**M3 D1 ES2**

## GIORNO 3 – NMAP SCAN

## NETWORK SCANNING CON NMAP

**-sT scan: metodo più invasivo, il controllo avviene completando il three-way handshake.
Dalla cattura pacchetti si nota che vengono inviati i pacchetti successivi al SYN scan (sS).
Il comportamento in caso di porta chiusa è uguale per entrambe le metodologie di scansione.**

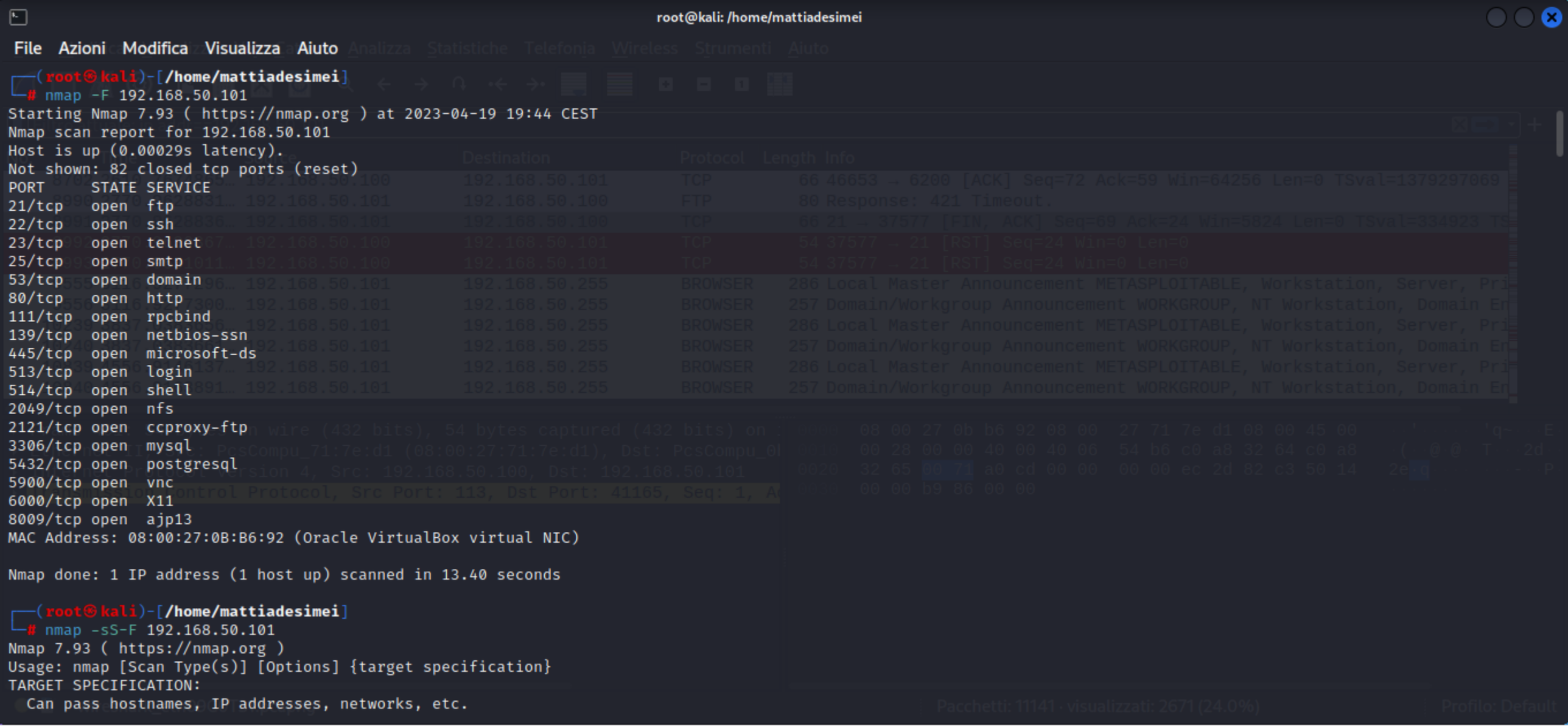
**-sS scan: riguarda il SYN scan, le richieste inviate non concludono il three-way handshake, una volta accertato che la porta è aperta chiude la comunicazione.
Se la risposta è RST/ACK la porta è chiusa e senza servizi attivi.
In caso di risposta SYN/ACK la porta è aperta e la macchina bersaglio ci risponde con un pacchetto. La macchina attaccante invia un altro pacchetto RST andando a chiudere la connessione evitando l' handshake.**

