

FIREWALL SPENTO

OS FINGERSPRINT

The screenshot displays the Zenmap application window. The top menu bar includes 'File', 'Macchina', 'Visualizza', 'Inserimento', 'Dispositivi', and 'Aiuto'. The main interface shows a scan of the target IP 192.168.1.62. The command used is 'nmap -O 192.168.1.62'. The scan results are displayed in the 'Nmap Output' tab, showing the following details:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:25 EST
Nmap scan report for 192.168.1.62 (192.168.1.62)
Host is up (0.00081s 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:CC:7A:F4 (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 2.48 seconds
```

SYN SCAN

ScanToolsProfileHelp

Target: 192.168.1.62Profile: ScanCancel

Command: nmap -sS 192.168.1.62

HostsServices

OSHost

192.168.1.62 (192.168.1.62)

Filter Hosts

Nmap OutputPorts / HostsTopologyHost DetailsScans

nmap -sS 192.168.1.62Details

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 13:27 EST
Nmap scan report for 192.168.1.62 (192.168.1.62)
Host is up (0.00029s 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:CC:7A:F4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds

TCP CONNECT

ScanToolsProfileHelp

Target: 192.168.1.62Profile: ScanCancel

Command: nmap -sT 192.168.1.62

HostsServices

OSHost

192.168.1.62 (192.168.1.62)

Filter Hosts

Nmap OutputPorts / HostsTopologyHost DetailsScans

nmap -sT 192.168.1.62Details

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 13:28 EST
Nmap scan report for 192.168.1.62 (192.168.1.62)
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (conn-refused)

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:CC:7A:F4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds

VERSION DETECTION

Scan Tools Profile Help

Target: 192.168.1.62 Profile: Scan Cancel

Command: nmap -sV 192.168.1.62

Hosts Services

OS Host

192.168.1.62 (192.168.1.62)

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV 192.168.1.62

Details

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 13:29 EST
Nmap scan report for 192.168.1.62 (192.168.1.62)
Host is up (0.00037s latency).
Not shown: 991 closed tcp ports (reset)

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	Microsoft Windows 7 - 10 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
49158/tcp	open	msrpc	Microsoft Windows RPC

MAC Address: 08:00:27:CC:7A:F4 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 60.41 seconds

FIREWALL ACCESSO

OS FINGERPRINT

The screenshot shows the Zenmap application window. The 'Target' field is set to 192.168.1.62, and the 'Command' is nmap -O 192.168.1.62. The 'Nmap Output' tab is selected, displaying the following scan results:

