S5L3,
BENVENUTI LUIGI

Traccia: Tecniche di scansione con Nmap
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows 7:

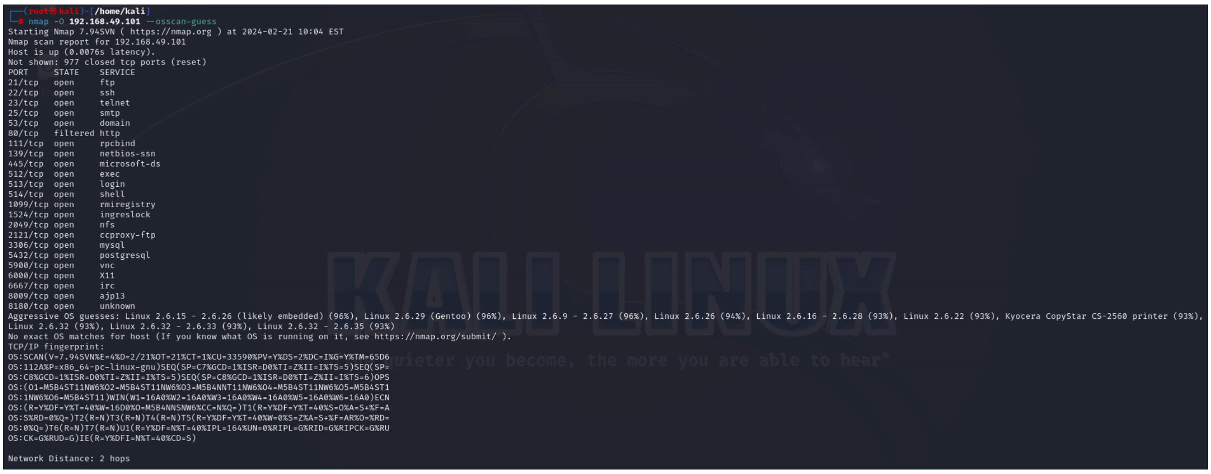
- OS fingerprint.

1- Metasploitable

1a - Per visualizzare l'OS fingerprint della macchina target Metaspolitable si utilizza il comando

nmap -O iptarget –osscan-guess

Output:

