

CONFIGURAZIONE DI UNA POLICY SUL FIREWALL WINDOWS + PACKET CAPTURE CON WIRESHARK

- 1) CONFIGURARE POLICY PER PERMETTERE IL PING DA MACCHINE LINUX A MACCHINA WINDOWS 7 NEL NOSTRO LABORATORIO VM (WINDOWS FIREWALL)

#KALI LINUX IP: 192.168.50.100

#METASPLOITABLE IP: 192.168.50.101

#WINDOWS 7 IP: 192.168.50.102

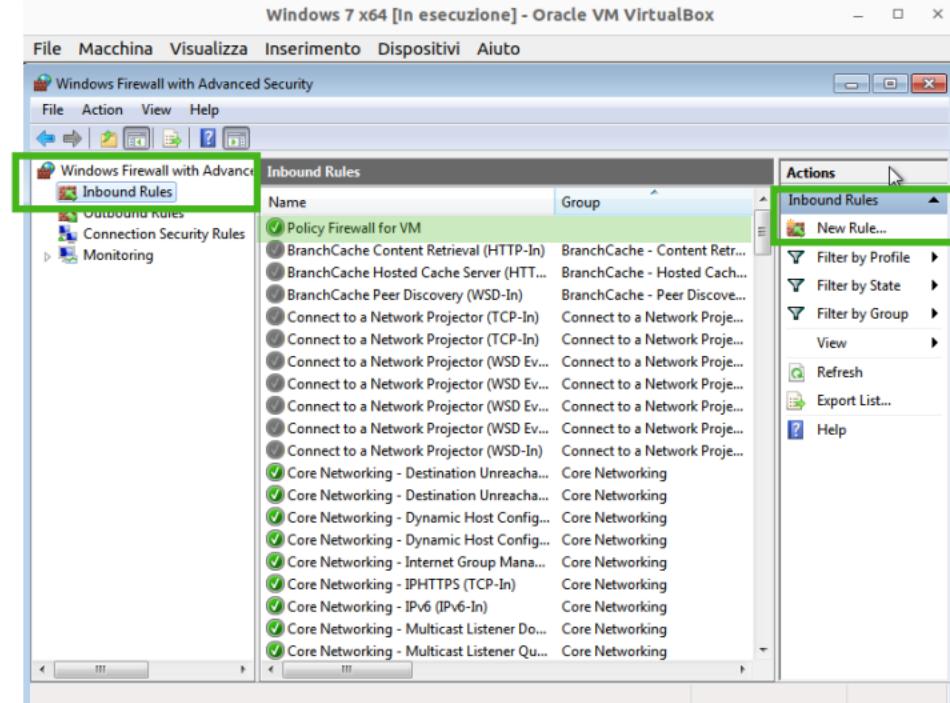
- 2) UTILIZZO DELL'UTILITY InetSim PER L'EMULAZIONE DI SERVIZI INTERNET

- 3) CATTURA DI PACCHETTI CON WIRESHARK (DIFFERENZA TRA HTTP e HTTPS)

#FIREWALL POLICY

SI DEVONO MODIFICARE LE IMPOSTAZIONI AVANZATE DI WINDOWS FIREWALL PER PERMETTERE IL TRAFFICO DA UN DEVICE DELLA STESSA RETE, ALTRIMENTI BLOCCA IL PING

IMPOSTAZIONI AVANZATE -> INBOUND RULES -> NEW



CAMPPI NECESSARI:

#PROTOCOLS AND PORTS SETTANDO IL CAMPO "PROTOCOL TYPE" SU ICMPv4

#SCOPE SETTANDO GLI IP A CUI CONCEDIAMO DI INVIARE PING

#GENERAL (FACOLTATIVO) INSERENDO UN RIFERIMENTO AL PROTOCOLLO PER DISTINGUERLO DA ALTRI

The image displays three windows for configuring a new inbound rule:

- General Tab:** Shows 'Protocol type: ICMPv4' and 'Protocol number: 1'. It also includes sections for Local port, Remote port, and Internet Control Message Protocol (ICMP) settings.
- Programs and Services Tab:** Shows 'Local IP address' set to 'Any IP address' and 'Remote IP address' set to 'Any IP address'. It includes 'Add...', 'Edit...', and 'Remove...' buttons.
- Advanced Tab:** Shows 'Name: Policy Firewall for VM', 'Description: permesso IPv4 x Metasploitable & Kali', and 'Enabled' checked. It includes 'Action' options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'.

