

# Cybersecurity Analyst

**Week 9** - W9D1 Pratica 2

# Tools di Kali Linux Nmap

## Esercizio

Esecuzione di diversi tipi di scan su macchina Metasploitable:

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

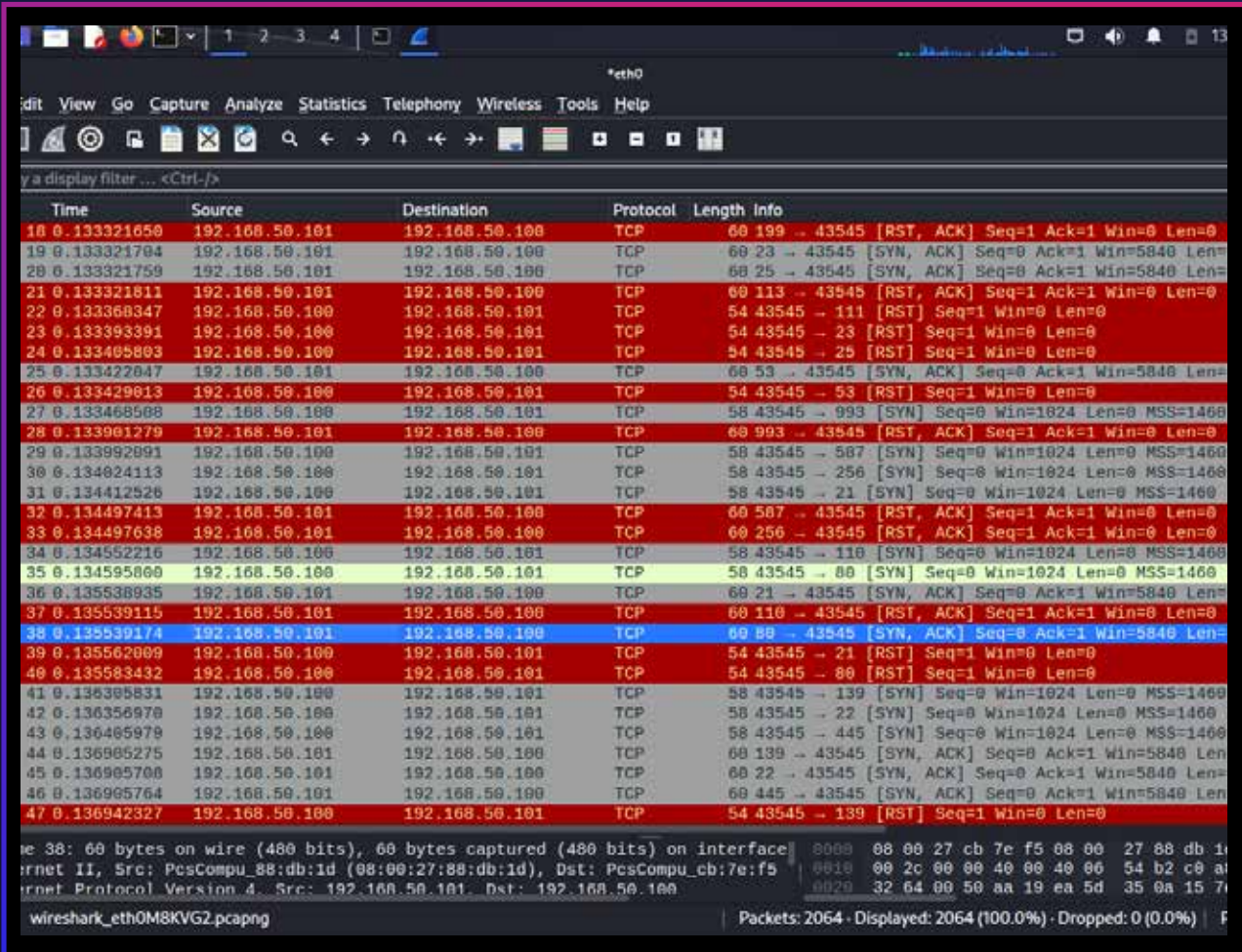
Intercettazione delle richieste inviate dalla macchina sorgente con Wireshark.

