

OS FINGERSPRINT: identifica il sistema operativo del target

Scan Tools Profile Help

Target: 192.168.1.101 Profile: Scan Cancel

Command: nmap -O 192.168.1.101

Hosts Services

OS Host

192.168.1.101 (19

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -O 192.168.1.101

Details

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 12:28 EST

Nmap scan report for 192.168.1.101 (192.168.1.101)

Host is up (0.0015s 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:E5:4A:BF (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

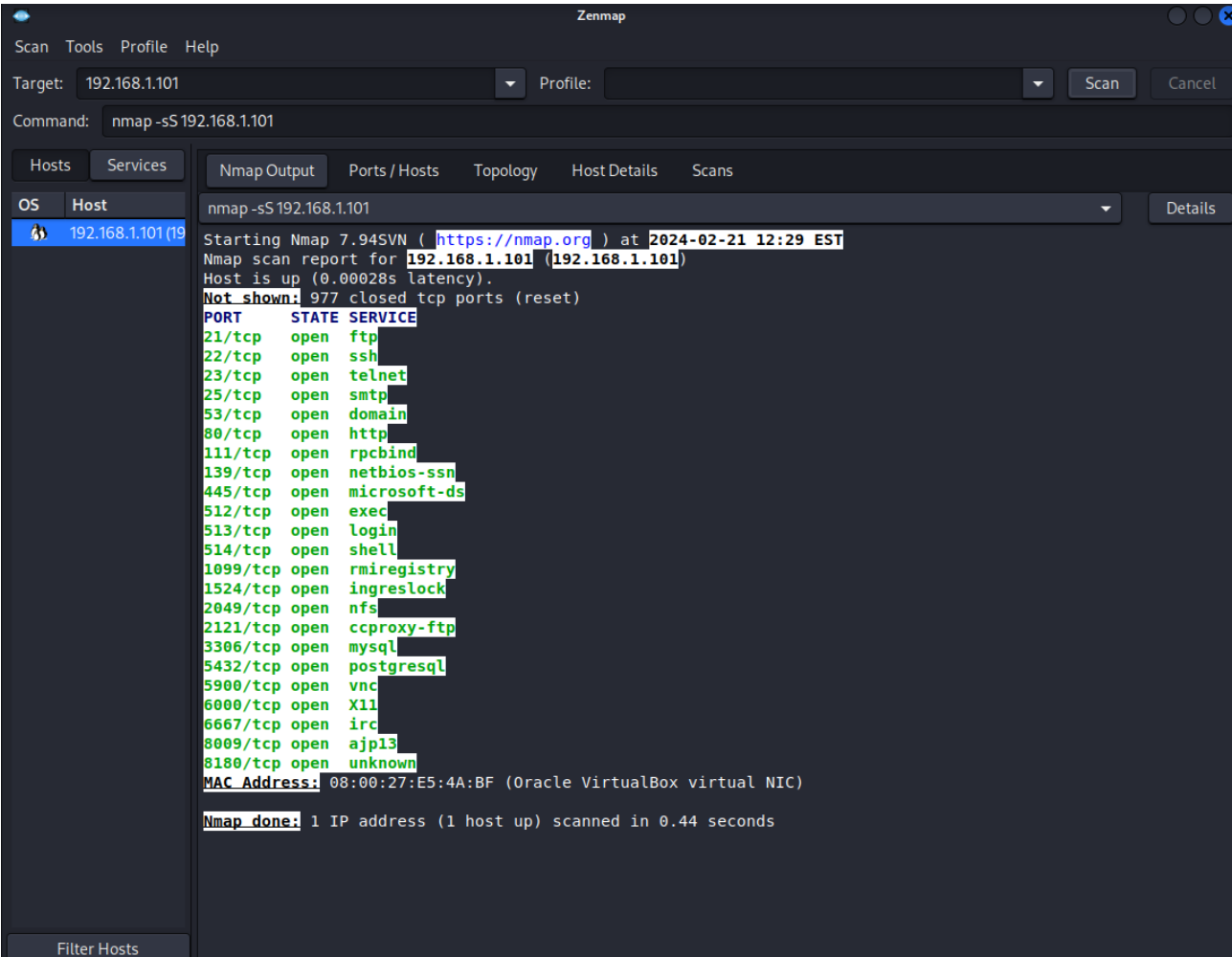
OS details: Linux 2.6.9 - 2.6.33

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 1.95 seconds

SYN: si connette in segreto ai demoni attivi (applicazioni in background che forniscono servizi all'utente) su una rete target



TCP CONNECT: tipo di scansione che ascolta le applicazioni web sulla rete del target

Zenmap

Scan Tools Profile Help

Target: 192.168.1.101 Profile: Scan Cancel

Command: nmap -sT 192.168.1.101

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.1.101 (192.168.1.101) Details

nmap -sT 192.168.1.101

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 12:31 EST

Nmap scan report for 192.168.1.101 (192.168.1.101)

Host is up (0.00068s 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:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

Filter Hosts

VERSION DETECTION: identifica tutti i servizi in ascolto sulle porte

Scan Tools Profile Help

Target: 192.168.1.101 Profile: Scan Cancel

Command: nmap -sV 192.168.1.101

Hosts Services

OS Host

192.168.1.101(19

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV 192.168.1.101

Details

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-02-21 12:33 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00062s 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 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	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

MAC Address:

08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)

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 52.81 seconds

Filter Hosts