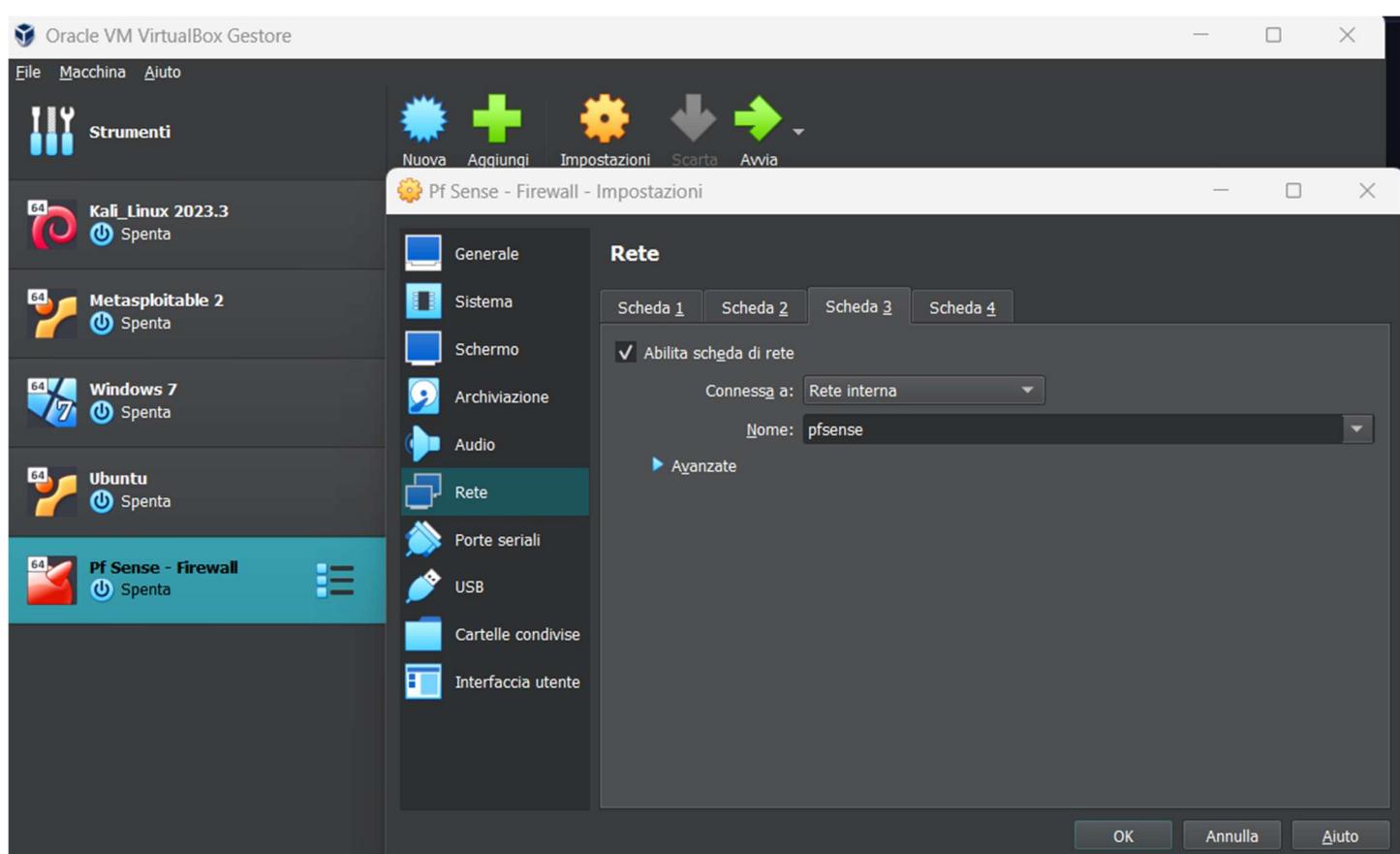