## SCANSIONE SYN

```
(kali㉿kali)-[~]  
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 12:58 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.0031s latency).  
Not shown: 1012 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  
MAC Address: 08:00:27:88:DB:1D (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
```

# SCANSIONE SYN

Analisi WIRESHARK (la 3-way-handshake **non viene chiusa**)



Time	Source	Destination	Protocol	Length	Info
18 0.133321650	192.168.50.101	192.168.50.100	TCP	60	199 → 43545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19 0.133321704	192.168.50.101	192.168.50.100	TCP	60	23 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
20 0.133321759	192.168.50.101	192.168.50.100	TCP	60	25 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
21 0.133321811	192.168.50.101	192.168.50.100	TCP	60	113 → 43545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 0.133368347	192.168.50.100	192.168.50.101	TCP	54	43545 → 111 [RST] Seq=1 Win=0 Len=0
23 0.133393391	192.168.50.100	192.168.50.101	TCP	54	43545 → 23 [RST] Seq=1 Win=0 Len=0
24 0.133405893	192.168.50.100	192.168.50.101	TCP	54	43545 → 25 [RST] Seq=1 Win=0 Len=0
25 0.133422047	192.168.50.101	192.168.50.100	TCP	60	53 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
26 0.133429013	192.168.50.100	192.168.50.101	TCP	54	43545 → 53 [RST] Seq=1 Win=0 Len=0
27 0.133468508	192.168.50.100	192.168.50.101	TCP	58	43545 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28 0.133901279	192.168.50.101	192.168.50.100	TCP	60	993 → 43545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 0.133992091	192.168.50.100	192.168.50.101	TCP	58	43545 → 507 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30 0.134024113	192.168.50.100	192.168.50.101	TCP	58	43545 → 250 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31 0.134412526	192.168.50.100	192.168.50.101	TCP	58	43545 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32 0.134497413	192.168.50.101	192.168.50.100	TCP	60	507 → 43545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 0.134497638	192.168.50.101	192.168.50.100	TCP	60	250 → 43545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34 0.134552216	192.168.50.100	192.168.50.101	TCP	58	43545 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35 0.134595060	192.168.50.100	192.168.50.101	TCP	58	43545 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36 0.135538935	192.168.50.101	192.168.50.100	TCP	60	21 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
37 0.135539115	192.168.50.101	192.168.50.100	TCP	60	110 → 43545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38 0.135539174	192.168.50.101	192.168.50.100	TCP	60	80 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
39 0.135562009	192.168.50.100	192.168.50.101	TCP	54	43545 → 21 [RST] Seq=1 Win=0 Len=0
40 0.135583432	192.168.50.100	192.168.50.101	TCP	54	43545 → 80 [RST] Seq=1 Win=0 Len=0
41 0.136305831	192.168.50.100	192.168.50.101	TCP	58	43545 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42 0.136356970	192.168.50.100	192.168.50.101	TCP	58	43545 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43 0.136405979	192.168.50.100	192.168.50.101	TCP	58	43545 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44 0.136905275	192.168.50.101	192.168.50.100	TCP	60	139 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
45 0.136905700	192.168.50.101	192.168.50.100	TCP	60	22 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
46 0.136905764	192.168.50.101	192.168.50.100	TCP	60	445 → 43545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
47 0.136942327	192.168.50.100	192.168.50.101	TCP	54	43545 → 139 [RST] Seq=1 Win=0 Len=0

38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0  
 Internet II, Src: PcsCompu\_88:db:1d (08:00:27:88:db:1d), Dst: PcsCompu\_cb:7e:f5  
 Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.100

wireshark\_eth0M8KV2.pcapng | Packets: 2064 · Displayed: 2064 (100.0%) · Dropped: 0 (0.0%)

