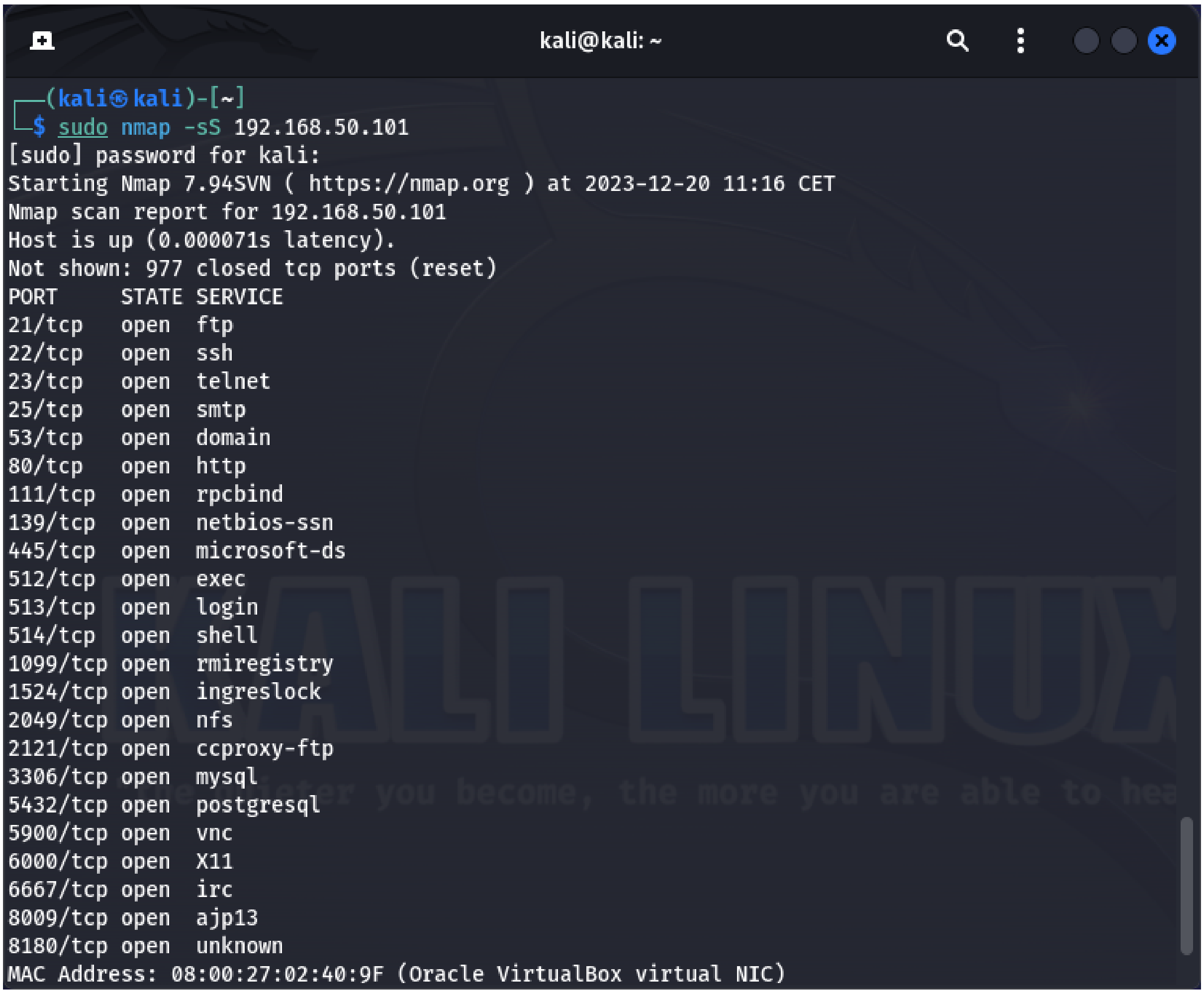
S5/L3

SCANSIONE DEI SERVIZI CON NMAP

MACCHINA KALI:
IP: 192.168.50.100

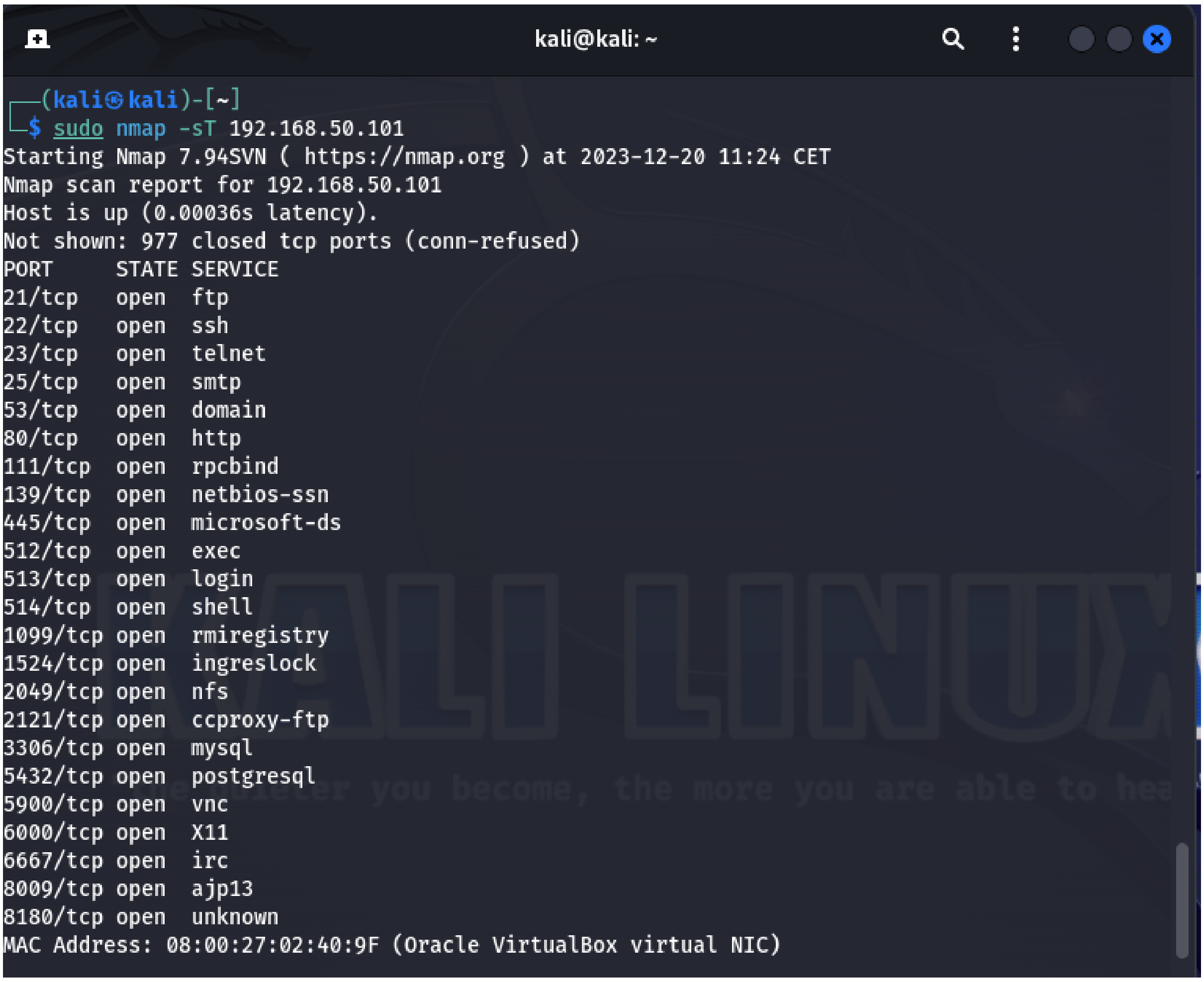
MACCHINA META:
IP: 192.168.50.101

SCAN SYN (-sS):



