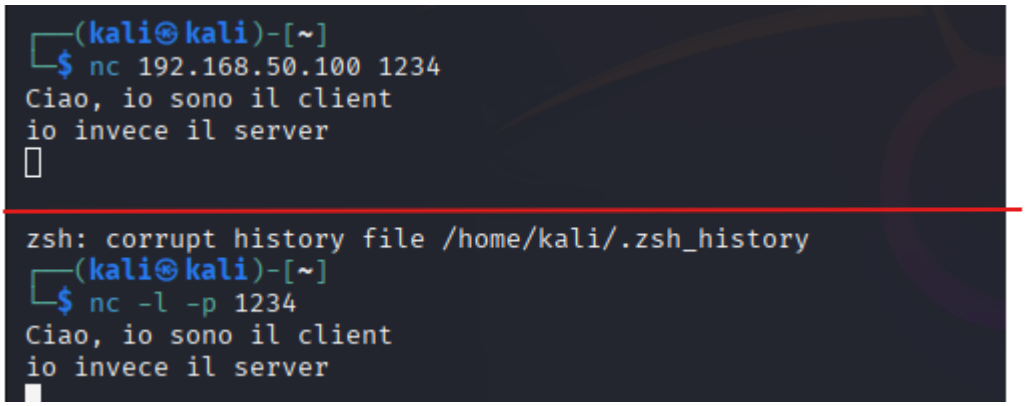
Netcat e Nmap

Netcat

Shell

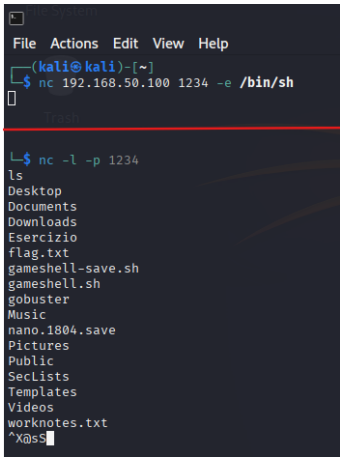
Esempio di shell con Netcat

Nel terminale in basso, netcat apre un listener (-l) per le connessioni in entrata e assegna un numero di porta (-p) 1234



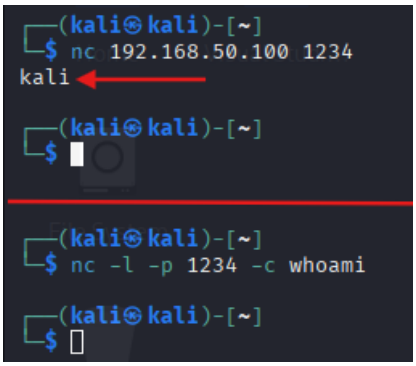
Il comando nel terminale in alto si connette all'indirizzo 192.168.100 sulla porta 1234, avviando quindi una comunicazione Client – Server

