

# W9D4 Esercitazione

*L'esercitazione di oggi ci richiedeva di creare una policy di firewall tramite PfSense che impedisse il traffico http tra Kali e Metasploitable.*

*Iniziamo con il configurare un'interfaccia alla quale Metasploitable si possa connettere:*

**General Configuration**

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN2 <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>
Speed and Duplex	Default (no preference, typically autoselect) <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small>

**Static IPv4 Configuration**

IPv4 Address	192.168.50.1	/ 24
IPv4 Upstream gateway	None	<a href="#">+ Add a new gateway</a>

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).  
Gateways can be managed by [clicking here](#).

*attiviamo su di esso il servizio di DHCP:*

**LAN LAN2**

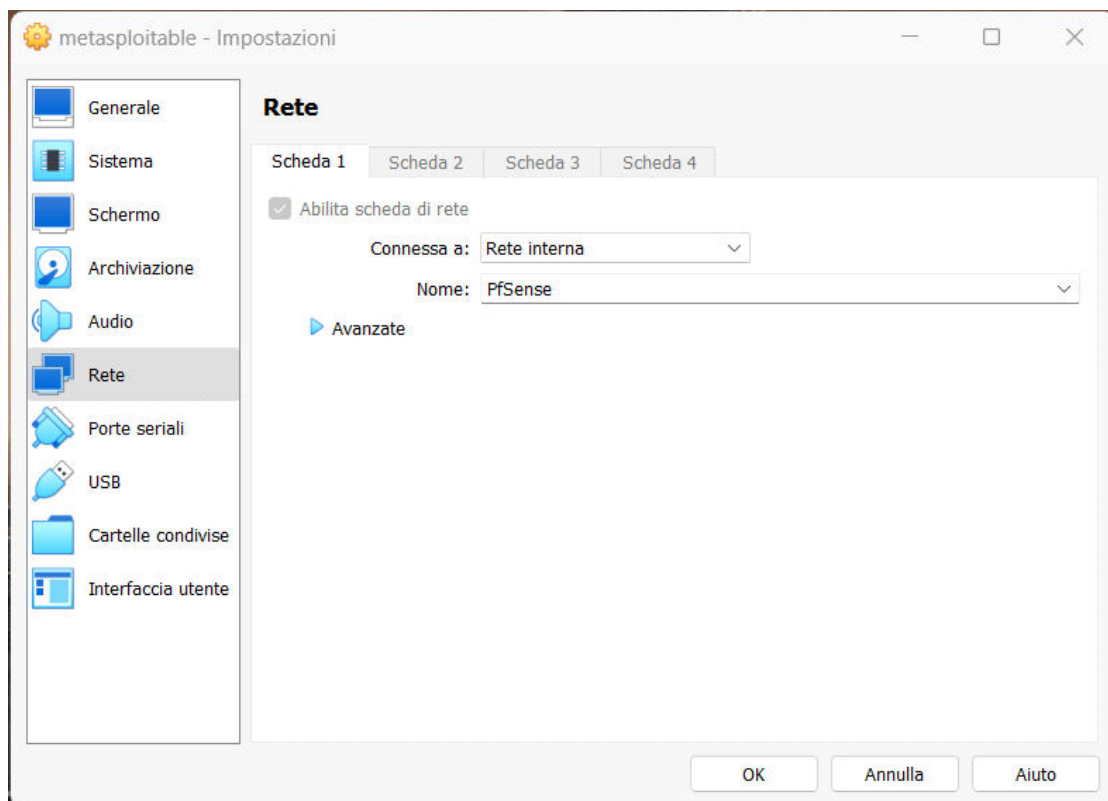
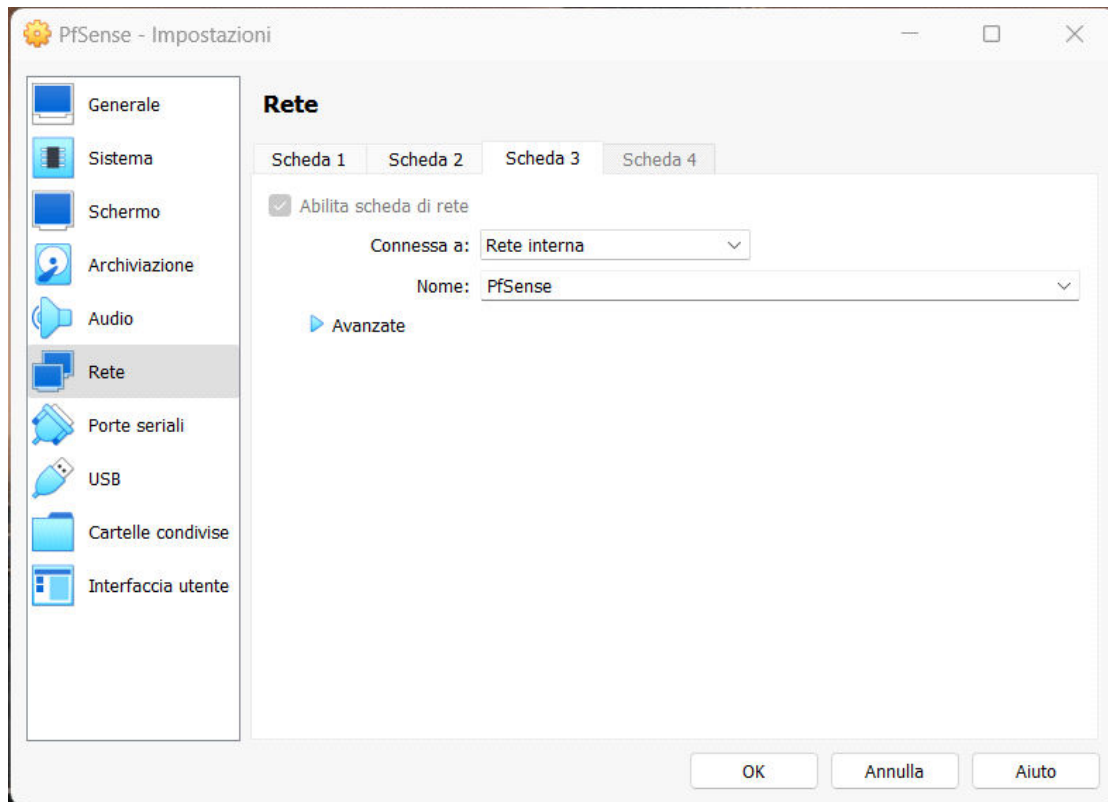
**General DHCP Options**