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:16 CET
Nmap scan report for 192.168.50.101
Host is up (0.000071s 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: 08:00:27:02:40:9F (Oracle VirtualBox virtual NIC)
```

SCAN FULL TCP (-sT):

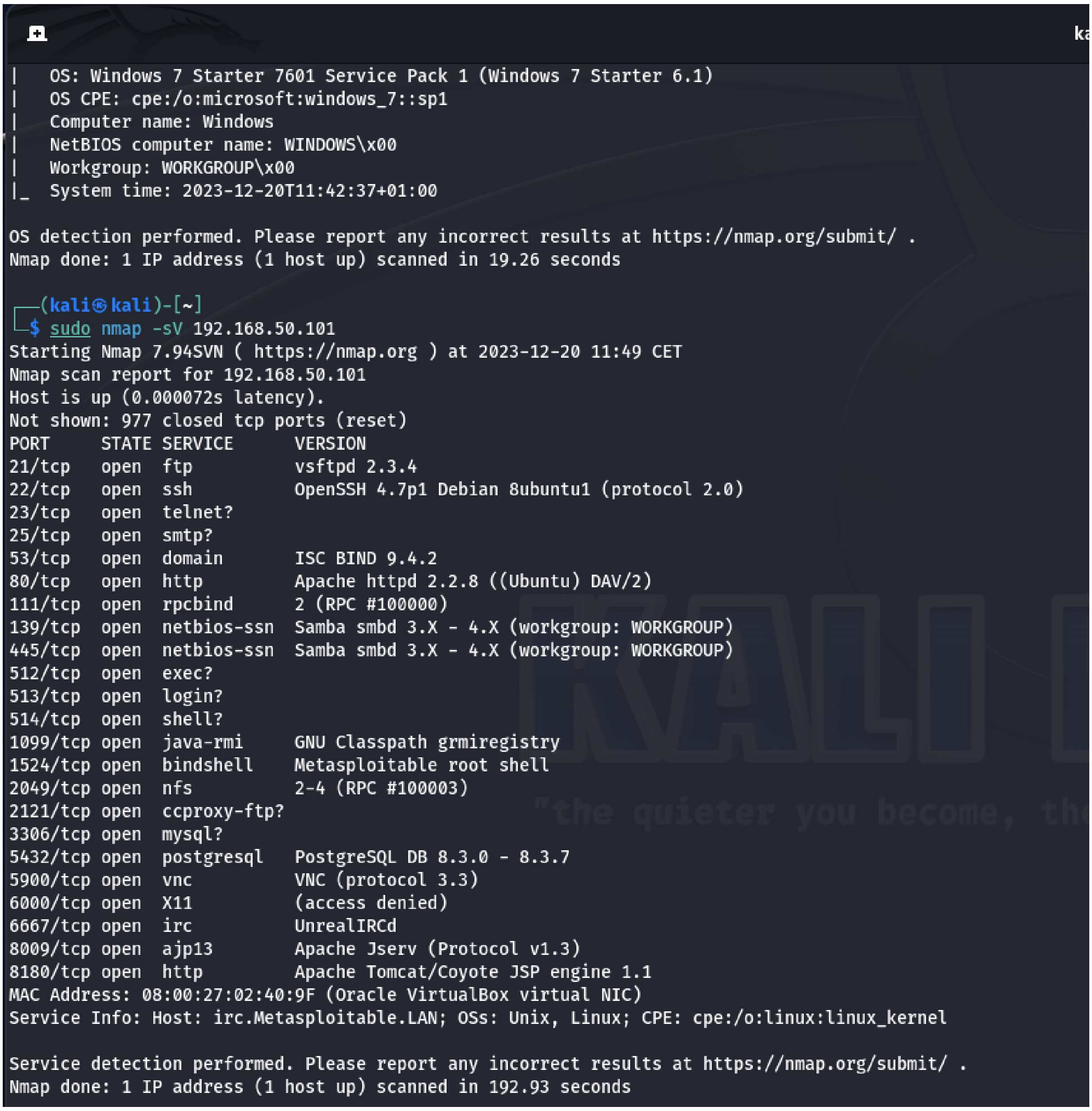


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:24 CET
Nmap scan report for 192.168.50.101
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:02:40:9F (Oracle VirtualBox virtual NIC)
```

DIFFERENZE:
Nello screen dello scan SYN notiamo che nmap risponde al SYN/ACK del destinatario con un comando di reset (RST), non concludendo dunque il 3-WHS. Ci da comunque in output lo stato delle porte e i servizi in ascolto annessi.