Il comando **-e /bin/sh** dice a netcat di eseguire **/bin/sh**



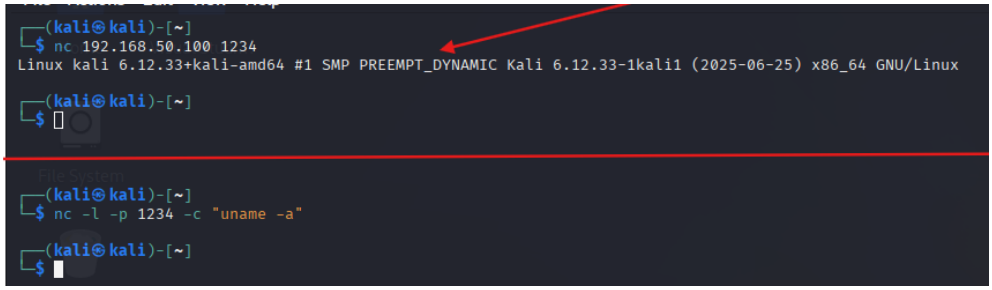
WHOAMI

In questo caso visualizzeremo l'utente



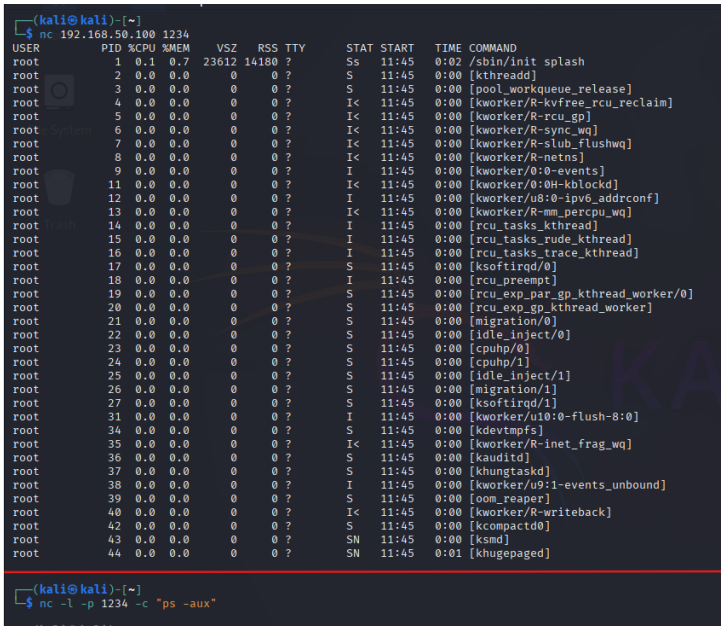
uname -a

Con **uname -a** otteniamo informazioni sul sistema operativo e il kernel



ps -aux

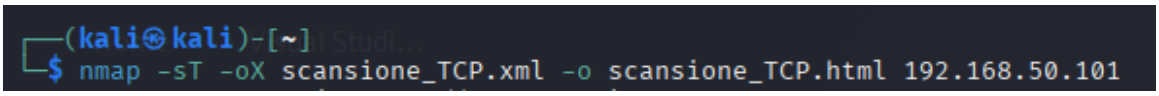
Mostrerà i processi in esecuzione



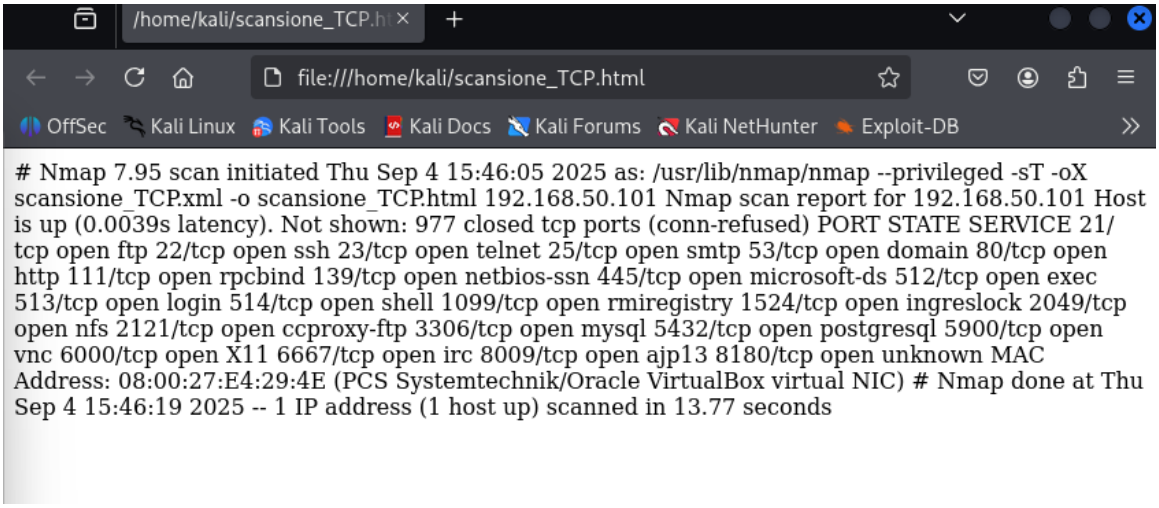
Traccia Nmap

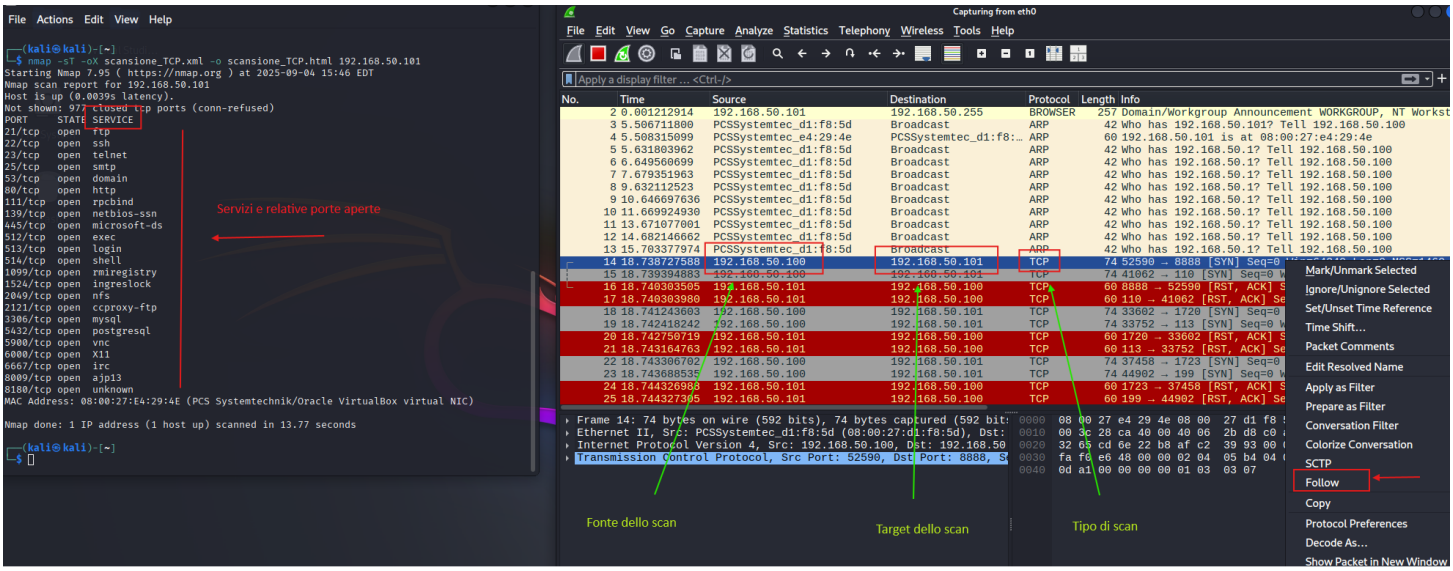
Scansione TCP sulle porte well-known

