CYBER SECURITY LAB

Analysis of LAN-Based Attacks Captured in Splunk

ARP Poisoning:

ARP poisoning (or ARP spoofing) is a type of cyberattack that manipulates the ARP (Address Resolution Protocol) tables in a network. This attack allows an attacker to intercept, modify, or block communication between devices on a local network.

How ARP Works

- ARP maps IP addresses to MAC (Media Access Control) addresses in a network.
- When a device wants to communicate with another device, it sends an ARP request asking, "Who has this IP address?" The device with the matching IP responds with its MAC address.
- This mapping is stored in an ARP cache for future use.

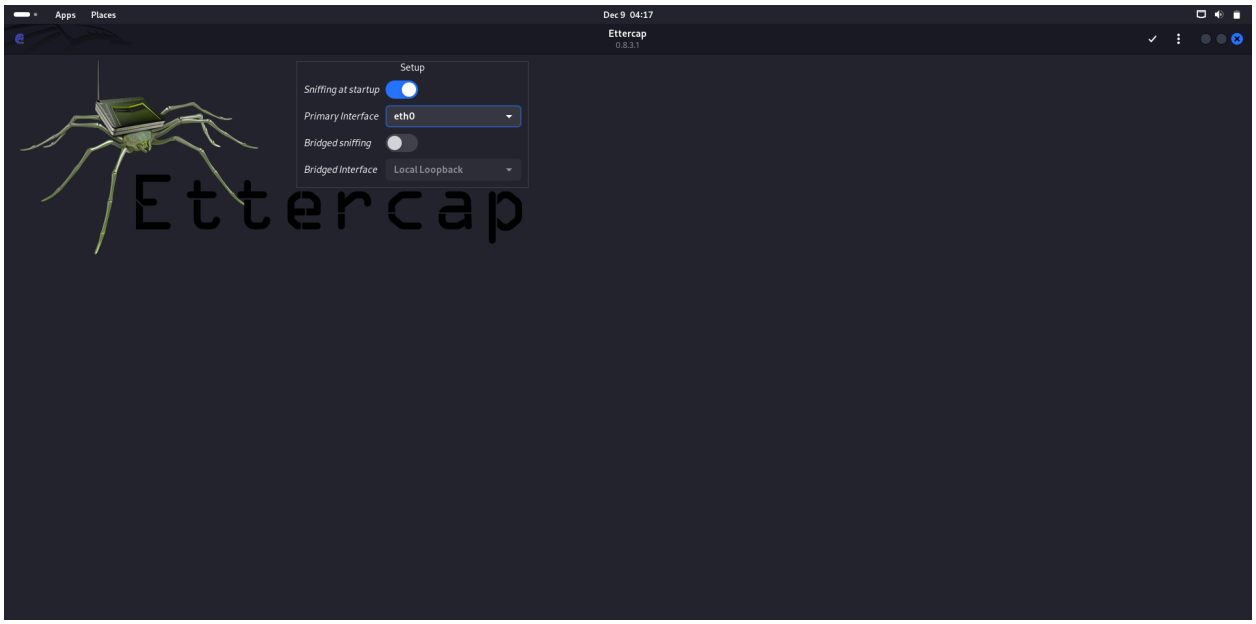
How ARP Spoofing Happens

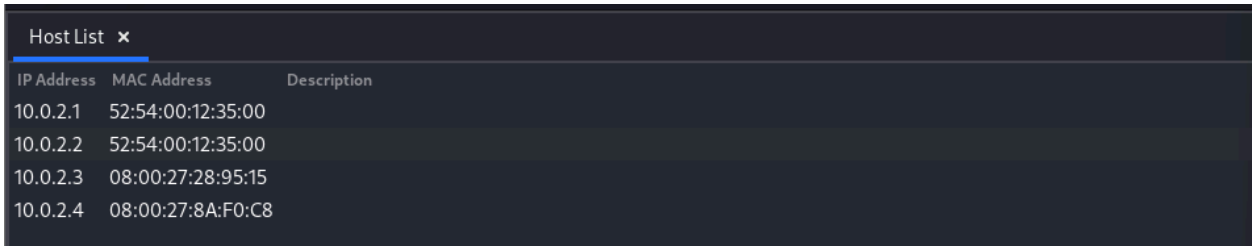
1. The attacker sends falsified ARP messages on the local network.
2. These messages associate the attacker’s MAC address with the IP address of another device (e.g., the router or another host).
3. This causes the victim devices to update their ARP cache with the incorrect mapping, redirecting traffic to the attacker.