Nello screen dello scan FULL TCP in teoria nmap dovrebbe chiudere il 3-WHS e creare quindi il canale di comunicazione con meta, ma notiamo come in risposta ci appaia “Conn. Refused”, probabilmente il firewall di Meta meta ce lo impedisce.

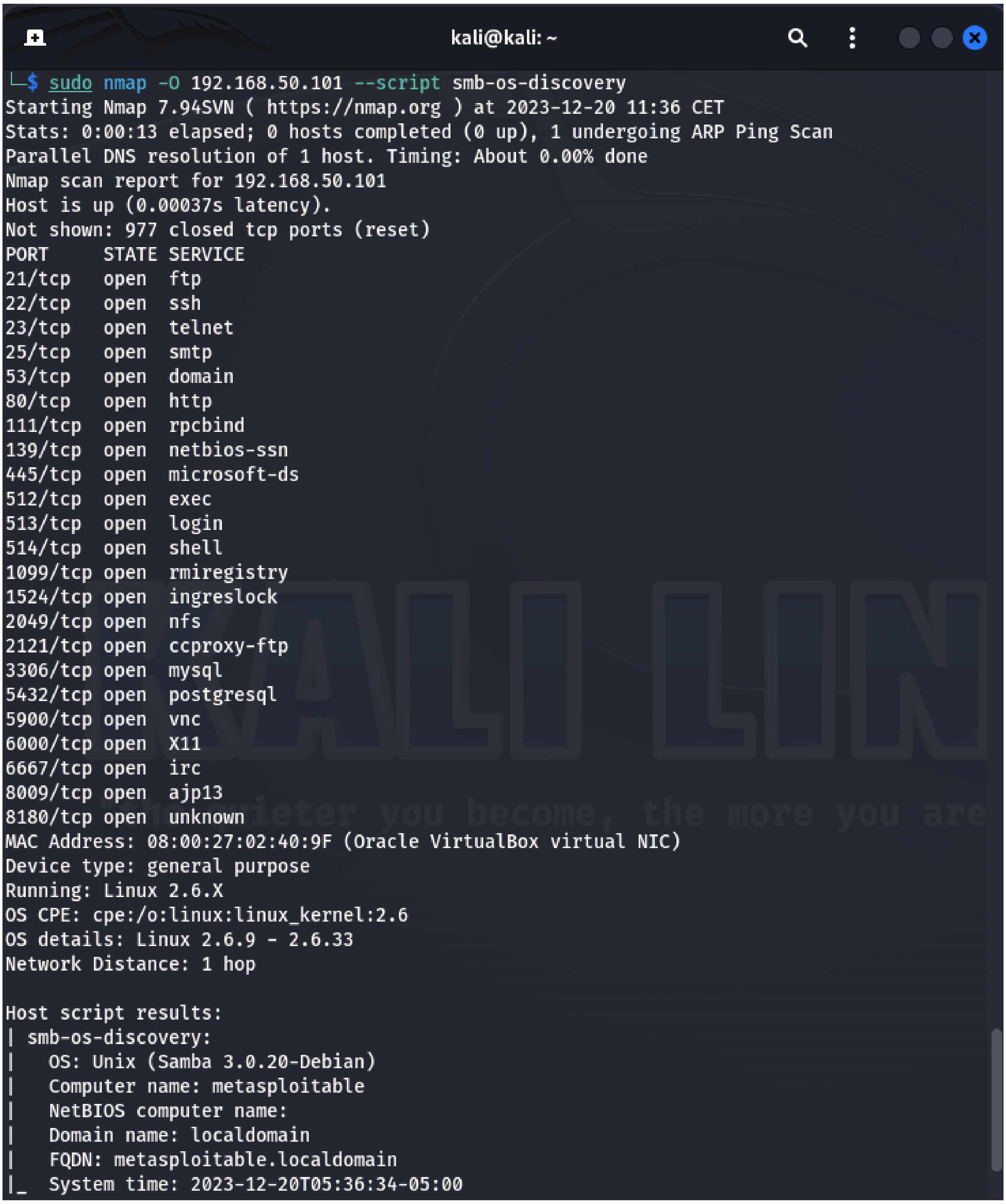
VERSION DETECTION:



```
|   OS: Windows 7 Starter 7601 Service Pack 1 (Windows 7 Starter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Windows
|   NetBIOS computer name: WINDOWS\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-12-20T11:42:37+01:00

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.26 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:49 CET
Nmap scan report for 192.168.50.101
Host is up (0.000072s 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  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:02:40:9F (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 192.93 seconds
```

