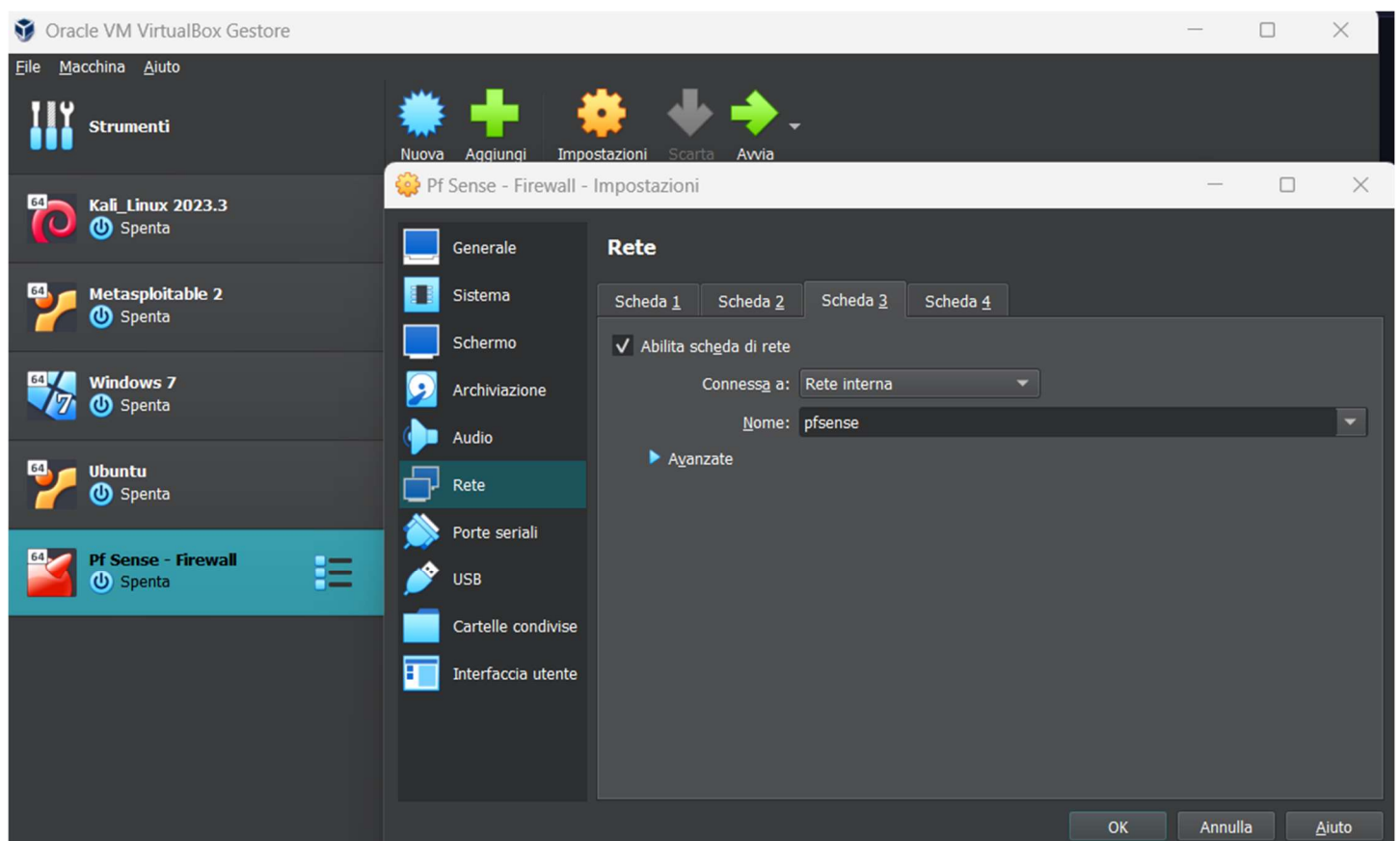