## SCANSIONE TCP

```
(kali@kali)-[~]  
$ sudo nmap -sT 192.168.50.101 -p 1-1024  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 13:34 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.0023s latency).  
Not shown: 1012 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  
MAC Address: 08:00:27:88:DB:1D (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```



# SCANSIONE TCP

Analisi WIRESHARK (la 3-way-handshake **viene chiusa**)

Time	Source	Destination	Protocol	Length	Info
33 0.171024943	192.168.50.101	192.168.50.100	TCP	60	256 → 53936 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34 0.171073064	192.168.50.100	192.168.50.101	TCP	74	60362 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
35 0.171153496	192.168.50.100	192.168.50.101	TCP	74	50152 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
36 0.171221403	192.168.50.100	192.168.50.101	TCP	74	51478 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
37 0.171284164	192.168.50.100	192.168.50.101	TCP	74	59916 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
38 0.171758796	192.168.50.101	192.168.50.100	TCP	74	21 → 40042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
39 0.171759017	192.168.50.101	192.168.50.100	TCP	60	113 → 60362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 0.171796530	192.168.50.100	192.168.50.101	TCP	60	40042 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
41 0.172180069	192.168.50.100	192.168.50.100	TCP	74	80 → 50152 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
42 0.172180280	192.168.50.101	192.168.50.100	TCP	60	135 → 51478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43 0.172180356	192.168.50.101	192.168.50.100	TCP	74	22 → 59916 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
44 0.172203133	192.168.50.100	192.168.50.101	TCP	66	50152 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
45 0.172239345	192.168.50.100	192.168.50.101	TCP	66	59916 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
46 0.172276311	192.168.50.100	192.168.50.101	TCP	74	53224 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
47 0.172446623	192.168.50.100	192.168.50.101	TCP	74	33498 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
48 0.172689927	192.168.50.101	192.168.50.100	TCP	74	139 → 53224 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
49 0.172708869	192.168.50.100	192.168.50.101	TCP	66	53224 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
50 0.172761102	192.168.50.100	192.168.50.101	TCP	74	54908 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
51 0.172975066	192.168.50.101	192.168.50.100	TCP	74	53 → 33498 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
52 0.172997845	192.168.50.100	192.168.50.101	TCP	66	33498 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