Qua in output abbiamo non soltanto lo stato delle porte e il servizio in ascolto, ma anche la corrispondente versione.

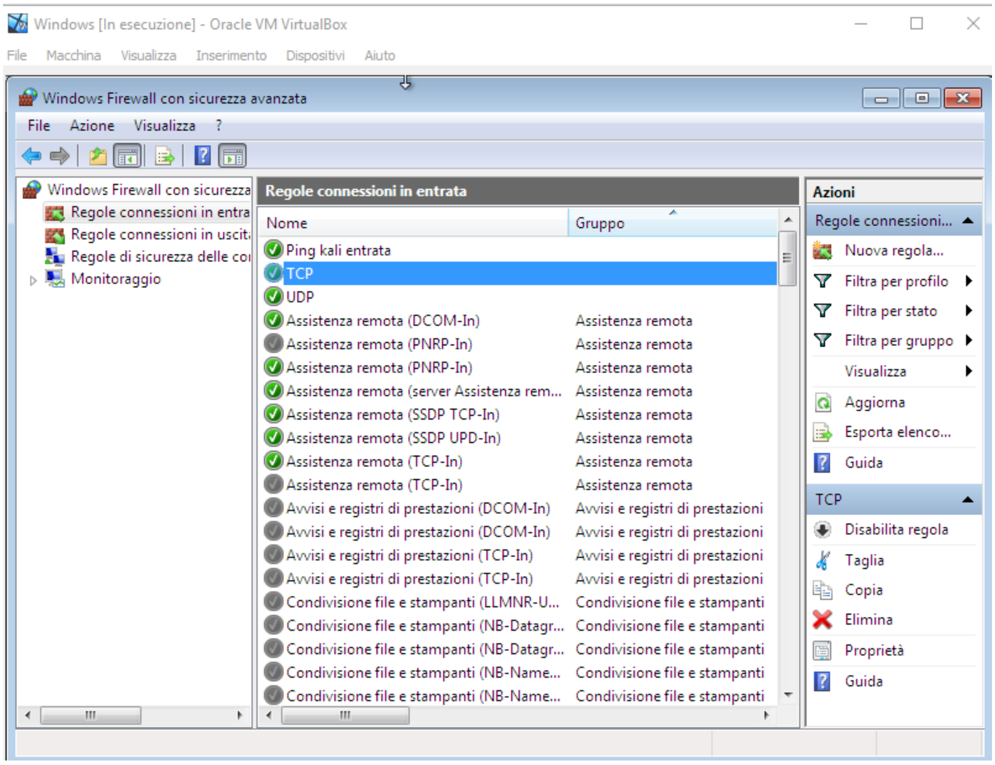
DISCOVERY OS KALI:



```
└─$ sudo nmap -O 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:36 CET
Stats: 0:00:13 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.101
Host is up (0.00037s 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: 08:00:27:02:40:9F (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

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-20T05:36:34-05:00
```

