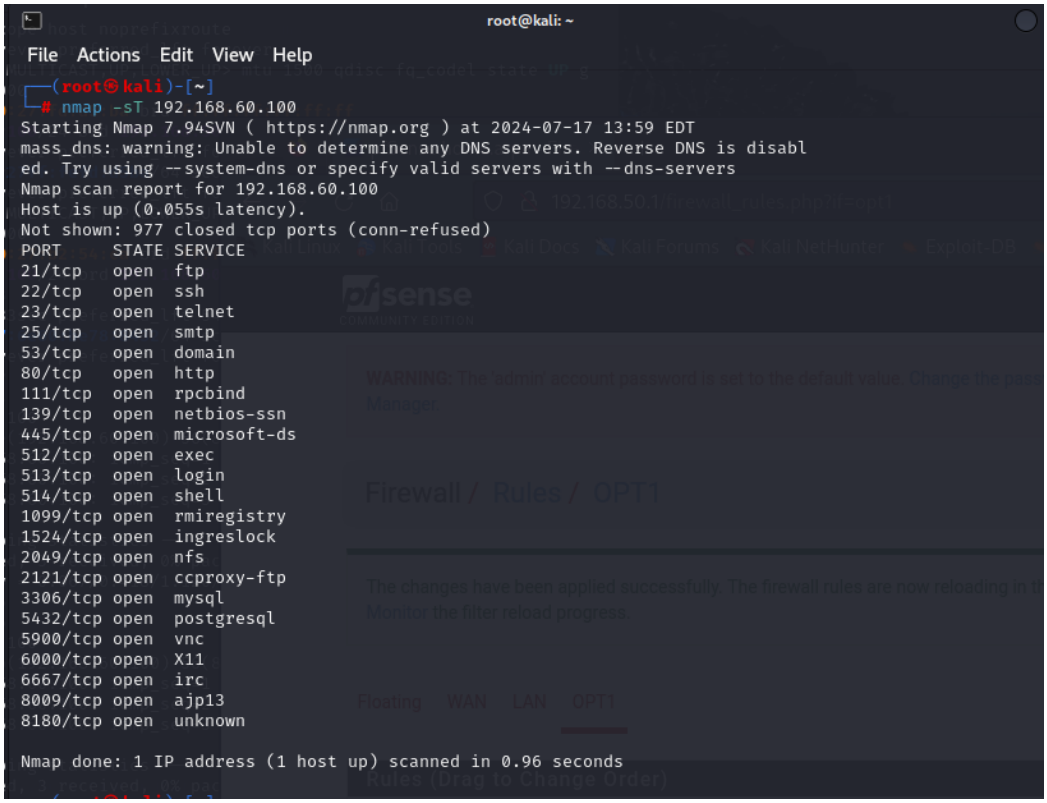


Scansione SYN con le macchine su reti diverse.



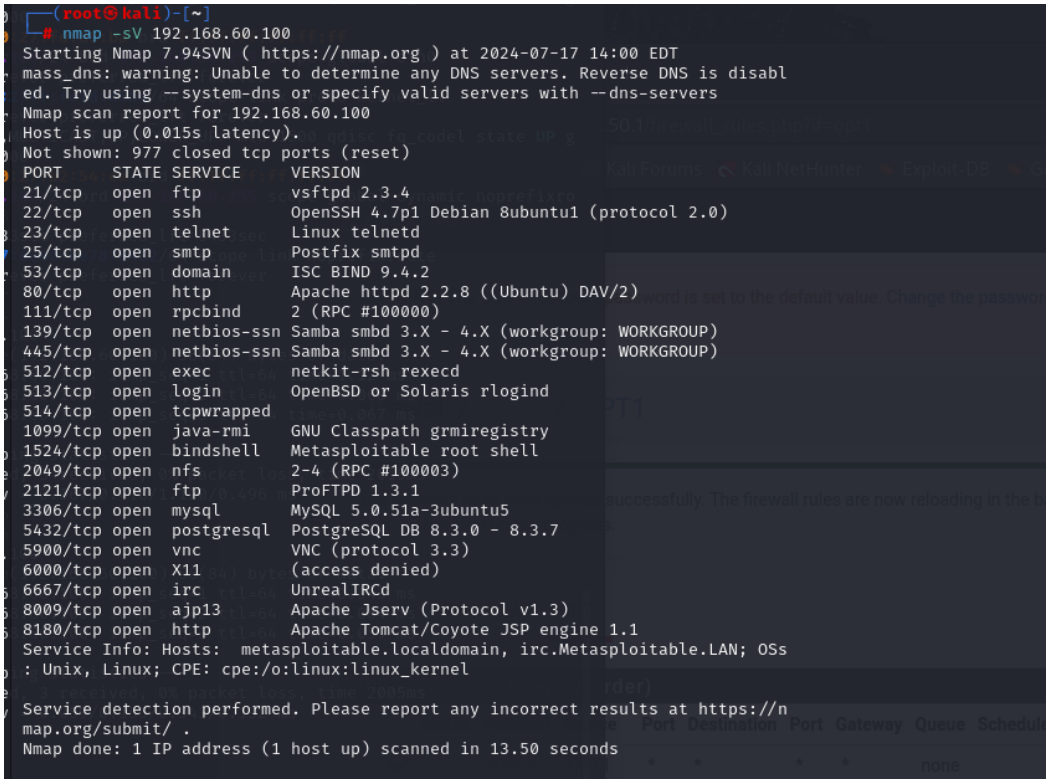
```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.60.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 14:00 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.60.100
Host is up (0.048s 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 0.86 seconds
```

