

SCANSIONE SYN CON WIRESHARK SU MACCHINA METASPLOTABLE

The screenshot displays a Kali Linux virtual machine environment. On the left, a terminal window shows the execution of an Nmap scan against the IP address 192.168.50.101. The scan identifies several open ports, including 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), and 514/tcp (shell). The scan report indicates that 1012 closed TCP ports were reset.

On the right, the Wireshark network protocol analyzer is open, displaying a list of captured packets. The selected packet (No. 2075) is a TCP RST, ACK packet from 192.168.50.101 to 192.168.50.100, with sequence number 858 and window size 0. The packet details pane shows the Transmission Control Protocol (TCP) segment, including the source and destination ports.

Terminal Output:

```
kali@kali: ~  
File Actions Edit View Help  
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: 08:00:27:23:D1:7E (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds  
$ sudo nmap -sS -p 1-1024 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 05:32 EST  
Host is up (0.00050s 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: 08:00:27:23:D1:7E (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds  
$
```

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
2056	21.842696698	192.168.50.100	192.168.50.101	TCP	58	56046 → 286 [SYN] Seq=0 Win=0
2057	21.842722567	192.168.50.100	192.168.50.101	TCP	58	56046 → 122 [SYN] Seq=0 Win=0
2058	21.842748166	192.168.50.100	192.168.50.101	TCP	58	56046 → 976 [SYN] Seq=0 Win=0
2059	21.842806308	192.168.50.101	192.168.50.100	TCP	60	166 → 56046 [RST, ACK] Seq=1
2060	21.842806337	192.168.50.101	192.168.50.100	TCP	60	462 → 56046 [RST, ACK] Seq=1
2061	21.842806358	192.168.50.101	192.168.50.100	TCP	60	670 → 56046 [RST, ACK] Seq=1
2062	21.842773894	192.168.50.100	192.168.50.101	TCP	58	56046 → 455 [SYN] Seq=0 Win=0
2063	21.842822202	192.168.50.100	192.168.50.101	TCP	58	56046 → 16 [SYN] Seq=0 Win=0
2064	21.842964969	192.168.50.101	192.168.50.100	TCP	60	705 → 56046 [RST, ACK] Seq=1
2065	21.842964997	192.168.50.101	192.168.50.100	TCP	60	89 → 56046 [RST, ACK] Seq=1
2066	21.842965019	192.168.50.101	192.168.50.100	TCP	60	687 → 56046 [RST, ACK] Seq=1
2067	21.842965040	192.168.50.101	192.168.50.100	TCP	60	521 → 56046 [RST, ACK] Seq=1
2068	21.842965062	192.168.50.101	192.168.50.100	TCP	60	369 → 56046 [RST, ACK] Seq=1
2069	21.843135248	192.168.50.101	192.168.50.100	TCP	60	498 → 56046 [RST, ACK] Seq=1
2070	21.843136730	192.168.50.101	192.168.50.100	TCP	60	175 → 56046 [RST, ACK] Seq=1
2071	21.843136753	192.168.50.101	192.168.50.100	TCP	60	912 → 56046 [RST, ACK] Seq=1
2072	21.843136773	192.168.50.101	192.168.50.100	TCP	60	292 → 56046 [RST, ACK] Seq=1
2073	21.843136796	192.168.50.101	192.168.50.100	TCP	60	558 → 56046 [RST, ACK] Seq=1
2074	21.843306196	192.168.50.101	192.168.50.100	TCP	60	274 → 56046 [RST, ACK] Seq=1
2075	21.843306223	192.168.50.101	192.168.50.100	TCP	60	858 → 56046 [RST, ACK] Seq=1
2076	21.843306244	192.168.50.101	192.168.50.100	TCP	60	286 → 56046 [RST, ACK] Seq=1
2077	21.843306266	192.168.50.101	192.168.50.100	TCP	60	122 → 56046 [RST, ACK] Seq=1
2078	21.843306288	192.168.50.101	192.168.50.100	TCP	60	976 → 56046 [RST, ACK] Seq=1
2079	21.843474881	192.168.50.101	192.168.50.100	TCP	60	455 → 56046 [RST, ACK] Seq=1
2080	21.843474909	192.168.50.101	192.168.50.100	TCP	60	16 → 56046 [RST, ACK] Seq=1

Wireshark Packet Details:

Frame 2075: 60 bytes on wire (480 bits), Ethernet II, Src: PcsCompu.23:d1:7e (08:00:27:23:d1:7e), Dst: 192.168.50.100 (08:00:27:23:d1:7e), Internet Protocol Version 4, Src: 192.168.50.101, Destination: 192.168.50.100, Transmission Control Protocol, Src Port: 858, Dst Port: 56046

SCANSIONE TCP CON WIRESHARK SU MACCHINA METASPLOTABLE

The image shows a Kali Linux virtual machine environment. On the left, a terminal window displays the results of an Nmap scan performed on 192.168.50.101. The scan identified several open ports, including 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), and 514/tcp (shell). The MAC address is 08:00:27:23:D1:7E.