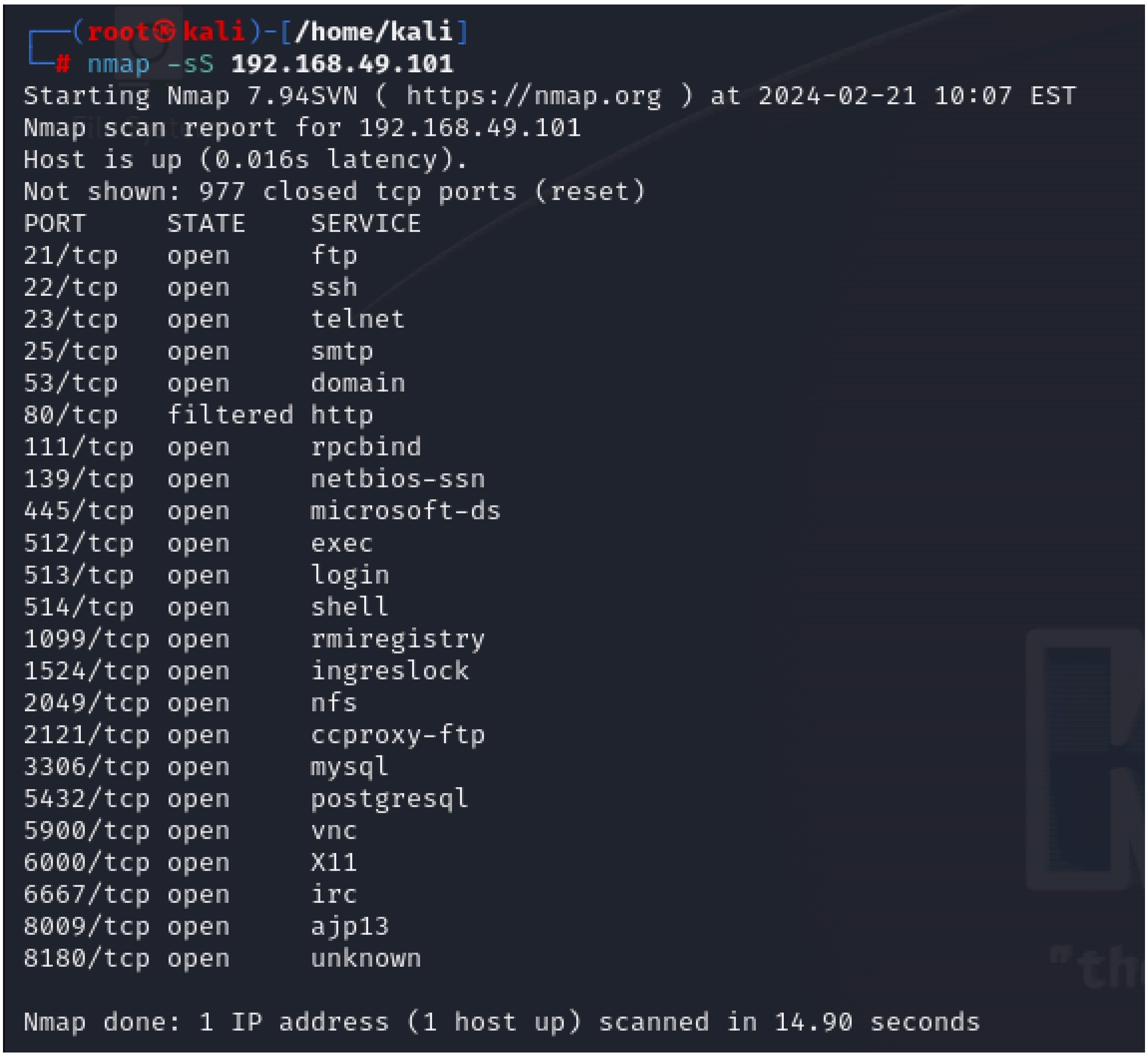


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.49.101 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:04 EST
Nmap scan report for 192.168.49.101
Host is up (0.0076s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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
Aggressive OS guesses: Linux 2.6.15 - 2.6.26 (likely embedded) (96%), Linux 2.6.29 (Gentoo) (96%), Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.26 (94%), Linux 2.6.16 - 2.6.28 (93%), Linux 2.6.22 (93%), Kyocera CopyStar CS-2560 printer (93%),
Linux 2.6.32 (93%), Linux 2.6.32 - 2.6.33 (93%), Linux 2.6.32 - 2.6.35 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/21%OT=21%CT=1%CU=33590%PV=Y%DS=2%DC=I%G=Y%TM=65D6
OS:112A%P=x86_64-pc-linux-gnu)SEQ(SP=C7%GCD=1%ISR=D0%TI=Z%II=I%TS=5)SEQ(SP=