Scansione TCP con le macchine su reti diverse.

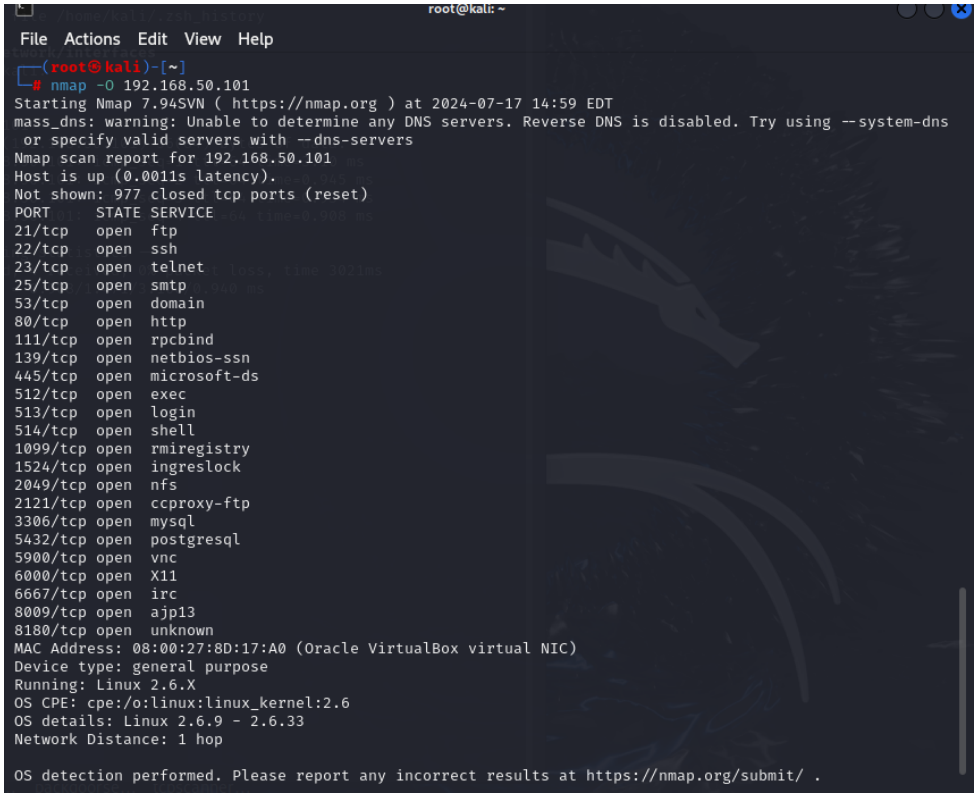


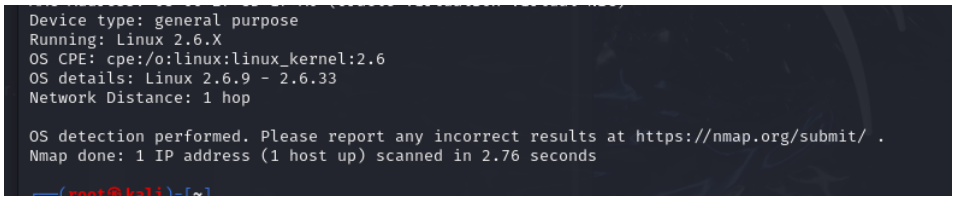
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.60.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 13:59 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.60.100
Host is up (0.055s 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 0.96 seconds
```

Version detection con le macchine su reti diverse

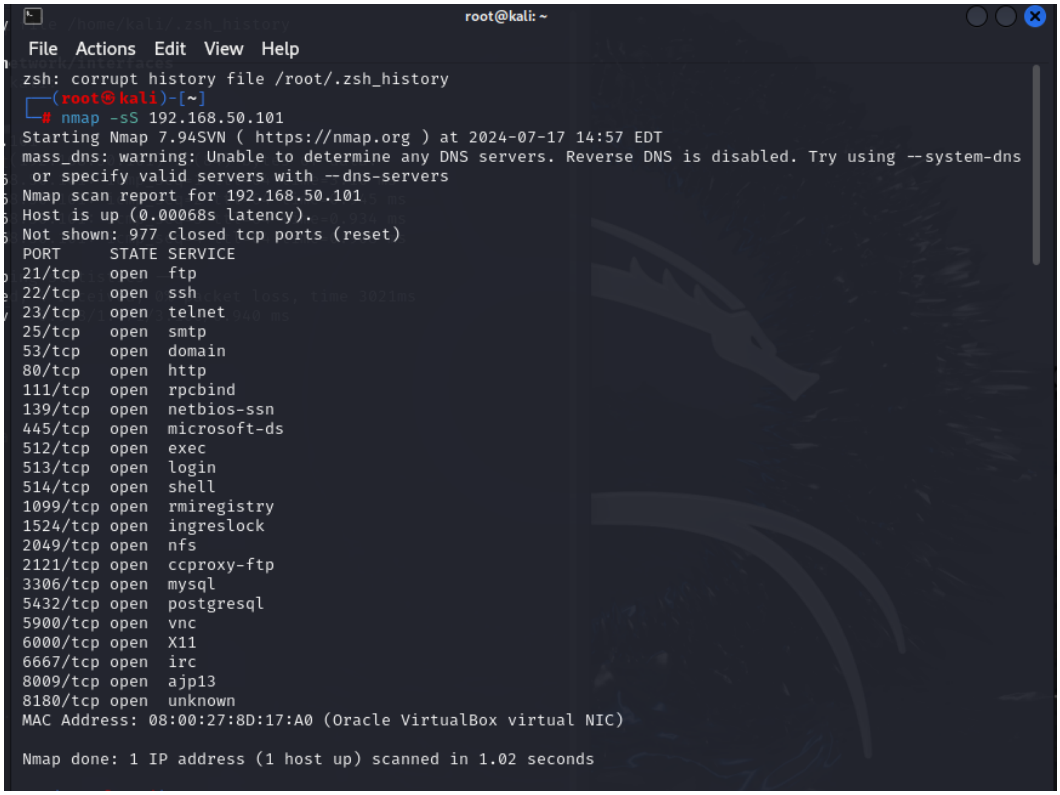


OS fingerprint con le macchine sulla stessa rete





Scansione SYN con le macchine sulla stessa rete.



Scansione TCP con le macchine sulla stessa rete.

```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 14:57 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 192.168.50.101
Host is up (0.0014s 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
MAC Address: 08:00:27:8D:17:A0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Scansione version detection con le macchine sulla stessa rete.