Ho eseguito la scansione sulle porte well-known, che si ottengono senza specificare il range di porte da scansionare, con il comando **-sT** che consente la scansione TCP.

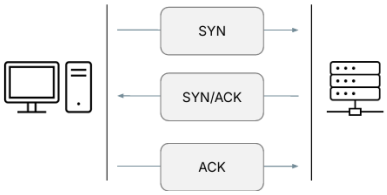


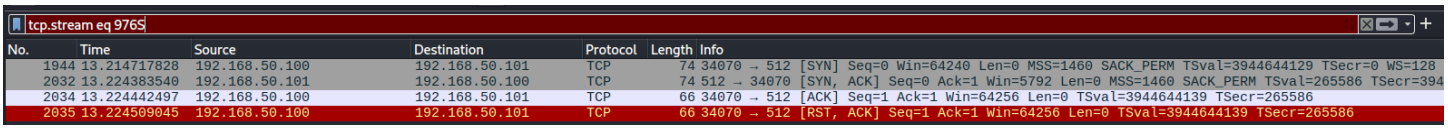
-oX <nomefile> -o <nome file> servono per salvare il risultato della scansione in un file HTML, per poi aprirlo in un formato spesso (non in questo caso) utilizzabile in un report.





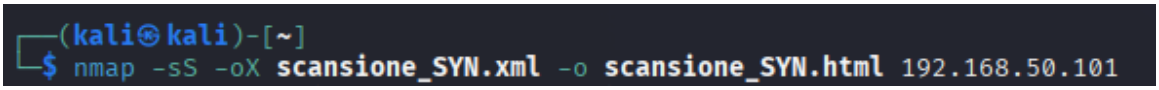
Facendo clic su Follow è possibile seguire lo stream di un pacchetto e notare che il 3-way-handshake viene completato.