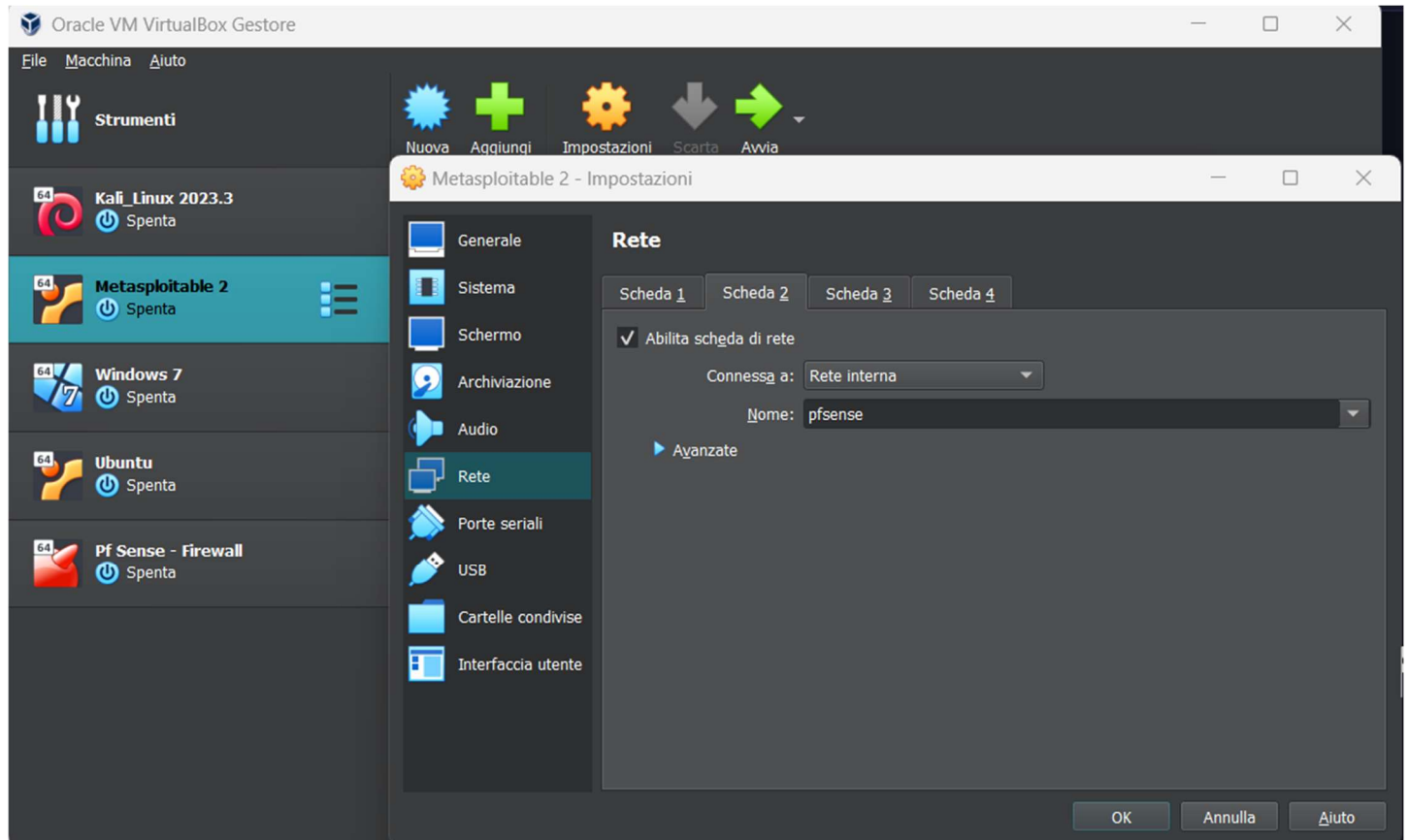


