

Scansione servizi con nMap

Durante l'esercizio di oggi dobbiamo effettuare delle scansioni verso Metasploitable e Windows utilizzando nMap.

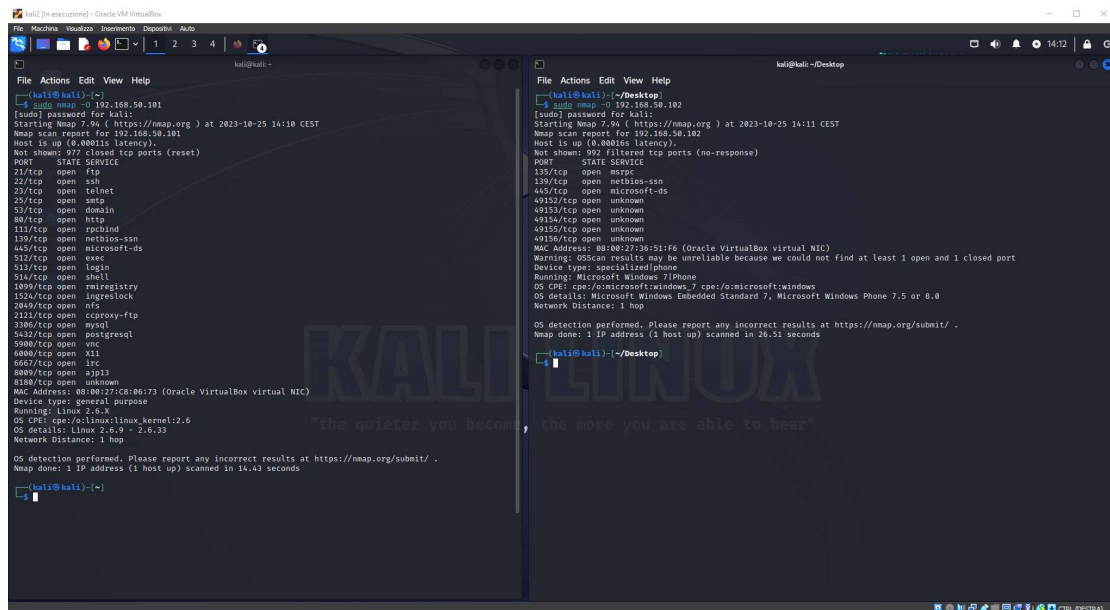
Gli IP utilizzati sono i seguenti:

IP Kali 192.168.50.100 (macchina attaccante)

IP Metasploitable 192.168.50.101 (macchina vittima)

IP Windows 192.168.50.102 (macchina vittima)

Come prima cosa sono andato a scansionare che tipo di sistema operativo hanno i due IP vittima utilizzando il comando `nmap -O <IP target>`



```
kali@kali:~$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:10 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0001s 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
32/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  mircrsoft-ssn
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5988/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C8:06:73 (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 14.42 seconds

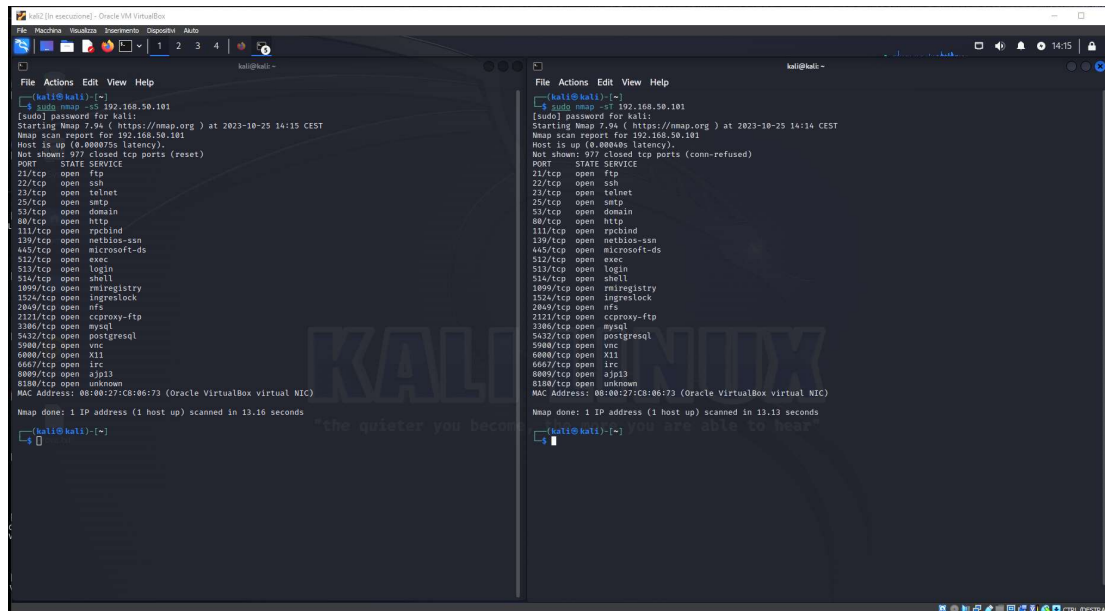
kali@kali:~$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:11 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0001s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    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: 08:00:27:36:51:F6 (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
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.51 seconds

kali@kali:~$
```