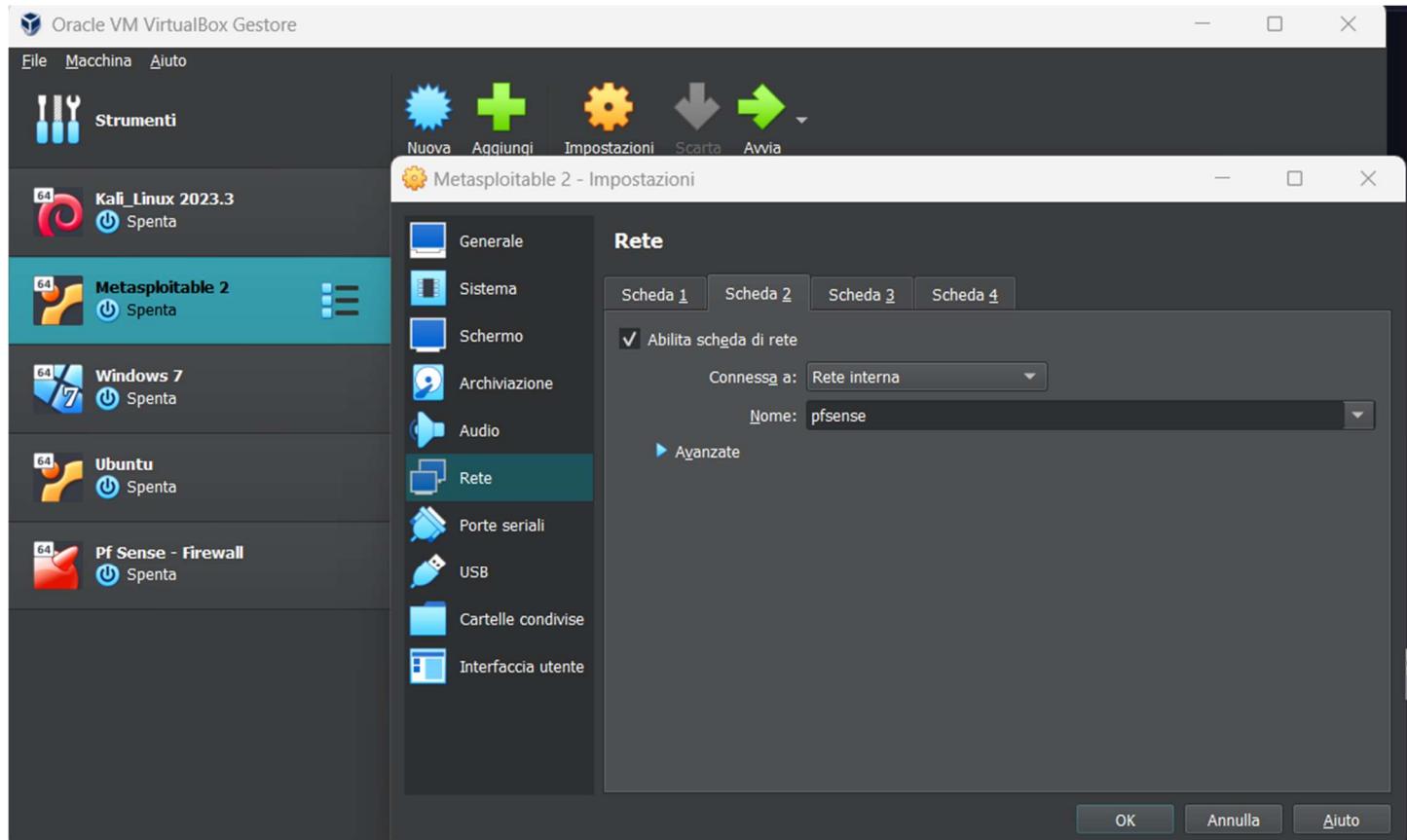