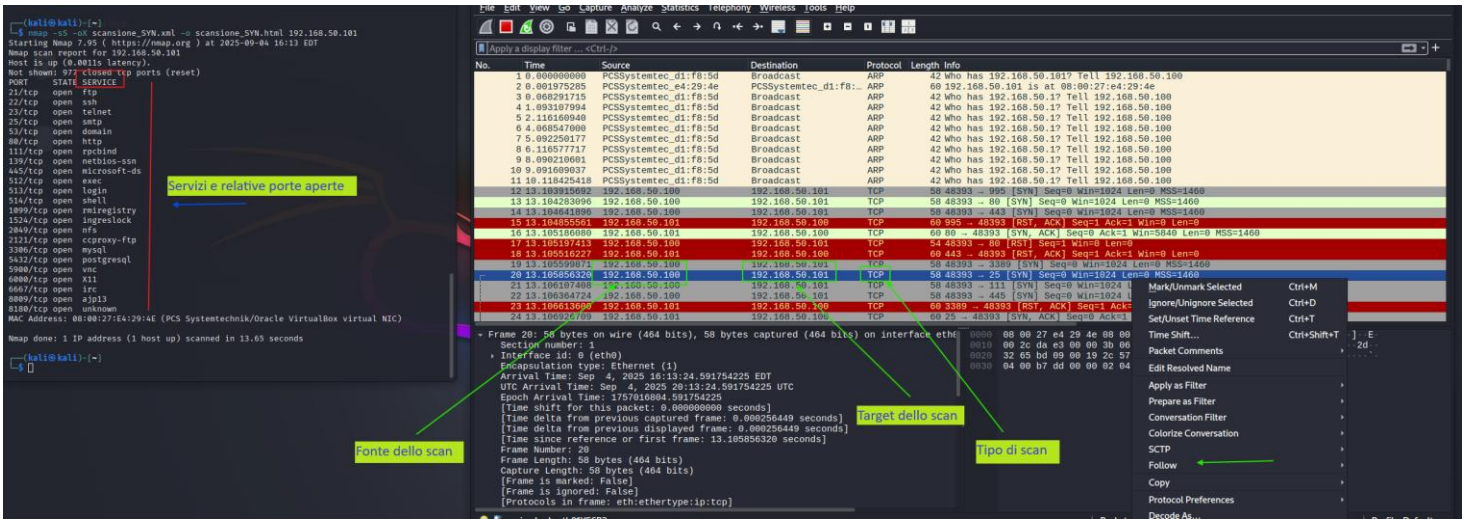




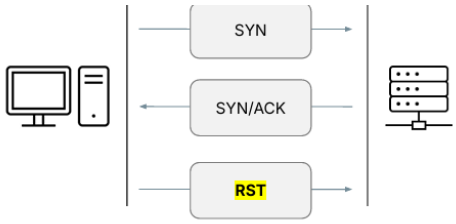
Scansione SYN sulle porte well-known

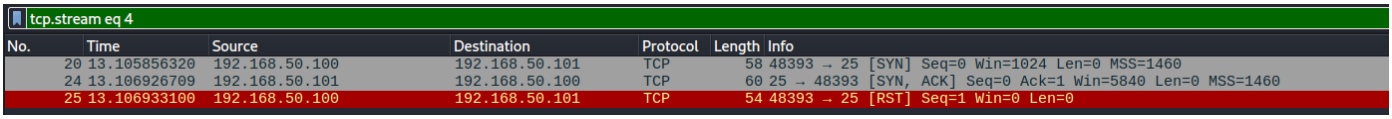
La scansione SYN è possibile con il comando -sS





Il comando **-sS** non completa il 3-way-handshake ma chiude la comunicazione inviando un pacchetto RST (reset), riesce però a recuperare informazioni sullo stato della porta.