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	Allow all clients <small>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</small>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>

**Primary Address Pool**

Subnet	192.168.50.0/24
Subnet Range	192.168.50.1 - 192.168.50.254
Address Pool Range	From 192.168.50.1 To 192.168.50.254 <small>The specified range for this pool must not be within the range configured on any other address pool for this interface.</small>
Additional Pools	<a href="#">+ Add Address Pool</a> <small>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here:</small>

*Adesso dalle impostazioni di VM Ware connettiamo Metasploitable a PfSense tramite una rete interna che chiamiamo pfsense:*

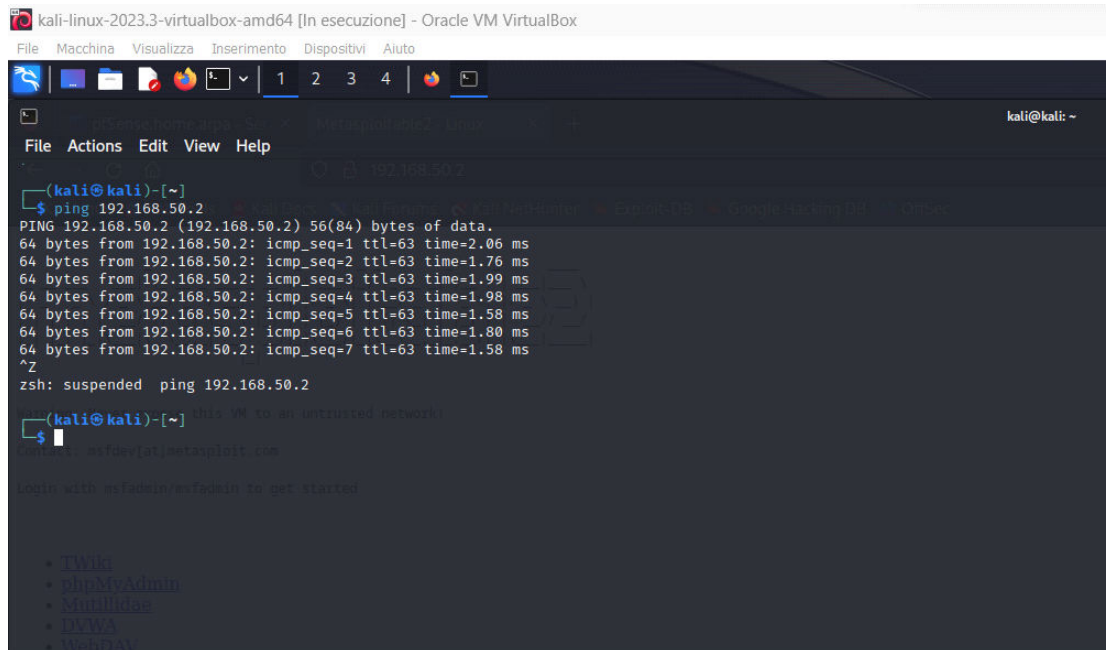


*Una volta che meta è connesso possiamo controllare l'ip che PfSense gli ha assegnato*

```
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:5b:c1:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.2/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe5b:c11a/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

*Nel nostro caso 192.168.50.2*