A sinistra si può vedere il comando lanciato verso Metasploitable e come risultato vediamo che utilizza Linux 2.6.9 - 2.6.33, mentre per quanto riguarda Windows (screen a destra) abbiamo 3 possibilità. Questo perchè il comando utilizzato non è molto invasivo e quindi non è al 100% preciso ma allo stesso tempo non crea troppo traffico e quindi è meno probabile che la vittima si accorga della nostra ricerca. A fine report ho utilizzato un'altro comando per verificare più accuratamente la versione

di Windows.

Come seconda cosa ho scansionato le porte su Metasploitable prima utilizzando il Syn Scan utilizzando il comando `nmap -sS <IP target>` a sinistra dello screen, mentre a destra ho utilizzato `nmap -sT <IP target>` che è una scansione TCP Connect.



```
kali@kali:~$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:15 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000075s latency).
Not shown: 992 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
1050/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cprsync-ftp
3306/tcp  open  mysql
3432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6080/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C8:06:73 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

kali@kali:~$ sudo nmap -sT 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:14 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00044s latency).
Not shown: 992 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
1050/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cprsync-ftp
3306/tcp  open  mysql
3432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6080/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C8:06:73 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds

kali@kali:~$
```

Le differenze principali di queste due scansioni sono:

- il metodo `sT` è molto più invasivo del `sS` perchè per controllare se una porta è aperta e recuperare le informazioni sul servizio in ascolto utilizza il 3 way handshake (SYN-SYN/ACK-ACK) mentre il metodo `sS` è meno invasiva e più difficile da rilevare poichè invia solo un pacchetto SYN e aspetta una risposta.

