Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:
1- OS fingerprint
2- Syn Scan TCP connect
3- trovate differenze tra i risultati della scansioni TCP connect e SYN?
4- Version detection

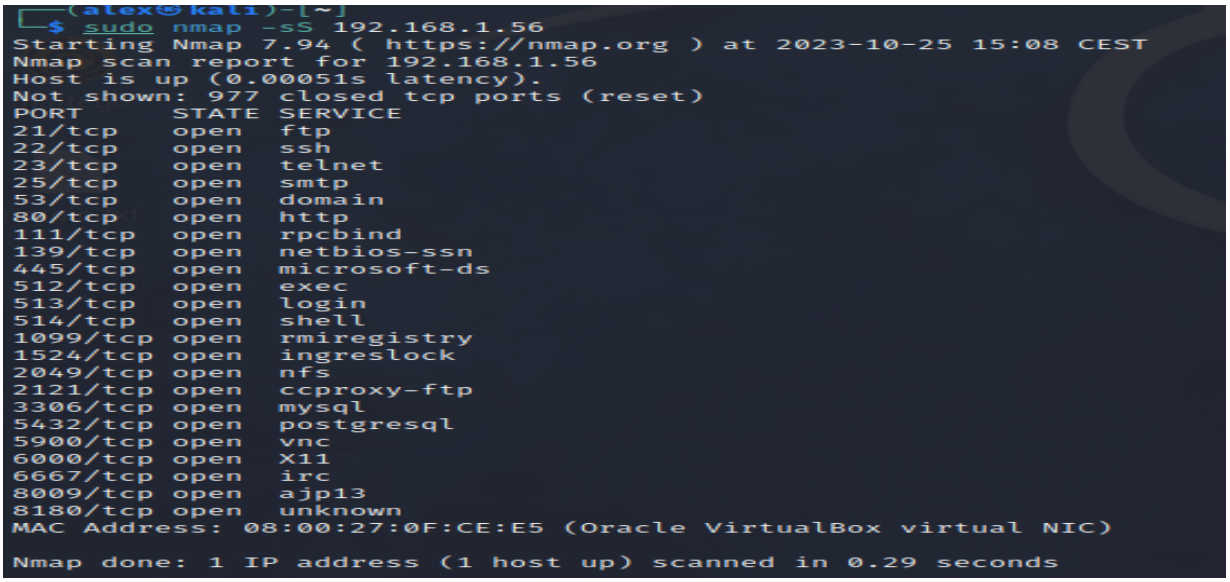
1- Utilizzeremo il seguente codice per estrapolare informazioni sul S.O. (con relativi dettagli sulla versione della macchina target).Inoltre possiamo notare che, oltre il S.O. , abbiamo altre info sulle relative porte attive e il mac-address(info utile per un attacco MAC address spoofing)

```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.56
[sudo] password for alex:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:56 CEST
Nmap scan report for 192.168.1.56
Host is up (0.00065s 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: 08:00:27:0F:CE:E5 (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 1.63 seconds
```

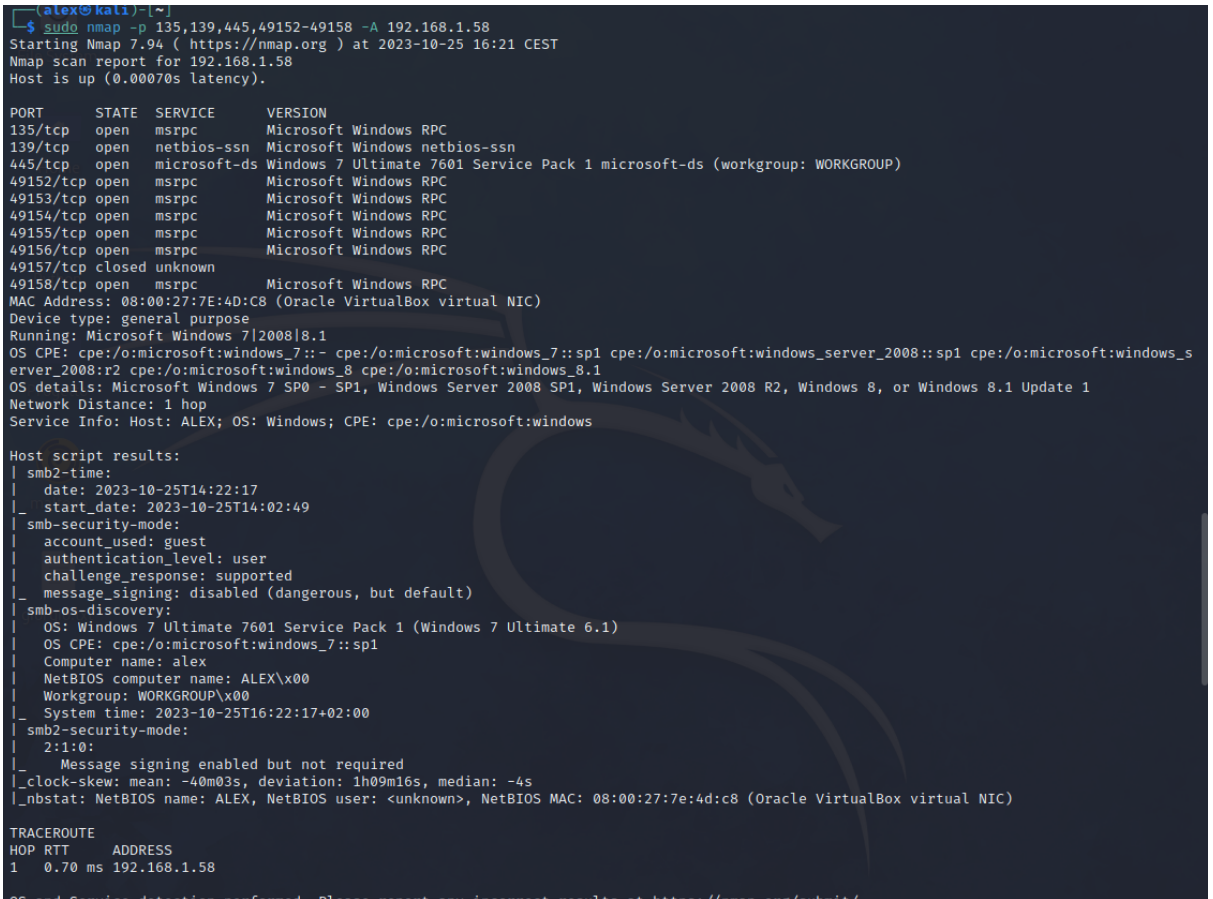
2-Syn Scan TCP connect

```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -p 135,139,445,49152-49158 -A 192.168.1.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:21 CEST
Nmap scan report for 192.168.1.58
Host is up (0.00070s latency).

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 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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 closed unknown
49158/tcp open   msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:7E:4D:C8 (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_s
erver_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: ALEX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-25T14:22:17
|_  start_date: 2023-10-25T14:02:49
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: alex
|   NetBIOS computer name: ALEX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-25T16:22:17+02:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: -40m03s, deviation: 1h09m16s, median: -4s
|_nbstat: NetBIOS name: ALEX, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:7e:4d:c8 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.1.58
```