On the right, the Wireshark network protocol analyzer is open, displaying a packet capture on the eth0 interface. The packet list shows a series of TCP packets. Packet 2053 is highlighted, showing a SYN packet from 192.168.50.100 to 192.168.50.101 on port 926. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and the Transmission Control Protocol header.

Terminal Output:

```
kali@kali: ~  
File Actions Edit View Help  
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: 08:00:27:23:D1:7E (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds  
  
(kali@kali)-[~]  
$ nmap -sT 192.168.50.101 -p 1-1024  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 05:38 ES  
T  
Nmap scan report for 192.168.50.101  
Host is up (0.0013s 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  
  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds  
  
(kali@kali)-[~]  
$
```

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
2051	1.717965616	192.168.50.100	192.168.50.101	TCP	74	49596 → 125 [SYN] Seq=0 Win=0
2052	1.718061789	192.168.50.101	192.168.50.100	TCP	60	19 → 52020 [RST, ACK] Seq=1
2053	1.718101829	192.168.50.100	192.168.50.101	TCP	74	51332 → 926 [SYN] Seq=0 Win=0
2054	1.718199864	192.168.50.101	192.168.50.100	TCP	60	125 → 49596 [RST, ACK] Seq=1
2055	1.718199919	192.168.50.101	192.168.50.100	TCP	60	926 → 51332 [RST, ACK] Seq=1
2056	1.718355277	192.168.50.100	192.168.50.101	TCP	74	37720 → 457 [SYN] Seq=0 Win=0
2057	1.718473841	192.168.50.100	192.168.50.101	TCP	74	55434 → 240 [SYN] Seq=0 Win=0
2058	1.718679901	192.168.50.101	192.168.50.100	TCP	60	457 → 37720 [RST, ACK] Seq=1
2059	1.718679948	192.168.50.101	192.168.50.100	TCP	60	240 → 55434 [RST, ACK] Seq=1
2060	1.718721118	192.168.50.100	192.168.50.101	TCP	74	49936 → 433 [SYN] Seq=0 Win=0
2061	1.718930812	192.168.50.101	192.168.50.100	TCP	60	433 → 49936 [RST, ACK] Seq=1
2062	1.718965435	192.168.50.100	192.168.50.101	TCP	74	60542 → 985 [SYN] Seq=0 Win=0
2063	1.719062864	192.168.50.101	192.168.50.100	TCP	60	985 → 60542 [RST, ACK] Seq=1
2064	1.719257412	192.168.50.100	192.168.50.101	TCP	74	57002 → 935 [SYN] Seq=0 Win=0
2065	1.719386813	192.168.50.100	192.168.50.101	TCP	74	46918 → 134 [SYN] Seq=0 Win=0
2066	1.719489201	192.168.50.101	192.168.50.100	TCP	60	935 → 57002 [RST, ACK] Seq=1
2067	1.719632303	192.168.50.101	192.168.50.100	TCP	60	134 → 46918 [RST, ACK] Seq=1
2068	1.719689917	192.168.50.100	192.168.50.101	TCP	74	51718 → 702 [SYN] Seq=0 Win=0
2069	1.719932656	192.168.50.100	192.168.50.101	TCP	74	40682 → 500 [SYN] Seq=0 Win=0
2070	1.720261306	192.168.50.101	192.168.50.100	TCP	60	702 → 51718 [RST, ACK] Seq=1
2071	1.720261391	192.168.50.101	192.168.50.100	TCP	60	500 → 40682 [RST, ACK] Seq=1
2072	1.720315264	192.168.50.100	192.168.50.101	TCP	74	41672 → 56 [SYN] Seq=0 Win=0
2073	1.720439082	192.168.50.100	192.168.50.101	TCP	74	41494 → 253 [SYN] Seq=0 Win=0
2074	1.720553927	192.168.50.101	192.168.50.100	TCP	60	56 → 41672 [RST, ACK] Seq=1
2075	1.720607319	192.168.50.100	192.168.50.101	TCP	74	47258 → 341 [SYN] Seq=0 Win=0