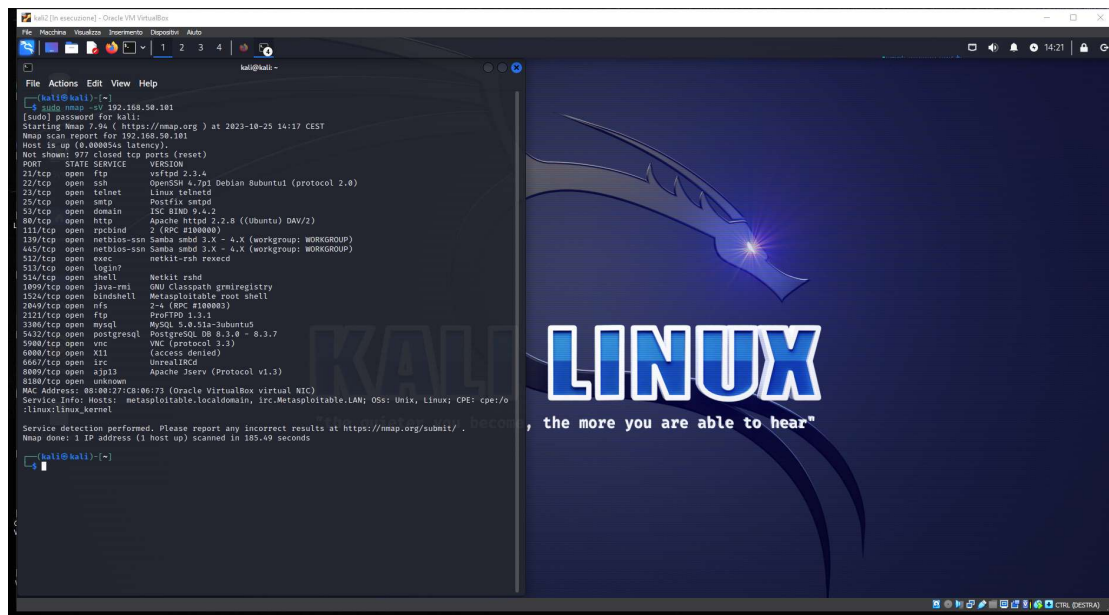
- il metodo `sS` è sicuramente più rapido e sicuro come detto prima ma è anche meno preciso ed affidabile rispetto al metodo `sT`.

- un'altra differenza si nota alla 4 riga della risposta quando dice:
Not shown: 992 filtered tcp ports (reset) con l'`sS` perchè non si riceve alcuna risposta invece con `sT` al posto di "reset" dice "conn.refused" perchè la scansione rileva delle porte ma non sono ne aperte ne chiuse

ma bloccate da qualche protezione es. firewall.