*In seguito eseguiamo un test di ping e di connessione I servizio di DVWA dalla macchina di kali:*



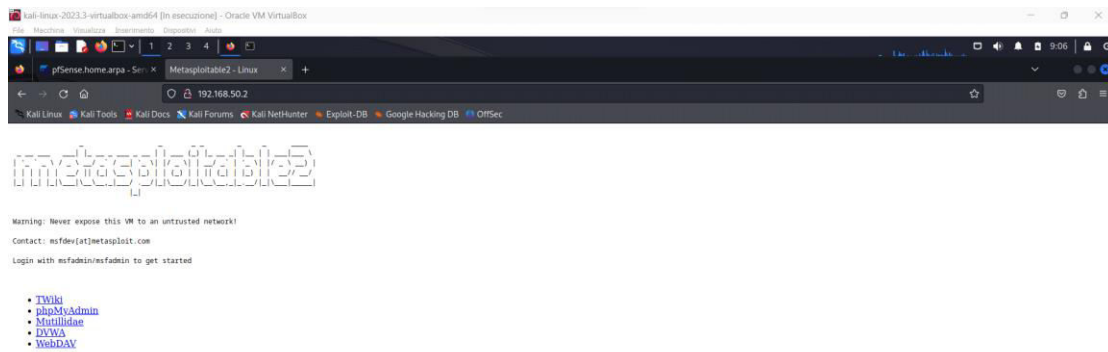
The screenshot shows a Kali Linux terminal window titled "kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal output shows a successful ping to 192.168.50.2 with 7 packets received. Below the ping test, a list of web services is displayed, including TWiki, phpMyAdmin, Metasploit, DVWA, and WordPress.

```
(kali@kali)-[~]
$ ping 192.168.50.2
PING 192.168.50.2 (192.168.50.2) 56(84) bytes of data:
64 bytes from 192.168.50.2: icmp_seq=1 ttl=63 time=2.06 ms
64 bytes from 192.168.50.2: icmp_seq=2 ttl=63 time=1.76 ms
64 bytes from 192.168.50.2: icmp_seq=3 ttl=63 time=1.99 ms
64 bytes from 192.168.50.2: icmp_seq=4 ttl=63 time=1.98 ms
64 bytes from 192.168.50.2: icmp_seq=5 ttl=63 time=1.58 ms
64 bytes from 192.168.50.2: icmp_seq=6 ttl=63 time=1.80 ms
64 bytes from 192.168.50.2: icmp_seq=7 ttl=63 time=1.58 ms
^Z
zsh: suspended ping 192.168.50.2

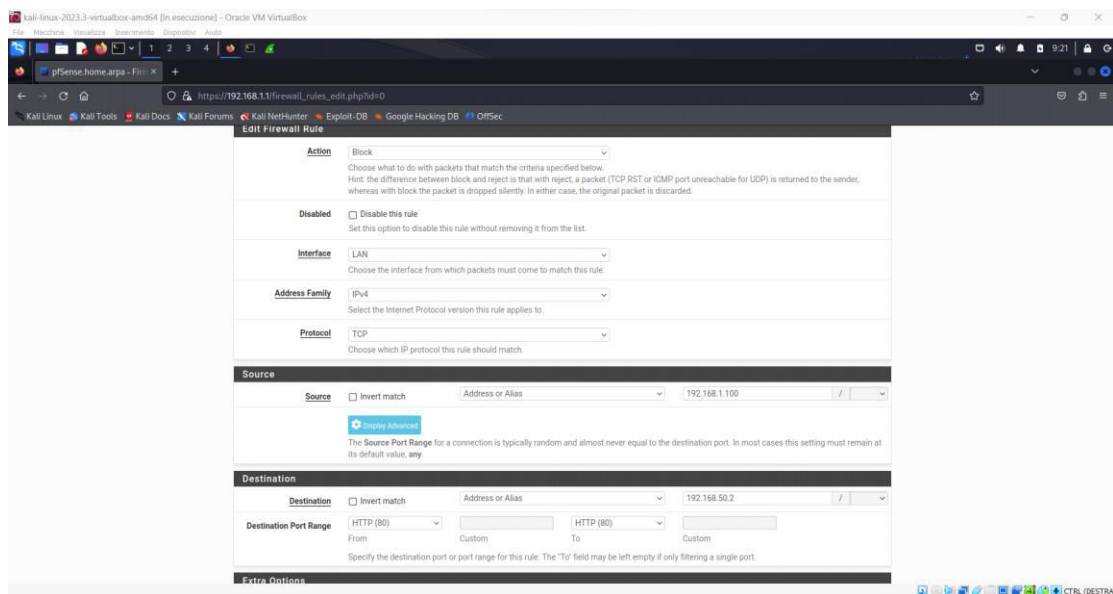
(kali@kali)-[~] this VM is an untrusted network!
$ cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 64 | xargs echo | sh
msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