CREAZIONE POLICY PFSENSE

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
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
Deny Unknown Clients	<div>Allow all clients</div> <p>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.</p>
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request 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.

Primary Address Pool

Subnet	192.168.51.0/24
Subnet Range	192.168.51.1 - 192.168.51.254
Address Pool Range	<div>192.168.51.10192.168.51.20</div> <div>FromTo</div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>
Additional Pools	<div>+ Add Address Pool</div> <p>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</p>

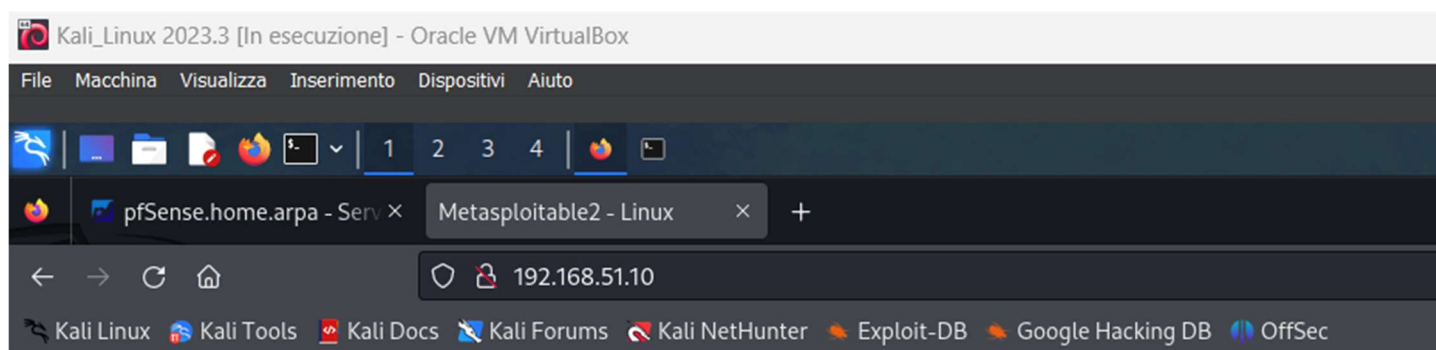
```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

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:~$
```

Eseguo una prova di connessione alla pagina Metasploitable.



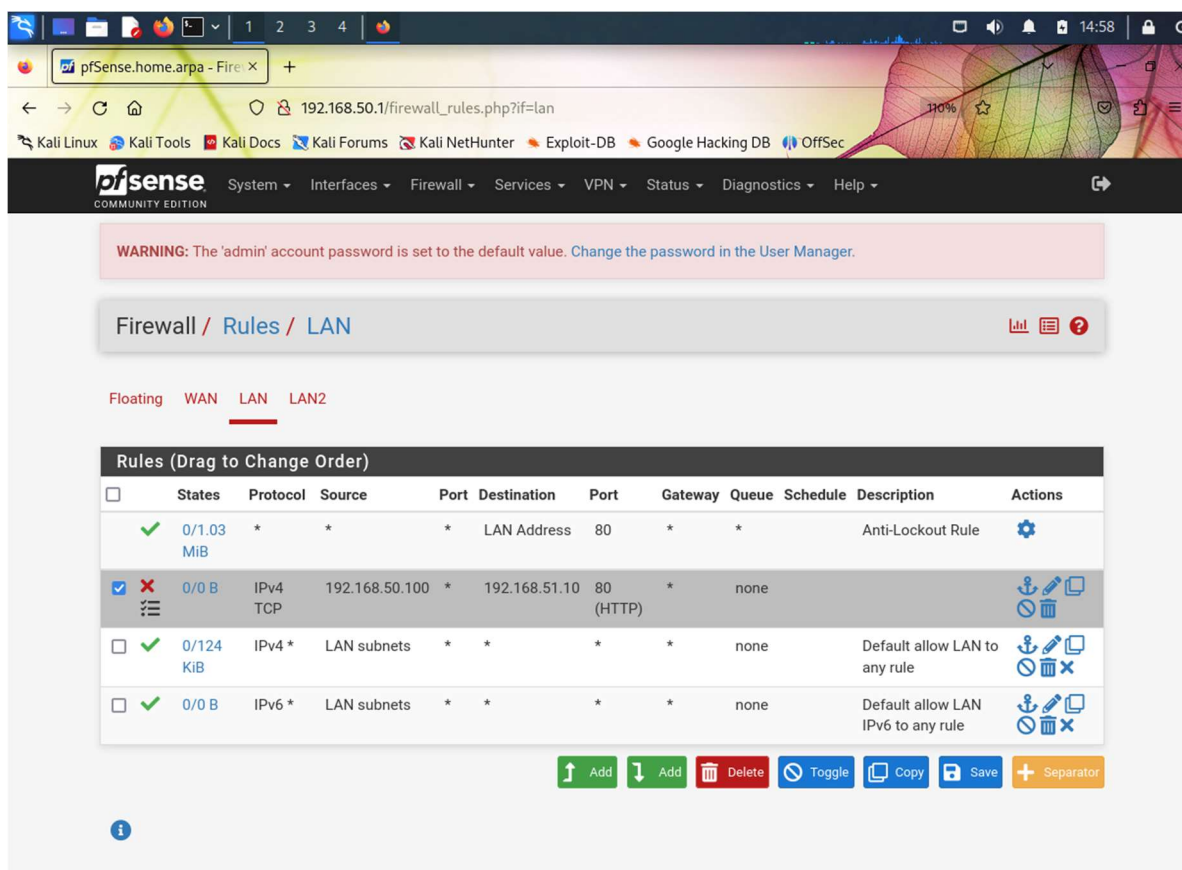
Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