PING VS WINDOWS 7 RICEVUTO DA #METASPLOITABLE E #KALI

```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
No mail.
msfadmin@metasploitable:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=5.87 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.59 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.40 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.32 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.21 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.55 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=1.21 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=1.16 ms
64 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=1.24 ms
64 bytes from 192.168.50.102: icmp_seq=10 ttl=128 time=1.42 ms
64 bytes from 192.168.50.102: icmp_seq=11 ttl=128 time=1.29 ms
64 bytes from 192.168.50.102: icmp_seq=12 ttl=128 time=1.14 ms
64 bytes from 192.168.50.102: icmp_seq=13 ttl=128 time=1.37 ms
64 bytes from 192.168.50.102: icmp_seq=14 ttl=128 time=1.32 ms
64 bytes from 192.168.50.102: icmp_seq=15 ttl=128 time=1.23 ms
64 bytes from 192.168.50.102: icmp_seq=16 ttl=128 time=1.38 ms
64 bytes from 192.168.50.102: icmp_seq=17 ttl=128 time=0.330 ms
--- 192.168.50.102 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16007ms
rtt min/avg/max/mdev = 0.330/1.535/5.875/1.117 ms
msfadmin@metasploitable:~$
```

```
(django㉿kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.662 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.62 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.449 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.659 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.55 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.16 ms
^C
--- 192.168.50.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5071ms
rtt min/avg/max/mdev = 0.449/1.017/1.620/0.456 ms
```

#INETSIM

InetSim È UN SOFTWARE CHE SIMULA LE FEATURES DELLA RETE/SERVIZI INTERNET, DA CONFIGURARE ALL'INTERNO DELLA VM DI KALI LINUX (CHE RICORDIAMO ESSERE IL NOSTRO OS ATTACCANTE). ALL'INTERNO DI "NANO" (EDITOR DI TESTO CHE CONSENTE DI MODIFICARE FILE) COMMENTEREMO CON "#" DAVANTI I SERVIZI CHE NON UTILIZZEREMO LASCIANDO INTATTI HTTP/HTTPS. FINGEREMO SUCESSIVAMENTE DI ACCEDERE AD UN SITO FAKE SU LOCAL HOST (IP - 127.0.0.1 - detto LOOPBACK) SIMULANDO UNA CONNESSIONE INTERNET PROTETTA E NON PROTETTA.

PASSAGGI DI CONFIGURAZIONE DI INETSIM:

- cd /etc/inetsim (dir)
- ls (file presenti nella dir)
- sudo nano inetsim.conf
- # per commentare i servizi da "spegnere" (tranne http/https)
- nella riga "service_bind_address" inseriamo il local host e sovrascriviamo con ^O
- sudo inetsim (per avviare la simulazione)

```
django@kali: /etc/inetsim
File Actions Edit View Help
GNU nano 7.2          inetsim.conf
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
#start_service dns
#start_service http
#start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
```

IP DI ACCESSO AL SITO INTERNET SIMULATO:

```
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
#service_bind_address 127.0.0.1
```

FILE FAKE ACCESSIBILI NELLA SIMULAZIONE:

```
# Syntax: https_fakefile <extension> <filename> <mime-type>
#
# Default: none
#
https_fakefile txt sample.txt      text/plain
https_fakefile htm sample.html     text/html
https_fakefile html sample.html    text/html
https_fakefile php sample.php     text/html
https_fakefile gif sample.gif     image/gif
https_fakefile jpg sample.jpg     image/jpeg
https_fakefile jpeg sample.jpg    image/jpeg
https_fakefile png sample.png    image/png
https_fakefile bmp sample.bmp    image/x-ms-bmp
https_fakefile ico favicon.ico   image/x-icon
https_fakefile exe sample_gui.exe x-msdos-program
https_fakefile com sample_gui.exe x-msdos-program
```