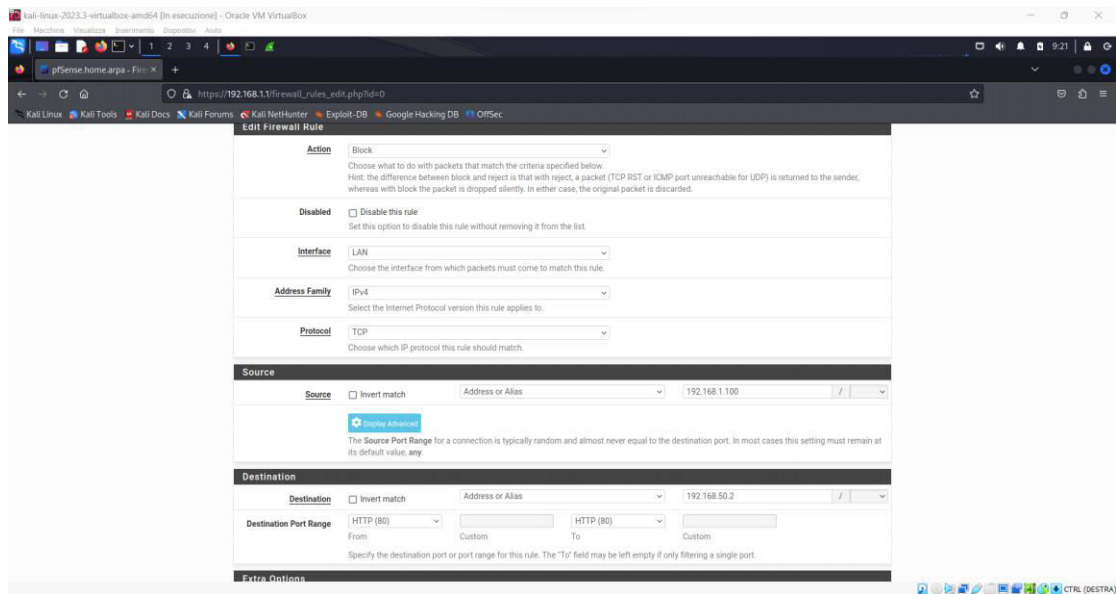
• TWiki
• phpMyAdmin
• Metasploit
• DVWA
• WordPress
```



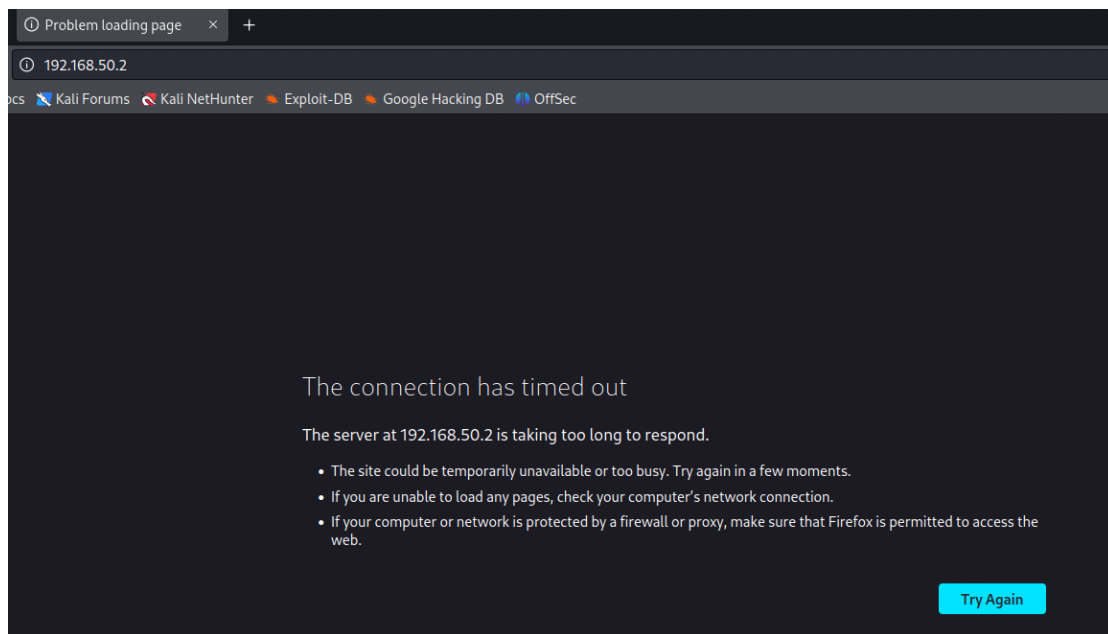
***Adesso possiamo proseguire creando e applicando la regola di firewall che bloccherà i tentativi di connessione alla porta 80 ovvero quella del servizio HTTP***



***dopo che verrà salvata dovremmo vederla nella lista delle regole di firewall presenti:***



*quindi se eseguiamo il test possiamo notare che cercando di connetterci alla DVWA di Metasploitable non ci sarà possibile*



*E lo possiamo notare anche in dettaglio facendo un'analisi con wireshark:*

Kali Linux 2023.3 virtualbox-ami64 [In esecuzione] - Oracle VM VirtualBox

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capturing from eth0

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
148	87.741463252	192.168.1.100	34.120.115.102	TLShv1.3	93	Application Data
149	87.742068163	34.120.115.102	192.168.1.100	TCP	60	443 → 50324 [ACK] Seq=1228 Win=55520 Len=0
142	89.141529168	192.168.1.100	192.168.50.2	TCP	74	50556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260755780 TSecr=0 WS=128
143	89.391849177	192.168.1.100	192.168.50.2	TCP	74	50610 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260756031 TSecr=0 WS=128
144	90.171517962	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50596 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260756030 TSecr=0 WS=128
145	90.390636334	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50610 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260757835 TSecr=0 WS=128
146	92.107057288	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50596 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260758826 TSecr=0 WS=128
147	92.418237469	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50610 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260759821 TSecr=0 WS=128
148	92.455635551	PcsCompu_cb:7e:f5	PcsCompu_b0:24:60	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
149	92.868415533	PcsCompu_b0:24:60	PcsCompu_cb:7e:f5	ARP	60	192.168.1.1 is at 08:00:27:b0:24:60