Attacker ip address: 10.0.2.5
Victim ip address: 10.0.2.4

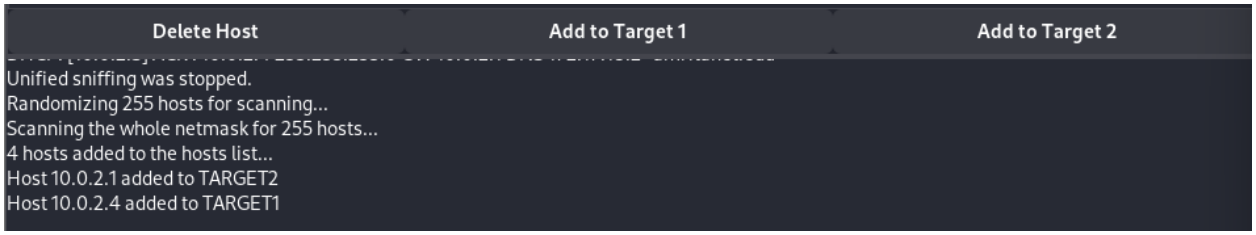
```
varshini@varshini-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::fcc:fb30:ee06:e6c1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:8a:f0:c8  txqueuelen 1000  (Ethernet)
        RX packets 266  bytes 313317 (313.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 145  bytes 15063 (15.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 123  bytes 10647 (10.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 123  bytes 10647 (10.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ettercap interface

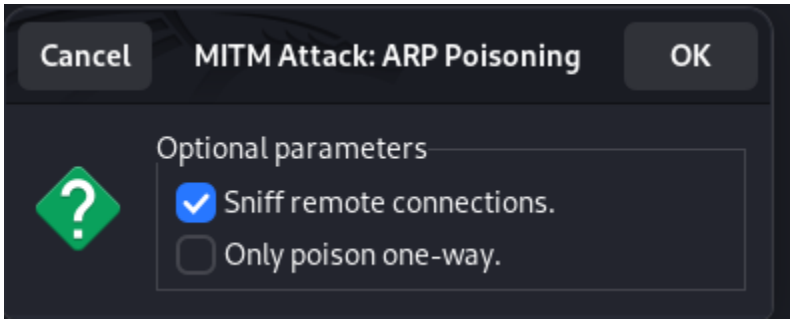




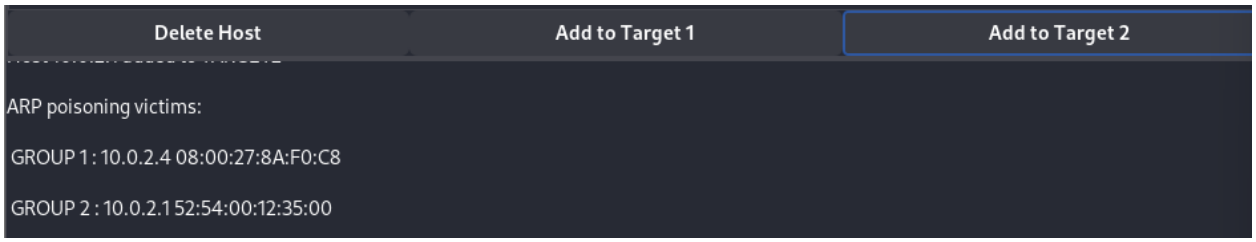
-> Added 10.0.2.4 as Target 1
-> Added 10.0.2.1 as Target 2



-> Select the “sniff remote connections”



-> ARP Poisoning is activated