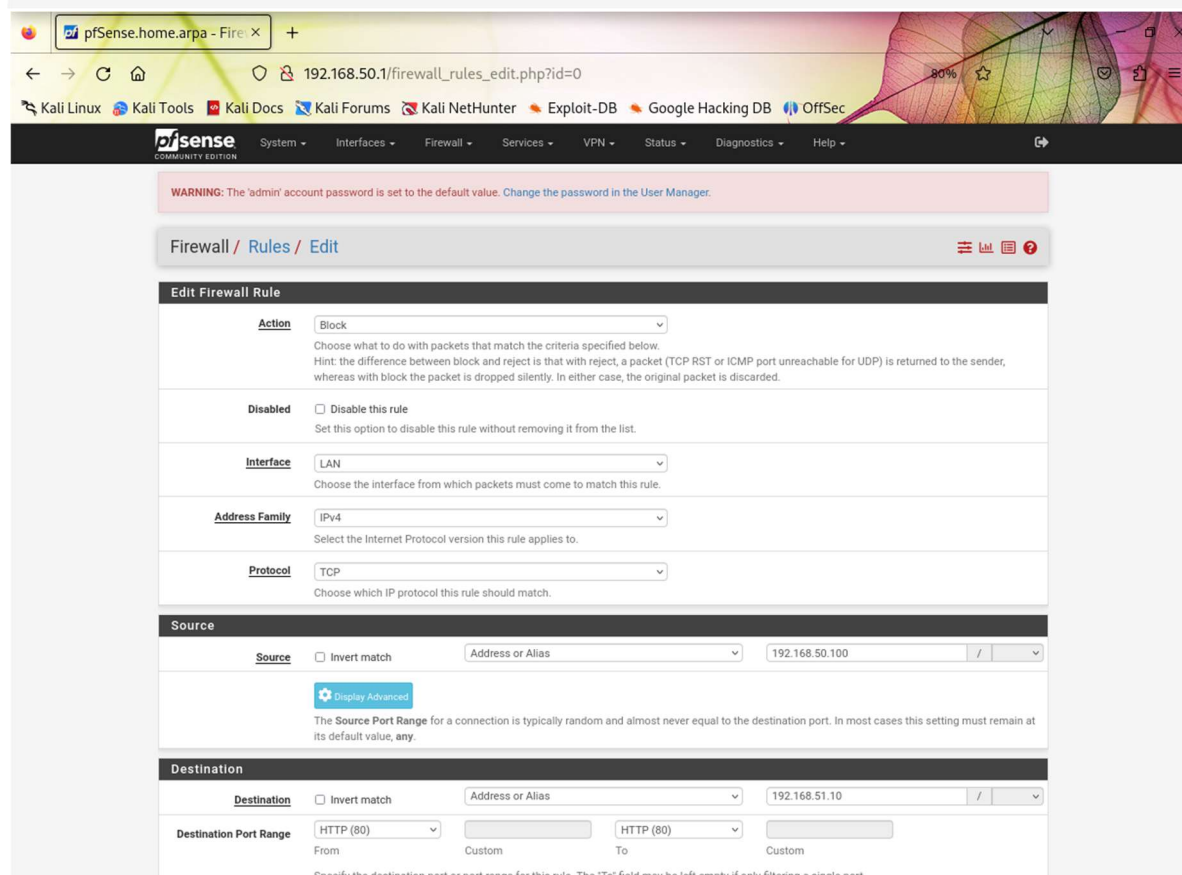
- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