53 0.173050371	192.168.50.100	192.168.50.101	TCP	74	33646 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
54 0.173506101	192.168.50.101	192.168.50.100	TCP	74	23 → 54908 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
55 0.173526473	192.168.50.100	192.168.50.101	TCP	66	54908 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
56 0.173776405	192.168.50.101	192.168.50.100	TCP	60	443 → 33646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57 0.173924092	192.168.50.100	192.168.50.101	TCP	74	37818 → 1009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
58 0.173997724	192.168.50.100	192.168.50.101	TCP	74	49138 → 431 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
59 0.174414147	192.168.50.101	192.168.50.100	TCP	60	1009 → 37818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60 0.174414334	192.168.50.101	192.168.50.100	TCP	60	431 → 49138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 0.174466782	192.168.50.100	192.168.50.101	TCP	74	46734 → 35 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
62 0.174538092	192.168.50.100	192.168.50.101	TCP	74	54114 → 774 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Time 35: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0  
 Ethernet II, Src: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu\_88:db:1d (08:00:27:88:db:1d)  
 Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101  
 wireshark\_eth0R7JYG2.pcapng

Packets: 2076 · Displayed: 2076 (100.0%) · Dropped: 0 (0.0%)

# SCANSIONE CON SWITCH -A

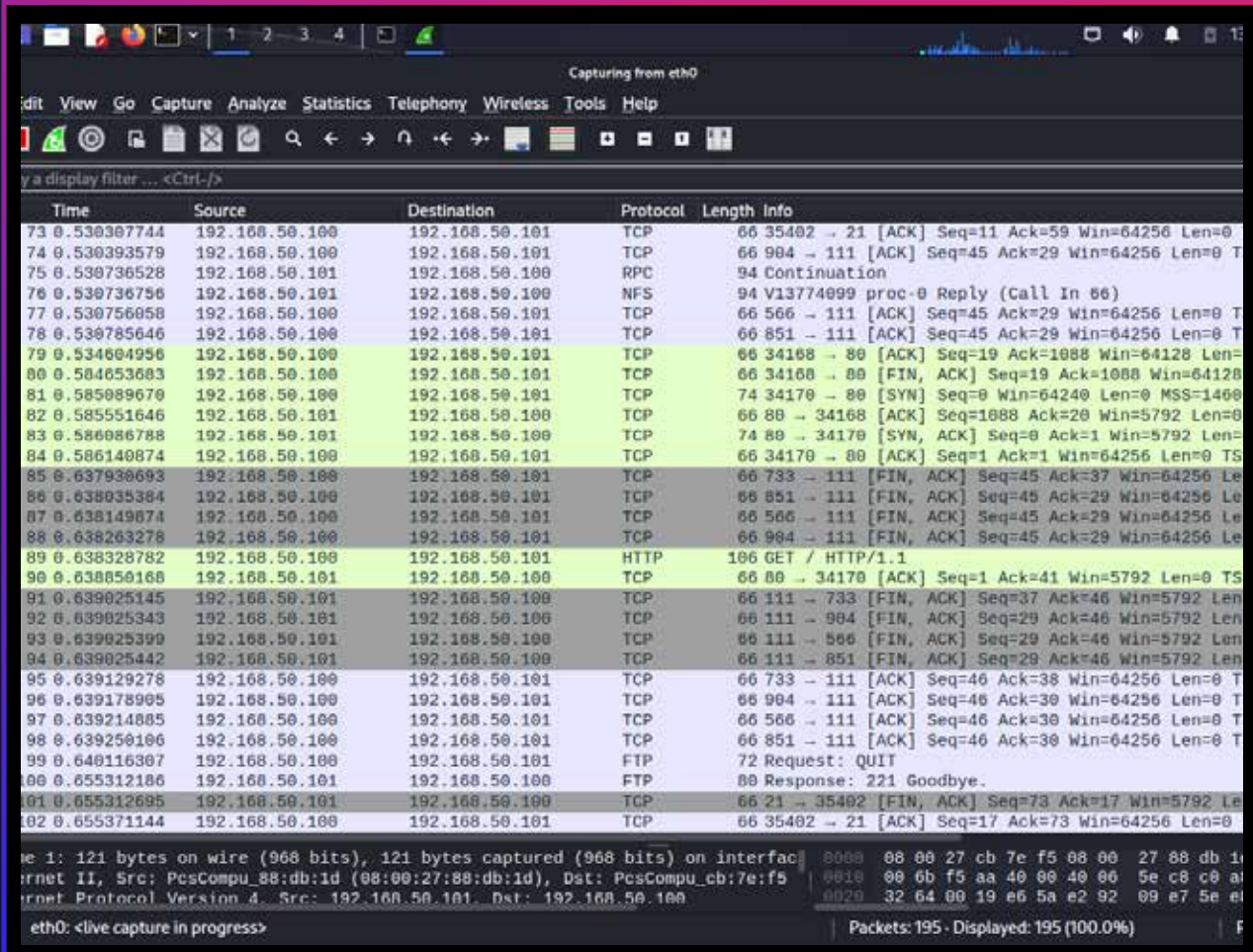
```
(kali@kali)~$ sudo nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 13:43 EST
Nmap scan report for 192.168.50.101
Host is up (0.00065s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 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 6B:8F:CF:E1:C8:5F:6A:74:D6:9B:24:FA:4C:D5:6C:CD (DSA)
|_   2048 56:96:24:0F:21:1D:0E:A7:2B:AE:61:01:24:3D:E8:F3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-command: 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:
|_   100005 1,2,3      36546/udp  mountd
|_   100005 1,2,3      38467/tcp  mountd
|_   100021 1,3,4      39541/udp  nlockmgr
|_   100021 1,3,4      41053/tcp  nlockmgr
|_   100024 1          34816/udp  status
|_   100024 1          53266/tcp  status
129/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 rshcd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
MAC Address: 08:00:27:08:00:1D (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:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h30m02s, deviation: 3h32m06s, median: 1s
|_smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|_   OS: Unix (Samba 3.0.20-Debian)
|_   Computer name: metasploitable
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: metasploitable.localdomain
|_   System time: 2024-01-04T13:44:39-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```



