W9D4 – NICHOLAS DI ANGELO -

Relazione sulla Creazione di una Regola Firewall

Introduzione

Nella configurazione di un firewall, una delle operazioni fondamentali è la creazione di regole che definiscono come il traffico di rete deve essere gestito. In questa relazione, verrà descritto il processo di creazione di una regola firewall utilizzando il software pfSense.

Procedura

1. **Accesso all'Interfaccia di Gestione di pfSense**: Innanzitutto, è necessario accedere all'interfaccia di gestione di pfSense tramite un browser web. Dopo essersi autenticati, è possibile accedere alla sezione Firewall e poi alle regole.
2. **Scelta dell'Interfaccia e Creazione della Regola**: All'interno della sezione delle regole del firewall, è possibile selezionare l'interfaccia di rete su cui si desidera applicare la regola. In questo caso, si sceglie l'interfaccia LAN e si fa clic su "Aggiungi regola".
3. **Configurazione della Regola**: Una volta selezionata l'interfaccia, si procede con la configurazione della regola. I principali parametri da definire includono:
    - **Azione**: si sceglie se permettere o bloccare il traffico.
    - **Famiglia di Indirizzi**: si specifica se la regola si applica a IPv4 o IPv6.
    - **Protocollo**: si specifica il protocollo del traffico (ad esempio TCP, UDP, ICMP).
    - **Sorgente e Destinazione**: si definiscono gli indirizzi IP o le reti sorgente e destinazione del traffico.
    - **Porta di Destinazione**: si specifica la porta di destinazione del traffico.
4. **Applicazione della Regola**: Una volta configurata la regola, viene applicata al firewall. Questo definisce il comportamento del firewall rispetto al traffico di rete in base ai criteri specificati.
5. **Test della Regola**: Dopo aver applicato la regola, è importante testarla per assicurarsi che funzioni correttamente. In questo caso, si può testare il blocco dell'accesso alla DVWA (Damn Vulnerable Web Application) su Metasploitable dalla macchina Kali Linux.

Risultati

Dopo aver creato e applicato la regola firewall, si è effettuato un test per verificare che l'accesso alla DVWA su Metasploitable fosse effettivamente bloccato dalla macchina Kali Linux. Prima della creazione della regola, lo scan per DVWA funzionava correttamente, come dimostrato dalla visualizzazione della pagina web. Tuttavia, dopo l'applicazione della regola, lo scan non funziona più e l'accesso alla DVWA è bloccato, come confermato da uno screenshot della pagina web non caricata.

Conclusioni

La creazione di regole firewall è un'operazione fondamentale nella configurazione di un firewall per gestire il traffico di rete in modo sicuro ed efficiente. Utilizzando pfSense, è possibile configurare regole personalizzate per soddisfare le esigenze specifiche dell'ambiente di rete. La corretta configurazione delle regole firewall aiuta a proteggere la rete da potenziali minacce e violazioni della sicurezza.

Wireshark è uno strumento di analisi del traffico di rete ampiamente utilizzato per esaminare e comprendere il comportamento dei pacchetti di rete. In questa relazione, esamineremo l'analisi dei pacchetti TCP utilizzando Wireshark mentre le regole del firewall con filtraggio SYN sono attive su pfSense. Lo scopo di questo esercizio è esaminare come il firewall gestisce i pacchetti SYN in arrivo.

Procedura

1. Avvio di Wireshark: Innanzitutto, è necessario avviare Wireshark su una macchina all'interno della rete monitorata.
2. Cattura dei Pacchetti: Utilizzando Wireshark, si avvia la cattura dei pacchetti sulla rete desiderata, ad esempio l'interfaccia LAN.
3. Generazione di Pacchetti SYN: Utilizzando uno strumento di test, ad esempio Nmap, si generano pacchetti SYN verso una macchina all'interno della rete.
4. Monitoraggio dei Pacchetti: Durante la cattura dei pacchetti con Wireshark, si osserva il traffico in arrivo e si identificano i pacchetti SYN inviati al sistema di destinazione.
5. Analisi dei Pacchetti: Utilizzando le funzionalità di analisi di Wireshark, si esamina il comportamento dei pacchetti SYN e si determina se vengono ricevute risposte appropriate in base alle regole del firewall.

Risultati Durante l'analisi dei pacchetti con Wireshark, si è osservato che i pacchetti SYN inviati al sistema di destinazione sono stati filtrati correttamente dalle regole del firewall SYN attive su pfSense. Questo è evidenziato dall'assenza di risposte ACK per i pacchetti SYN, indicando che il sistema non accetta le connessioni in entrata in risposta ai pacchetti SYN.

Conclusioni L'analisi dei pacchetti TCP con Wireshark ha dimostrato l'efficacia delle regole del firewall SYN attive su pfSense nel filtrare il traffico indesiderato. La corretta configurazione delle regole del firewall è essenziale per garantire la sicurezza della rete e impedire l'accesso non autorizzato ai sistemi. Utilizzando strumenti come Wireshark, è possibile monitorare e valutare l'efficacia delle regole del firewall nel proteggere la rete dagli attacchi SYN e altre minacce di sicurezza.