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



The screenshot shows the pfSense Firewall Rules configuration page for the LAN interface. The browser address bar displays `192.168.50.1/firewall_rules.php?if=lan`. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb navigation is "Firewall / Rules / LAN". Below the tabs (Floating, WAN, LAN, LAN2), the "Rules (Drag to Change Order)" table is visible. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The first rule is "Anti-Lockout Rule" with a status of 0/1.03 MiB. The second rule is selected, showing details: Protocol: IPv4, Source: 192.168.50.100, Port: *, Destination: 192.168.51.10, Port: 80 (HTTP). Below the table are buttons for Add, Add, Delete, Toggle, Copy, Save, and Separator.

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

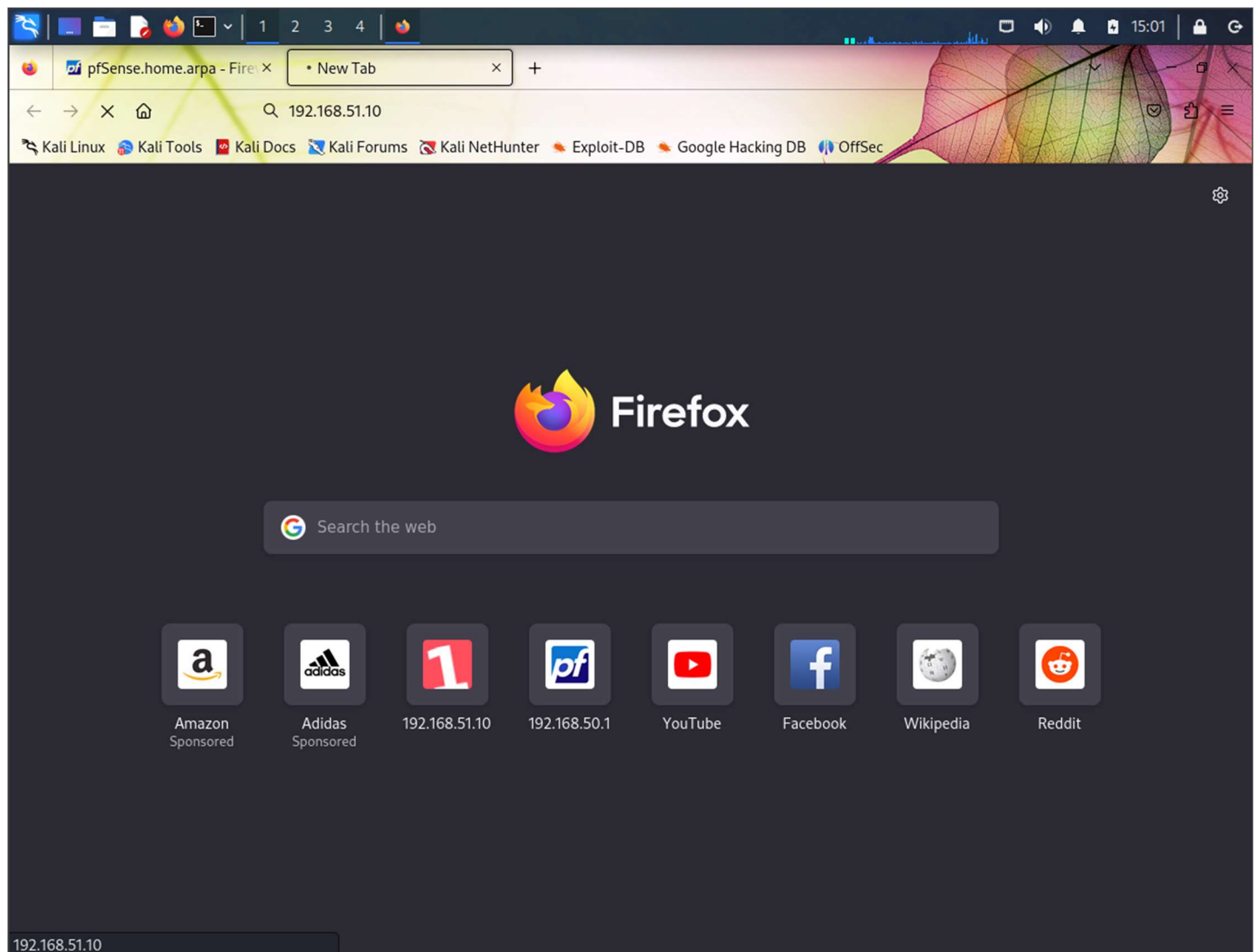


The screenshot shows the pfSense Firewall Rule Edit page. The browser address bar displays `192.168.50.1/firewall_rules_edit.php?id=0`. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb navigation is "Firewall / Rules / Edit". The "Edit Firewall Rule" form is displayed with the following settings:

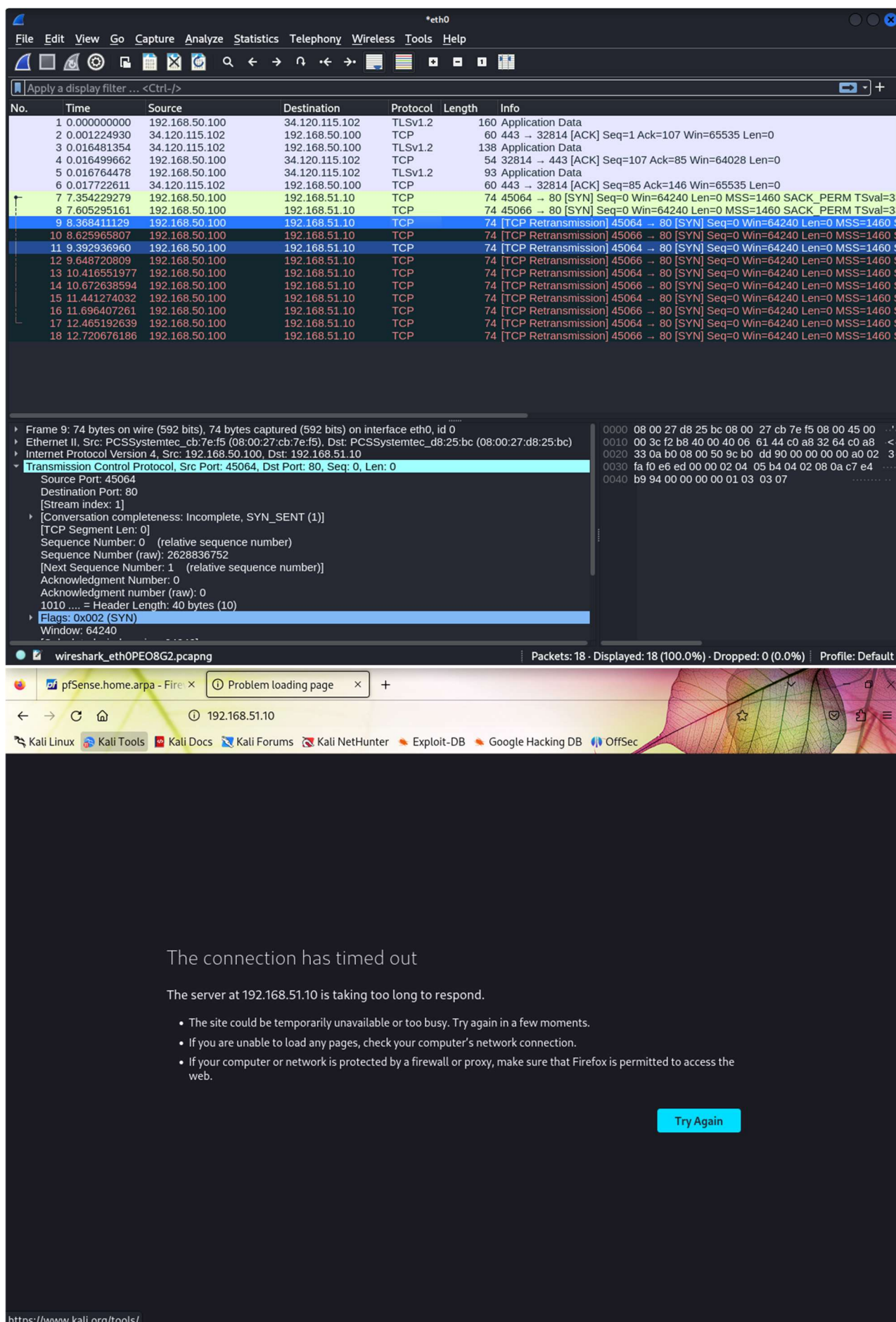
- Action:** Block (dropdown)
- Disabled:** ☐ Disable this rule (checkbox)
- Interface:** LAN (dropdown)
- Address Family:** IPv4 (dropdown)
- Protocol:** TCP (dropdown)
- Source:**
 - Source:** ☐ Invert match (checkbox)
 - Address or Alias:** Address or Alias (dropdown)
 - Address:** 192.168.50.100 (text)
- Destination:**
 - Destination:** ☐ Invert match (checkbox)
 - Address or Alias:** Address or Alias (dropdown)
 - Address:** 192.168.51.10 (text)
 - Destination Port Range:** HTTP (80) (dropdown)
 - From:** Custom (text)
 - To:** Custom (text)

Buttons for "Display Advanced" and "Save" are visible at the bottom.

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 image shows a Wireshark packet capture on interface eth0. The packet list displays 18 packets, with the selected packet (No. 7) being a TCP SYN packet from 192.168.50.100 to 192.168.51.10. The packet details pane shows the TCP header information, including the sequence number 0 and the SYN flag. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Below the Wireshark interface, a browser window is open at the URL 192.168.51.10. The browser displays a message: "The connection has timed out. The server at 192.168.51.10 is taking too long to respond." Below this message, there are three bullet points providing troubleshooting advice: "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.", and "If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web." A "Try Again" button is located at the bottom right of the message area.

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

Kali Linux 2023.3 [In esecuzione] - Oracle VM VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

1234

pfSense.home.arpa - Sta

+

192.168.50.1/status_logs_filter.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

pfSenseCOMMUNITY EDITION

SystemInterfacesFirewallServicesVPNStatusDiagnosticsHelp

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

Status / System Logs / Firewall / Normal View

Tf?

SystemFirewallDHCPAuthenticationIPsecPPPPPPoE/L2TP ServerOpenVPNNTPPackagesSettings

Normal ViewDynamic ViewSummary 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 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 10:58:43	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 10:58:59	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:10	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:12	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:14	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:18	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:27	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:44	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:55	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:57	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:04:59	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:05:04	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:05:12	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:05:29	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:05:39	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP
✗	Dec 26 11:05:41	LAN	Default deny rule IPv4 (1000000103)	i 0.0.0.0:68	i+ 255.255.255.255:67	UDP

192.168.50.1/status_logs.php?logfile=ipsec