```
varshini@varshini-VirtualBox:~$ sudo su
[sudo] password for varshini:
root@varshini-VirtualBox:/home/varshini# arp -a >> /var/log/arp.log
root@varshini-VirtualBox:/home/varshini# sudo tcpdump -i enp0s3 arp -w /var/log/
arp_traffic.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
```

10	0.004682006	10.0.2.4	172.17.18.4	DNS	95	Standard query 0xae5c A google.com.amritanet.edu OPT
11	0.005323029	10.0.2.4	172.17.18.2	DNS	115	Standard query 0x7a53 A incoming.telemetry.mozilla.org.an
12	0.990225510	PCSSystemtec_0c:64:…	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
13	1.518608236	10.0.2.4	172.17.18.4	DNS	81	Standard query 0xa607 AAAA google.com OPT
14	1.518608650	10.0.2.4	172.17.18.4	DNS	95	Standard query 0xfa2f AAAA google.com.amritanet.edu OPT
15	1.519719264	10.0.2.4	172.17.18.4	DNS	81	Standard query 0xf86c A google.com OPT
16	1.522174062	10.0.2.4	172.17.18.4	DNS	122	Standard query 0xf525 A firefox.settings.services.mozilla
17	1.522174331	10.0.2.4	172.17.18.4	DNS	108	Standard query 0x38c4 AAAA firefox.settings.services.mozi
18	2.019865921	PCSSystemtec_0c:64:…	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
19	2.266857689	10.0.2.4	172.17.18.4	DNS	122	Standard query 0x86ee AAAA firefox.settings.services.mozi
20	2.266858155	10.0.2.4	172.17.18.4	DNS	108	Standard query 0xf60a A firefox.settings.services.mozilla
21	2.573030794	10.0.2.4	10.11.131.19	TCP	74	48364 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
22	2.639206708	PCSSystemtec_0c:64:…	PCSSystemtec_8a:f0:…	ARP	42	10.0.2.1 is at 08:00:27:0c:64:94
23	2.639370400	PCSSystemtec_0c:64:…	52:54:00:12:35:00	ARP	42	10.0.2.4 is at 08:00:27:0c:64:94 (duplicate use of 10.0.2
24	2.641363679	PCSSystemtec_8a:f0:…	Broadcast	ARP	60	ARP Announcement for 10.0.2.4
25	3.023074043	10.0.2.4	172.17.18.4	DNS	120	Standard query 0xca3c AAAA content-signature-2.cdn.mozill
26	3.037735977	PCSSystemtec_0c:64:…	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
27	3.767850411	10.0.2.4	172.17.18.4	DNS	120	Standard query 0x3e22 A content-signature-2.cdn.mozilla.n
28	3.768116518	10.0.2.4	172.17.18.4	DNS	106	Standard query 0x4e82 AAAA content-signature-2.cdn.mozill
29	3.768526805	10.0.2.4	172.17.18.4	DNS	106	Standard query 0x0cc1 A content-signature-2.cdn.mozilla.n

