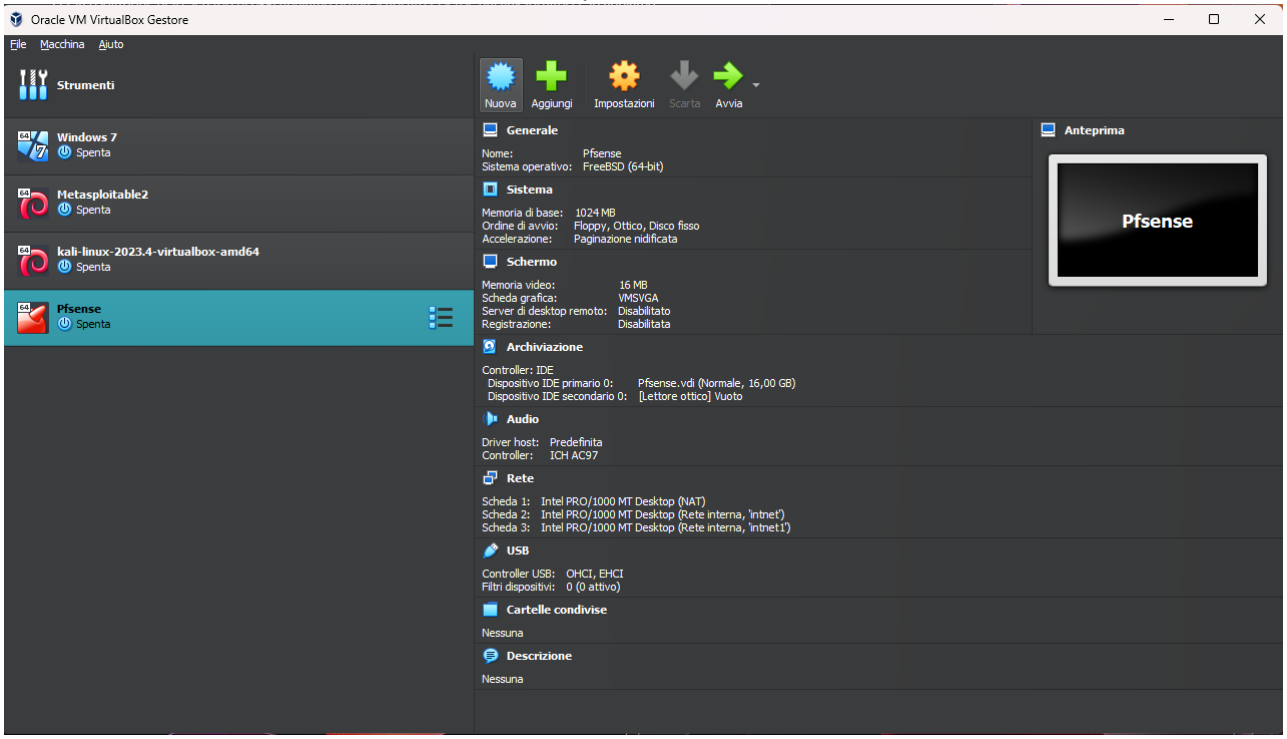
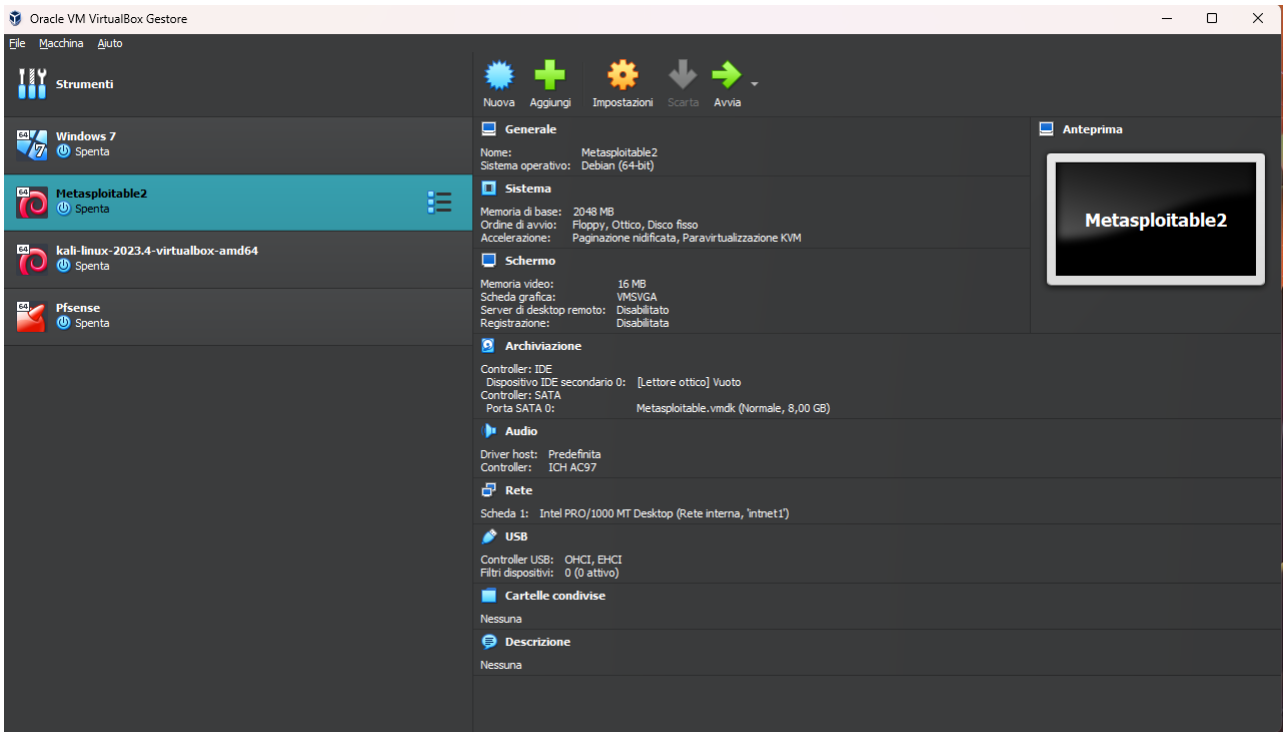
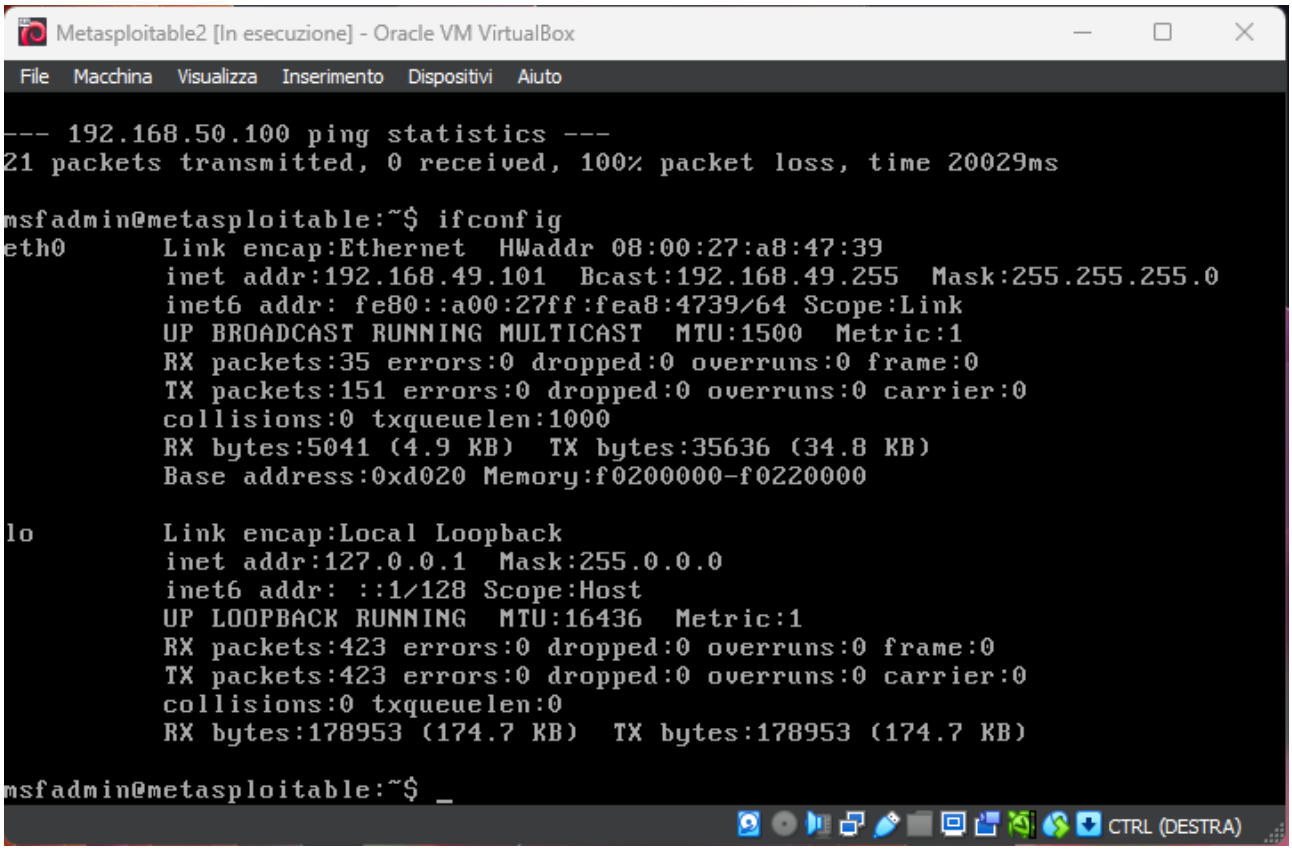
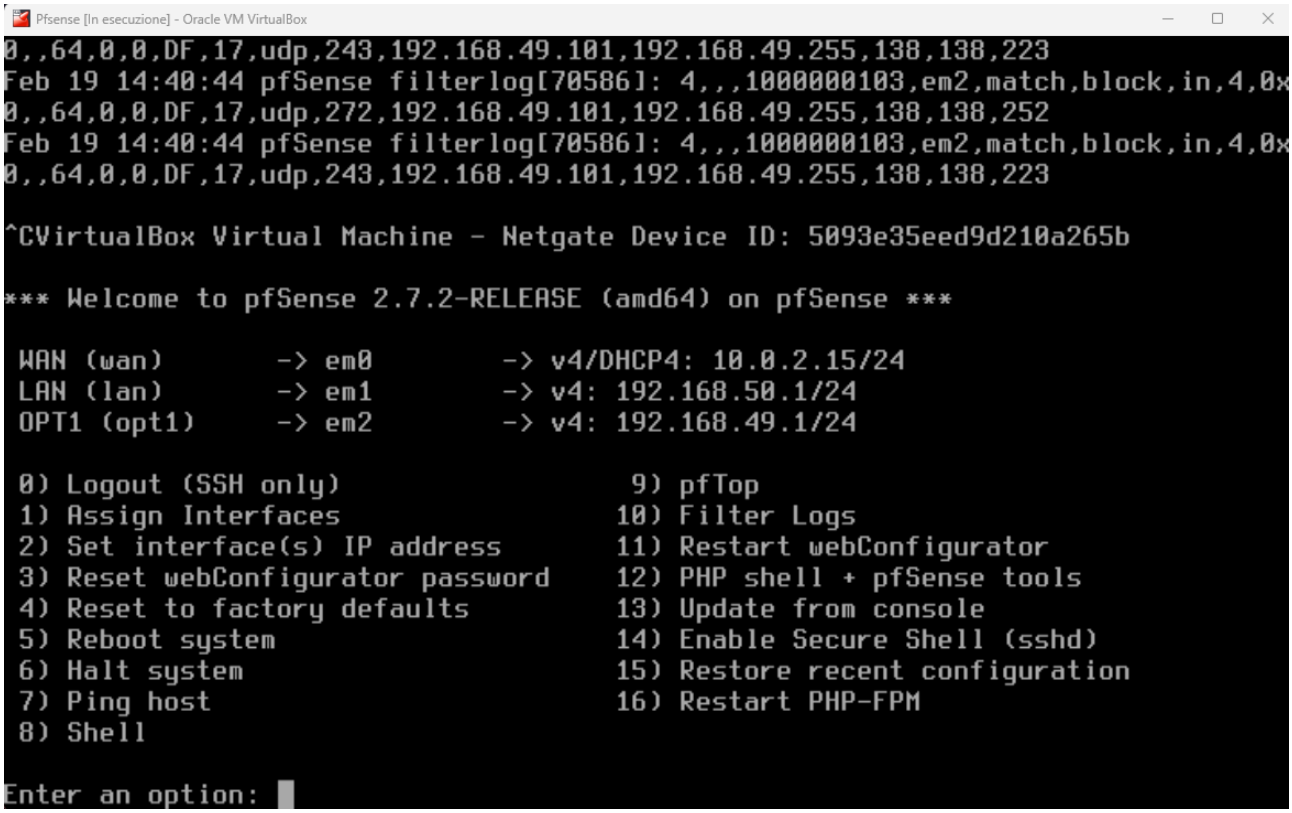
Per la risoluzione dell'esercizio di oggi abbiamo prima scaricato Pfsense dal link fornitoci e lo abbiamo installato tramite oracle virtual box, successivamente siamo andati ad abilitare le schede di rete su Pfsense, nello specifico abbiamo abilitato tre schede di rete di cui una NAT e due reti interne, una "intnet" ed una "intnet1". Abbiamo modificato l'indirizzo ip sulla macchina virtuale metasploitable sotituendo l'indirizzo ip precedmente impostato come 192.168.50.101 con l'indirizzo 192.168.49.101 cambiando anche l'indirizzo di gateway e modificando il nome della scheda di rete in "intent1". Successivamente siamo ritornati su Pfsense ed abbiamo d'apprima assegnato le diverse interfacce come WAN, LAN, OPT1 con gli indirizzi di Gateway di Kali e Metasploitable. Pfsense fungerà da Firewall e potremo impostargli delle regole per gestire il flusso di dati.