**-A scan: con l' aggiunta di questa funzione si recuperano molte info della macchina bersaglio, inclusa la lista dei servizi in ascolto sulle diverse porte aperte e la loro versione.**

```
┌──(mattiadesimei㉿kali)-[~]
└─$ nmap -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 19:42 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

┌──(mattiadesimei㉿kali)-[~]
└─$ sudo su
[sudo] password di mattiadesimei:
Riprovare.
[sudo] password di mattiadesimei:
┌──(root㉿kali)-[/home/mattiadesimei]
└─# nmap -F 192.168.50.101
```


root@kali: /home/mattiadesimei
File Azioni Modifica Visualizza Aiuto
┌──(root㉿kali)-[/home/mattiadesimei]
└─# nmap -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 19:44 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00029s latency).
Not shown: 82 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
513/tcp open login
514/tcp open shell
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
8009/tcp open ajp13
MAC Address: 08:00:27:0B:B6:92 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
┌──(root㉿kali)-[/home/mattiadesimei]
└─# nmap -sS-F 192.168.50.101
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.

```
┌──(root㉿kali)-[/home/mattiadesimei]
└─# nmap -sS-F 192.168.50.101
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
```

```
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
          directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
          <Lua scripts> is a comma-separated list of script-files or
          script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
```

```
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
```

```
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype - not supported

┌──(root㉿kali)-[/home/mattiadesimei]
└─# nmap -A-F 192.168.50.101
nmap: invalid option -- '-'
See the output of nmap -h for a summary of options.

┌──(root㉿kali)-[/home/mattiadesimei]
└─# nmap -A -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 19:55 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00039s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
```

```
| 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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDS
TATUSCODES, 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      35080/tcp   mountd
|   100005  1,2,3      47619/udp   mountd
|   100021  1,3,4      55370/udp   nlockmgr
```

```
|   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      35080/tcp   mountd
|   100005  1,2,3      47619/udp   mountd
|   100021  1,3,4      55370/udp   nlockmgr
|   100021  1,3,4      56370/tcp   nlockmgr
|   100024  1          54787/tcp   status
|_  100024  1          55426/udp   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)
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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: 10
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumn
Flag, Support41Auth, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: f&%)=7<gt16[F-N"Y~/i
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=T
here 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: 2023-04-19T19:57:42+00:00; +2h00m00s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
```

```
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
MAC Address: 08:00:27:0B:B6:92 (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:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 3h20m00s, deviation: 2h18m34s, median: 1h59m59s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-04-19T15:56:13-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.39 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 146.52 seconds

┌──(root㉿kali)-[/home/mattiadesimei]
└─# msfconsole


*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0x CD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337
*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
```

*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337
*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackst
reetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleed
sOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad
 Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownow
browncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hyd
ra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswi
thsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseAr
ch*MadDawgs*
*HInc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*B
yteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyl
e*Panic*
*B0NG0R3*                                                                    *Les Cadet
s Rouges*buf*
*Les Tontons Fl4gueurs*                                                      *404 : Fla
g Not Found*
*' UNION SELECT 'password*                                                   *OCD247*Sp
arkle Pony*
*burner_herz0g*                                                              *Kill$hot*
ConEmu*
*here_there_be_trolls*                                                       *;echo"hac
ked"*
*r4t5_*6rung4nd4*NYUSEC*                                                     *karamel4e
*
*IkastenIO*TWC*balkansec*                                                    *cybersecu
rity.li*
*TofuEelRoll*Trash Pandas*                                                   *OneManArm

```
arkle Pony*
*burner_herz0g*                                                    *Kill$hot*
ConEmu*
*here_there_be_trolls*                                             *;echo"hac
ked"*
*r4t5_*6rung4nd4*NYUSEC*                                           *karamel4e
*
*IkastenIO*TWC*balkansec*                                          *cybersecu
rity.li*
*TofuEelRoll*Trash Pandas*                                         *OneManArm
y*cyb3r_w1z4rd5*
*Astra*Got Schwartz?*tmux*                                         *AreYouStu
ck*Mr.Robot.0*
*\nls*Juicy white peach*                                           *EPITA Ren
nes*
*HackerKnights*                                                    *guildOfGe
ngar*Titans*
*Pentest Rangers*                                                  *The Libby
rators*
*placeholder name*bitup*                                           *JeffTadas
hi*Mikeal*
*UCASers*onotch*                                                   *ky_dong_d
ay_song*
*NeNiNuMmOk*                                                       *JustForFu
n!*
*Maux de tête*LalaNG*                                              *g3tsh3Lls
0on*
*crr0tz*z3r0p0rn*clueless*                                         *Phở Đặc B
iệt*Paradox*
*HackWara*                                                         *KaRIPux*i
nf0sec*
*Kugelschreibertester*                                             *bluehens*
Antoine77*
*icemasters*                                                       *genxy*TRA
DE_NAMES*
```