Oracle VM VirtualBox Gestore

Strumenti

- **metasploitable2** — Spenta
- **window7** — Spenta
- **mint** — Spenta
- **kali linux 1 1** — Spenta
- **pfsense** — In esecuzione

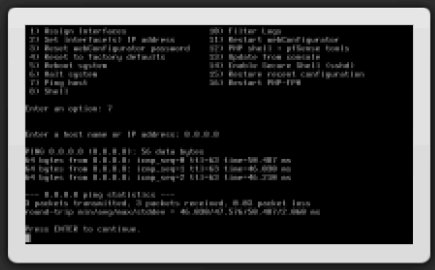
Nuova | Aggiungi | Impostazioni | Scarta | Mostra

Generale

Nome: pfsense
Sistema operativo: FreeBSD (64-bit)

Sistema

Anteprima



pfsense [Running]

```
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart webConfigurator
3) Reset webConfigurator password   12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: 7


Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=63 time=50.487 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=46.030 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=46.210 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 46.030/47.576/50.487/2.060 ms

Press ENTER to continue.
```

Left ⌘

RELEASE-amd64.iso (834,15 MB)

Audio

Driver host: Predefinita
Controller: ICH AC97

Rete

Scheda 1: Intel PRO/1000 MT Desktop (NAT)
Scheda 2: Intel PRO/1000 MT Desktop (Rete interna, 'HostNetwork')

