ESERCIZIO M3 D5

OS FINGERPRINT

Nmap -O

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:43 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0010s 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:A0:26:54 (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
```

Nmap Script SMB-OS-Discovery

```
tarting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:46 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00054s 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:A0:26:54 (Oracle VirtualBox virtual NIC)

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: 2023-05-02T14:46:48-04:00
```

SYN SCAN

Nmap -sS

Starting Nmap 7.93 (https://nmap.org) at 2023-05-02 20:49 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00028s 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:A0:26:54 (Oracle VirtualBox virtual NIC)

TCP Connect Scan

Nmap -sT

Starting Nmap 7.93 (https://nmap.org) at 2023-05-02 20:51 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00022s 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:A0:26:54 (Oracle VirtualBox virtual NIC)

Version Scan

Nmap -sV

Starting Nmap 7.93 (https://nmap.org) at 2023-05-02 20:53 CEST

Nmap scan report for 192.168.50.101

Host is up (0.000062s 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:A0:26:54 (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 193.63 seconds

Scan All

Nmap -A

Starting Nmap 7.93 (https://nmap.org) at 2023-05-02 21:11 CEST

Nmap scan report for 192.168.50.101

Host is up (0.00086s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.50.100

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|_End of status

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)

|_ 2048 5656240f211ddea72bae61b1243de8f3 (RSA)

23/tcp open telnet?

25/tcp open smtp?

|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-title: Metasploitable2 - Linux

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 35391/tcp mountd

| 100005 1,2,3 43399/udp mountd

| 100021 1,3,4 51204/udp nlockmgr

| 100021 1,3,4 58331/tcp nlockmgr

| 100024 1 35989/udp status

|_ 100024 1 36122/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (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

|_ssl-date: 2023-05-02T19:16:12+00:00; -1s from scanner time.

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

ng outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|_Not valid after: 2010-04-16T14:07:45

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-favicon: Apache Tomcat

|_http-title: Apache Tomcat/5.5

MAC Address: 08:00:27:A0:26:54 (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

Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: 1h19m58s, deviation: 2h18m33s, median: -1s

| **smb-os-discovery:**

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|_ System time: 2023-05-02T15:14:21-04:00

| smb-security-mode:

| account_used: <blank>

| **authentication_level: user**

| challenge_response: supported

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_smb2-time: Protocol negotiation failed (SMB2)

|_nbstat: **NetBIOS name: METASPLOITABLE**, NetBIOS user: <unknown>, NetBIOS MAC:000000000000 (Xerox)

TRACEROUTE

HOP RTT ADDRESS

1 0.86 ms 192.168.50.101

REPORT

IP:192.168.50.101

S.O.:LINUX 2.6.9/2.6.33

PORTE APERTE:

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

SERVIZI IN ASCOLTO CON VERSIONE: in rosa possibilità di exploit

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

SECURE SHELL - è un protocollo che permette di stabilire una connessione remota cifrata

53/tcp open domain ISC BIND 9.4.2

DNS - Domain name system - usata per le query dns

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

HTTP - il server web Apache attende la richiesta di contenuti da parte del browser su questa porta

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Netbios - utilizzata per il riconoscimento dei PC tramite nome in una rete locale (LAN) e la condivisione di devices

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

SMB - server message block - protocollo utilizzato per la condisione di file e stampanti in rete locale

1099/tcp open java-rmi GNU Classpath grmiregistry

Rmi registry - processo di tipo daemon che tiene traccia di tutti gli oggetti remoti disponibili su un dato server

1524/tcp open bindshell Metasploitable root shell

Shell di root di Metasplotable

2049/tcp open nfs 2-4 (RPC #100003)5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

Postgresql - database

5900/tcp open vnc VNC (protocol 3.3)

VNC – virtual network computing – consente di visualizzare il desktop di un computer remoto ed interagirci

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

Protocollo che converte in binario il traffico web in http

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Piattaforma per applicazioni sviluppate in Java, supporta http tramite Coyote. Coyote ascolta le connessioni in entrata e inoltra la richiesta al Tomcat engineper processare la richiesta e restituire la risposta.