TECNICHE DI SCANSIONE CON #NMAP, TARGET:

#METASPLOITABLE

MODIFICARE LE IMPOSTAZIONI IN MODO CHE LE DUE MACCHINE SIANO SULLA STESSA RETE.
PRODURRE UN REPORT CONTENENTE LE SEGUENTI INFO:

- **IP ADDRESS**
- **SISTEMA OPERATIVO**
- **PORTE APERTE**
- **SERVIZI IN ASCOLTO CON VERSIONE**
- **DESCRIZIONE DEI SERVIZI**

(https://www-poftut.com/nmap-output)
(nmap -oN report1 IP)

SI RICHIEDE DI EFFETTUARE LE SEGUENTI SCANSIONI SUL TARGET METASPLOITABLE:

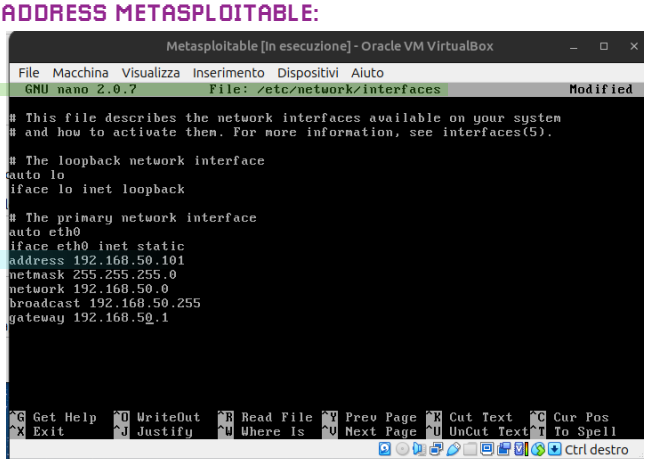
- **OS FINGERPRINT**
- **SYN SCAN**
- **TCP CONNECT**
- **VERSION DETECTION**

INDICARE LE DIFFERENZE TRA SYN SCAN E TCP CONNECT

AL FINE DELL'ESERCIZIO SERVE CHE LE DUE MACCHINE (KALI E METASPLOITABLE) SIANO SULLA STESSA RETE, REIMPOSTO QUINDI L'IP DI METASPLOITABLE CON L'EDITOR NANO DA SHELL SU 192.168.50.101, MENTRE QUELLO DI KALI LINUX RESTA 192.168.50.100. RIAVVIO IL SERVIZIO CON SUDO SERVICE NETWORKING RESTART E PROSEGUO CON L'ESERCIZIO.

#IP ADDRESS METASPLOITABLE:

IP



#IP ADDRESS E VERSIONE OS KALI LINUX:

IP

```
┌──(root㉿kali)-[/home/django]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
 group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UP group default qlen 1000
    link/ether 08:00:27:fa:dd:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
       valid_lft 83038sec preferred_lft 83038sec
    inet6 fe80::a00:27ff:fefa:dd14/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UP group default qlen 1000
    link/ether 08:00:27:62:34:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe62:3451/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

```
┌──(root㉿kali)-[/home/django]
└─# cat /etc/*release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"

┌──(root㉿kali)-[/home/django]
└─# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

#REPORT SULLE MACCHINE:

- ifconfig O ip -a PER VEDERE IP/MAC ADDRESS DELLE MACCHINE (NELLE IMG PRECEDENTI)
- ESEGUO UN OS FINGERPRINT CON NMAP PER CONOSCERE IL SISTEMA OPERATIVO (nmap -O <IP>)
- ESEGUO UNO SCAN TCP E UDP CON VERSION DETECTION CON NMAP PER IDENTIFICARE LE PORTE APERTE, IL SERVIZIO IN ASCOLTO ASSOCIATO E LA SUA VERSIONE (nmap -sV <IP> -A / nmap -sU <IP> -A)

```
┌──(root㉿kali)-[/home/django]
└─# nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 07:06 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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:A3:DF:62 (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 1.69 seconds
```

OS FINGERPRINT:
STIMA DEL SISTEMA OPERATIVO,
TCP SCAN CON ASSOCIAZIONE
PORTE APERTE - SERVIZIO

```
┌──(root㉿kali)-[/home/django]
└─# nmap -sV 192.168.50.101 -A
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 07:20 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      51186/tcp   mountd
|   100005  1,2,3      52818/udp   mountd
|   100021  1,3,4      49029/udp   nlockmgr
|   100021  1,3,4      53972/tcp   nlockmgr
|   100024  1          32789/tcp   status
|_  100024  1          52892/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  c•D(bQ?D  Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SupportsCompression, Support41Auth
|   Status: Autocommit
|_  Salt: U#M;~~^uPnZZ31<vadRK
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-01-23T12:21:38+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
| 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-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:A3:DF:62 (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: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h40m01s, deviation: 2h53m12s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-01-23T07:21:08-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   1.06 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.21 seconds
```

