```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:01 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00057s 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
MAC Address: 08:00:27:F1:EF:B9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 07:58 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00090s 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
MAC Address: 08:00:27:F1:EF:B9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:02 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00076s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:2E:13:03 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.02 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:06 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:2E:13:03 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.97 seconds
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:45 EDT
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:47 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:2E:13:03 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server
_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:13 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0019s 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:F1:EF:B9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

Per l'analisi della sicurezza dei sistemi, ho utilizzato lo strumento Nmap per condurre una serie di scansioni sul target Metasploitable e su un sistema Windows 7.

Per quanto riguarda Metasploitable, ho eseguito diverse scansioni per ottenere informazioni dettagliate sul sistema operativo, le porte aperte e i servizi in esecuzione. Utilizzando la funzione di fingerprinting dell'OS di Nmap, ho identificato il sistema operativo come Linux. Successivamente, ho eseguito una scansione SYN per individuare le porte aperte e i servizi in ascolto, seguita da una scansione TCP Connect per confrontare i risultati e rilevare eventuali discrepanze. Inoltre, ho eseguito una scansione di rilevamento delle versioni dei servizi per ottenere informazioni sulle versioni specifiche dei servizi in esecuzione.

Per quanto riguarda il sistema Windows 7, ho eseguito una scansione di fingerprinting dell'OS per identificare il sistema operativo. Tuttavia, durante la scansione, non sono state rilevate porte aperte, suggerendo una possibile configurazione di rete più restrittiva o una minore esposizione rispetto al sistema Metasploitable.

Le informazioni raccolte durante queste scansioni sono cruciali per valutare la sicurezza dei sistemi e identificare eventuali vulnerabilità che potrebbero essere sfruttate da potenziali attaccanti. Il confronto tra le scansioni SYN e TCP Connect su Metasploitable ha evidenziato le differenze di velocità e precisione tra i due metodi di scansione, fornendo utili informazioni per futuri test di penetrazione e analisi della sicurezza dei sistemi.