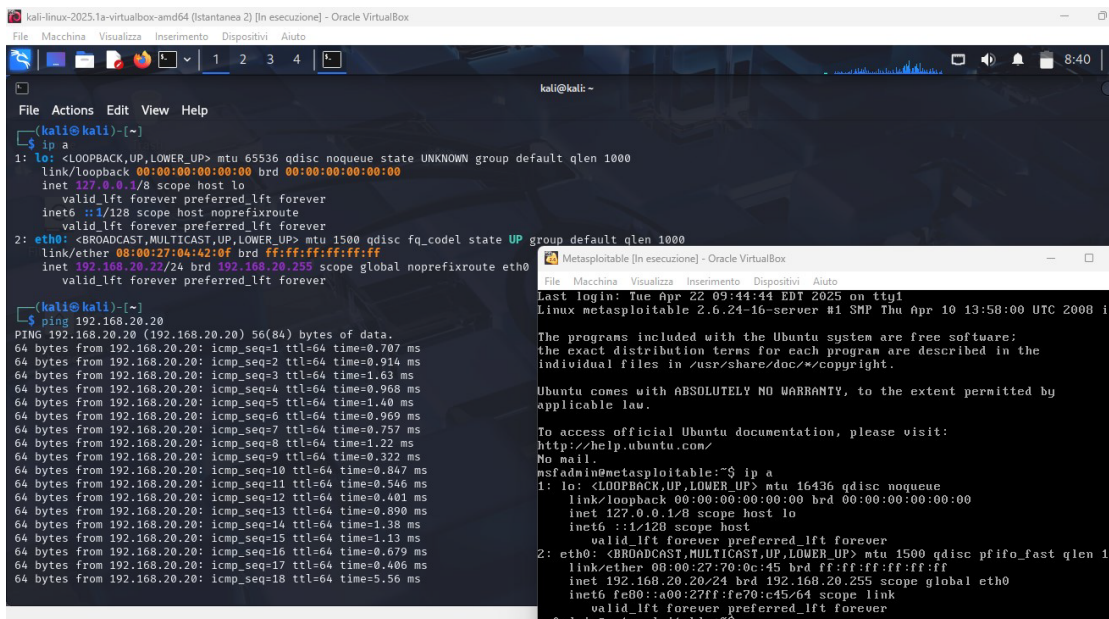


ESERCIZIO 1

IP TARGET: 192.168.20.20

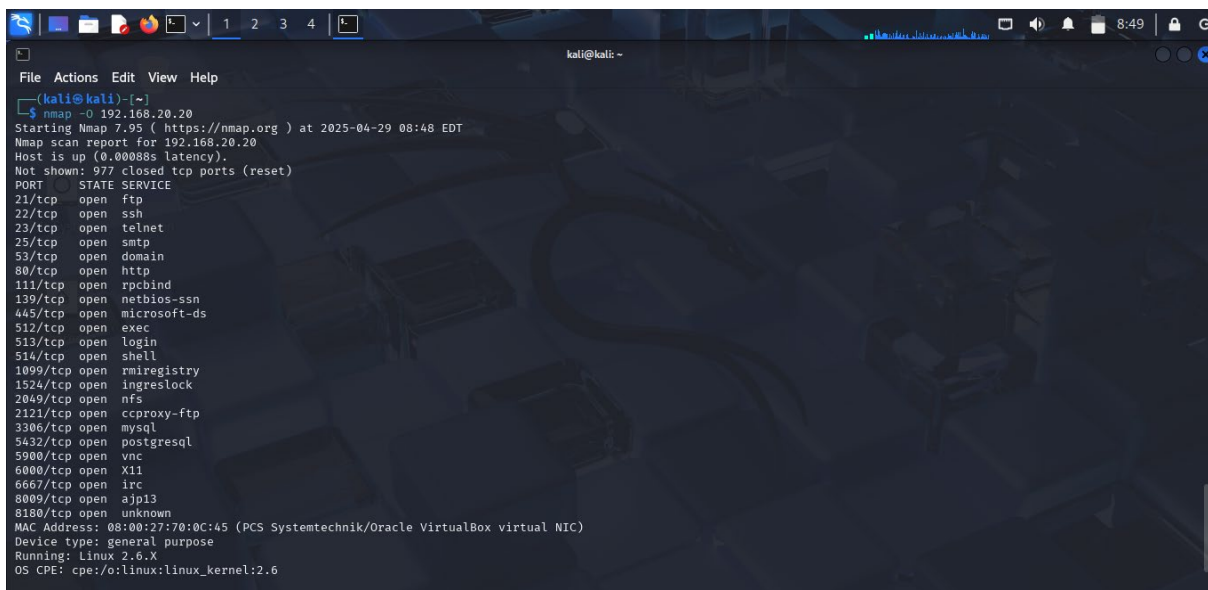
CON IL COMANDO PING VERIFICO CHE METASPLOITABLE È RAGGIUNGIBILE DA KALI.



```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.22/24 brd 192.168.20.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever

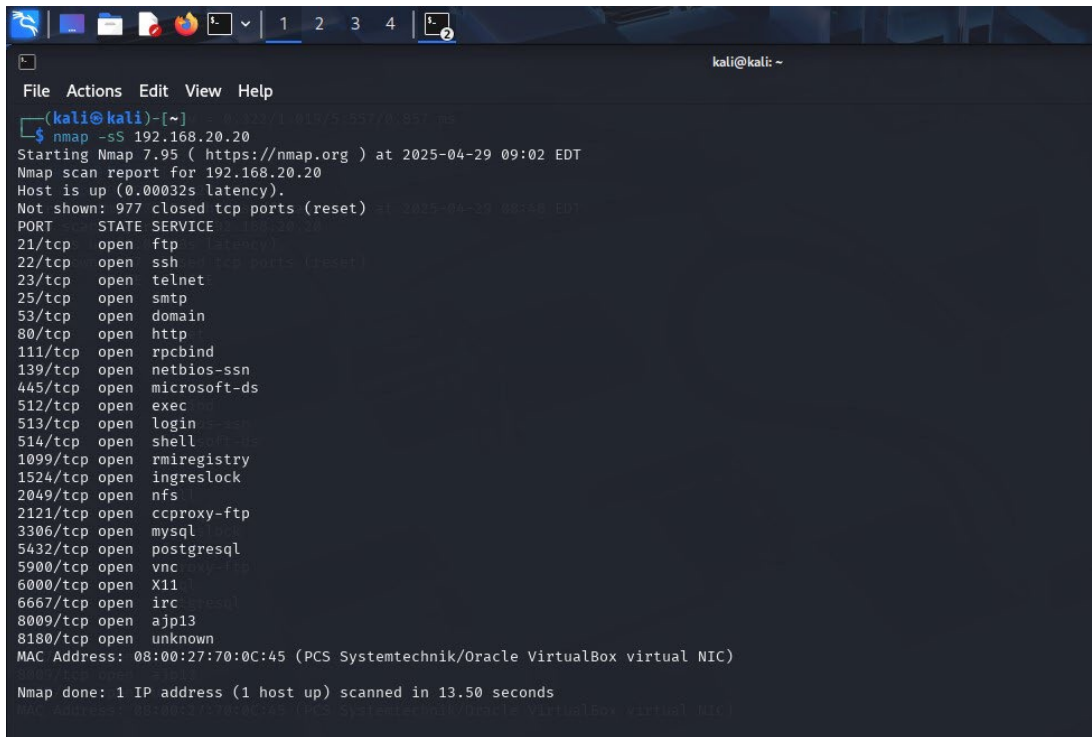
kali@kali:~$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data:
64 bytes from 192.168.20.20: icmp_seq=1 ttl=64 time=0.707 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=64 time=0.914 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=64 time=1.63 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=64 time=0.968 ms
64 bytes from 192.168.20.20: icmp_seq=5 ttl=64 time=1.40 ms
64 bytes from 192.168.20.20: icmp_seq=6 ttl=64 time=0.969 ms
64 bytes from 192.168.20.20: icmp_seq=7 ttl=64 time=0.757 ms
64 bytes from 192.168.20.20: icmp_seq=8 ttl=64 time=1.22 ms
64 bytes from 192.168.20.20: icmp_seq=9 ttl=64 time=0.322 ms
64 bytes from 192.168.20.20: icmp_seq=10 ttl=64 time=0.847 ms
64 bytes from 192.168.20.20: icmp_seq=11 ttl=64 time=0.546 ms
64 bytes from 192.168.20.20: icmp_seq=12 ttl=64 time=0.401 ms
64 bytes from 192.168.20.20: icmp_seq=13 ttl=64 time=0.890 ms
64 bytes from 192.168.20.20: icmp_seq=14 ttl=64 time=1.38 ms
64 bytes from 192.168.20.20: icmp_seq=15 ttl=64 time=1.13 ms
64 bytes from 192.168.20.20: icmp_seq=16 ttl=64 time=0.679 ms
64 bytes from 192.168.20.20: icmp_seq=17 ttl=64 time=0.406 ms
64 bytes from 192.168.20.20: icmp_seq=18 ttl=64 time=5.56 ms
```