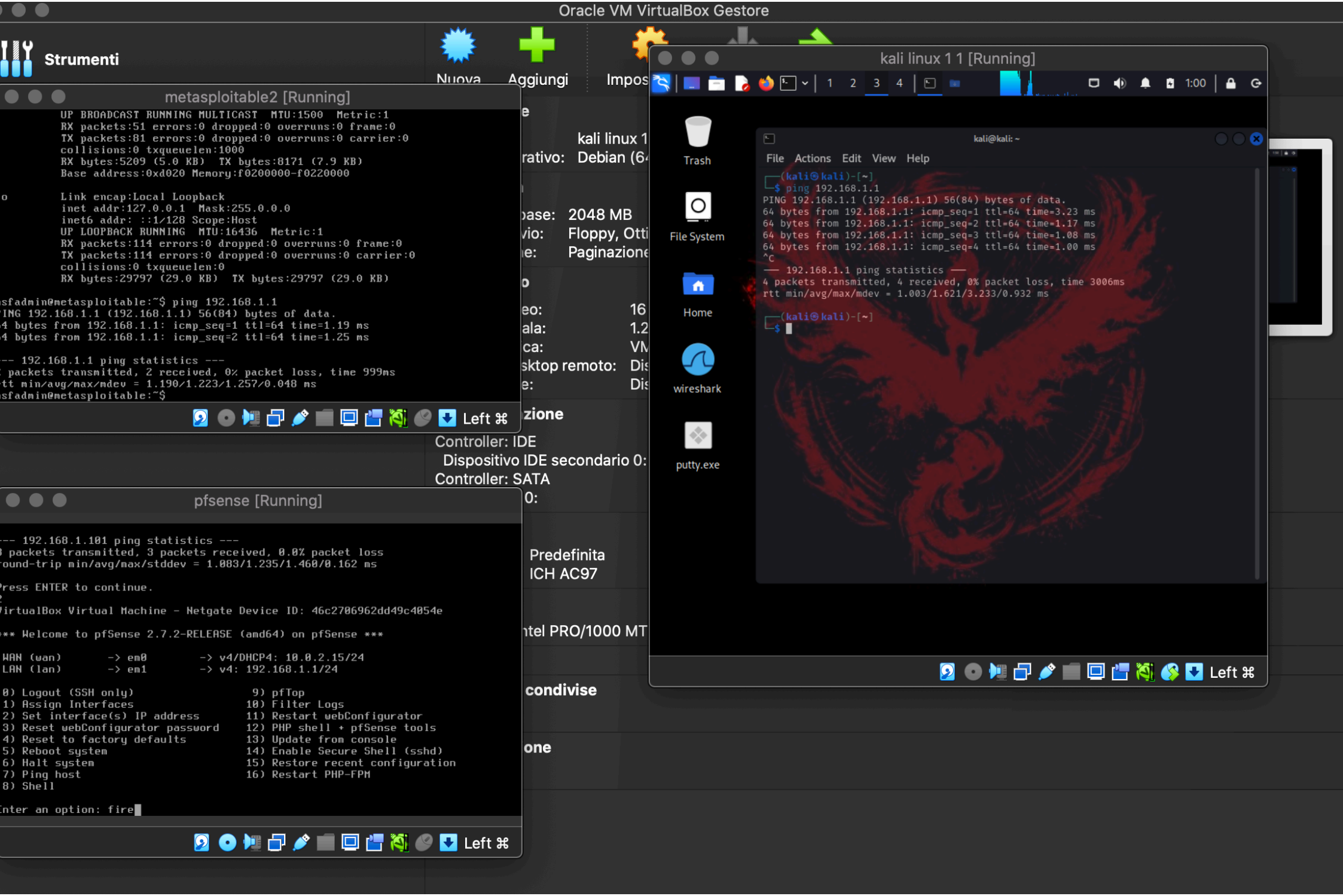
USB

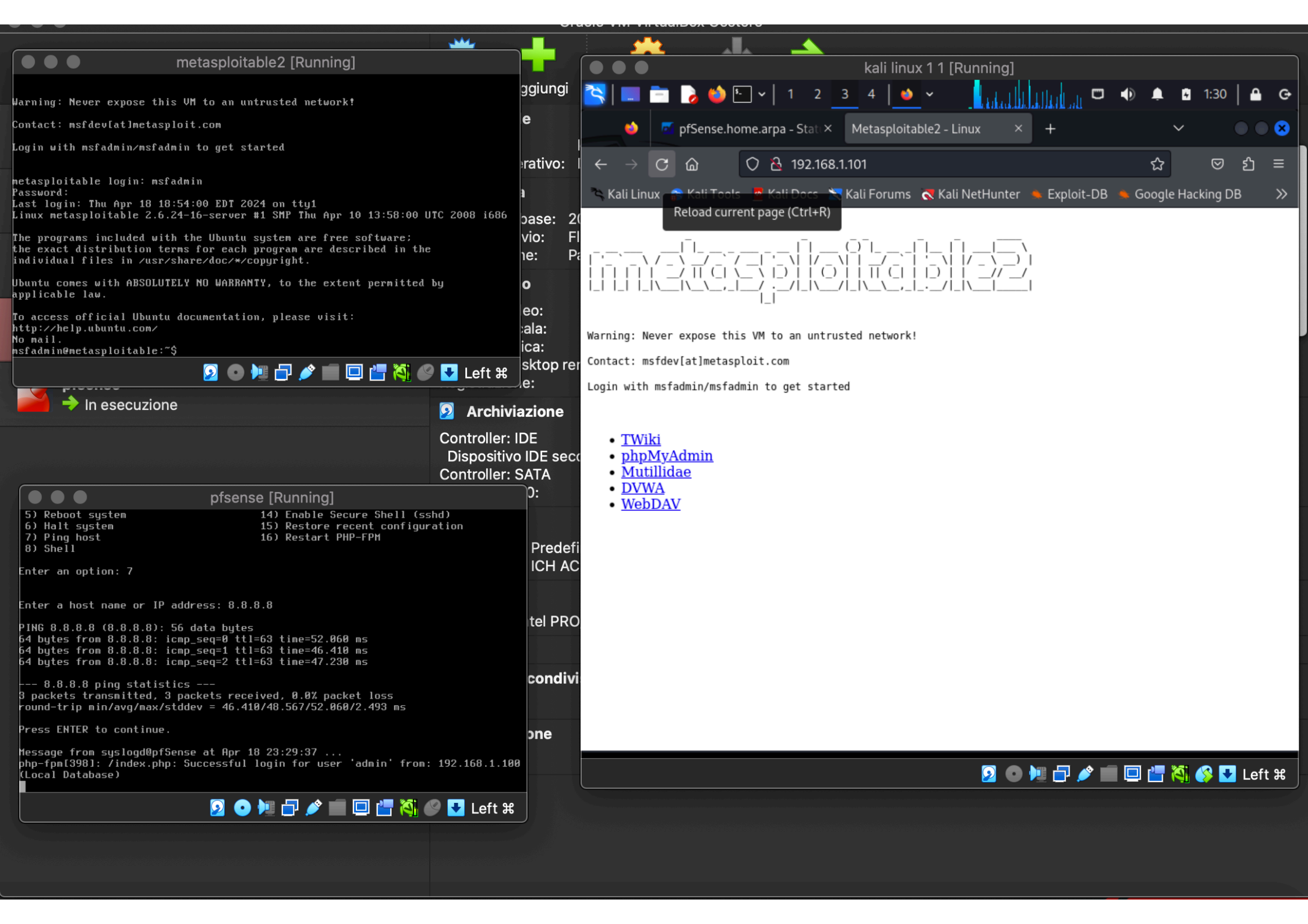
Cartelle condivise

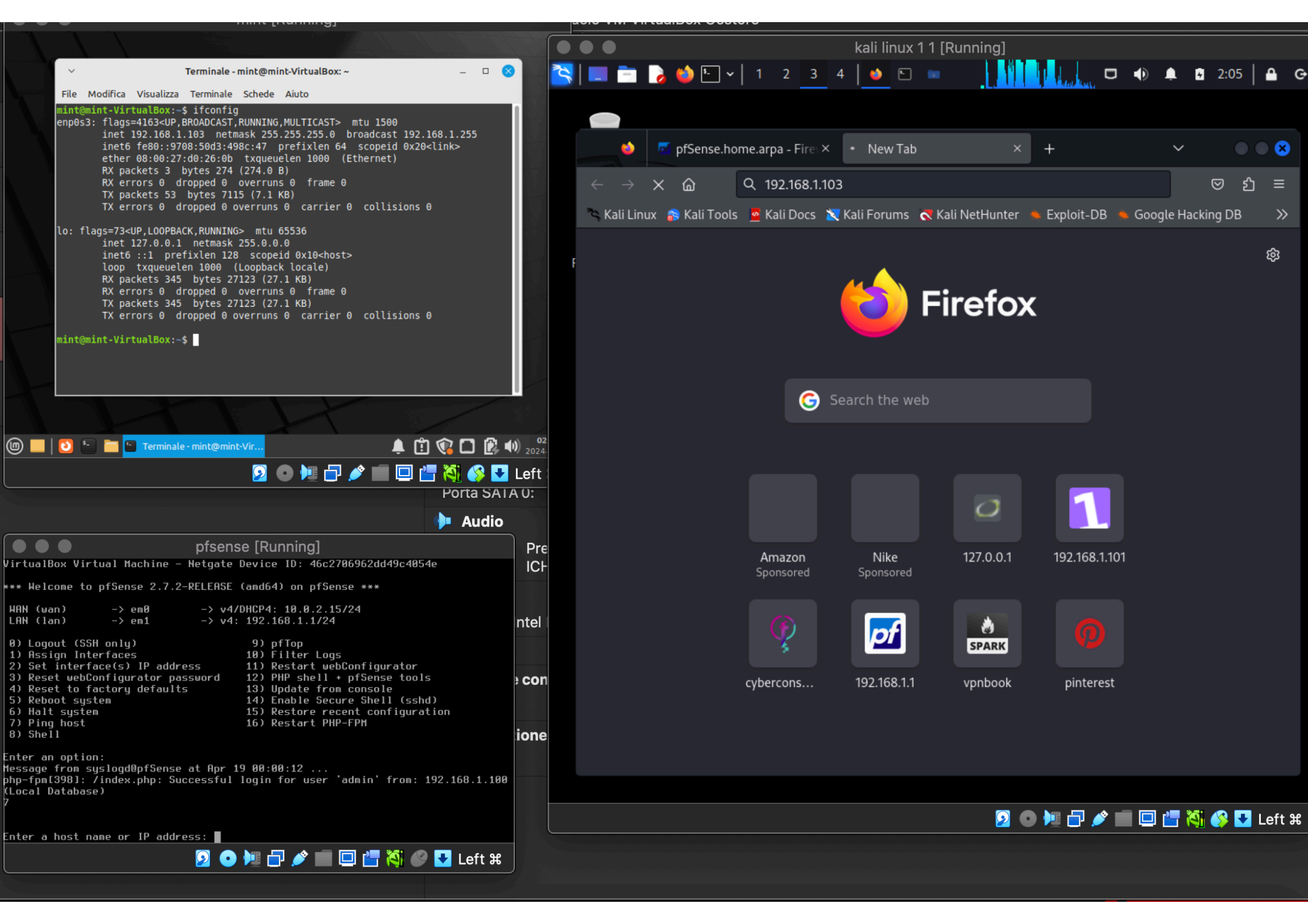
Nessuna

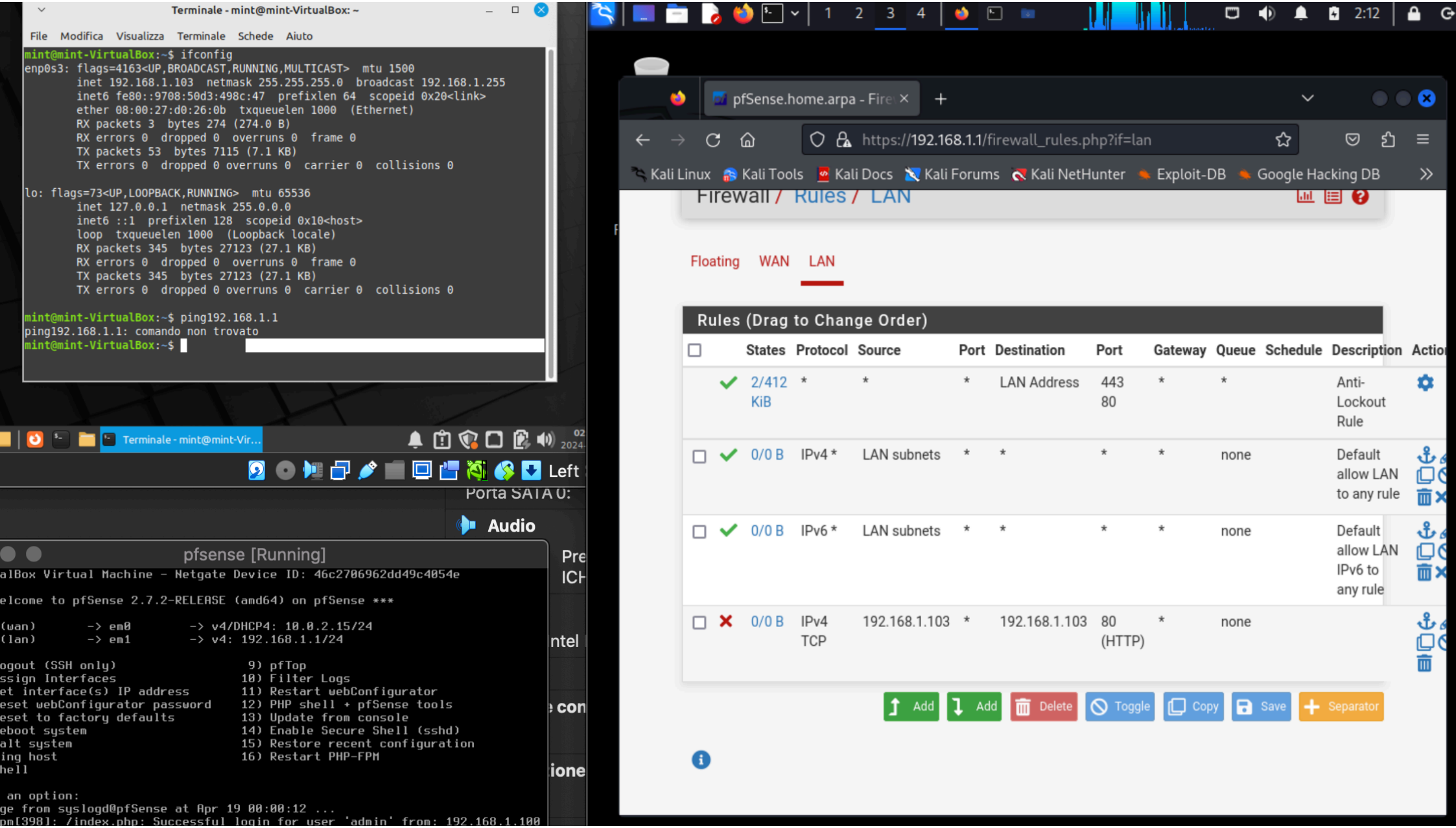
Descrizione

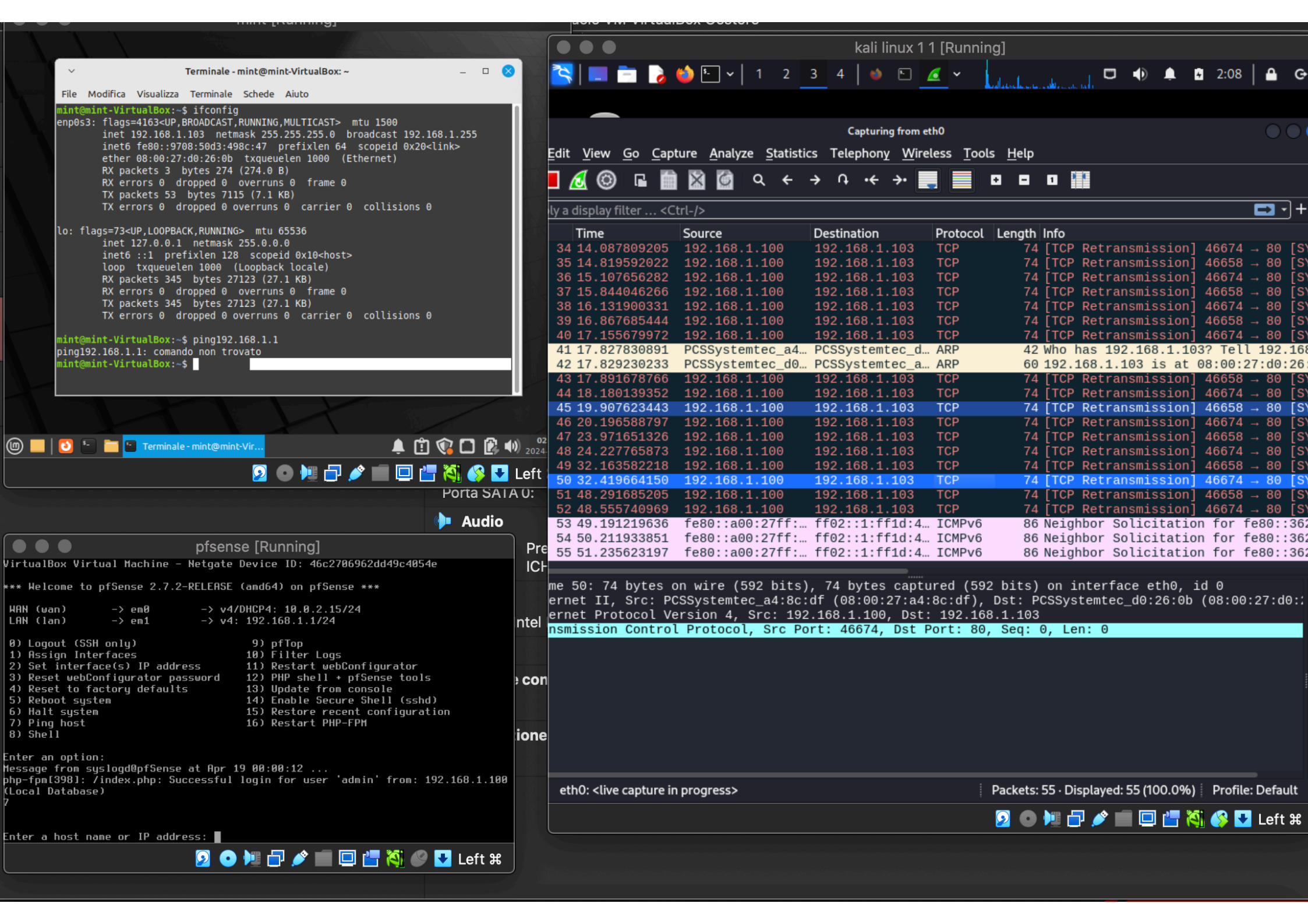
Nessuna

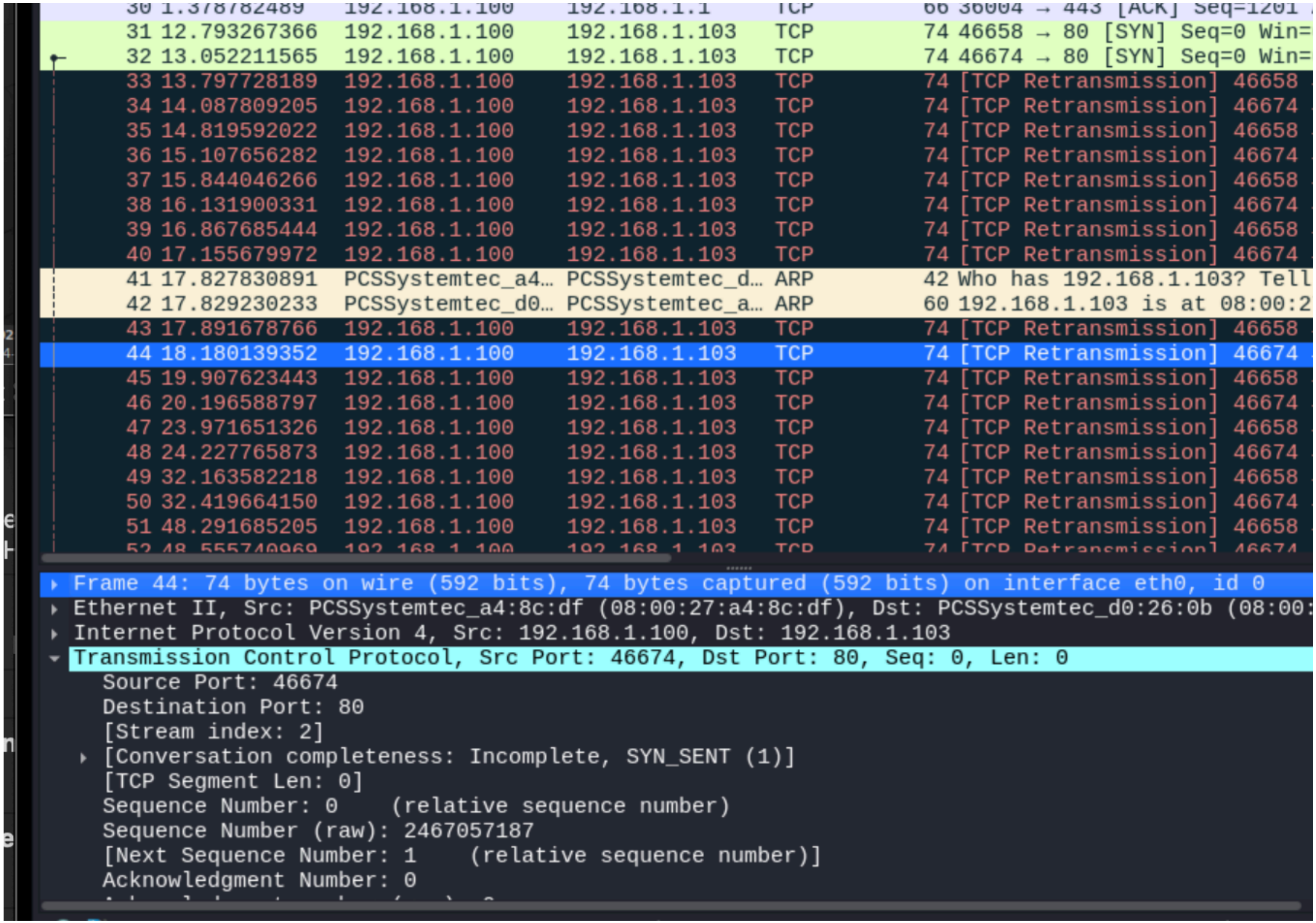

Oracle VM VirtualBox Gestore
Strumenti
Nuova
Aggiungi
metasploitable2 [Running]
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:51 errors:0 dropped:0 overruns:0 frame:0
TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5209 (5.0 KB) TX bytes:8171 (7.9 KB)
Base address:0xd020 Memory:f0200000-f0220000
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:114 errors:0 dropped:0 overruns:0 frame:0
TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:29797 (29.0 KB) TX bytes:29797 (29.0 KB)
msfadmin@metasploitable:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.25 ms
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 1.190/1.223/1.257/0.048 ms
msfadmin@metasploitable:~$
Left ⌘
pfsense [Running]
--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.083/1.235/1.460/0.162 ms
Press ENTER to continue.
VirtualBox Virtual Machine - Netgate Device ID: 46c2706962dd49c4054e
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
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: fire
Left ⌘
kali linux 1 1 [Running]
Trash
File System
Home
wireshark
putty.exe
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.23 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.00 ms
^C
— 192.168.1.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.003/1.621/3.233/0.932 ms
(kali㉿kali)-[~]
$
Left ⌘
kali linux 1
Debian (64
2048 MB
Floppy, Otti
Paginazione
16
1.2
VM
Dis
Dis
zione
Controller: IDE
Dispositivo IDE secondario 0:
Controller: SATA
0:
Predefinita
ICH AC97
Intel PRO/1000 MT
condivise
one