## CREAZIONE POLICY PFSENSE

Creo delle nuove schede di rete su macchina Metasploitable e su PfSense



## Configuro la nuova scheda di rete in PfSense con servizio DHCP Attivo e che abbia come rete 192.168.51.0/24

LAN LAN2

### General DHCP Options

DHCP Backend	Kea DHCP
<b>Enable</b>	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
<b>Deny Unknown Clients</b>	<input type="button" value="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 <i>any</i> 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>
<b>Ignore Client Identifiers</b>	<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

<b>Subnet</b>	192.168.51.0/24	
<b>Subnet Range</b>	192.168.51.1 - 192.168.51.254	
<b>Address Pool Range</b>	<input type="text" value="192.168.51.10"/> From	<input type="text" value="192.168.51.20"/> To
The specified range for this pool must not be within the range configured on any other address pool for this interface.		
<b>Additional Pools</b>	<input type="button" value="+ Add Address Pool"/> <small>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</small>	

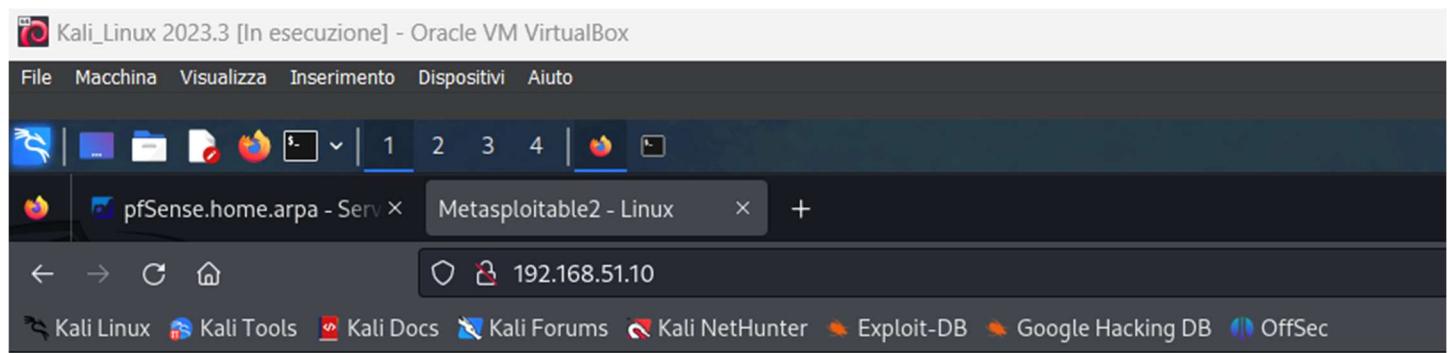
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth1      Link encap:Ethernet HWaddr 08:00:27:6c:63:3f  
          inet addr:192.168.51.10  Bcast:192.168.51.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe6c:633f/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:4 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:47 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:790 (790.0 B)  TX bytes:5070 (4.9 KB)  
            Base address:0xd240 Memory:f0820000-f0840000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING  MTU:16436  Metric:1  
            RX packets:91 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)  
  