Wireshark Packet Details (Frame 2053):

- Frame 2053: 74 bytes on wire (592 bits), Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:23:d1:7e), Dst: 192.168.50.101 (08:00:27:23:d1:7e)
- Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
- Transmission Control Protocol, Src Port: 51332, Dst Port: 926

Wireshark File: wireshark_eth0XU0DG2.pcapng | Packets: 2104 · Displayed: 2104 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

SCANSIONE SWITCH -A CON WIRESHARK SU MACCHINA METASPLOTABLE

The image displays a Kali Linux virtual machine environment. On the left, a terminal window shows the execution of an Nmap scan on 192.168.50.101. The scan results indicate that the host is up and several services are running, including FTP, SSH, Telnet, SMTP, and HTTP. The terminal output is as follows:

```
(kali@kali)-[~]
$ nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 05:43 EST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 05:44 (0:00:03 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 05:44 (0:00:03 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.00% done; ETC: 05:45 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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 1024000, 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
```

On the right, the Wireshark interface shows a packet capture on the eth0 interface. The packet list pane displays a series of packets, with packet 221 highlighted. The packet details pane shows the structure of the selected packet, which is an ARP request. The packet bytes pane displays the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
198	9.220674418	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.102? Tell 1
199	9.220674667	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.60? Tell 1
200	9.713710724	PcsCompu_23:d1:7e	Broadcast	ARP	60	who has 192.168.50.1? Tell 1
201	9.769720052	192.168.50.100	192.168.50.101	TCP	66	46158 → 25 [FIN, ACK] Seq=1 A
202	9.771811417	192.168.50.101	192.168.50.100	TCP	66	25 → 46158 [ACK] Seq=1 Ack=2
203	9.775880199	192.168.50.101	192.168.50.100	SMTP	121	S: 220 metasploitable.localdo
204	9.775880321	192.168.50.101	192.168.50.100	SMTP	177	S: 502 5.5.2 Error: command f
205	9.775893796	192.168.50.100	192.168.50.101	TCP	54	46148 → 25 [RST] Seq=2 Win=0
206	9.775933592	192.168.50.100	192.168.50.101	TCP	54	46148 → 25 [RST] Seq=2 Win=0
207	9.825188585	192.168.50.100	192.168.50.101	TCP	74	34362 → 25 [SYN] Seq=0 Win=64
208	9.826615216	192.168.50.101	192.168.50.100	TCP	74	25 → 34362 [SYN, ACK] Seq=0 A
209	9.826706592	192.168.50.100	192.168.50.101	TCP	66	34362 → 25 [ACK] Seq=1 Ack=1
210	10.144462310	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.60? Tell 1
211	10.246240361	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.102? Tell 1
212	10.539240624	192.168.50.100	192.168.50.101	TCP	66	46160 → 25 [FIN, ACK] Seq=1 A
213	10.539588980	192.168.50.100	192.168.50.101	TCP	74	34366 → 25 [SYN] Seq=0 Win=64
214	10.539936571	192.168.50.101	192.168.50.100	TCP	74	25 → 34366 [SYN, ACK] Seq=0 A
215	10.539986369	192.168.50.100	192.168.50.101	TCP	66	34366 → 25 [ACK] Seq=1 Ack=1
216	10.540156526	192.168.50.100	192.168.50.101	SMTP	583	C: DATA fragment, 517 bytes
217	10.540391776	192.168.50.101	192.168.50.100	TCP	66	25 → 34366 [ACK] Seq=1 Ack=51
218	10.552325187	192.168.50.101	192.168.50.100	TCP	66	25 → 46160 [ACK] Seq=1 Ack=2
219	11.167567035	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.102? Tell 1
220	11.167567474	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.60? Tell 1
221	12.192323582	AmazonTe_8b:33:db	Broadcast	ARP	60	who has 192.168.1.60? Tell 1

The Wireshark interface also shows the packet details for the selected packet (221), which is an ARP request. The packet bytes pane displays the raw data of the packet.

Frame 221: 60 bytes on wire (480 bits),
Ethernet II, Src: AmazonTe_8b:33:db (90:
Address Resolution Protocol (request)

0000 ff ff ff ff ff 90 a8 22 8b 33 db 08 06 00 01
0010 08 00 06 04 00 01 90 a8 22 8b 33 db c0 a8 01 90
0020 00 00 00 00 00 00 c0 a8 01 3c 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

wireshark_eth0E029F2.pcapng | Packets: 221 - Displayed: 221 (100.0%) - Dropped: 0 (0.0%) | Profile: Default