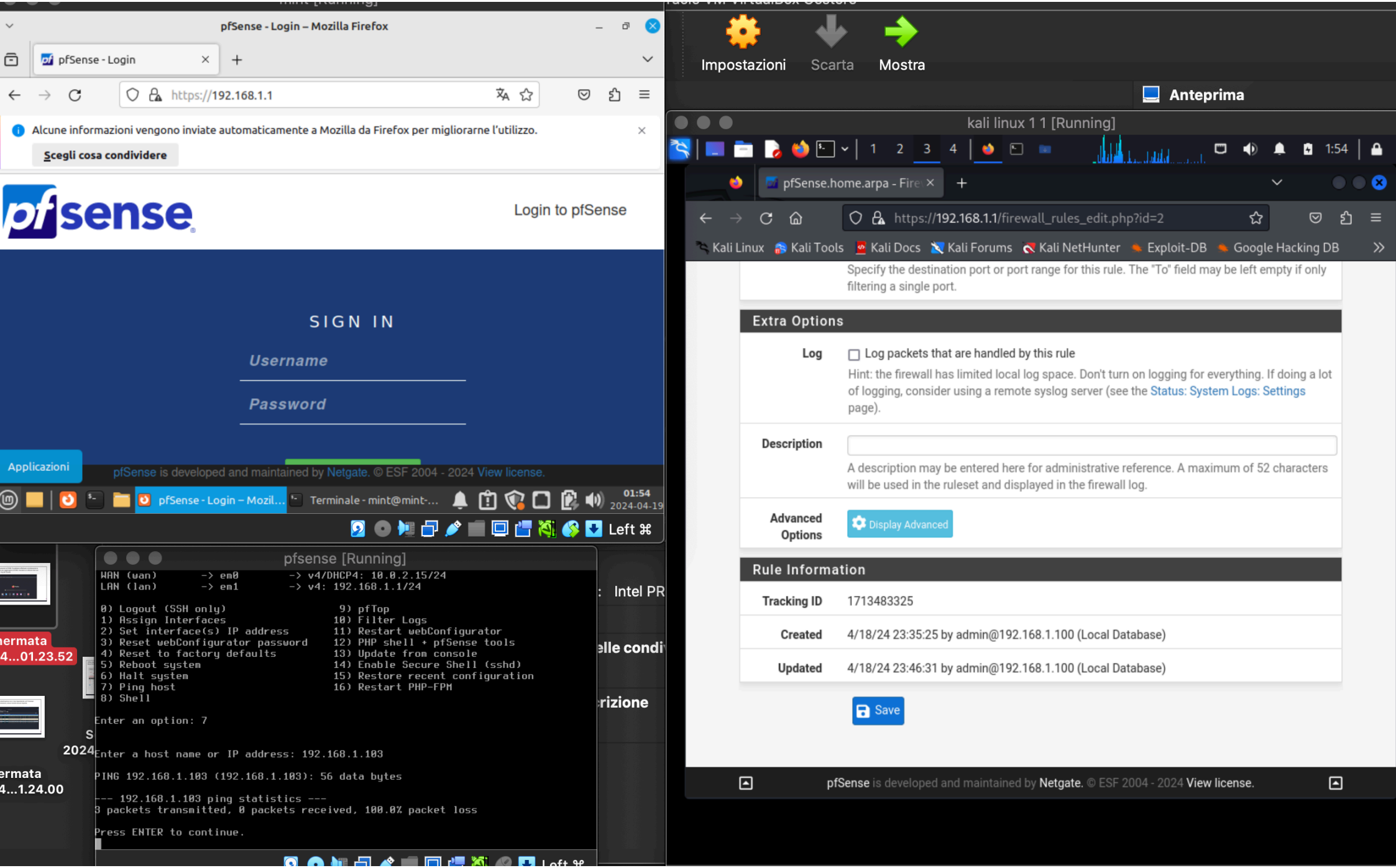

metasploitable2 [Running]
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Thu Apr 18 18:54:00 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
Left ⌘
kali linux 1 1 [Running]
1:30
pfSense.home.arpa - Stat
Metasploitable2 - Linux
192.168.1.101
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Reload current page (Ctrl+R)
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
Left ⌘
In esecuzione
Archiviazione
Controller: IDE
Dispositivo IDE sec
Controller: SATA
pfsense [Running]
5) Reboot system
6) Halt system
7) Ping host
8) Shell
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option: 7
Enter a host name or IP address: 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=63 time=52.060 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=46.410 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=47.230 ms
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 46.410/48.567/52.060/2.493 ms
Press ENTER to continue.
Message from syslogd@pfSense at Apr 18 23:29:37 ...
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.100
(Local Database)
Left ⌘


Terminale - mint@mint-VirtualBox: ~
File Modifica Visualizza Terminale Schede Aiuto
mint@mint-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::9708:50d3:498c:47 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:d0:26:0b txqueuelen 1000 (Ethernet)
RX packets 3 bytes 274 (274.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 53 bytes 7115 (7.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Loopback locale)
RX packets 345 bytes 27123 (27.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 345 bytes 27123 (27.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
mint@mint-VirtualBox:~$
Terminale - mint@mint-Vir...
Left
Porta SATA 0:
Audio
pfsense [Running]
VirtualBox Virtual Machine - Netgate Device ID: 46c2706962dd49c4054e
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only) 9) pfTop
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell
Enter an option:
Message from syslogd@pfSense at Apr 19 00:00:12 ...
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.100
(Local Database)
7
Enter a host name or IP address:
Left ⌘
kali linux 1 1 [Running]
1 2 3 4
2:05
pfSense.home.arpa - Fire
New Tab
192.168.1.103
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Firefox
Search the web
Amazon
Sponsored
Nike
Sponsored
127.0.0.1
192.168.1.101
cybercons...
192.168.1.1
vpnbook
pinterest
Left ⌘


Terminale - mint@mint-VirtualBox: ~
File Modifica Visualizza Terminale Schede Aiuto
mint@mint-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::9708:50d3:498c:47 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:d0:26:0b txqueuelen 1000 (Ethernet)
RX packets 3 bytes 274 (274.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 53 bytes 7115 (7.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Loopback locale)
RX packets 345 bytes 27123 (27.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 345 bytes 27123 (27.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
mint@mint-VirtualBox:~$ ping192.168.1.1
ping192.168.1.1: comando non trovato
mint@mint-VirtualBox:~$
Terminale - mint@mint-Vir...
Left
Porta SATA 0:
Audio
pfsense [Running]
alBox Virtual Machine - Netgate Device ID: 46c2706962dd49c4054e
elcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
(wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
(lan) -> em1 -> v4: 192.168.1.1/24
ogout (SSH only) 9) pfTop
ssign Interfaces 10) Filter Logs
et interface(s) IP address 11) Restart webConfigurator
eset webConfigurator password 12) PHP shell + pfSense tools
eset to factory defaults 13) Update from console
eboot system 14) Enable Secure Shell (sshd)
alt system 15) Restore recent configuration
ing host 16) Restart PHP-FPM
hell
an option:
ge from syslogd@pfSense at Apr 19 00:00:12 ...
pm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.100
pfSense.home.arpa - Fire
https://192.168.1.1/firewall_rules.php?if=lan
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Firewall / Rules / LAN
Floating WAN LAN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actio
2/412 KiB * * * LAN Address 443 80 * * Anti-Lockout Rule
0/0 B IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
0/0 B IPv4 TCP 192.168.1.103 * 192.168.1.103 80 (HTTP) * none
Add Add Delete Toggle Copy Save Separator