msfadmin@metasploitable:~$
```


CTRL (DESTRA)

Eseguo una prova di connessione alla pagina Metasploitable.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Ora configuro la regola Firewall di PfSense per impedire a Kali di poter accedere alla pagina web di Metasploitable.

**pfSense Firewall / Rules / LAN**

Floating WAN LAN LAN2

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/1.03 MiB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	
✗ 0/0 B 	IPv4 TCP	192.168.50.100	*	192.168.51.10	80 (HTTP)	*	none			
✓ 0/124 KiB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

**pfSense Firewall / Rules / Edit**

**Edit Firewall Rule**

Action: Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: LAN

Address Family: IPv4

Protocol: TCP

**Source**

Source:  Invert match Address or Alias: 192.168.50.100 /

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

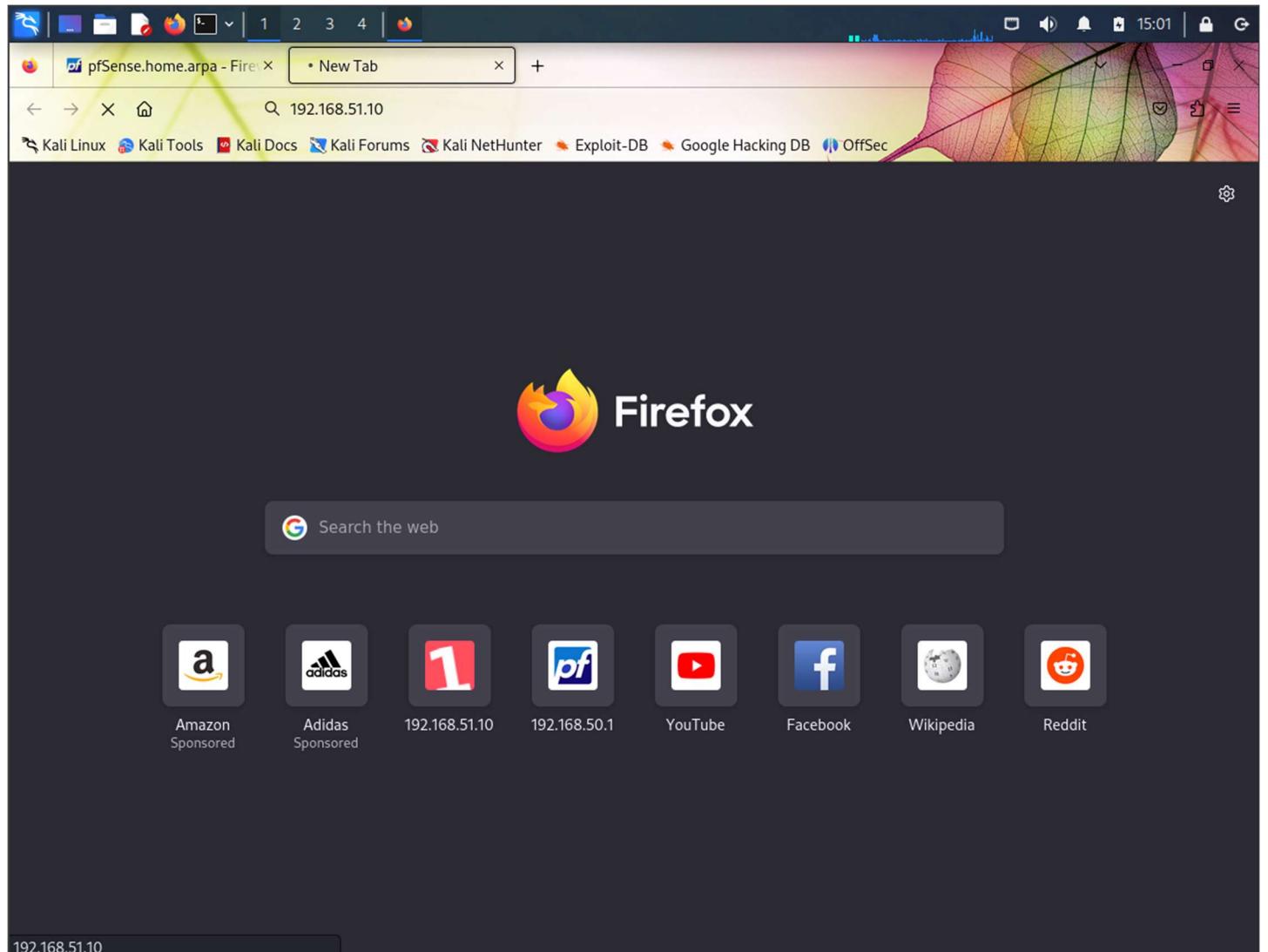
**Destination**

Destination:  Invert match Address or Alias: 192.168.51.10 /

Destination Port Range: From: HTTP (80) To: HTTP (80)  Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Verifico che venga bloccata la richiesta di apertura della pagina



Come si può vedere da immagini di seguito la richiesta che esegue Kali verso Metasploitable viene bloccata. Di fatto Kali tenta di effettuare la three-way-handshake ma la richiesta rimane bloccata. Quelli a seguire sono le attese di SYN-ACK. Quando passa troppo tempo dalla richiesta, il browser genera errore.

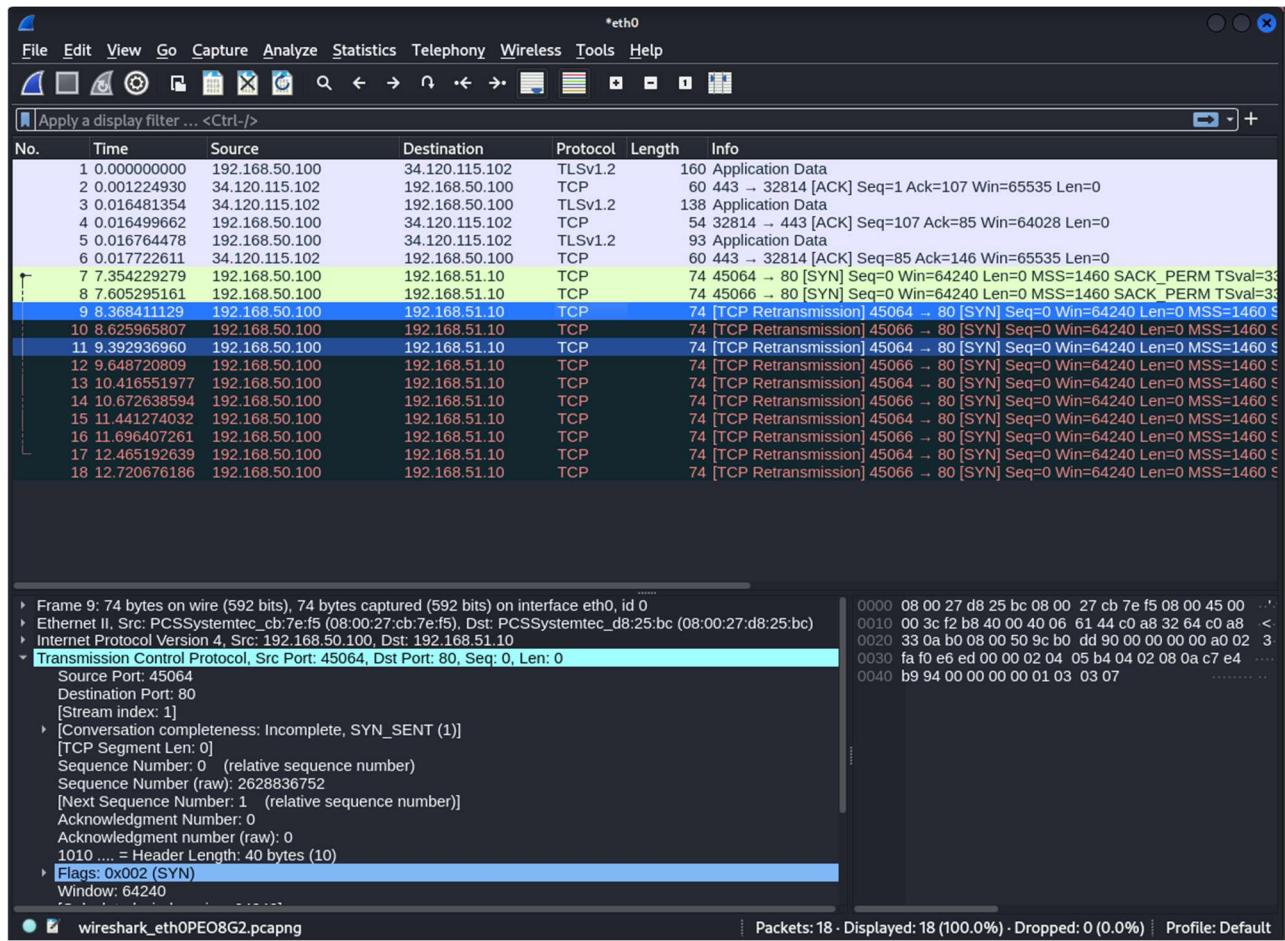
The connection has timed out

The server at 192.168.51.10 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

[Try Again](#)

<https://www.kali.org/tools/>



Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0  
 Ethernet II, Src: PCSSystemtec\_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PCSSystemtec\_d8:25:bc (08:00:27:d8:25:bc)  
 Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.51.10  
 Transmission Control Protocol, Src Port: 45064, Dst Port: 80, Seq: 0, Len: 0

Source Port: 45064  
 Destination Port: 80  