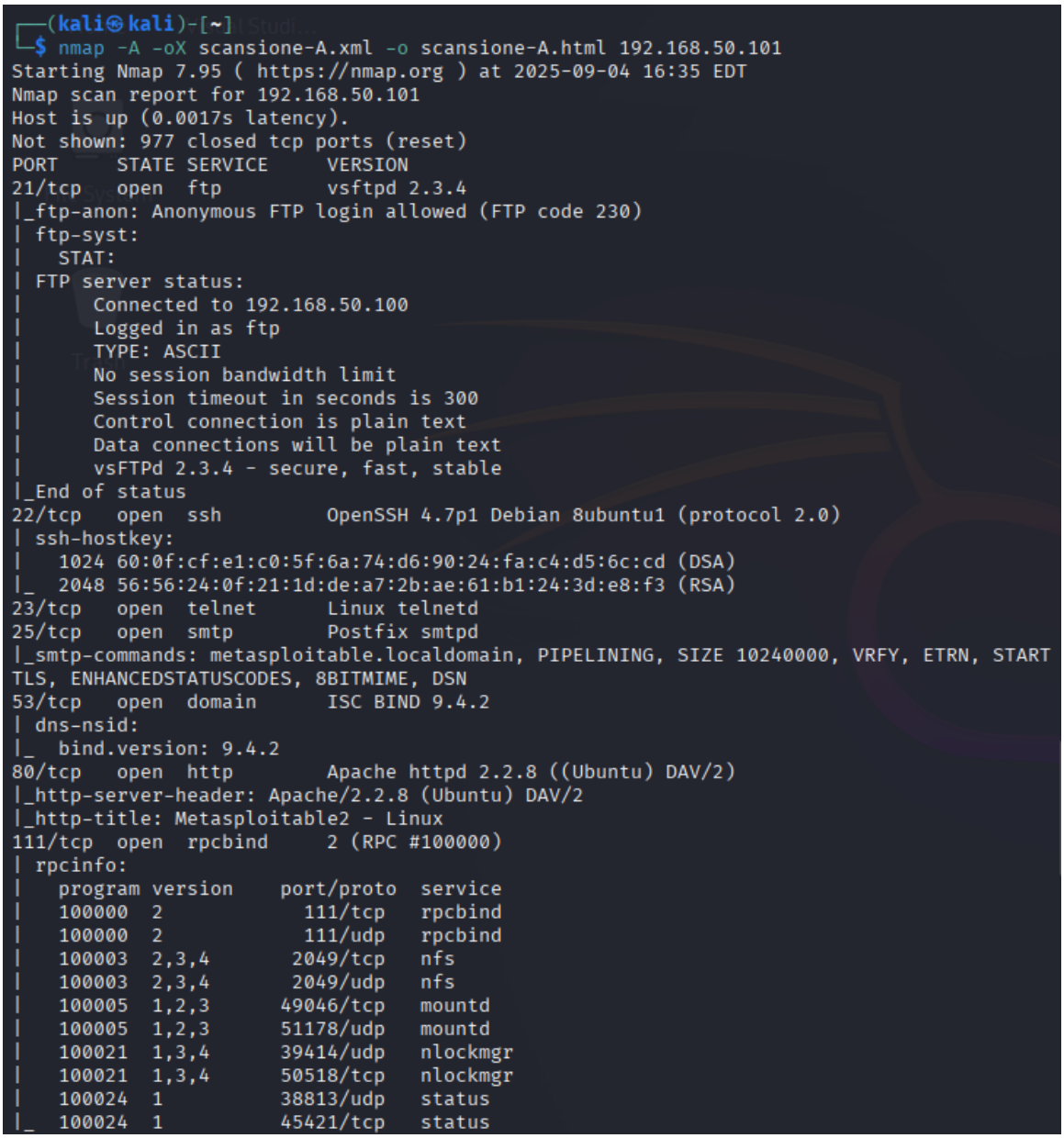
Scansione con switch «-A» sulle porte well-known

La scansione con **-A** prova a identificare il sistema operativo del target, le versioni dei servizi in ascolto sulle porte aperte, esegue la scansione degli script e il traceroute, tracciando il percorso dei pacchetti fino al target.