```
▸ Frame 23: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_0c:64:94 (08:00:27:0c:64:94), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PCSSystemtec_0c:64:94 (08:00:27:0c:64:94)
    Sender IP address: 10.0.2.4
    Target MAC address: 52:54:00:12:35:00 (52:54:00:12:35:00)
    Target IP address: 10.0.2.1
▸ [Duplicate IP address detected for 10.0.2.4 (08:00:27:0c:64:94) - also in use by 08:00:27:8a:f0:c8 (frame 22)]
▸ [Duplicate IP address detected for 10.0.2.1 (52:54:00:12:35:00) - also in use by 08:00:27:0c:64:94 (frame 22)]
```

SSL Stripping:

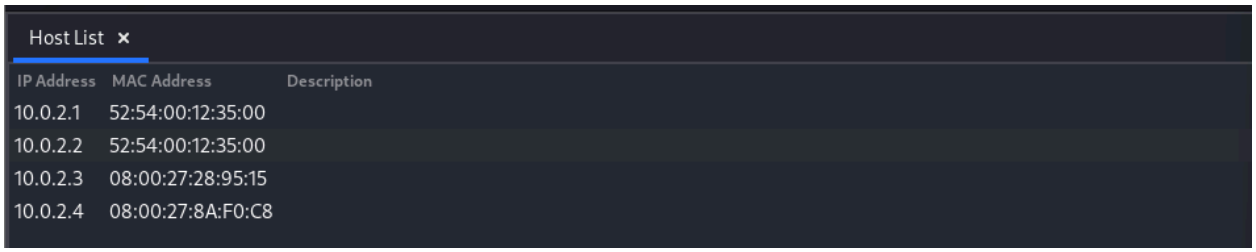
SSL stripping is a type of cyberattack that downgrades a secure HTTPS connection to an unencrypted HTTP connection. The attacker intercepts traffic between a client (e.g., a web browser) and a server, removing the encryption that HTTPS provides, allowing them to read and manipulate the data in plaintext.

How SSL Stripping Works

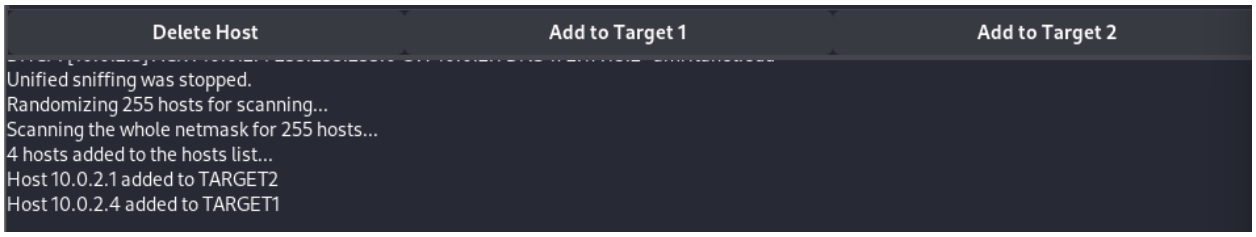
1. Intercept the Traffic: The attacker positions themselves between the client and the server using a Man-in-the-Middle (MITM) attack (e.g., ARP spoofing or DNS spoofing).
2. Downgrade the Connection:

- When a user tries to visit an HTTPS website, the browser first sends an HTTP request (if they don't type `https://` explicitly).
- The server responds with a redirect to HTTPS (`HTTP 301/302` response).
- The attacker intercepts this redirect and replaces it with an HTTP version of the page, preventing the client from upgrading to HTTPS.

3. Proxy the Connection:
   - The attacker establishes an HTTPS connection with the server but maintains an HTTP connection with the client.
   - This makes the client unaware that their communication with the server is not encrypted.



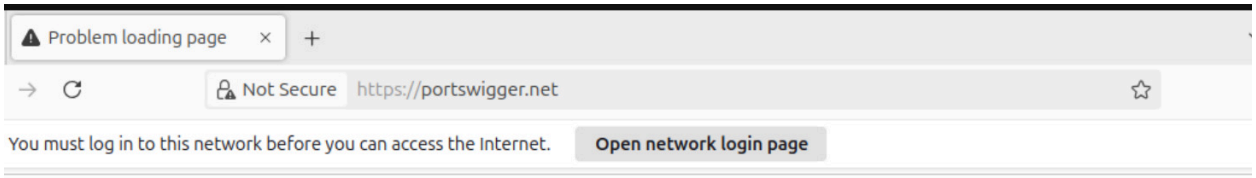
-> Target 1 = 10.0.2.4
-> Target 2 = 10.0.2.1

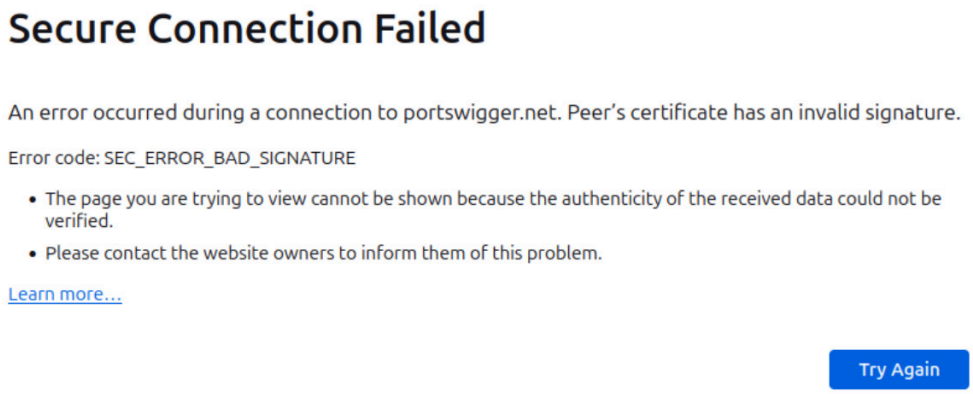


-> Activate the sslstrip

Name	Version	Info
krb5_downgrade	1.0	Downgrades Kerberos V5 security by modifying AS-REQ packets
link_type	1.0	Check the link type (hub/switch)
mdns_spoof	1.0	Sends spoofed mDNS replies
nbns_spoof	1.1	Sends spoof NBNS replies & sends SMB challenges with custom challenge
pptp_chapms1	1.0	PPTP: Forces chapms-v1 from chapms-v2
pptp_clear	1.0	PPTP: Tries to force cleartext tunnel
pptp_pap	1.0	PPTP: Forces PAP authentication
pptp_reneg	1.0	PPTP: Forces tunnel re-negotiation
rand_flood	1.0	Flood the LAN with random MAC addresses
remote_browser	1.2	Sends visited URLs to the browser
reply_arp	1.0	Simple arp responder
repoison_arp	1.0	Repoison after broadcast ARP
scan_poisoner	1.0	Actively search other poisoners
search_promisc	1.2	Search promisc NICs in the LAN
smb_clear	1.0	Tries to force SMB cleartext auth
smb_down	1.0	Tries to force SMB to not use NTLM2 key auth
smurf_attack	1.0	Run a smurf attack against specified hosts
sslstrip	1.2	SSLStrip plugin
stp_mangler	1.0	Become root of a switches spanning tree