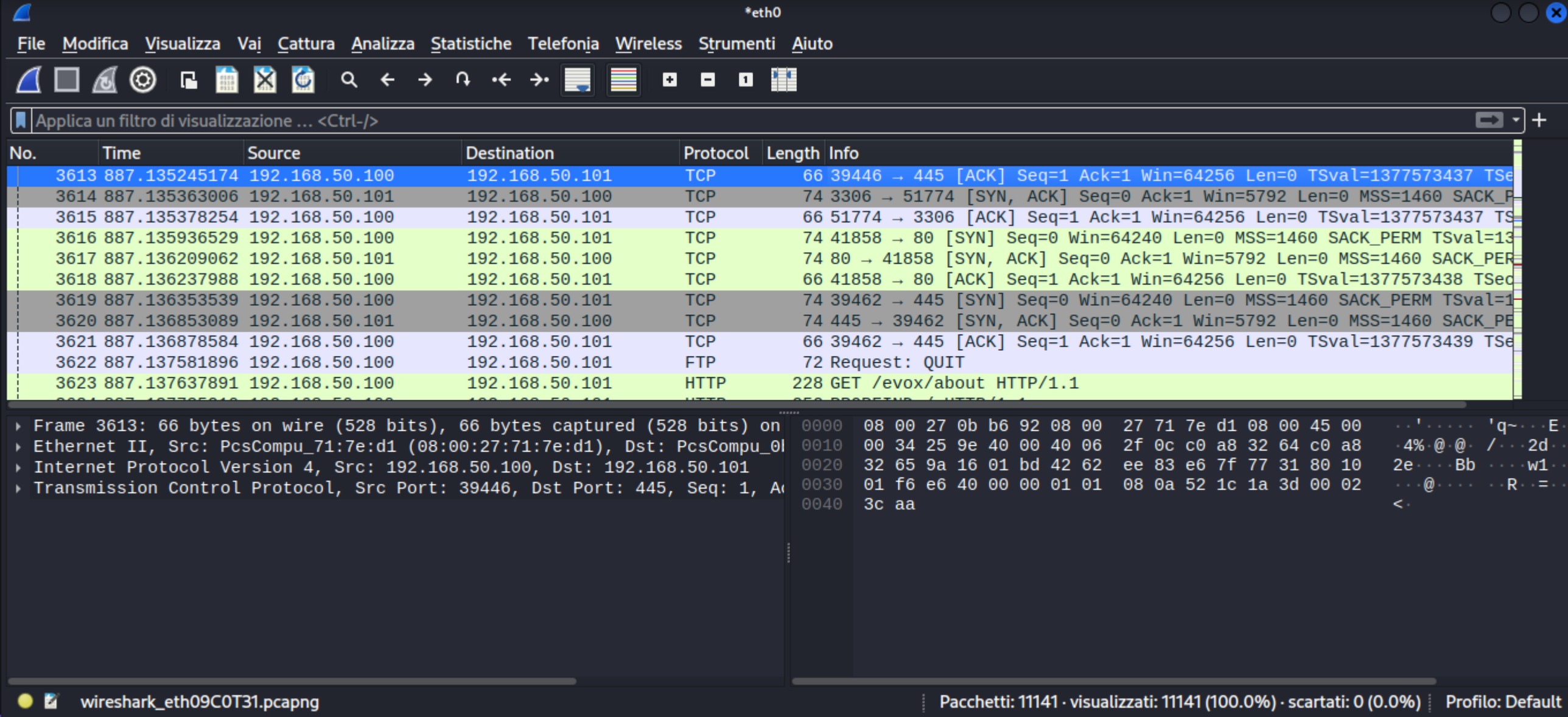
n!*
*Maux de tête*LalaNG* *g3tsh3Lls
0on*
*crr0tz*z3r0p0rn*clueless* *Phở Đặc B
iệt*Paradox*
*HackWara* *KaRIPux*i
nf0sec*
*Kugelschreibertester* *bluehens*
Antoine77*
*icemasters* *genxy*TRA
DE_NAMES*
*Spartan's Ravens* *BadByte*f
ontwang_tw*
*g0ldd1gg3rs*pappo* *ghoti*
*Les CRACKS*c0dingRabbits* *LinuxRide
rs*
*2Cr4Sh*RecycleBin* *Jalan Dur
ian*
*ExploitStudio* *WPICSC*lo
garitm*
*Car RamRod*0x41414141* *Orv1ll3*t
eam-fm4dd*
*Björkson*FlyingCircus* *PwnHub*H4
X0R*Yanee*
*Securifera*hot cocoa* *Et3rnal*P
elarianCP*
*n00bytes*DNC&G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcu
rity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Tea
m Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team
 Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-
team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTE

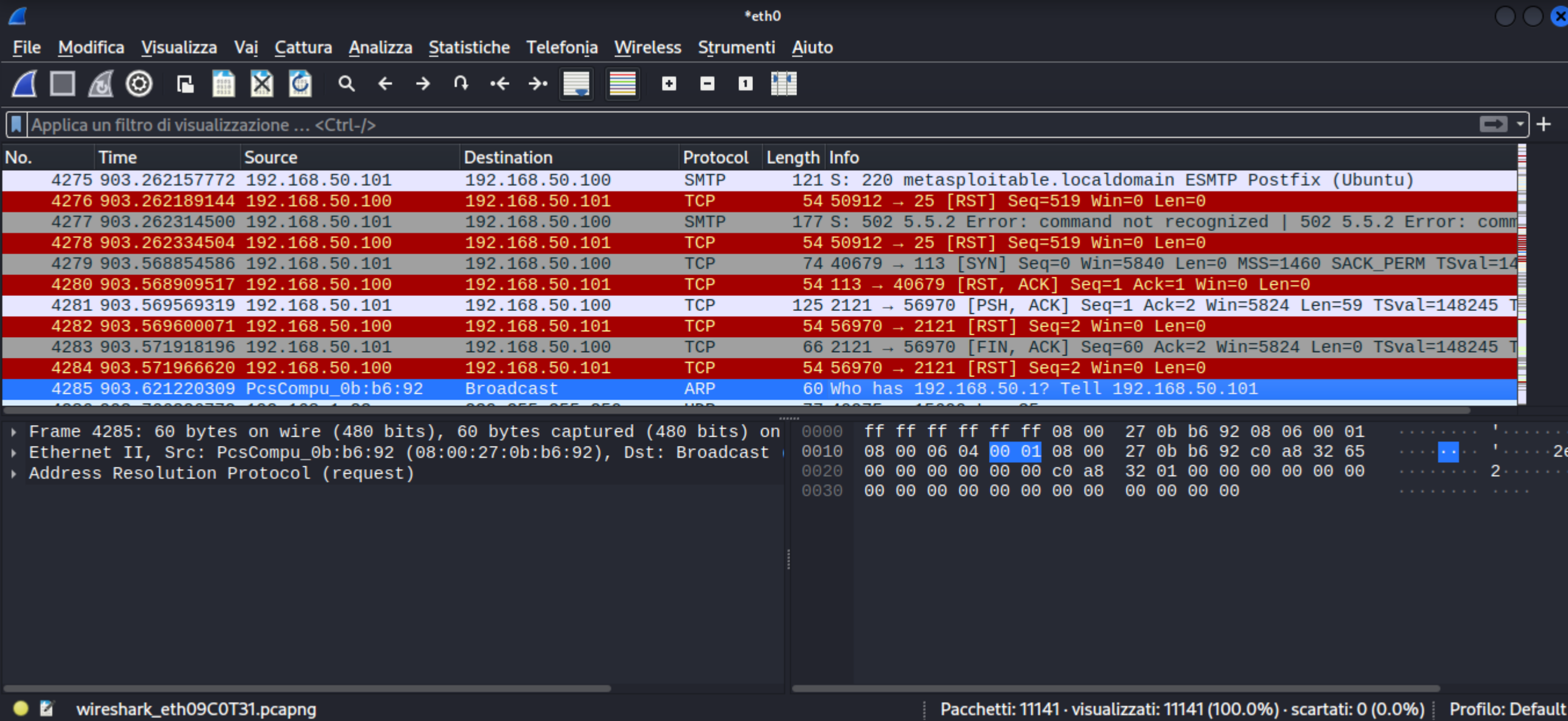
```
 Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-
team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTE
rr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pick
le_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO
*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety
*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_
alaviiva_turva*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs
*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemD
irtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*
InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*aras
an*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*



       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/
```


*eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3613 887.135245174 192.168.50.100 192.168.50.101 TCP 66 39446 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1377573437 TSe
3614 887.135363006 192.168.50.101 192.168.50.100 TCP 74 3306 → 51774 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_P
3615 887.135378254 192.168.50.100 192.168.50.101 TCP 66 51774 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1377573437 TS
3616 887.135936529 192.168.50.100 192.168.50.101 TCP 74 41858 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=13
3617 887.136209062 192.168.50.101 192.168.50.100 TCP 74 80 → 41858 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
3618 887.136237988 192.168.50.100 192.168.50.101 TCP 66 41858 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1377573438 TSec
3619 887.136353539 192.168.50.100 192.168.50.101 TCP 74 39462 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1
3620 887.136853089 192.168.50.101 192.168.50.100 TCP 74 445 → 39462 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
3621 887.136878584 192.168.50.100 192.168.50.101 TCP 66 39462 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1377573439 TSe
3622 887.137581896 192.168.50.100 192.168.50.101 FTP 72 Request: QUIT
3623 887.137637891 192.168.50.100 192.168.50.101 HTTP 228 GET /evox/about HTTP/1.1
Frame 3613: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
Ethernet II, Src: PcsCompu_71:7e:d1 (08:00:27:71:7e:d1), Dst: PcsCompu_0
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
Transmission Control Protocol, Src Port: 39446, Dst Port: 445, Seq: 1, A
0000 08 00 27 0b b6 92 08 00 27 71 7e d1 08 00 45 00
0010 00 34 25 9e 40 00 40 06 2f 0c c0 a8 32 64 c0 a8
0020 32 65 9a 16 01 bd 42 62 ee 83 e6 7f 77 31 80 10
0030 01 f6 e6 40 00 00 01 01 08 0a 52 1c 1a 3d 00 02
0040 3c aa
wireshark_eth09C0T31.pcapng
Pacchetti: 11141 · visualizzati: 11141 (100.0%) · scartati: 0 (0.0%)
Profilo: Default


*eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione … <Ctrl-/>
No. Time Source Destination Protocol Length Info
4275 903.262157772 192.168.50.101 192.168.50.100 SMTP 121 S: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
4276 903.262189144 192.168.50.100 192.168.50.101 TCP 54 50912 → 25 [RST] Seq=519 Win=0 Len=0
4277 903.262314500 192.168.50.101 192.168.50.100 SMTP 177 S: 502 5.5.2 Error: command not recognized | 502 5.5.2 Error: comm
4278 903.262334504 192.168.50.100 192.168.50.101 TCP 54 50912 → 25 [RST] Seq=519 Win=0 Len=0
4279 903.568854586 192.168.50.101 192.168.50.100 TCP 74 40679 → 113 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=14
4280 903.568909517 192.168.50.100 192.168.50.101 TCP 54 113 → 40679 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4281 903.569569319 192.168.50.101 192.168.50.100 TCP 125 2121 → 56970 [PSH, ACK] Seq=1 Ack=2 Win=5824 Len=59 TSval=148245 T
4282 903.569600071 192.168.50.100 192.168.50.101 TCP 54 56970 → 2121 [RST] Seq=2 Win=0 Len=0
4283 903.571918196 192.168.50.101 192.168.50.100 TCP 66 2121 → 56970 [FIN, ACK] Seq=60 Ack=2 Win=5824 Len=0 TSval=148245 T
4284 903.571966620 192.168.50.100 192.168.50.101 TCP 54 56970 → 2121 [RST] Seq=2 Win=0 Len=0
4285 903.621220309 PcsCompu_0b:b6:92 Broadcast ARP 60 Who has 192.168.50.1? Tell 192.168.50.101
Frame 4285: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: PcsCompu_0b:b6:92 (08:00:27:0b:b6:92), Dst: Broadcast
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 00 27 0b b6 92 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 0b b6 92 c0 a8 32 65
0020 00 00 00 00 00 00 c0 a8 32 01 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
wireshark_eth09C0T31.pcapng
Pacchetti: 11141 · visualizzati: 11141 (100.0%) · scartati: 0 (0.0%)
Profilo: Default