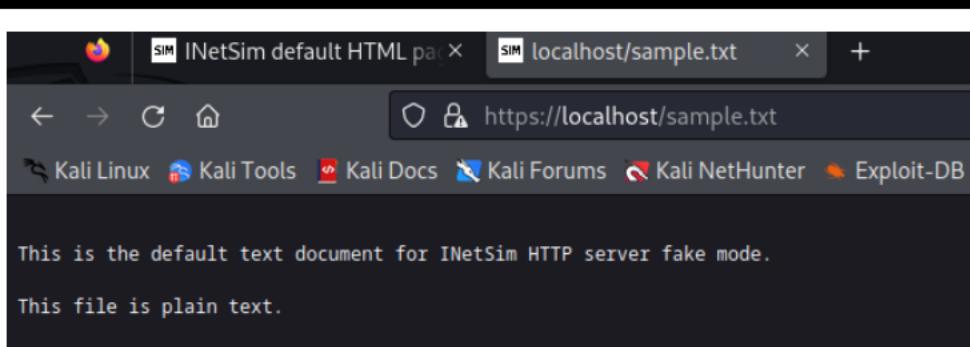
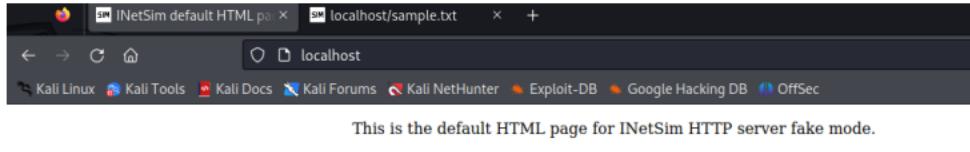
SIMULAZIONE AVVIATA CORRETTAMENTE:

```
└─(django㉿kali)-[~]
$ cd /etc/inetsim

└─(django㉿kali)-[/etc/inetsim]
$ sudo nano inetsim.conf

└─(django㉿kali)-[/etc/inetsim]
$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:          /var/log/inetsim/
Using data directory:         /var/lib/inetsim/
Using report directory:       /var/log/inetsim/report/
Using configuration file:    /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
≡≡ INetSim main process started (PID 5337) ≡≡
Session ID:      5337
Listening on:    127.0.0.1
Real Date/Time: 2023-11-13 10:00:43
Fake Date/Time: 2023-11-13 10:00:43 (Delta: 0 seconds)
Forking services ...
 * http_80_tcp - started (PID 5347)
 * https_443_tcp - started (PID 5348)
done.
Simulation running.
```

FAKE SITO INTERNET DA BROWSER + FAKE FILE .TXT DA WEB:



#WIRESHARK

SI UTILIZZA PER SNIFFARE AKA CATTURARE ED ANALIZZARE I PACCHETTI IN TRANSITO SU UNA DETERMINATA RETE. ATTRAVERSO LA SELEZIONE DI UNA SCHEDA DI RETE NE VIENE CATTURATO IL TRAFFICO CHE SI PUÒ SUCESSIVAMENTE FILTRARE PER VARIE NECESSITÀ/INTERESSE (IP / DNS / PORTA, ECC). eth0 - stessa rete (LE NOSTRA VM) / Loopback

Capture

...using this filter:  Enter a capture filter ...

```
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
```



MM

MM

HTTP://LOCALHOST: PORTA 80 – CONNESSIONE NON PROTETTA

RICHIESTA IN LOOPBACK SULLA PORTA 80 (HTTP) DA “GET” A “OK” DEL SERVER CON SEQUENZA DI THREE-WAY-HANDSHAKE. STRINGHE DA SYN/SYN ACK fino a FIN/ACK ACK.