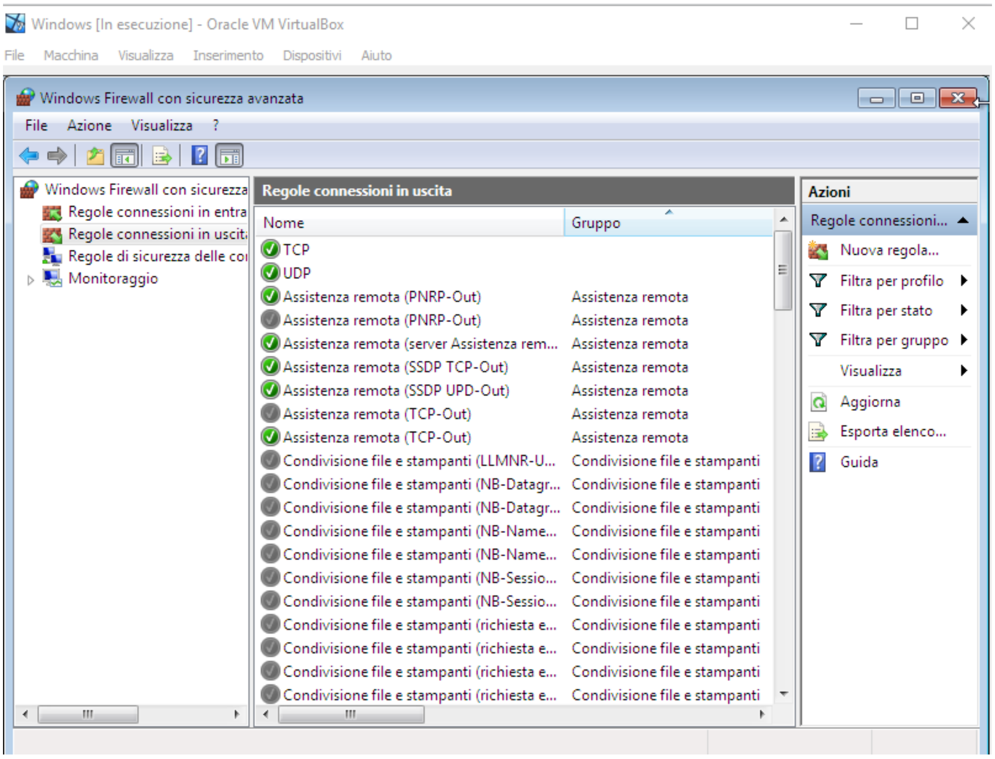
DISCOVERY OS WINDOWS7:

Inizialmente non riusciamo ad accertarcene poichè le comunicazioni TCP/UDP in Windows non sono abilitate, ottenendo come risultato dello scan un errore. Quindi le abilitiamo in entrate ed in uscita.


Windows [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Windows Firewall con sicurezza avanzata
File Azione Visualizza ?
Windows Firewall con sicurezza
Regole connessioni in entra
Regole connessioni in uscit
Regole di sicurezza delle co
Monitoraggio
Azioni
Regole connessioni...
Nuova regola...
Filtra per profilo
Filtra per stato
Filtra per gruppo
Visualizza
Aggiorna
Esporta elenco...
Guida
TCP
Disabilita regola
Taglia
Copia
Elimina
Proprietà
Guida