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 14:57 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 192.168.50.101
Host is up (0.00078s 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: 08:00:27:8D:17:A0 (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 55.99 seconds
```

Report della scansione e differenze tra la scansione svolta su reti diverse e la scansione svolta sulla stessa rete.

Il target della scansione è sempre stato la macchina Metasploitable 2, con l'IP 192.168.60.100 quando si trovava su una rete diversa rispetto alla macchina Kali Linux e

con l'IP 192.168.50.101 quando si trovava sulla stessa rete di Kali Linux. Il sistema operativo è stato individuato in entrambi i casi correttamente: con la macchina su reti diverse, il sistema operativo rilevato sulla macchina su reti diverse 192.168.60.100 è stato Linux versione 2.6.X. Il kernel è Linux e nei dettagli del sistema operativo è riportato che il sistema operativo è Linux 2.6.15-2.6.26, probabilmente embedded, e riporta anche le versioni di Linux 2.6.20-2.6.24, versione Ubuntu 7.04-8.04. Anche la macchina sulla stessa rete con IP 192.168.50.101 ha come sistema operativo Linux 2.6.X, ipotizzando una versione Linux tra 2.6.9 e 2.6.33. Non vi sono quindi grandi differenze in termini di OS fingerprint tra le macchine sulla stessa rete e le macchine su reti diverse, perché il sistema Linux 2.6.X è stato individuato in entrambi i casi con leggerissime differenze successive. Per quanto riguarda le porte aperte sulla macchina con IP 192.168.60.100 su reti diverse rispetto a Kali Linux, sia la scansione TCP che la scansione SYN hanno individuato 23 porte aperte e 977 porte chiuse. Le porte aperte sono le porte 21, 22, 23, 25 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180. I servizi in ascolto su queste porte sono, rispettivamente, ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsoft-ds, exec, login, shell, rmiregistry, ingreslock, nfs, ccproxy-ftp, mysql, postgresql, vnc, X11, irc, ajp13 ed un servizio sconosciuto. Le versioni di questi servizi sono, rispettivamente, vsftpd 2.3.4, OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0), Linux telnetd, Postfix smtpd, ISC BIND 9.4.2, Apache httpd 2.2.8, ((Ubuntu) DAV/2), 2 (RPC #100000), Samba smbd 3.X – 4.X(workgroup: WORKGROUP), Samba smbd 3.X – 4.X(workgroup: WORKGROUP), netkit-rsh rexecd, OpenBSD or Solaris rlogind, tcpwrapped, java-rmi GNU Classpath grmiregistry, bindshell Metasploitable root shell, 2-4 (RPC #100000), ProFTPD 1.3.1, mySQL 5.0.51a-3ubuntu5, postgreSQL DB 8.3.0 – 8.3.7, VNC protocol 3.3., accesso negato per X11, unrealIRCd, Apache Jserv (protocol v1.3), servizio http sulla porta 8180 con versione Apache Tomcat/Coyote JSP engine 1.1. Non vi sono differenze tra i risultati dati dalla scansione TCP e dalla scansione SYN, perché le porte aperte sono le stesse e i servizi attivi sono gli stessi. Cambia solamente la modalità con cui avviene la scansione, perché la scansione TCP instaura un canale di comunicazione completando il three-way-handshake, mentre la scansione SYN è meno invasiva e non instaura un canale perché non completa il three-way-handshake, come si vede catturando i pacchetti scambiati con Wireshark. Confrontando la scansione sulla macchina su reti diverse con la scansione effettuata con le due macchine sulla stessa rete, non sono emerse differenze. Vi è lo stesso numero di porte aperte, le porte aperte sono le stesse e i servizi attivi sono gli stessi. Anche le versioni dei servizi sono le stesse, tranne che per una piccola differenza per la macchina 192.168.50.101 nella porta 513, dove il servizio non è riportato, e nella porta 514 dove è riportato il servizio shell con versione Netkit rshd. Alla luce di questo, si può concludere che non vi siano differenze nella scansione con entrambe le macchine sulla stessa rete e le due macchine su reti diverse. Andando a descrivere brevemente i servizi attivi trovati, il servizio ftp file transfer protocol serve per trasferire file tra computer su internet, mentre il servizio ssh secure shell è un protocollo di rete crittografico per gli accessi remoti. Telnet è un protocollo di rete che serve per stabilire una connessione con un server remoto, smtp è simple mail transfer protocol ed è un servizio che consente di inviare e ricevere email.

Domain è il servizio DNS che traduce gli IP in domini e viceversa, http è un protocollo che consente la comunicazione tra client e server, rpcbind è specifico di Linux e converte i numeri RPC (remote procedure call) in indirizzi universali. Netbios-ssn è un servizio che consente a due nodi Netbios di stabilire una connessione e mantenere una sessione, microsoft-ds serve per la registrazione di dispositivi di rete, exec è un servizio scritto in linguaggio C che permette di sostituire segmenti di codice e dati di un processo in esecuzione con quelli di un programma contenuto in file eseguibile specificato, aprendo ad esempio un nuovo programma nello stesso processo mantenendo lo stesso PID. Login serve per la gestione dei login, mentre shell esegue comandi da linea di comando, rmiregistry tiene traccia di tutti gli oggetti remoti disponibili su un dato server ed ingreslock può essere usato come backdoor per eseguire del codice da linea di comando. NFS, network file system, consente di accedere a cartelle e directory presenti su server remoti come se fossero presenti nella rete locale, ccproxy-ftp è sempre legato al protocollo ftp descritto precedentemente, mySQL consente di gestire dei database e postgresql fornisce funzioni in supporto a mySQL per la gestione dei database. VNC virtual network computing, è un protocollo di desktop remoto che serve a visualizzare e controllare un computer da remoto tramite la rete, X11 serve a visualizzare le interfacce utente grafiche sullo schermo, irc (internet relay chat) facilita la comunicazione sotto forma di testo in una architettura client-server e infine ajp13 è un protocollo che consente la comunicazione tra un server Apache e un server di applicazioni.