53 18.885374243	127.0.0.1	127.0.0.1	TCP	74 49254 - 88 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM Tsvl=652981350 Tsec=652981350
54 18.885384994	127.0.0.1	127.0.0.1	TCP	74 49254 - 90 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM Tsvl=652981350
55 18.885394732	127.0.0.1	127.0.0.1	TCP	66 49254 - 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0 Tsvl=652981350 Tsec=652981350
56 19.051179334	127.0.0.1	127.0.0.1	HTTP	567 GET /sample.txt HTTP/1.1
57 19.051191548	127.0.0.1	127.0.0.1	TCP	66 88 - 49254 [ACK] Seq=1 Ack=442 Win=65192 Len=0 Tsvl=652981516 Tsec=652981516
58 19.156503595	127.0.0.1	127.0.0.1	TCP	216 88 - 49254 [PSH, ACK] Seq=1 Ack=442 Win=65536 Len=150 Tsvl=652981626 Tsec=652981626
59 19.156503793	127.0.0.1	127.0.0.1	TCP	66 49254 - 88 [ACK] Seq=1 Ack=451 Win=65486 Len=0 Tsvl=652981621 Tsec=652981616
60 19.205627781	127.0.0.1	127.0.0.1	TCP	66 49254 - 88 [ACK] Seq=1 Ack=452 Win=65486 Len=0 Tsvl=652981620 Tsec=652981615
61 19.205627568	127.0.0.1	127.0.0.1	HTTP	163 HTTP/1.1 200 OK [text/plain]
62 19.205627932	127.0.0.1	127.0.0.1	TCP	66 49254 - 88 [FIN, ACK] Seq=442 Ack=248 Win=65536 Len=0 Tsvl=652981671 Tsec=652981671
63 19.216826626	127.0.0.1	127.0.0.1	TCP	66 88 - 49254 [ACK] Seq=248 Ack=443 Win=65536 Len=0 Tsvl=652981682 Tsec=652981682
64 19.216847193	127.0.0.1	127.0.0.1	TCP	66 49254 - 88 [ACK] Seq=443 Ack=249 Win=65536 Len=0 Tsvl=652981682 Tsec=652981682

PACCHETTO IN TRANSITO “TEXT/PLAIN”.

HTTPS://LOCALHOST: PORTA 443 – CONNESSIONE PROTETTA

RICHIESTA IN LOOPBACK SULLA PORTA 443 (HTTPS) DA “Client Hello” A “Server Hello” CON SEQUENZA DI THREE-WAY-HANDSHAKE CON CIFRATURA PIÙ COMPLESSA.