Nell'ultimo screen possiamo vedere in funzione in codice
`nmap -sV <IP target>`

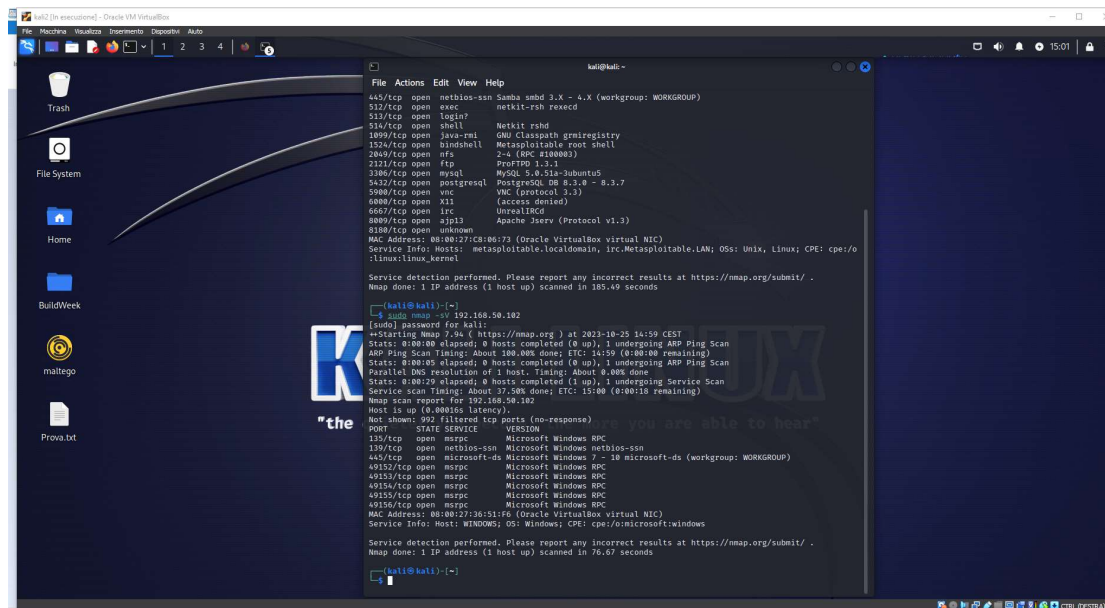
Questo codice effettua una scansione delle porte aperte sul dispositivo target e mostra anche le versioni dei servizi attivi, quindi avremmo più dettagli in caso di ricerca di exploit.



```
kali@kali:~$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-25 14:17 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0000000 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/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 rshcd
513/tcp   open  login?          netkit-rsh rshcd
514/tcp   open  shell           netkit-rshd
1800/tcp  open  java-rmi        GNU Classpath gmicregistry
1524/tcp  open  bindshell       Metasploitable root shell
2048/tcp  open  nfs             2.4 (RPC #100002)
2121/tcp  open  ftp             ProFTPD 1.3.1
3306/tcp  open  mysql           MySQL 5.0.51a-Jubuntus
5432/tcp  open  postgresql      PostgreSQL 9.0.3-0 - 8.3.7
5900/tcp  open  vnc             VNC (protocol 3.3)
6000/tcp  open  x11             (access denied)
6667/tcp  open  irc             UnrealIRCd
8080/tcp  open  http            Apache/2.2.8 ((Ubuntu) DAV/2)
8089/tcp  open  http            Apache/2.2.8 ((Ubuntu) DAV/2)
8180/tcp  open  unknown
MAC Address: 08:00:27:C8:86:73 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

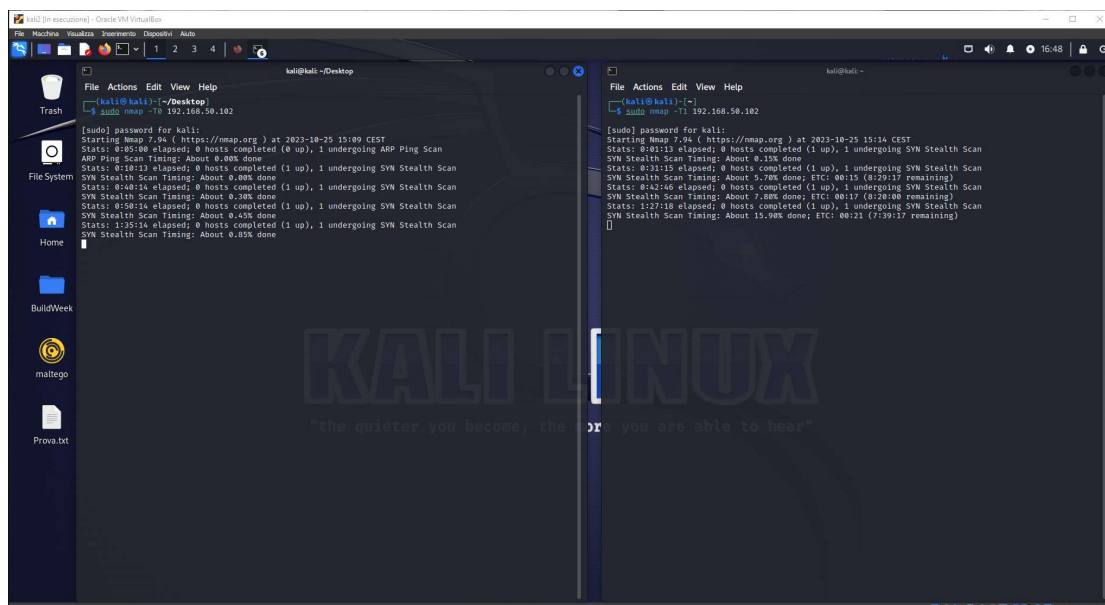
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 185.49 seconds
```

In caso di Windows abbiamo dei problemi nella scansione delle porte perchè è protetto da firewall come possiamo vedere dallo screen che segue.