```
Activating sslstrip plugin...
SSLStrip plugin: bind 80 on 59263
```





DOS ATTACK:

A DoS (Denial-of-Service) attack is a type of cyberattack where the attacker overwhelms a system, network, or application, making it unavailable to legitimate users. The goal is to disrupt the normal functioning of the targeted resource, often causing downtime or service interruptions.

1. Selection of Target

- The attacker identifies a vulnerable system, application, or network to exploit.

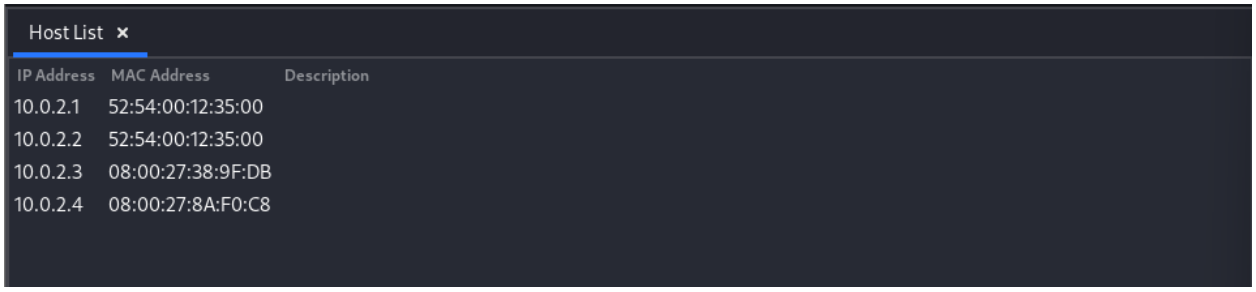
- Common targets include websites, servers, or network infrastructure.

2. Preparation for the Attack

   - Exploiting Vulnerabilities: If specific protocol or application-layer vulnerabilities are targeted (e.g., TCP/IP weaknesses, HTTP flaws), the attacker tailors the attack accordingly.

3. Execution of the Attack

   - The attacker sends a large volume of traffic or resource requests to the target system.
   - Depending on the type of DoS attack, different methods are used to overwhelm the target



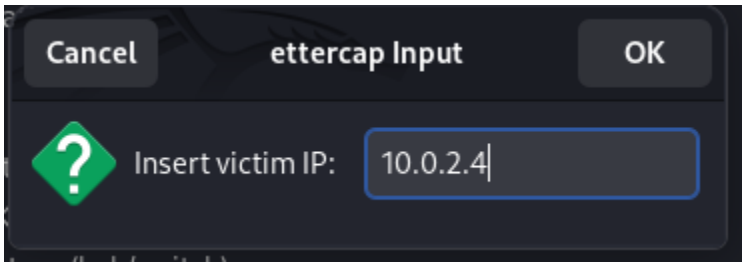
Host List ×

IP Address	MAC Address	Description
10.0.2.1	52:54:00:12:35:00	
10.0.2.2	52:54:00:12:35:00	
10.0.2.3	08:00:27:38:9F:DB	
10.0.2.4	08:00:27:8A:F0:C8	

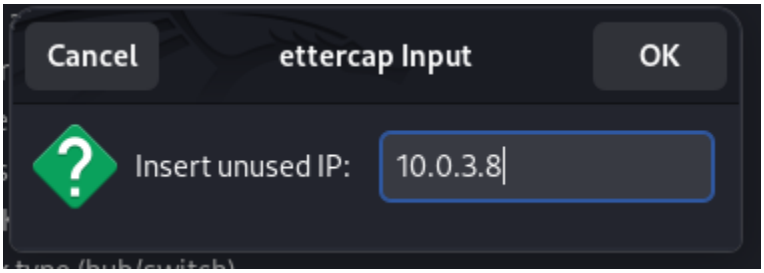
Host List × Plugins ×

	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
	dns_spoof	1.3	Sends spoofed dns replies
*	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin template (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet
	finger	1.6	Fingerprint a remote host
	finger_submit	1.0	Submit a fingerprint to ettercap's website
	fraggle_attack	1.0	Run a fraggle attack against hosts of target one

-> Enter the victim (ubuntu) ip address



-> Enter any unused ip



-> DOS attack is activated