 [Stream index: 1]  
 [Conversation completeness: Incomplete, SYN\_SENT (1)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 2628836752  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 0  
 Acknowledgment number (raw): 0  
 1010 .... = Header Length: 40 bytes (10)  
 Flags: 0x002 (SYN)

0000 08 00 27 d8 25 bc 08 00 27 cb 7e f5 08 00 45 00 ...  
 0010 00 3c f2 b8 40 00 40 06 61 44 c0 a8 32 64 c0 a8 ...<  
 0020 33 0a b0 08 00 50 9c b0 dd 90 00 00 00 00 a0 02 3  
 0030 fa f0 e6 ed 00 00 02 04 05 b4 04 02 08 0a c7 e4 ...  
 0040 b9 94 00 00 00 00 01 03 03 07 .....

wireshark\_eth0PEO8G2.pcapng

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Firefox browser window showing a failed connection attempt to 192.168.51.10. The status bar indicates "Problem loading page".

Kali\_Linux 2023.3 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

pfSense.home.arpa - Status

192.168.50.1/status\_logs\_filter.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Dec 26 10:58:34	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 10:58:43	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 10:58:59	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:10	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:12	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:14	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:18	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:27	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:44	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:55	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:57	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:04:59	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:05:04	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:05:12	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:05:29	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
✗	Dec 26 11:05:39	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP
192.168.50.1/status_logs.php?logfile=ipsec	41	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.68	i 255.255.255.255:67	UDP