No.	Time	Source	Destination	Protocol	Length Info
24 18.8853807901	127.0.0.1	127.0.0.1	TCP	56 43134 - 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM Tsvl=1548801392 Tsec=1548801392	
24 18.8853824812	127.0.0.1	127.0.0.1	TCP	74 443 - 49254 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM Tsvl=1548801394	
25 18.8853898373	127.0.0.1	127.0.0.1	TCP	66 43134 - 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 Tsvl=1548801392 Tsec=1548801392	
26 18.433975152	127.0.0.1	127.0.0.1	TLSv1.3	593 Client Hello	
27 18.439985956	127.0.0.1	127.0.0.1	TCP	66 443 - 34134 [ACK] Seq=1 Ack=518 Win=65024 Len=0 Tsvl=1548801398 Tsec=1548801398	
28 18.440000000	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data, Application Data, Application Data	
29 18.4426220487	127.0.0.1	127.0.0.1	TCP	66 443 - 34134 [ACK] Seq=1 Ack=422 Win=64384 Len=0 Tsvl=1548801500 Tsec=1548801500	
30 18.4426220487	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data, Application Data, Application Data	
31 18.4426220487	127.0.0.1	127.0.0.1	TCP	66 443 - 34134 [ACK] Seq=1 Ack=422 Win=64384 Len=0 Tsvl=1548801500 Tsec=1548801500	
32 18.429485985	127.0.0.1	127.0.0.1	TLSv1.3	321 Application Data	
33 18.429485985	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548801502 Tsec=1548801502	
34 18.429485985	127.0.0.1	127.0.0.1	TLSv1.3	322 Application Data	
35 18.427053912	127.0.0.1	127.0.0.1	TCP	66 43134 - 443 [ACK] Seq=598 Ack=1677 Win=65536 Len=0 Tsvl=1548801530 Tsec=1548801530	
36 18.376453518	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
37 18.376453518	127.0.0.1	127.0.0.1	TCP	66 43134 - 443 [FIN, ACK] Seq=622 Ack=1932 Win=65536 Len=0 Tsvl=1548801530 Tsec=1548801530	
38 17.630551016	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
39 17.630551016	127.0.0.1	127.0.0.1	TCP	66 43134 - 443 [FIN, ACK] Seq=622 Ack=1932 Win=65536 Len=0 Tsvl=1548801530 Tsec=1548801530	
40 17.644959774	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
41 17.644959774	127.0.0.1	127.0.0.1	TCP	66 43134 - 443 [FIN, ACK] Seq=622 Win=65536 Len=0 Tsvl=1548801530 Tsec=1548801530	
42 18.7025557726	127.0.0.1	127.0.0.1	TCP	54 43130 - 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM Tsvl=1548800666 Tsec=1548800666	
43 18.7025557726	127.0.0.1	127.0.0.1	TCP	74 443 - 34150 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM Tsvl=1548800666	
44 18.702606232	127.0.0.1	127.0.0.1	TCP	66 34150 - 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 Tsvl=1548800666 Tsec=1548800666	
45 18.702559772	127.0.0.1	127.0.0.1	TLSv1.3	687 Client Hello	
46 18.704662855	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548800666 Tsec=1548800666	
47 18.704662855	127.0.0.1	127.0.0.1	TLSv1.3	148 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data	
48 18.704662855	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548800666 Tsec=1548800666	
49 18.704662855	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data	
50 18.704662855	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548800666 Tsec=1548800666	
51 18.704662855	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data	
52 18.704662855	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548800666 Tsec=1548800666	
53 18.704662855	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data	
54 18.704662855	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548800666 Tsec=1548800666	
55 18.704662855	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data	
56 19.112345044	127.0.0.1	127.0.0.1	TCP	66 43178 - 443 [ACK] Seq=1 Ack=598 Win=64896 Len=0 Tsvl=1548800765 Tsec=1548800765	
57 19.112345044	127.0.0.1	127.0.0.1	TLSv1.3	583 Client Hello	
58 19.112345044	127.0.0.1	127.0.0.1	TCP	66 443 - 34166 [ACK] Seq=1 Ack=598 Win=65483 Len=0 Tsvl=1548800766 Tsec=1548800766	
59 18.3912332276	127.0.0.1	127.0.0.1	TCP	74 443 - 34178 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 Tsvl=1548800782 Tsec=1548800782	
60 18.3912332276	127.0.0.1	127.0.0.1	TLSv1.3	687 Client Hello	
61 18.3912332276	127.0.0.1	127.0.0.1	TCP	66 43178 - 443 [ACK] Seq=1 Ack=598 Win=65536 Len=0 Tsvl=1548800782 Tsec=1548800782	
62 18.2622027896	127.0.0.1	127.0.0.1	TCP	66 443 - 34150 [ACK] Seq=1422 Ack=1677 Win=65536 Len=0 Tsvl=1548800785 Tsec=1548800785	
63 19.203535151	127.0.0.1	127.0.0.1	TLSv1.3	321 Application Data	
64 18.434953440	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1422 Ack=1677 Win=65536 Len=0 Tsvl=1548800785 Tsec=1548800785	
65 18.390530316	127.0.0.1	127.0.0.1	TLSv1.3	321 Application Data	
66 18.390530316	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1422 Ack=1677 Win=65536 Len=0 Tsvl=1548800785 Tsec=1548800785	
67 20.352607795	127.0.0.1	127.0.0.1	TLSv1.3	1487 Client Hello, Change Cipher Spec, Application Data, Application Data, Application Data	
68 20.352624565	127.0.0.1	127.0.0.1	TCP	66 34160 - 443 [ACK] Seq=022 Ack=422 Win=64384 Len=0 Tsvl=1548800932 Tsec=1548800932	