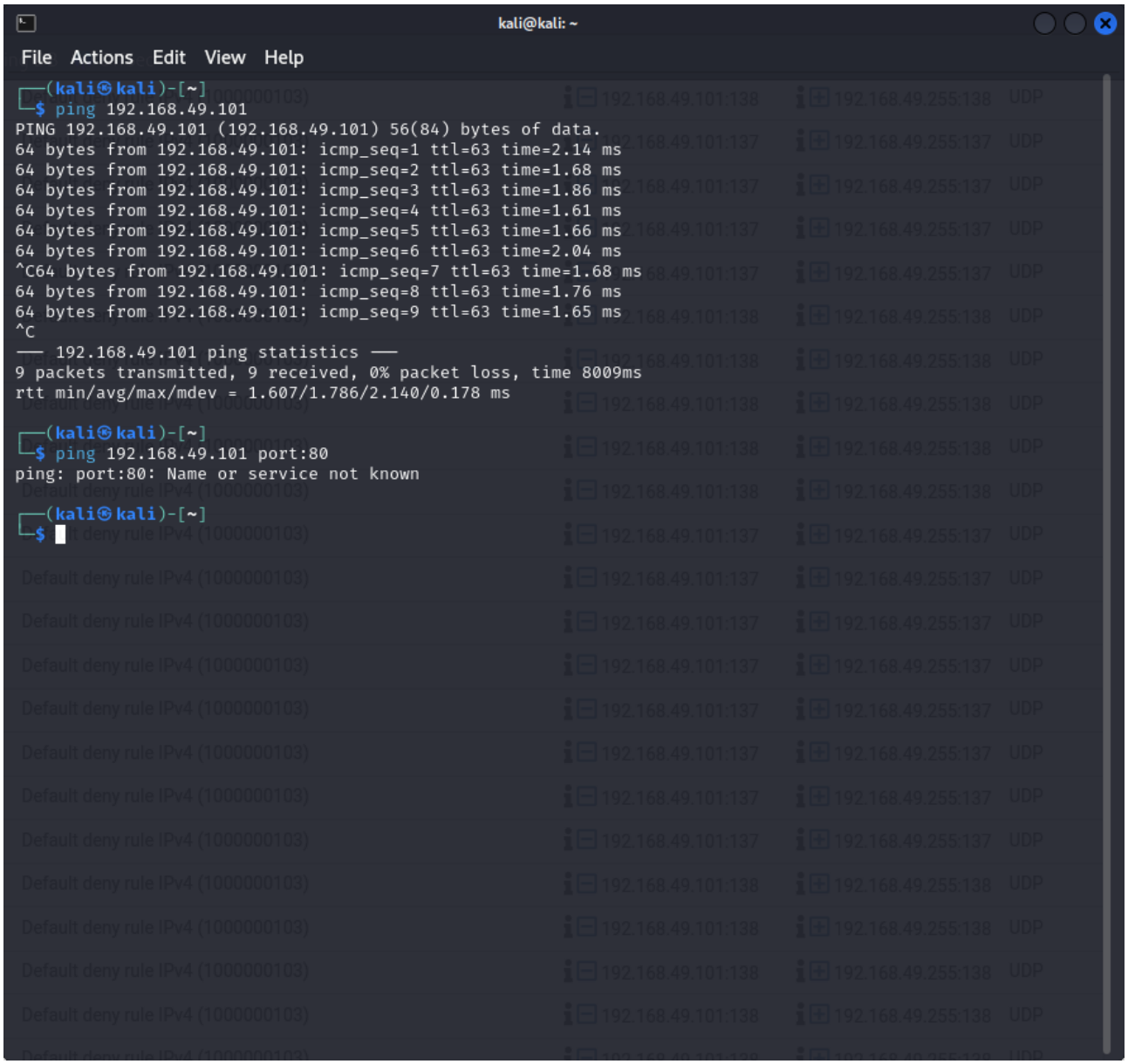
Una volta impostato tutto correttamente abbiamo avviato kali provando prima la comunicazione con metasploitable tramite il ping e poi abbiamo cercato da browser l'indirizzo di Pfsense, che nel mio caso è l'indirizzo ip 10.0.2.15. Una volta raggiunto abbiamo impostato il firewall con la seguente regola, ovvero quella di bloccare il traffico dalla source dikali alla destination di metasploitable, in questo modo non siamo più in grado di accedere a DVWA inserendo sulla barra di ricerca browser l'indirizzo di Metasploitable ma sarà comunque pingabile da kali a metasploitable. Volendo si può andare nella sezione system logs/firewall/normal views per vedere i log bloccati verso la porta 80 che abbiamo disabilitato e quindi tutte le richieste TCP, UDP ed ICMP bloccate secondo quanto abbiamo richiesto al firewall.