Regole connessioni in entrata

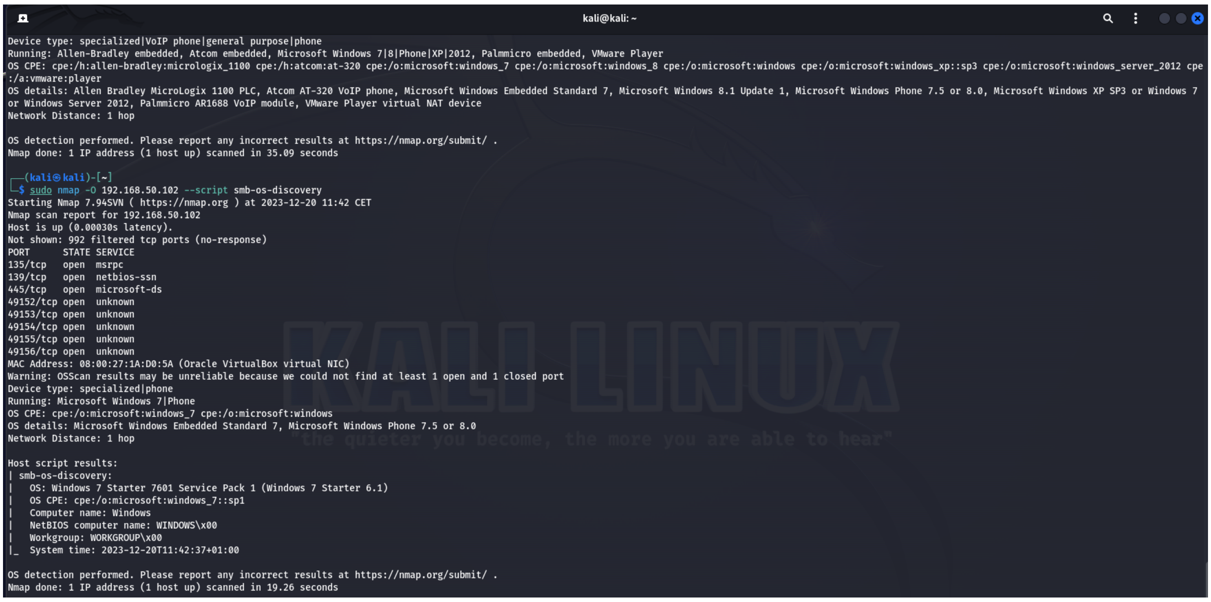
Nome	Gruppo
Ping kali entrata	
TCP	
UDP	
Assistenza remota (DCOM-In)	Assistenza remota
Assistenza remota (PNRP-In)	Assistenza remota
Assistenza remota (PNRP-In)	Assistenza remota
Assistenza remota (server Assistenza rem...	Assistenza remota
Assistenza remota (SSDP TCP-In)	Assistenza remota
Assistenza remota (SSDP UPD-In)	Assistenza remota
Assistenza remota (TCP-In)	Assistenza remota
Assistenza remota (TCP-In)	Assistenza remota
Avvisi e registri di prestazioni (DCOM-In)	Avvisi e registri di prestazioni
Avvisi e registri di prestazioni (DCOM-In)	Avvisi e registri di prestazioni
Avvisi e registri di prestazioni (TCP-In)	Avvisi e registri di prestazioni
Avvisi e registri di prestazioni (TCP-In)	Avvisi e registri di prestazioni
Condivisione file e stampanti (LLMNR-U...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti


Windows [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Windows Firewall con sicurezza avanzata
File Azione Visualizza ?
Windows Firewall con sicurezza
Regole connessioni in entra
Regole connessioni in uscit
Regole di sicurezza delle co
Monitoraggio
Azioni
Regole connessioni...
Nuova regola...
Filtra per profilo
Filtra per stato
Filtra per gruppo
Visualizza
Aggiorna
Esporta elenco...
Guida

Regole connessioni in uscita

Nome	Gruppo
TCP	
UDP	
Assistenza remota (PNRP-Out)	Assistenza remota
Assistenza remota (PNRP-Out)	Assistenza remota
Assistenza remota (server Assistenza rem...	Assistenza remota
Assistenza remota (SSDP TCP-Out)	Assistenza remota
Assistenza remota (SSDP UPD-Out)	Assistenza remota
Assistenza remota (TCP-Out)	Assistenza remota
Assistenza remota (TCP-Out)	Assistenza remota
Condivisione file e stampanti (LLMNR-U...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Sessio...	Condivisione file e stampanti
Condivisione file e stampanti (NB-Sessio...	Condivisione file e stampanti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti

Ora possiamo procedere col nostro comando.



```
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 2012, 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 35.09 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:42 CET
Nmap scan report for 192.168.50.102
Host is up (0.00030s latency).
Not shown: 992 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:1A:D0:5A (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|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Starter 7601 Service Pack 1 (Windows 7 Starter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Windows
|   NetBIOS computer name: WINDOWS\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-12-20T11:42:37+01:00

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.26 seconds
```