Con **nmap -h** vediamo il dettaglio dei comandi. Di seguito la descrizione di cosa rileva con **-A**:

```
-A: Enable OS detection, version detection, script scanning, and traceroute
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -oX scansione-A.xml -o scansione-A.html 192.168.50.101
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -oX scansione-A.xml -o scansione-A.html 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 16:35 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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
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, START
TLS, 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/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      49046/tcp   mountd
|   100005  1,2,3      51178/udp   mountd
|   100021  1,3,4      39414/udp   nlockmgr
|   100021  1,3,4      50518/tcp   nlockmgr
|   100024  1          38813/udp   status
|_  100024  1          45421/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        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: 11
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsTransactions, LongColu
mnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|_  Salt: 0?0oay]E#z_ONz:OawV(
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOr
ProvinceName=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
|_ssl-date: 2025-09-04T20:36:45+00:00; +1s from scanner time.
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-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/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, Linu
x; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (
unknown)
|_clock-skew: mean: 1h20m01s, deviation: 2h18m40s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-04T16:36:15-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   1.66 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.20 seconds
```

Come notiamo con Wireshark, **nmap -A** invia richieste di vario genere: FTP, http, ICMP e tanto altro.

```
4372 81.515362170  192.168.50.101  192.168.50.100  FTP   86 Response: 220 (vsFTPd 2.3.4)
4374 81.558620799  192.168.50.100  192.168.50.101  FTP  154 Request: \026\003\001\000S\001\000\000O\003\003h��U@尻'd@\000@@rJ@
4376 81.561656120  192.168.50.101  192.168.50.100  FTP  104 Response: 530 Please login with USER and PASS.
4378 81.562468493  192.168.50.101  192.168.50.100  FTP  104 Response: 530 Please login with USER and PASS.
4382 81.706433460  192.168.50.101  192.168.50.100  FTP   76 Response: 500 OOPS:
2145 19.475396564  192.168.50.100  192.168.50.101  HTTP  84 GET / HTTP/1.0
2257 19.896270596  192.168.50.101  192.168.50.100  HTTP  66 HTTP/1.1 200 OK  (text/html)
2320 24.525447825  192.168.50.100  192.168.50.101  HTTP  84 GET / HTTP/1.0
2391 29.526202533  192.168.50.100  192.168.50.101  HTTP  88 OPTIONS / HTTP/1.0
```

```
2589 50.403510343  192.168.50.101  192.168.50.100  ICMP  162 Echo (ping) reply    id=0x5a77, seq=295/9985, ttl=64 (request in 2588)
2590 50.429188735  192.168.50.100  192.168.50.101  ICMP  192 Echo (ping) request  id=0x5a78, seq=296/10241, ttl=53 (reply in 2591)
```

```
2130 14.500362926  192.168.50.101  192.168.50.100  IRC    136 Response (NOTICE)
2291 23.534078271  192.168.50.101  192.168.50.100  IRC    170 Response (NOTICE)
2293 23.534976433  192.168.50.101  192.168.50.100  IRC    121 Response (ERROR)
3120 57.944217408  192.168.50.100  192.168.50.101  IRC    115 Request (USER) (NICK)
3726 58.895270361  192.168.50.101  192.168.50.100  IRC    136 Response (NOTICE)
4111 67.891614894  192.168.50.101  192.168.50.100  IRC    170 Response (NOTICE)
4113 67.892479239  192.168.50.101  192.168.50.100  IRC   1514 Response (001) (002) (003) (004) (005) (005) (005) (251) (255) (265) (266) (422) (MOD
2259 23.464554763  192.168.50.101  192.168.50.100  MySQL  132 Server Greeting  proto=10 version=5.0.51a-3ubuntu5
2261 23.465300888  192.168.50.101  192.168.50.100  MySQL   86 Response  Error 1043
4042 61.455424582  192.168.50.101  192.168.50.100  MySQL  132 Server Greeting  proto=10 version=5.0.51a-3ubuntu5
```

```
  50 13.080759383  192.168.50.100  192.168.50.101  TCP  58 53669 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  51 13.080815323  192.168.50.100  192.168.50.101  TCP  58 53669 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  52 13.080869103  192.168.50.100  192.168.50.101  TCP  58 53669 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  53 13.080884884  192.168.50.101  192.168.50.100  TCP  60 22 → 53669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
```

```
2592 50.455087851  192.168.50.100  192.168.50.101  UDP  342 46888 → 35317 Len=300
2675 51.155102353  192.168.50.100  192.168.50.101  UDP   43 52008 → 1434 Len=1
```