```
Activating dos_attack plugin...
dos_attack: Starting scan against 10.0.2.4 [Fake Host: 10.0.3.8]
dos_attack: Starting attack...
```

ip.addr == 10.0.2.4 && tcp

No.	Time	Source	Destination	Protocol	Length	Info
10	4.554691622	10.0.2.4	10.11.137.69	TCP	74	57792 → 9997 [SYN] Seq=0 W
11	4.724701253	10.0.2.4	10.0.2.5	TCP	74	59604 → 9997 [SYN] Seq=0 W
12	4.724735777	10.0.2.5	10.0.2.4	TCP	54	9997 → 59604 [RST, ACK] Se
13	4.729145026	10.0.2.4	10.11.137.69	TCP	74	58640 → 9994 [SYN] Seq=0 W
31	5.452369160	10.0.2.4	172.17.18.4	TCP	78	50490 → 53 [SYN] Seq=0 Win
34	5.771259693	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
35	6.475776367	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 50490
36	6.795866732	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
37	7.500842942	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 50490
40	7.819811019	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
41	8.525352299	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 50490
42	8.844462364	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
43	9.548615793	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 50490
44	9.869458192	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
51	10.575046175	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 50490
52	11.919270272	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
55	12.622462877	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 50490
58	15.953088343	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
90	24.021245421	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 58640
113	33.818161538	10.0.2.4	10.11.137.69	TCP	74	35532 → 9994 [SYN] Seq=0 W
133	34.841847980	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
134	35.866323803	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
137	36.890682819	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
140	37.919219235	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
141	38.939668297	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
144	40.989118948	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
145	41.583361381	10.0.2.4	172.17.18.4	TCP	78	60150 → 53 [SYN] Seq=0 Win
146	42.590280002	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 60150
149	43.614445812	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 60150
150	44.639158409	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 60150
151	45.023121583	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
152	45.663315819	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 60150
153	46.688033184	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 60150
156	48.737340926	10.0.2.4	172.17.18.4	TCP	74	[TCP Retransmission] 60150
166	53.219409700	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 35532
167	53.671802289	10.0.2.4	10.11.137.69	TCP	74	43596 → 9997 [SYN] Seq=0 W
190	54.692196864	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 43596
191	55.717238477	10.0.2.4	10.11.137.69	TCP	74	[TCP Retransmission] 43596