The object of this exercise is to make practice with nmap in kali linux.
We have some targets:
- *Metasploitable2, IP 192.168.49.101*
- *Windows 7, IP 192.168.50.102*

NMAP code results
To Metasploitable2

In this case there aren't difference between SYN scan (with -sS) and TCP connect scan (-sT) because there isn't a firewall or IPS to block or reduce the traffic packets.
Often the SYN scan is more quietly and recommended in stealth mode to make any noises.

```
┌──(root㉿kali)-[/]
└─# nmap -sV 192.168.49.101 -O --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:06 CET
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 192.168.49.101
Host is up (0.00032s 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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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?
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  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.31 seconds
```

In this case we can see the ports that are open, the service in each port and the version of the service.
Another informations are the OS details.

To Windows 7


```
┌──(root㉿kali)-[/]
└─# nmap -sV 192.168.50.102 -O --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:44 CET
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 192.168.50.102
Host is up (0.00016s latency).
Not shown: 987 closed tcp ports (reset)
PORT       STATE SERVICE       VERSION
135/tcp    open  msrpc         Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc         Microsoft Windows RPC
49153/tcp  open  msrpc         Microsoft Windows RPC
49154/tcp  open  msrpc         Microsoft Windows RPC
49155/tcp  open  msrpc         Microsoft Windows RPC
49156/tcp  open  msrpc         Microsoft Windows RPC
49157/tcp  open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:02:00:03 (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
Service Info: Host: TIGER-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.24 seconds
```

In this case we can see the ports that are open, the service in each port and the version of the service.
Another informations are the OS details.