# SCANSIONE CON SWITCH - A

## Analisi WIRESHARK (molto più invasiva)



Time	Source	Destination	Protocol	Length	Info
73 0.530307744	192.168.50.100	192.168.50.101	TCP	66	35402 → 21 [ACK] Seq=11 Ack=59 Win=64256 Len=0
74 0.530393579	192.168.50.100	192.168.50.101	TCP	66	904 → 111 [ACK] Seq=45 Ack=29 Win=64256 Len=0
75 0.530736528	192.168.50.101	192.168.50.100	RPC	94	Continuation
76 0.530736756	192.168.50.101	192.168.50.100	NFS	94	V13774099 proc=0 Reply (Call In 66)
77 0.530756058	192.168.50.100	192.168.50.101	TCP	66	566 → 111 [ACK] Seq=45 Ack=29 Win=64256 Len=0
78 0.530785646	192.168.50.100	192.168.50.101	TCP	66	851 → 111 [ACK] Seq=45 Ack=29 Win=64256 Len=0
79 0.534604956	192.168.50.100	192.168.50.101	TCP	66	34168 → 80 [ACK] Seq=19 Ack=1088 Win=64128 Len=0
80 0.504653683	192.168.50.100	192.168.50.101	TCP	66	34168 → 80 [FIN, ACK] Seq=19 Ack=1088 Win=64128 Len=0
81 0.585089670	192.168.50.100	192.168.50.101	TCP	74	34170 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
82 0.585551646	192.168.50.101	192.168.50.100	TCP	66	80 → 34168 [ACK] Seq=1088 Ack=20 Win=5792 Len=0
83 0.586086788	192.168.50.101	192.168.50.100	TCP	74	80 → 34170 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
84 0.586140874	192.168.50.100	192.168.50.101	TCP	66	34170 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
85 0.637930693	192.168.50.100	192.168.50.101	TCP	66	733 → 111 [FIN, ACK] Seq=45 Ack=37 Win=64256 Len=0
86 0.638035384	192.168.50.100	192.168.50.101	TCP	66	851 → 111 [FIN, ACK] Seq=45 Ack=29 Win=64256 Len=0
87 0.638149074	192.168.50.100	192.168.50.101	TCP	66	566 → 111 [FIN, ACK] Seq=45 Ack=29 Win=64256 Len=0
88 0.638263278	192.168.50.100	192.168.50.101	TCP	66	904 → 111 [FIN, ACK] Seq=45 Ack=29 Win=64256 Len=0
89 0.638328782	192.168.50.100	192.168.50.101	HTTP	106	GET / HTTP/1.1
90 0.638850168	192.168.50.101	192.168.50.100	TCP	66	80 → 34170 [ACK] Seq=1 Ack=41 Win=5792 Len=0
91 0.639025145	192.168.50.101	192.168.50.100	TCP	66	111 → 733 [FIN, ACK] Seq=37 Ack=46 Win=5792 Len=0
92 0.639025343	192.168.50.101	192.168.50.100	TCP	66	111 → 904 [FIN, ACK] Seq=29 Ack=46 Win=5792 Len=0
93 0.639025399	192.168.50.101	192.168.50.100	TCP	66	111 → 566 [FIN, ACK] Seq=29 Ack=46 Win=5792 Len=0
94 0.639025442	192.168.50.101	192.168.50.100	TCP	66	111 → 851 [FIN, ACK] Seq=29 Ack=46 Win=5792 Len=0
95 0.639129278	192.168.50.100	192.168.50.101	TCP	66	733 → 111 [ACK] Seq=46 Ack=38 Win=64256 Len=0
96 0.639178905	192.168.50.100	192.168.50.101	TCP	66	904 → 111 [ACK] Seq=46 Ack=30 Win=64256 Len=0
97 0.639214885	192.168.50.100	192.168.50.101	TCP	66	566 → 111 [ACK] Seq=46 Ack=30 Win=64256 Len=0
98 0.639250106	192.168.50.100	192.168.50.101	TCP	66	851 → 111 [ACK] Seq=46 Ack=30 Win=64256 Len=0
99 0.640116307	192.168.50.100	192.168.50.101	FTP	72	Request: QUIT
100 0.655312186	192.168.50.101	192.168.50.100	FTP	80	Response: 221 Goodbye.
101 0.655312695	192.168.50.101	192.168.50.100	TCP	66	21 → 35402 [FIN, ACK] Seq=73 Ack=17 Win=5792 Len=0
102 0.655371144	192.168.50.100	192.168.50.101	TCP	66	35402 → 21 [ACK] Seq=17 Ack=73 Win=64256 Len=0

eth0: <live capture in progress>

Packets: 195 · Displayed: 195 (100.0%)