PER ESEGUIRE LA SCANSIONE OS Fingerprint ho utilizzato il comando nmap -O 192.168.20.20 così da determinare il **sistema operativo del target che in questo caso è Linux 2.6.X**



```
kali@kali:~$ nmap -O 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 08:48 EDT
Nmap scan report for 192.168.20.20
Host is up (0.00088s 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  xli
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:04:42:0f (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

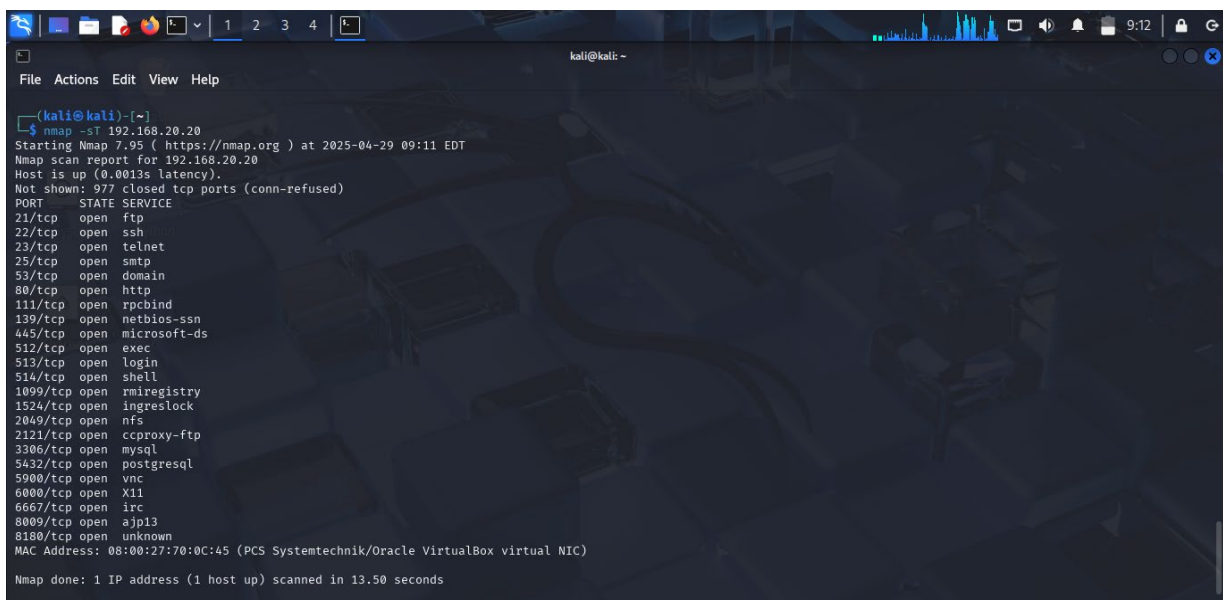
Per determinare la scansione Syn Scan ho usato il comando: **nmap -sS 192.168.20.20**, questo tipo di scansione non completa la connessione TCP



```
(kali@kali)-[~]
└─$ nmap -sS 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:02 EDT
Nmap scan report for 192.168.20.20
Host is up (0.00032s 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: 08:00:27:70:0C:45 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

Ora per la scansione TCP ho usato il comando **nmap -sT 192.168.20.20** questo tipo di scansione utilizza la connessione TCP completa.