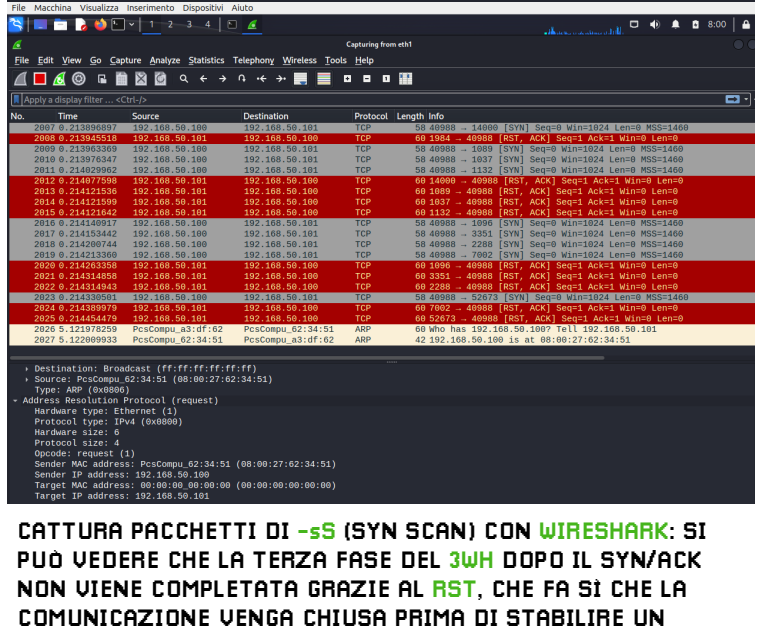
VERSION DETECTION
AGGRESSIVE SCAN:
TCP FAST SCAN CON ASSOCIAZIONE
PORTE TCP APERTE AL SERVIZIO
IN ASCOLTO E VERSIONE

```
┌──(root㉿kali)-[/home/django]
└─# nmap -sU 192.168.50.101 -A
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 07:34 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE     VERSION
53/udp   open          domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
69/udp   open|filtered tftp
111/udp  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      51186/tcp   mountd
|   100005  1,2,3      52818/udp   mountd
|   100021  1,3,4      49029/udp   nlockmgr
|   100021  1,3,4      53972/tcp   nlockmgr
|   100024  1          32789/tcp   status
|_  100024  1          52892/udp   status
137/udp  open          netbios-ns  Microsoft Windows netbios-ns (workgroup: WORKGROUP)
| nbns-interfaces:
|   hostname: METASPLOITABLE
|   interfaces:
|_    192.168.50.101
138/udp  open|filtered netbios-dgm
2049/udp open          nfs         2-4 (RPC #100003)
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: METASPLOITABLE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   1.20 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1205.42 seconds
```

UDP AGGRESSIVE SCAN: FAST SCAN CON ASSOCIAZIONE PORTE UDP APERTE AL SERVIZIO IN ASCOLTO

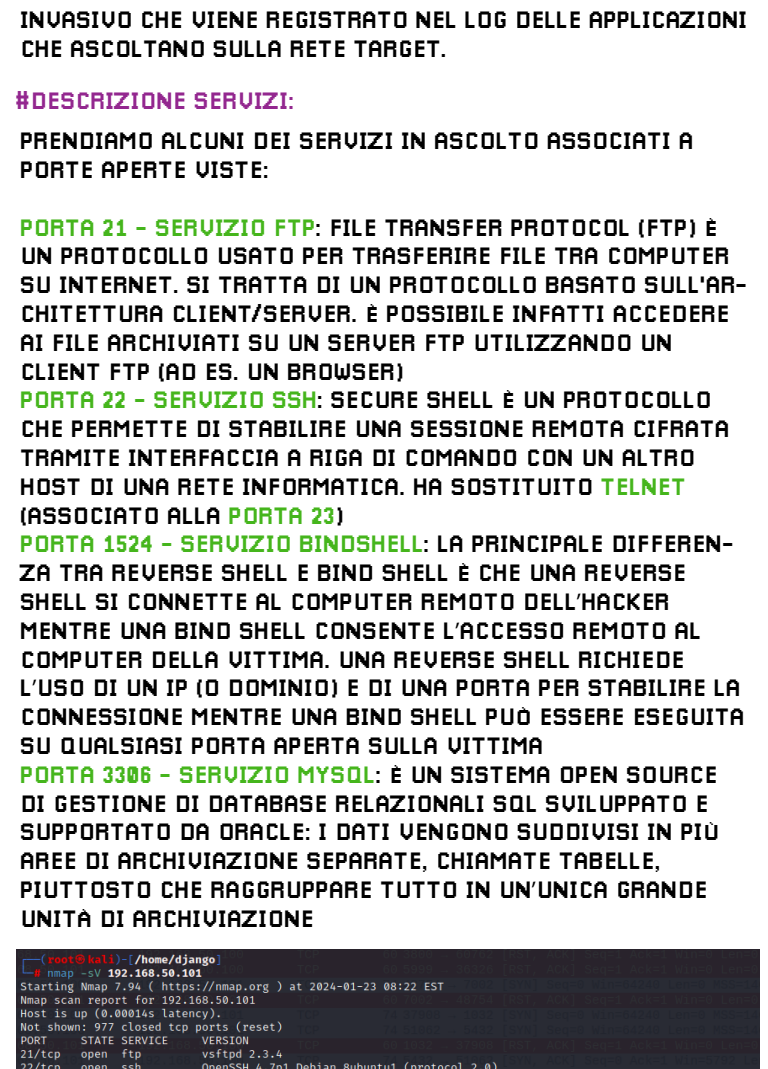
```
┌──(root㉿kali)-[/home/django]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 08:00 EST
Nmap scan report for 192.168.50.101
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

TCP SYN (STEALTH) SCAN: SCAN MENO INVASIVO, CHE NON COMPLETA IL 3-W-H, CON ASSOCIAZIONE PORTE UDP APERTE AL SERVIZIO IN ASCOLTO



CATTURA PACCHETTI DI -sS (SYN SCAN) CON WIRESHARK: SI PUÒ VEDERE CHE LA TERZA FASE DEL 3WH DOPO IL SYN/ACK NON VIENE COMPLETATA GRAZIE AL RST, CHE FA SÌ CHE LA COMUNICAZIONE VENGA CHIUSA PRIMA DI STABILIRE UN CANALE. È UN TIPO DI SCAN MENO INVASIVO CHE FA MENO RUMORE A LIVELLO DI NETWORK, QUINDI MENO IDENTIFICABILE RISPETTO AD UN TCP SCAN. PUÒ COMUNQUE ESSERE RILEVATO DA IDS/IPS CONFIGURATI AD HOC.