Terminale - mint@mint-VirtualBox: ~
File Modifica Visualizza Terminale Schede Aiuto
mint@mint-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::9708:50d3:498c:47 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:d0:26:0b txqueuelen 1000 (Ethernet)
RX packets 3 bytes 274 (274.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 53 bytes 7115 (7.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Loopback locale)
RX packets 345 bytes 27123 (27.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 345 bytes 27123 (27.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
mint@mint-VirtualBox:~$ ping192.168.1.1
ping192.168.1.1: comando non trovato
mint@mint-VirtualBox:~$
Terminale - mint@mint-Vir...
kali linux 1 1 [Running]
Capturing from eth0
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source Destination Protocol Length Info
34 14.087809205 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
35 14.819592022 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
36 15.107656282 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
37 15.844046266 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
38 16.131900331 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
39 16.867685444 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
40 17.155679972 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
41 17.827830891 PCSSystemtec_a4… PCSSystemtec_d… ARP 42 Who has 192.168.1.103? Tell 192.168
42 17.829230233 PCSSystemtec_d0… PCSSystemtec_a… ARP 60 192.168.1.103 is at 08:00:27:d0:26:
43 17.891678766 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
44 18.180139352 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
45 19.907623443 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
46 20.196588797 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
47 23.971651326 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
48 24.227765873 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
49 32.163582218 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
50 32.419664150 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
51 48.291685205 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658 → 80
52 48.555740969 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674 → 80
53 49.191219636 fe80::a00:27ff:… ff02::1:ff1d:4… ICMPv6 86 Neighbor Solicitation for fe80::362
54 50.211933851 fe80::a00:27ff:… ff02::1:ff1d:4… ICMPv6 86 Neighbor Solicitation for fe80::362
55 51.235623197 fe80::a00:27ff:… ff02::1:ff1d:4… ICMPv6 86 Neighbor Solicitation for fe80::362
me 50: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
ernet II, Src: PCSSystemtec_a4:8c:df (08:00:27:a4:8c:df), Dst: PCSSystemtec_d0:26:0b (08:00:27:d0:
ernet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.103
nsmission Control Protocol, Src Port: 46674, Dst Port: 80, Seq: 0, Len: 0
eth0: <live capture in progress>
Packets: 55 · Displayed: 55 (100.0%)
Profile: Default
Left ⌘
pfsense [Running]
VirtualBox Virtual Machine - Netgate Device ID: 46c2706962dd49c4054e
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only) 9) pfTop
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell
Enter an option:
Message from syslogd@pfSense at Apr 19 00:00:12 ...
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.100
(Local Database)
7
Enter a host name or IP address:
Left ⌘
Left
Porta SATA 0:
Audio


30 1.378782489 192.168.1.100 192.168.1.1 TCP 66 36004 → 443 [ACK] Seq=1201
31 12.793267366 192.168.1.100 192.168.1.103 TCP 74 46658 → 80 [SYN] Seq=0 Win=
32 13.052211565 192.168.1.100 192.168.1.103 TCP 74 46674 → 80 [SYN] Seq=0 Win=
33 13.797728189 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
34 14.087809205 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
35 14.819592022 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
36 15.107656282 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
37 15.844046266 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
38 16.131900331 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
39 16.867685444 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
40 17.155679972 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
41 17.827830891 PCSSystemtec_a4… PCSSystemtec_d… ARP 42 Who has 192.168.1.103? Tell
42 17.829230233 PCSSystemtec_d0… PCSSystemtec_a… ARP 60 192.168.1.103 is at 08:00:2
43 17.891678766 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
44 18.180139352 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
45 19.907623443 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
46 20.196588797 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
47 23.971651326 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
48 24.227765873 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
49 32.163582218 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
50 32.419664150 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46674
51 48.291685205 192.168.1.100 192.168.1.103 TCP 74 [TCP Retransmission] 46658
Frame 44: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_a4:8c:df (08:00:27:a4:8c:df), Dst: PCSSystemtec_d0:26:0b (08:00:
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.103
Transmission Control Protocol, Src Port: 46674, Dst Port: 80, Seq: 0, Len: 0
Source Port: 46674
Destination Port: 80
[Stream index: 2]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2467057187
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0


pfSense - Login – Mozilla Firefox
pfSense - Login
https://192.168.1.1
Alcune informazioni vengono inviate automaticamente a Mozilla da Firefox per migliorarne l'utilizzo.
Scegli cosa condividere
pfsense
Login to pfSense
SIGN IN
Username
Password
Applicazioni
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
pfSense - Login – Mozil...
Terminale - mint@mint-...
01:54
2024-04-19
Left ⌘
pfsense [Running]
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
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: 7
Enter a host name or IP address: 192.168.1.103
PING 192.168.1.103 (192.168.1.103): 56 data bytes
--- 192.168.1.103 ping statistics ---
8 packets transmitted, 0 packets received, 100.0% packet loss
Press ENTER to continue.
Impostazioni
Scarta
Mostra
Anteprima
kali linux 1 1 [Running]
pfSense.home.arpa - Fire
https://192.168.1.1/firewall_rules_edit.php?id=2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Rule Information
Tracking ID
1713483325
Created
4/18/24 23:35:25 by admin@192.168.1.100 (Local Database)
Updated
4/18/24 23:46:31 by admin@192.168.1.100 (Local Database)
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.