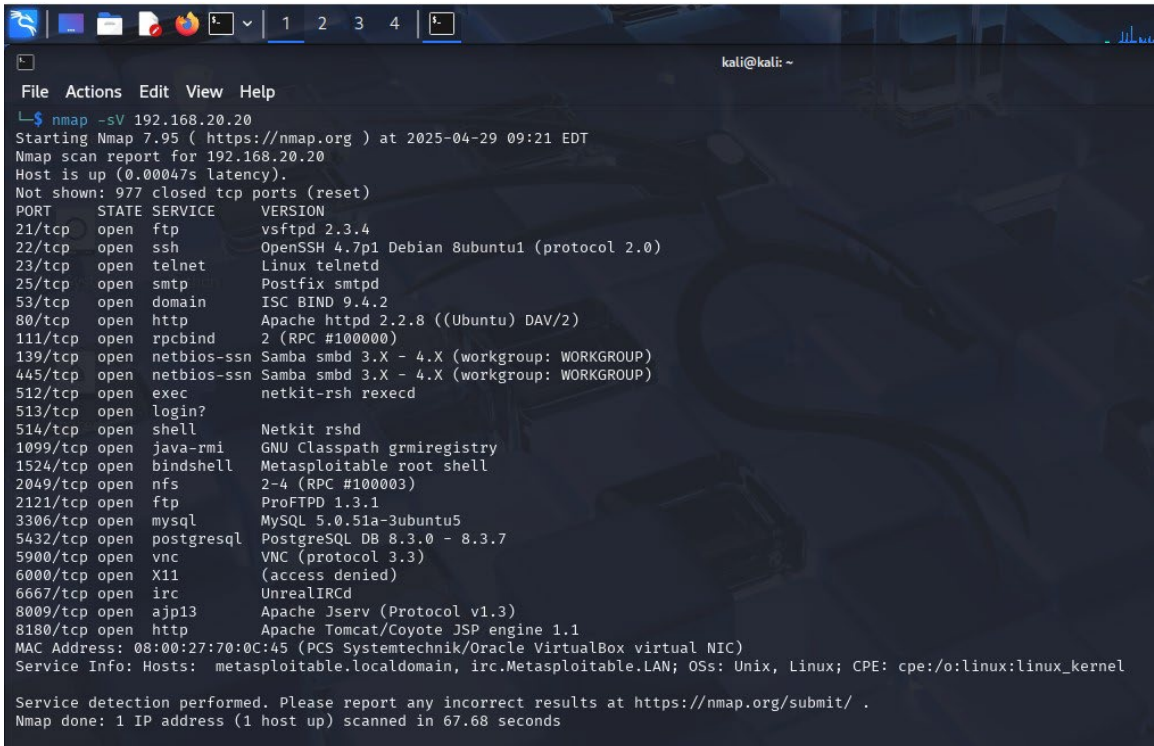
```
(kali@kali)-[~]
└─$ nmap -sT 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:11 EDT
Nmap scan report for 192.168.20.20
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  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: 08:00:27:70:0C:45 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

Di seguito, una tabella che riporta le porte aperte rilevate dalle scansioni precedentemente eseguite in SYN e TCP

Porta	Servizio
21	ftp
22	ssh
23	telnet
25	smtp
53	domain
80	http
111	rpcbind
139	netbios-ssn
445	microsoft-ds
512	exec
513	login
514	shell
1094	rmiregistry
1524	ingreslock
2049	nfs
2121	ccpnoxy-ftp
3306	mysql
5432	postgresql
5900	vnc
6000	X11
6667	irc
8009	ajp13
8180	http-alt

Per la scansione Version Detection ho usato il comando **nmap -sV 192.168.20.20** che identifica le versioni dei servizi in esecuzione nelle porte aperte



```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -sV 192.168.20.20  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:21 EDT  
Nmap scan report for 192.168.20.20  
Host is up (0.00047s 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: 08:00:27:70:0C:45 (PCS Systemtechnik/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 67.68 seconds
```

Di seguito, una tabella che riporta servizi in ascolto e relativa versione:

Servizio	Versione
ftp	vsftpd 2.3.4
ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
telnet	Linux telnetd
smtp	Postfix smtpd
domain	ISC BIND 9.4.2
http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
rpcbind	2 (RPC #100000)
netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
microsoft-ds	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec	netkit-rsh rexecd
login	login?
shell	Netkit rshd
java-rmi	GNU Classpath grmiregistry
bindshell	Metasploitable root shell
nfs	2-4 (RPC #100003)
ftp	ProFTPD 1.3.1
mysql	MySQL 5.0.51a-3ubuntu5
postgresql	PostgreSQL DB 8.3.0 - 8.3.7
vnc	VNC (protocol 3.3)
X11	access denied
irc	UnrealIRCd
ajp13	Apache JServ Protocol v1.3
http-alt	Apache Tomcat/Coyote JSP engine 1.1

Esercizio 2

IP TARGET: 192.168.10.10

PER ESEGUIRE LA SCANSIONE OS Fingerprint ho utilizzato il comando **nmap -O 192.168.10.10** così da determinare il sistema operativo del target, che in questo caso è Windows 10.



```
(kali@kali)~$ nmap -O 192.168.10.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:36 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 192.168.10.10
Host is up (0.0011s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:2F:94:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
```