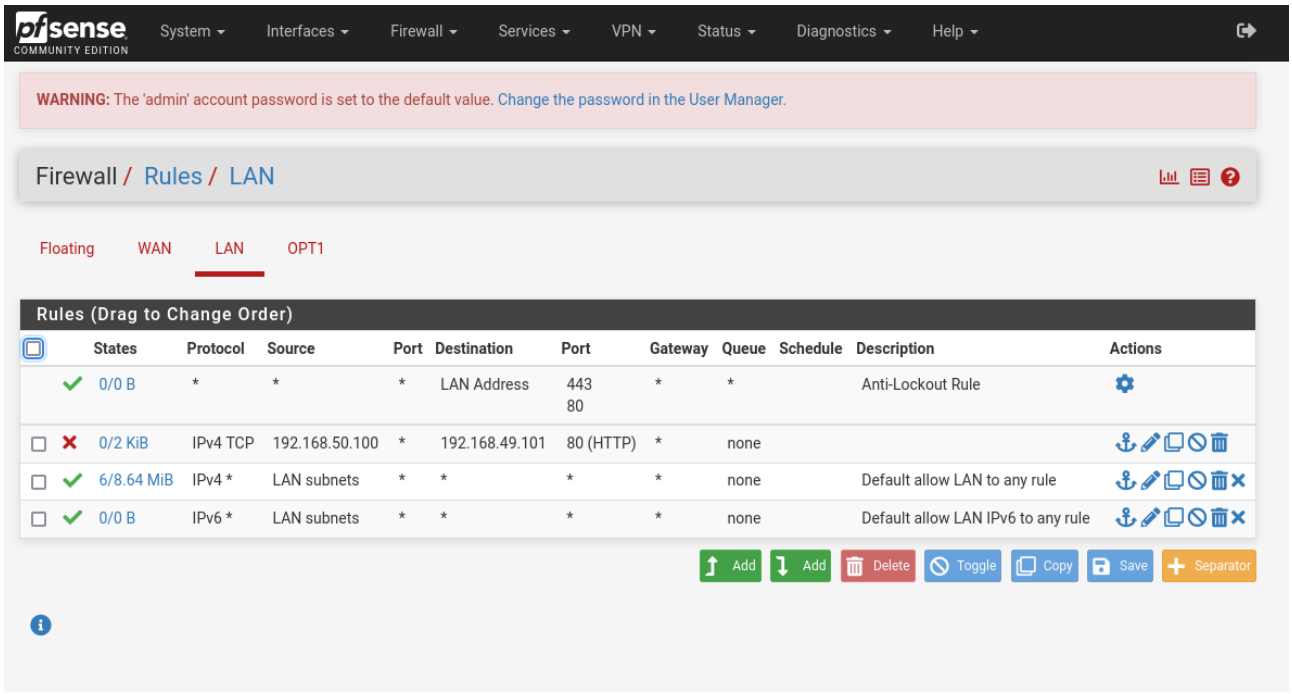



Oracle VM VirtualBox Gestore
File Macchina Aiuto
Strumenti
Windows 7
Spenta
Metasploitable2
Spenta
kali-linux-2023.4-virtualbox-amd64
Spenta
Pfsense
Spenta
Nuova
Aggiungi
Impostazioni
Scarta
Avvia
Generale
Nome: Metasploitable2
Sistema operativo: Debian (64-bit)
Sistema
Memoria di base: 2048 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata, Paravirtualizzazione KVM
Schermo
Memoria video: 16 MB
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata
Archiviazione
Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: Metasploitable.vmdk (Normale, 8,00 GB)
Audio
Driver host: Predefinita
Controller: ICH AC97
Rete
Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet1')
USB
Controller USB: OHCI, EHCI
Filtri dispositivi: 0 (0 attivo)
Cartelle condivise
Nessuna
Descrizione
Nessuna
Anteprima
Metasploitable2


Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
--- 192.168.50.100 ping statistics ---
21 packets transmitted, 0 received, 100% packet loss, time 20029ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a8:47:39
inet addr:192.168.49.101 Bcast:192.168.49.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea8:4739/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:35 errors:0 dropped:0 overruns:0 frame:0
TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5041 (4.9 KB) TX bytes:35636 (34.8 KB)
Base address:0xd020 Memory:f0200000-f0220000
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:423 errors:0 dropped:0 overruns:0 frame:0
TX packets:423 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:178953 (174.7 KB) TX bytes:178953 (174.7 KB)
msfadmin@metasploitable:~$ _
CTRL (DESTRA)


Pfsense [In esecuzione] - Oracle VM VirtualBox
0,,64,0,0,DF,17,udp,243,192.168.49.101,192.168.49.255,138,138,223
Feb 19 14:40:44 pfSense filterlog[70586]: 4,,,1000000103,em2,match,block,in,4,0x
0,,64,0,0,DF,17,udp,272,192.168.49.101,192.168.49.255,138,138,252
Feb 19 14:40:44 pfSense filterlog[70586]: 4,,,1000000103,em2,match,block,in,4,0x
0,,64,0,0,DF,17,udp,243,192.168.49.101,192.168.49.255,138,138,223
^CVirtualBox Virtual Machine - Netgate Device ID: 5093e35eed9d210a265b
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.50.1/24
OPT1 (opt1) -> em2 -> v4: 192.168.49.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=2.14 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=1.68 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=1.86 ms
64 bytes from 192.168.49.101: icmp_seq=4 ttl=63 time=1.61 ms
64 bytes from 192.168.49.101: icmp_seq=5 ttl=63 time=1.66 ms