```
┌──(root㉿kali)-[/home/django]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 08:03 EST
Nmap scan report for 192.168.50.101
Host is up (0.00085s 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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```



CATTURA PACCHETTI DI -sT (TCP SCAN) CON WIRESHARK: SI PUÒ VEDERE CHE PER CONTROLLARE SE UNA PORTA È APERTA E RECUPERARE INFORMAZIONI SUL SERVIZIO IN ASCOLTO LA TERZA FASE DEL 3WH DOPO IL SYN/ACK VIENE COMPLETATA STABILENDO DI FATTO UN CANALE. È UN TIPO DI SCAN PIÙ INVASIVO CHE VIENE REGISTRATO NEL LOG DELLE APPLICAZIONI CHE ASCOLTANO SULLA RETE TARGET.

#DESCRIZIONE SERVIZI:

PRENDIAMO ALCUNI DEI SERVIZI IN ASCOLTO ASSOCIATI A PORTE APERTE VISTE:

PORTA 21 - SERVIZIO FTP: FILE TRANSFER PROTOCOL (FTP) È UN PROTOCOLLO USATO PER TRASFERIRE FILE TRA COMPUTER SU INTERNET. SI TRATTA DI UN PROTOCOLLO BASATO SULL'ARCHITETTURA CLIENT/SERVER. È POSSIBILE INFATTI ACCEDERE AI FILE ARCHIVIATI SU UN SERVER FTP UTILIZZANDO UN CLIENT FTP (AD ES. UN BROWSER)
PORTA 22 - SERVIZIO SSH: SECURE SHELL È UN PROTOCOLLO CHE PERMETTE DI STABILIRE UNA SESSIONE REMOTA CIFRATA TRAMITE INTERFACCIA A RIGA DI COMANDO CON UN ALTRO HOST DI UNA RETE INFORMATICA. HA SOSTITUITO TELNET (ASSOCIATO ALLA PORTA 23)
PORTA 1524 - SERVIZIO BINDSHELL: LA PRINCIPALE DIFFERENZA TRA REVERSE SHELL E BIND SHELL È CHE UNA REVERSE SHELL SI CONNETTE AL COMPUTER REMOTO DELL'HACKER MENTRE UNA BIND SHELL CONSENTE L'ACCESSO REMOTO AL COMPUTER DELLA VITTIMA. UNA REVERSE SHELL RICHIEDE L'USO DI UN IP (O DOMINIO) E DI UNA PORTA PER STABILIRE LA CONNESSIONE MENTRE UNA BIND SHELL PUÒ ESSERE ESEGUITA SU QUALSIASI PORTA APERTA SULLA VITTIMA
PORTA 3306 - SERVIZIO MYSQL: È UN SISTEMA OPEN SOURCE DI GESTIONE DI DATABASE RELAZIONALI SQL SVILUPPATO E SUPPORTATO DA ORACLE: I DATI VENGONO SUDDIVISI IN PIÙ AREE DI ARCHIVIAZIONE SEPARATE, CHIAMATE TABELLE, PIUTTOSTO CHE RAGGRUPPARE TUTTO IN UN'UNICA GRANDE UNITÀ DI ARCHIVIAZIONE

```
┌──(root㉿kali)-[/home/django]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 08:22 EST
Nmap scan report for 192.168.50.101
Host is up (0.00014s 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:A3:DF:62 (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 52.91 seconds
```