```
nmap -O 192.168.1.62

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 14:35 EST
Nmap scan report for 192.168.1.62 (192.168.1.62)
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.62 (192.168.1.62) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:CC:7A:F4 (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 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 22.20 seconds
```

The interface also includes a 'Hosts' list on the left with the entry 192.168.1.62 (192.168.1.62) highlighted. The bottom of the window has a 'Filter Hosts' button.

SYN SCAN

ScanToolsProfileHelp

Target: 192.168.1.62Profile: ScanCancel

Command: nmap -sS 192.168.1.62

HostsServices

OSHost

192.168.1.62 (192.168.1.62)

Filter Hosts

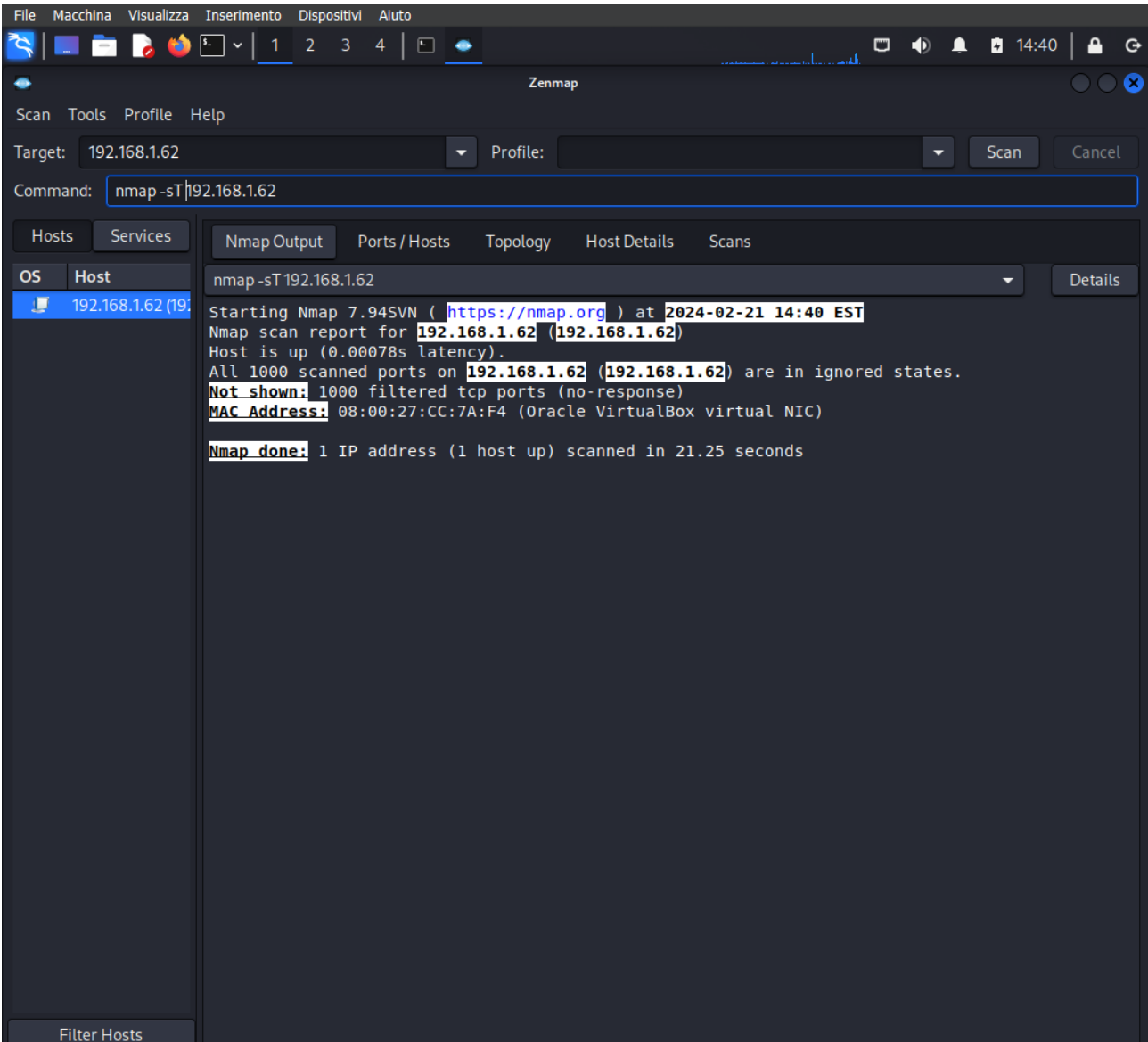
Nmap OutputPorts / HostsTopologyHost DetailsScans

nmap -sS 192.168.1.62Details

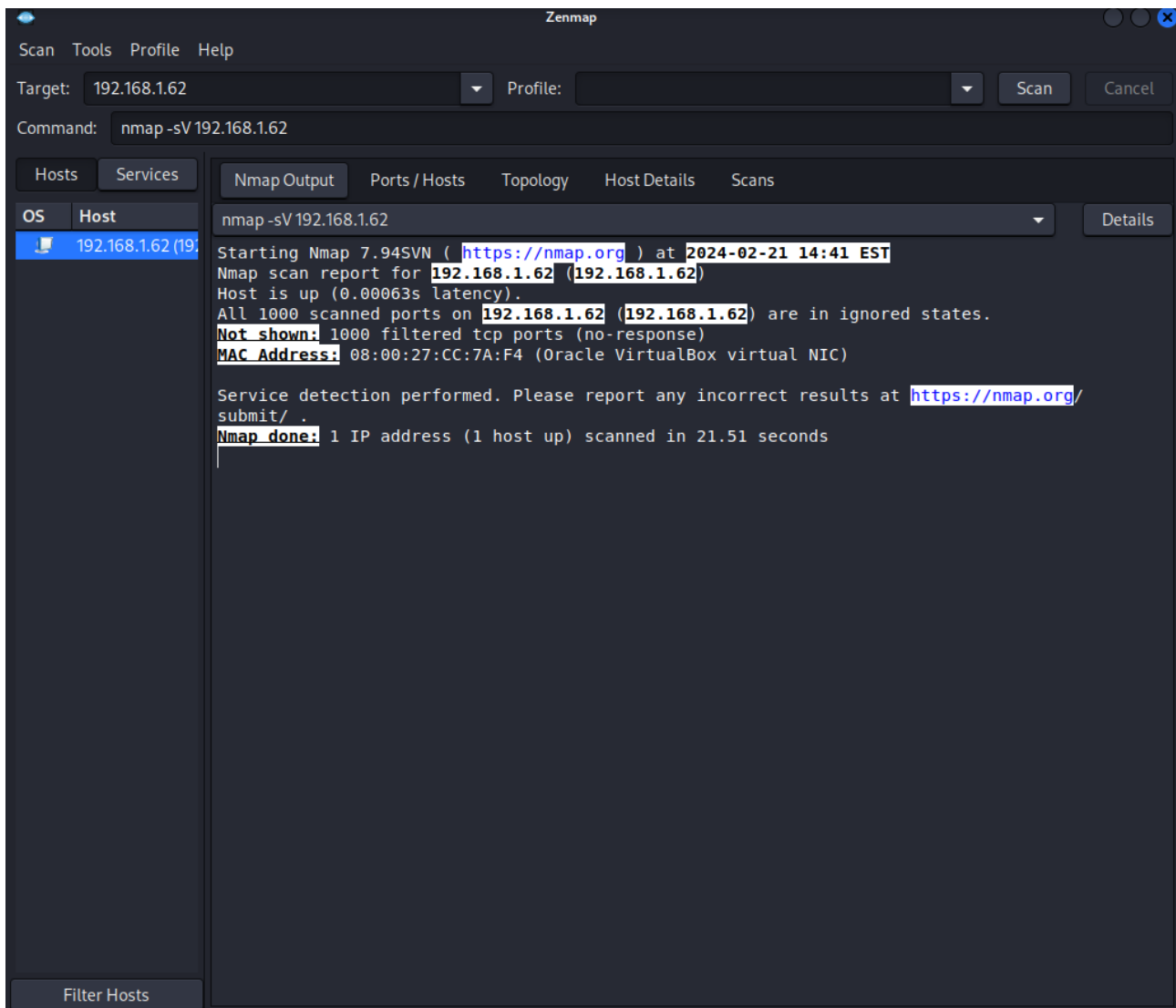
Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 14:39 EST
Nmap scan report for 192.168.1.62 (192.168.1.62)
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.1.62 (192.168.1.62) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:CC:7A:F4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds

TCP CONNECT



VERSION DETECTION



Con il firewall attivo, sono fallite tutte le scansioni