OS:C8%GCD=1%ISR=D0%TI=Z%II=I%TS=5)SEQ(SP=C8%GCD=1%ISR=D0%TI=Z%II=I%TS=6)OPS
OS:(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST1
OS:1NW6%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN
OS:(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RU
OS:CK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
```

1b - Effettuiamo poi un Syn Scan con il comando:

nmap -sS iptarget



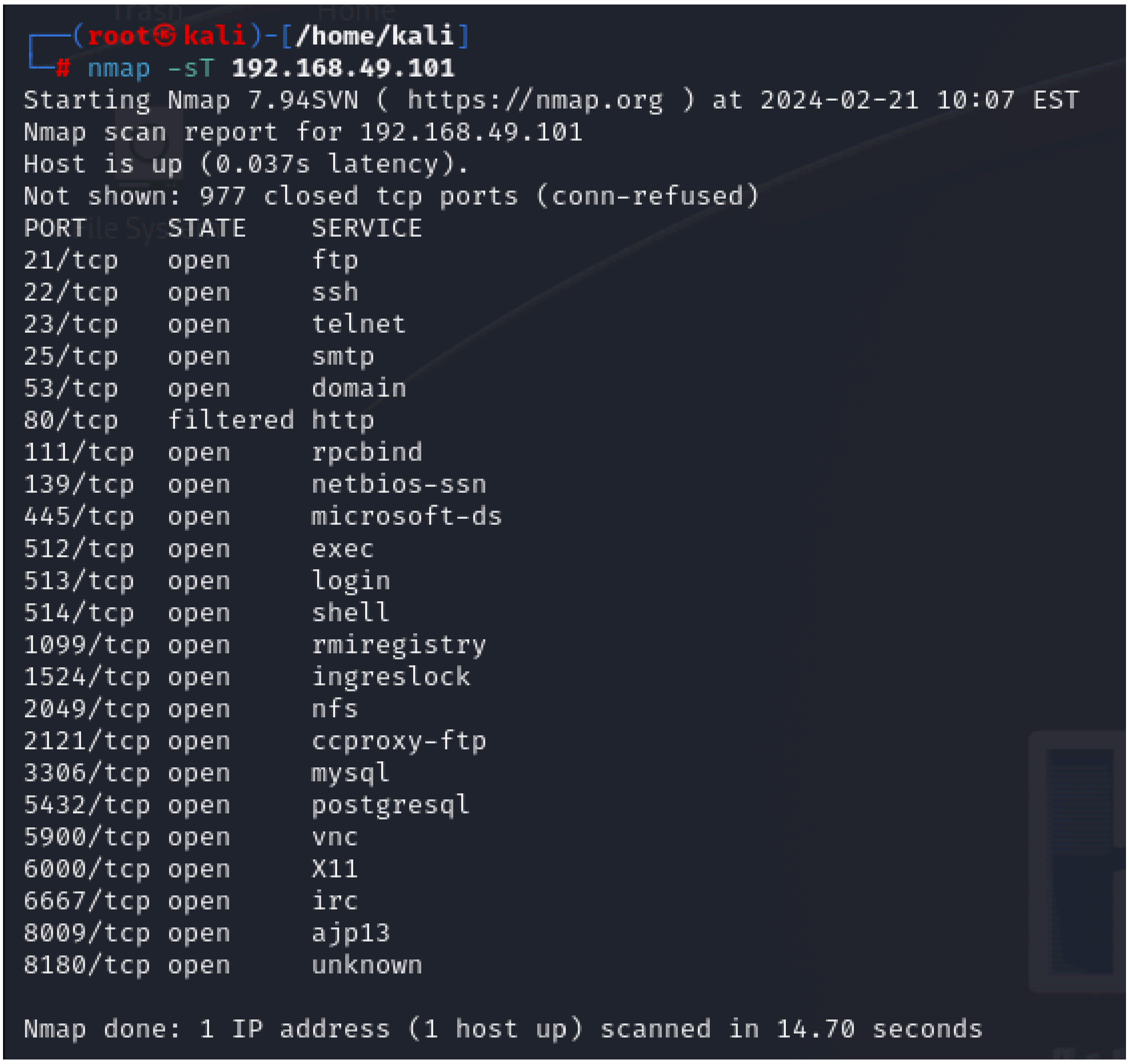
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:07 EST
Nmap scan report for 192.168.49.101
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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 14.90 seconds
```

1c - Effettuiamo poi un TCP Connect con il comando:

nmap -sT iptarget

Non ci sono differenze con la scansione precedente.