Utilizzeremo il seguente codice per estrapolare info sulle porte attive,mac-address questo codice viene utilizzato per essere meno invasivi ma naturalmente avremo anche meno info



3-trovate differenze tra i risultati della scansioni TCP connect e SYN?



```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.56
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:17 CEST
Nmap scan report for 192.168.1.56
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: 08:00:27:0F:CE:E5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

┌──(alex㉿kali)-[~]
└─$
```

Con questo codice effettuiamo una scansione più precisa a discapito della velocità ,inoltre il tcp connect proverà direttamente la disponibilità delle porte
sS- sarà più veloce , meno preciso ,meno invasiva
sT- meno veloce,più precisa,più invasiva
Inoltre la sS può produrre falsi positivi (porta aperta) se un firewall risponde con un pacchetto SYN-ACK a qualsiasi porta, indipendentemente dallo stato effettivo della porta.

4- Version detection

```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -p 135,139,445,49152-49158 -A 192.168.1.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:21 CEST
Nmap scan report for 192.168.1.58
Host is up (0.00070s latency).

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 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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 closed unknown
49158/tcp open   msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:7E:4D:C8 (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_s
erver_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: ALEX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-25T14:22:17
|_  start_date: 2023-10-25T14:02:49
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: alex
|   NetBIOS computer name: ALEX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-25T16:22:17+02:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: -40m03s, deviation: 1h09m16s, median: -4s
|_nbstat: NetBIOS name: ALEX, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:7e:4d:c8 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.1.58
```

```
┌──(alex㉿kali)-[~]
└─$ nmap -sV 192.168.1.56
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:34 CEST
Nmap scan report for 192.168.1.56
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  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: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 11.29 seconds
```

con questo codice effettuiamo un controllo delle porte attive ma oltre a questo possiamo avere anche la versione delle porte attive.E’ un tipo di scansione che prende il nome di "Banner”

```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -p 135,139,445,49152-49158 -A 192.168.1.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:21 CEST
Nmap scan report for 192.168.1.58
Host is up (0.00070s latency).

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 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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 closed unknown
49158/tcp open   msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:7E:4D:C8 (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_s
erver_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: ALEX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-25T14:22:17
|_  start_date: 2023-10-25T14:02:49
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: alex
|   NetBIOS computer name: ALEX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-25T16:22:17+02:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: -40m03s, deviation: 1h09m16s, median: -4s
|_nbstat: NetBIOS name: ALEX, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:7e:4d:c8 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.1.58
```

```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:10 CEST
Nmap scan report for 192.168.1.58
Host is up (0.00063s 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
49158/tcp open  unknown
MAC Address: 08:00:27:7E:4D:C8 (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_serve
8: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 2.27 seconds
```

stesso codice del punto 1 ,ma con una macchina windows .
si possono vedere anche le porte attive

con questo codice si è provato a forzare la scansione ,infatti in questo modo possiamo notare come le porte che risultavano aperte ,ma con la dicitura”unknown” ,adesso portano il servizio in chiaro .

```
┌──(alex㉿kali)-[~]
└─$ sudo nmap -p 135,139,445,49152-49158 -A 192.168.1.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:21 CEST
Nmap scan report for 192.168.1.58
Host is up (0.00070s latency).

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 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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 closed unknown
49158/tcp open   msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:7E:4D:C8 (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_s
erver_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: ALEX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-25T14:22:17
|_  start_date: 2023-10-25T14:02:49
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: alex
|   NetBIOS computer name: ALEX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-25T16:22:17+02:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: -40m03s, deviation: 1h09m16s, median: -4s
|_nbstat: NetBIOS name: ALEX, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:7e:4d:c8 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.1.58
```