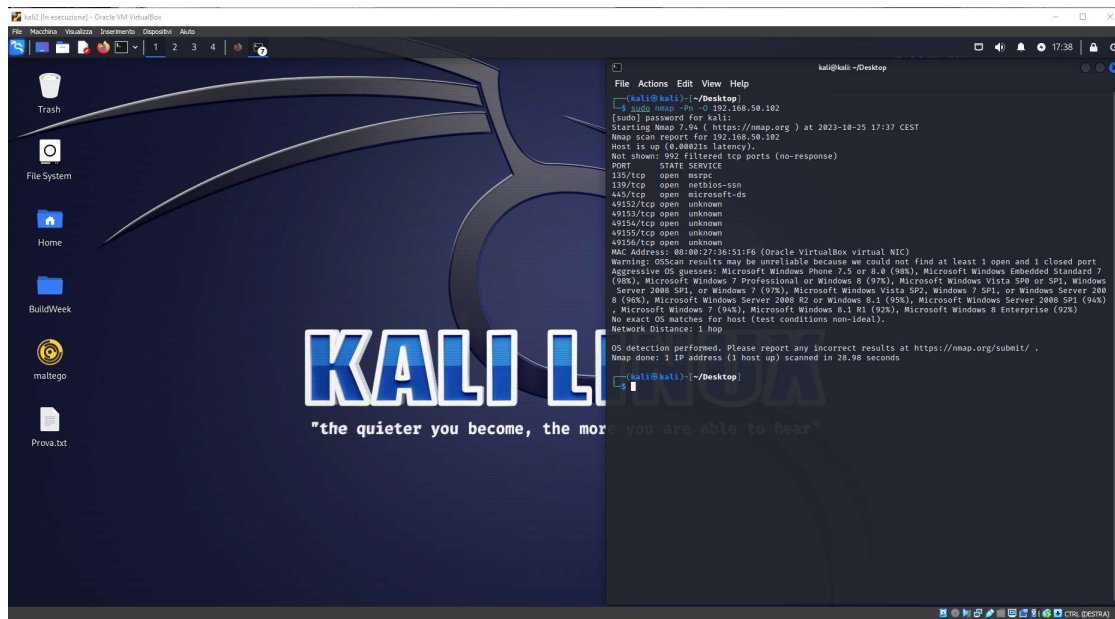
Il firewall di windows blocca nmap dalla scansione delle porte perchè rileva un accesso non autorizzato, quindi possiamo provare ad utilizzare il Timing della scansione ovvero utilizzando il comando `nmap -T0 <IPtarget>` in questa modalità gli scan sono molto più lenti e poco invasivi e quindi diminuiscono la possibilità di essere intercettati.

Nello screen successivo ho provato ad utilizzare T0 e T1 e si vede quanto lenti sono.



Altro modo per riuscire a scansionare Windows possiamo utilizzare il comando `nmap -Pn -O 192.168.50.102` così si evita di mandare il ping

con -Pn e si scansiona Windows sono con il 3 way handshake.



The screenshot shows a Kali Linux desktop environment. The desktop background features the Kali Linux logo and the quote "the quieter you become, the more you are able to hear". On the left side, there is a sidebar with icons for Trash, File System, Home, BuildWeek, maltego, and Prova.txt. A terminal window is open on the right side, displaying the following output:

```
kali@kali:~/Desktop$ sudo nmap -Pn -sS 192.168.58.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 17:27 CEST
Nmap scan report for 192.168.58.102
Host is up (0.00021s 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: 08:00:27:36:51:F6 (Oracle VirtualBox virtual NIC)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (98%), Microsoft Windows Embedded Standard 7 (98%), Microsoft Windows 7 Professional or Windows 8 (97%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (97%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 R2 (96%), Microsoft Windows Server 2008 R2 or Windows 8.1 (95%), Microsoft Windows Server 2008 SP1 (94%), Microsoft Windows 7 (94%), Microsoft Windows 8.1 R1 (92%), Microsoft Windows 8 Enterprise (92%)
No exact OS matches for host (test conditions non-ideal).
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 28.98 seconds
kali@kali:~/Desktop$
```