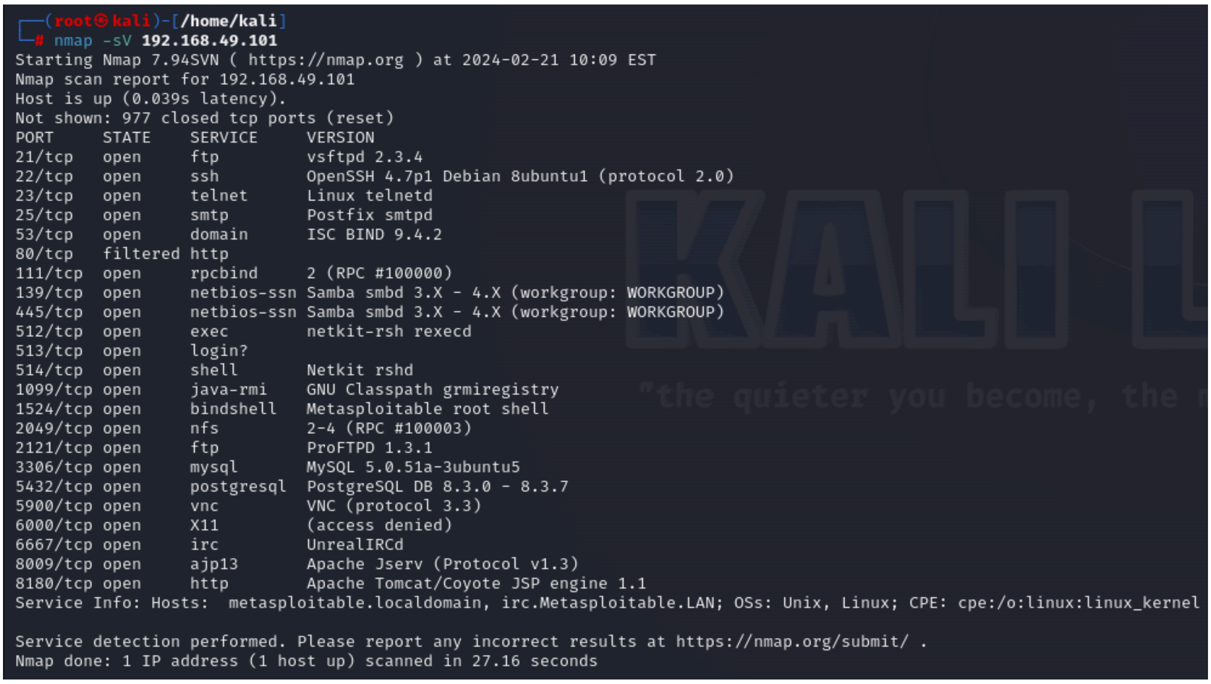


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:07 EST
Nmap scan report for 192.168.49.101
Host is up (0.037s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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 14.70 seconds
```

1d - Version detection:

nmap -sV target

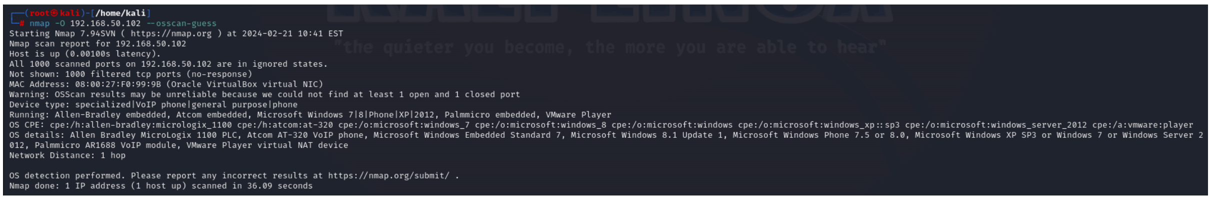


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:09 EST
Nmap scan report for 192.168.49.101
Host is up (0.039s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 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   filtered http
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
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 27.16 seconds
```

2a - OS fingerprint Win7:

<u>nmap -O iptarget –osscan-guess</u>

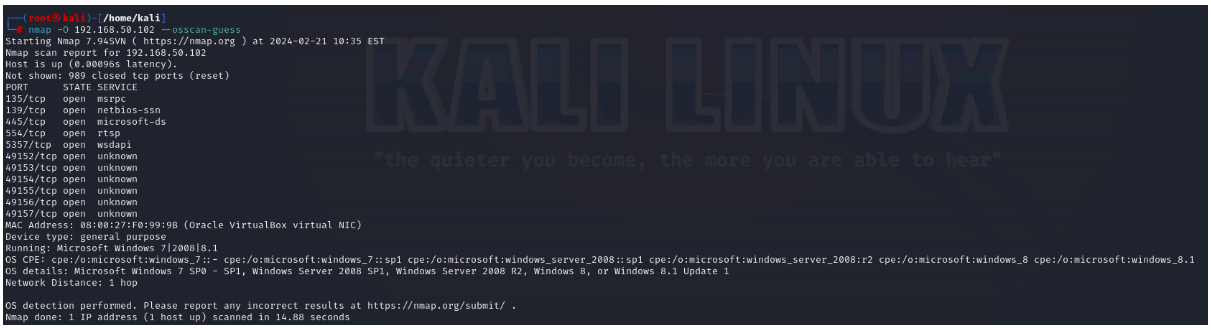


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:41 EST
Nmap scan report for 192.168.50.102
Host is up (0.00100s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:F0:99:9B (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2
012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 36.09 seconds
```

Il firewall ci impedisce di ottenere informazioni. Settiamo su rete domestica e disattiviamo il firewall di Win7. Ripetiamo il comando precedente:

2b - fixing OS fingerprint Win7:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:35 EST
Nmap scan report for 192.168.50.102
Host is up (0.00096s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
5357/tcp  open  wsdapi
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:F0:99:9B (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 14.88 seconds
```