64 bytes from 192.168.49.101: icmp_seq=6 ttl=63 time=2.04 ms
^C64 bytes from 192.168.49.101: icmp_seq=7 ttl=63 time=1.68 ms
64 bytes from 192.168.49.101: icmp_seq=8 ttl=63 time=1.76 ms
64 bytes from 192.168.49.101: icmp_seq=9 ttl=63 time=1.65 ms
^C
— 192.168.49.101 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8009ms
rtt min/avg/max/mdev = 1.607/1.786/2.140/0.178 ms
┌──(kali㉿kali)-[~]
└─$ ping 192.168.49.101 port:80
ping: port:80: Name or service not known
┌──(kali㉿kali)-[~]
└─$

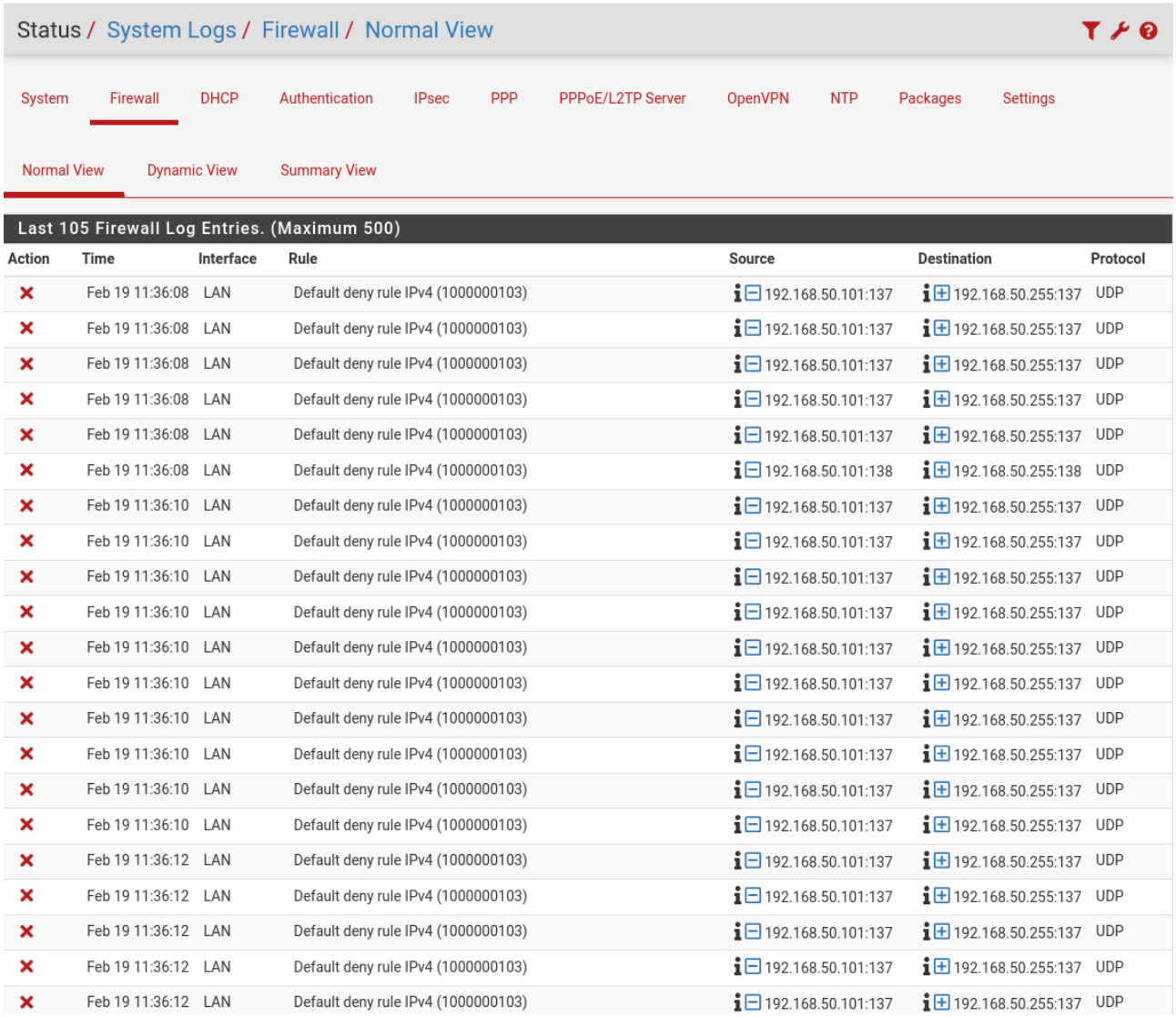


WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / LAN

Rules (Drag to Change Order)

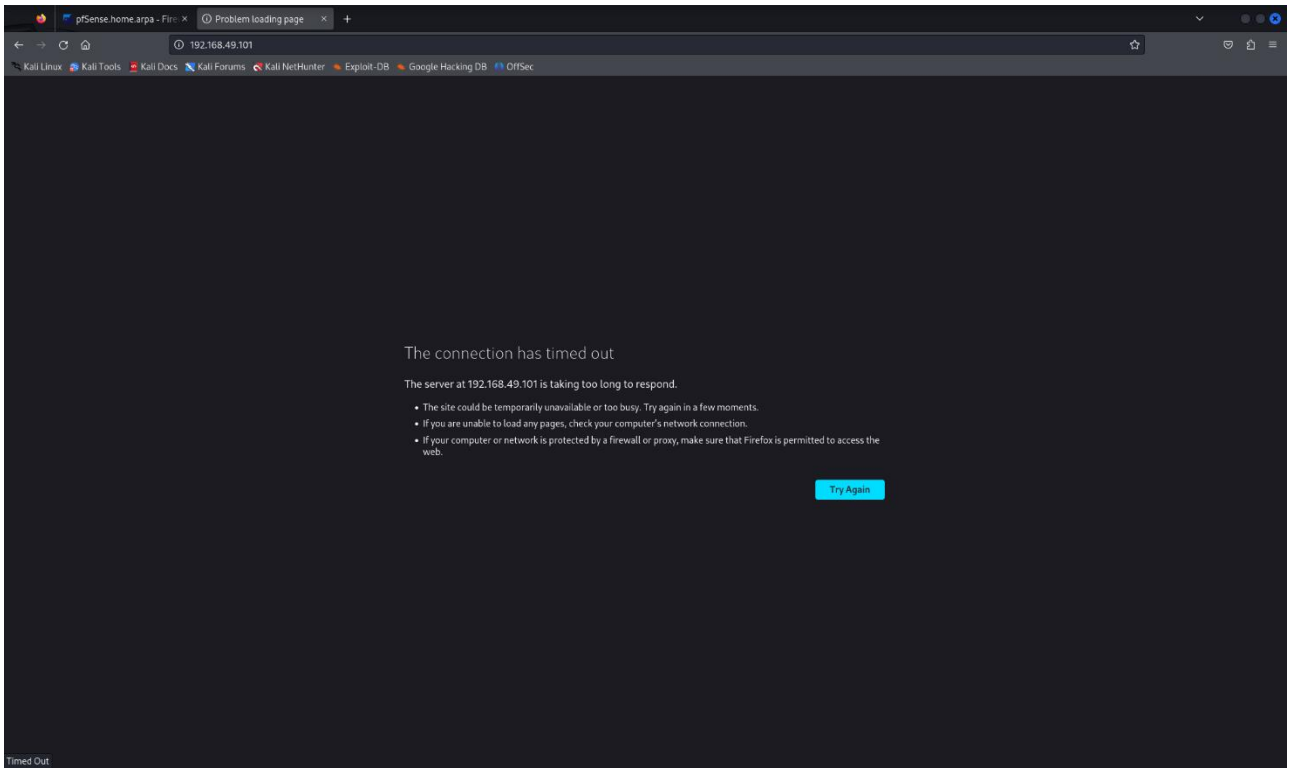
☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	✗	0/2 KiB	IPv4 TCP	192.168.50.100	*	192.168.49.101	80 (HTTP)	*	none			
☐	✓	6/8.64 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
☐	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

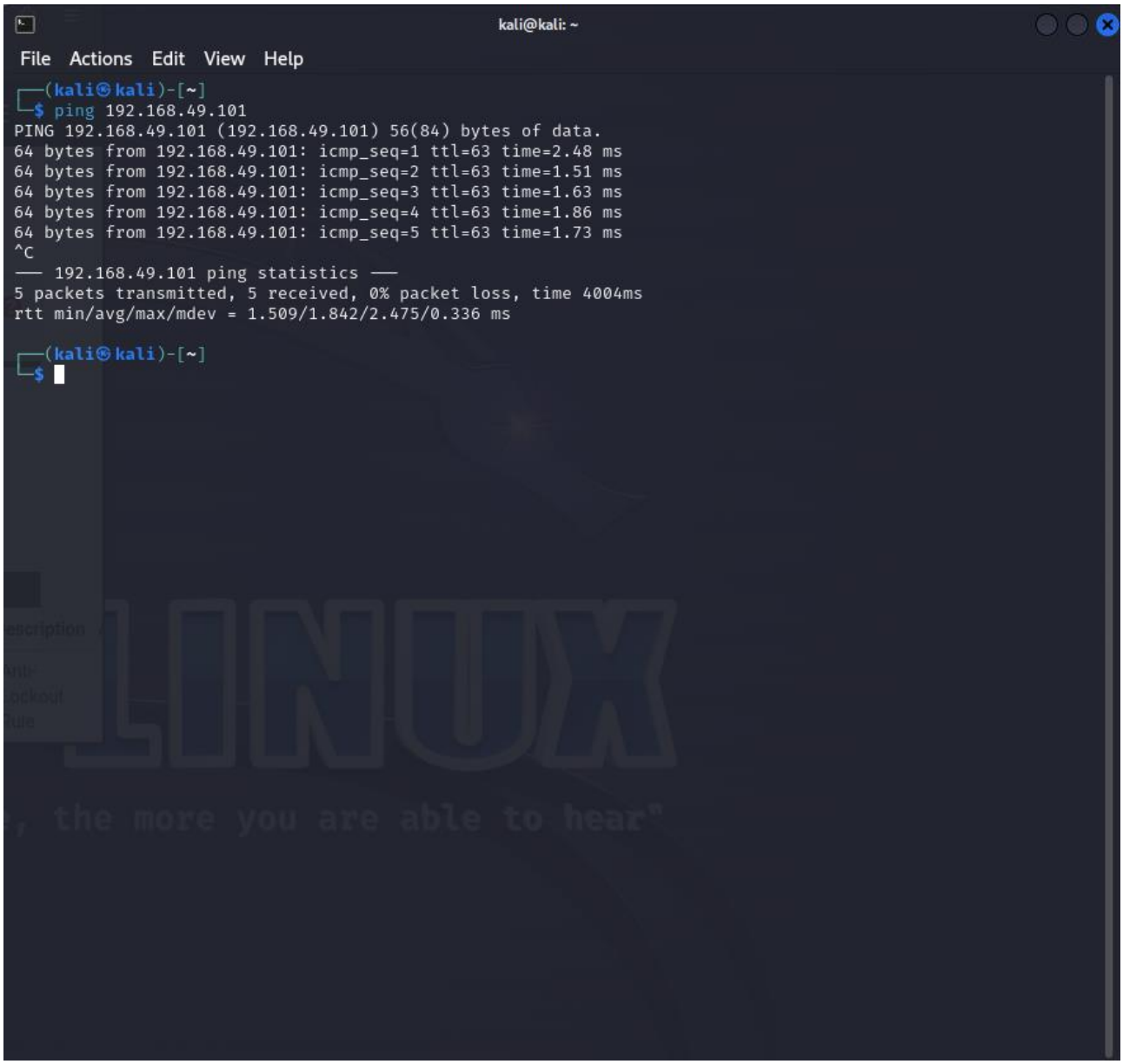


Status / System Logs / Firewall / Normal View

Last 105 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Feb 19 11:36:08	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:08	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:08	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:08	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:08	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:08	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:138	192.168.50.255:138	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:10	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:12	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:12	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:12	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:12	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP
✗	Feb 19 11:36:12	LAN	Default deny rule IPv4 (1000000103)	192.168.50.101:137	192.168.50.255:137	UDP


pfSense.home.arpa - Fire
Problem loading page
192.168.49.101
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
The connection has timed out
The server at 192.168.49.101 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
Timed Out


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=2.48 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=1.51 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=1.63 ms
64 bytes from 192.168.49.101: icmp_seq=4 ttl=63 time=1.86 ms
64 bytes from 192.168.49.101: icmp_seq=5 ttl=63 time=1.73 ms
^C
— 192.168.49.101 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.509/1.842/2.475/0.336 ms
(kali㉿kali)-[~]
$