150	94.390494388	192.168.1.100	192.168.50.2	TCP	74	50572 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260761035 TSecr=0 WS=128
151	95.420995432	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50572 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260762986 TSecr=0 WS=128
152	96.444339529	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50596 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260763083 TSecr=0 WS=128
153	97.442897007	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50572 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260764061 TSecr=0 WS=128
154	98.562886062	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50572 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260766282 TSecr=0 WS=128
155	98.648956399	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50596 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260771280 TSecr=0 WS=128
156	100.756364566	192.168.1.100	192.168.50.2	TCP	74	[TCP Retransmission] 50572 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4260776365 TSecr=0 WS=128
157	112.179660897	192.168.1.100	192.168.1.1	TLShv1.2	105	Application Data
158	112.189399629	192.168.1.1	192.168.1.100	TCP	66	443 → 60144 [ACK] Seq=34813 Ack=710 Win=514 Len=0 TSval=3381637958 TSecr=2388175142
159	113.164842761	192.168.1.100	192.168.1.100	TLShv1.2	105	Application Data
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0						0000 08 00 27 b0 24 60 08 00 27 cb 7e f5 08 00 45 00 ...\$...E
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_b0:24:60 (08:00:27:b0:24:60)						0020 08 00 27 b0 24 60 08 00 27 0e c9 08 01 04 00 00 ...d...
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.50.2						0020 32 02 b2 06 00 50 f6 0b 5d 21 00 00 00 00 02 2 f p j l ...
Transmission Control Protocol, Src Port: 45070, Dst Port: 80, Seq: 0, Len: 0						0030 fa f0 b4 e5 00 00 02 84 05 04 04 02 00 0a fd f4 ...
						0040 5d 0f 00 00 00 00 01 03 03 07 .....

eth0: alive capture in progress

Packets: 185. Displayed: 185 (100.0%)

Profile: Default