69 20.352624565	127.0.0.1	127.0.0.1	TLSv1.3	1487 Client Hello, Change Cipher Spec, Application Data, Application Data, Application Data	
70 20.352624565	127.0.0.1	127.0.0.1	TCP	66 34160 - 443 [ACK] Seq=022 Ack=422 Win=64384 Len=0 Tsvl=1548800932 Tsec=1548800932	
71 20.352624565	127.0.0.1	127.0.0.1	TLSv1.3	1487 Client Hello, Change Cipher Spec, Application Data, Application Data, Application Data	
72 20.373879707	127.0.0.1	127.0.0.1	TCP	66 34178 - 443 [ACK] Seq=518 Ack=422 Win=64384 Len=0 Tsvl=1548800933 Tsec=1548800933	
73 20.373879707	127.0.0.1	127.0.0.1	TLSv1.3	583 Client Hello	
74 20.373879707	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=518 Ack=422 Win=64384 Len=0 Tsvl=1548800933 Tsec=1548800933	
75 20.373879707	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data, Application Data, Application Data	
76 20.373879707	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=518 Ack=422 Win=64384 Len=0 Tsvl=1548800933 Tsec=1548800933	
77 20.373879707	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data, Application Data, Application Data	
78 20.373879707	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=518 Ack=422 Win=64384 Len=0 Tsvl=1548800934 Tsec=1548800934	
79 20.373879707	127.0.0.1	127.0.0.1	TLSv1.3	148 Change Cipher Spec, Application Data, Application Data, Application Data	
80 20.373879707	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=518 Ack=422 Win=64384 Len=0 Tsvl=1548800934 Tsec=1548800934	
81 20.415588516	127.0.0.1	127.0.0.1	TLSv1.3	321 Application Data	
82 20.415588516	127.0.0.1	127.0.0.1	TCP	66 44178 - 443 [ACK] Seq=598 Ack=1932 Win=65496 Len=0 Tsvl=1548800934 Tsec=1548800934	
83 20.415588516	127.0.0.1	127.0.0.1	TLSv1.3	529 Application Data	
84 20.415588516	127.0.0.1	127.0.0.1	TCP	66 44178 - 443 [ACK] Seq=598 Ack=1932 Win=65536 Len=0 Tsvl=1548800934 Tsec=1548800934	
85 20.415588516	127.0.0.1	127.0.0.1	TLSv1.3	321 Application Data	
86 20.415588516	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=598 Ack=1932 Win=65536 Len=0 Tsvl=1548800934 Tsec=1548800934	
87 20.415588516	127.0.0.1	127.0.0.1	TLSv1.3	148 Application Data	
88 20.415588516	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=598 Ack=1932 Win=65496 Len=0 Tsvl=1548800934 Tsec=1548800934	
89 20.415588516	127.0.0.1	127.0.0.1	TLSv1.3	148 Application Data	
90 20.415588516	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=598 Ack=1932 Win=65496 Len=0 Tsvl=1548800934 Tsec=1548800934	
91 20.415588516	127.0.0.1	127.0.0.1	TLSv1.3	148 Application Data	
92 22.088471593	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [FIN, ACK] Seq=1189 Ack=2224 Win=65536 Len=0 Tsvl=1548801935 Tsec=1548801935	
93 22.088471593	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [FIN, ACK] Seq=1189 Ack=2224 Win=65536 Len=0 Tsvl=1548801935 Tsec=1548801935	
94 23.1030612162	127.0.0.1	127.0.0.1	TCP	54 34150 - 443 [RST] Seq=1190 Win=0 Len=0	
95 23.1030612162	127.0.0.1	127.0.0.1	TLSv1.3	462 Application Data	
96 23.1030612162	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
97 23.1030612162	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
98 23.1030612162	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1192 Ack=1132 Win=65536 Len=0 Tsvl=1548801934 Tsec=1548801934	
99 23.227257392	127.0.0.1	127.0.0.1	TCP	66 7443 - 34106 [ACK] Seq=1192 Ack=1132 Win=65152 Len=0 Tsvl=15488012185 Tsec=15488012185	
100 23.227257392	127.0.0.1	127.0.0.1	TLSv1.3	242 Application Data	
101 23.227257392	127.0.0.1	127.0.0.1	TCP	66 34160 - 443 [RST] Seq=1123 Win=0 Len=0	
102 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
103 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1123 Ack=1132 Win=65536 Len=0 Tsvl=15488012185 Tsec=15488012185	
104 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
105 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1123 Ack=1132 Win=65536 Len=0 Tsvl=15488012185 Tsec=15488012185	
106 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
107 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1123 Ack=1132 Win=65536 Len=0 Tsvl=15488012185 Tsec=15488012185	
108 23.229221816	127.0.0.1	127.0.0.1	TCP	66 34170 - 443 [RST] Seq=1123 Win=0 Len=0	
109 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
110 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1123 Ack=1132 Win=65536 Len=0 Tsvl=15488012185 Tsec=15488012185	
111 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
112 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1123 Ack=1132 Win=65536 Len=0 Tsvl=15488012185 Tsec=15488012185	
113 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
114 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=1123 Ack=1132 Win=65536 Len=0 Tsvl=15488012185 Tsec=15488012185	
115 23.229221816	127.0.0.1	127.0.0.1	TLSv1.3	98 Application Data	
116 23.229221816	127.0.0.1	127.0.0.1	TCP	66 43190 - 443 [ACK] Seq=112	