

Progetto Firewall

Obbiettivo:

creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

screen 1

```
You can now access the webConfigurator by opening the following URL in your web browser:
      http://192.168.70.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 8a206f5da3f4fde0baeb

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.0.73/24
                                   v6: 2a0e:416:c1e8:0:a00:27ff:fe12:de2e/64
LAN (lan)      -> vtnet1      -> v4: 192.168.10.1/24
OPT1 (opt1)    -> em0         -> v4: 192.168.70.1/24

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: 
```



Session Actions Edit View Help

(kali@kali)-[~]

\$ ping 192.168.70.10

PING 192.168.70.10 (192.168.70.10) 56(84) bytes of data.

64 bytes from 192.168.70.10: icmp_seq=1 ttl=63 time=5.49 ms

64 bytes from 192.168.70.10: icmp_seq=2 ttl=63 time=25.1 ms

64 bytes from 192.168.70.10: icmp_seq=3 ttl=63 time=2.15 ms

64 bytes from 192.168.70.10: icmp_seq=4 ttl=63 time=14.7 ms

64 bytes from 192.168.70.10: icmp_seq=5 ttl=63 time=5.39 ms

^C

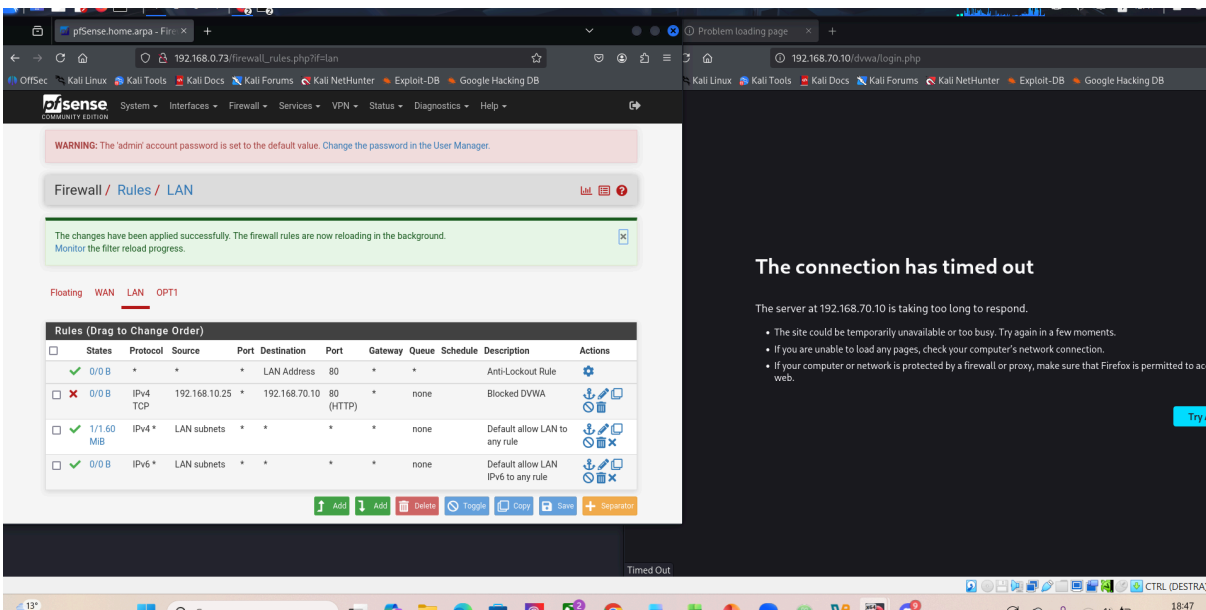
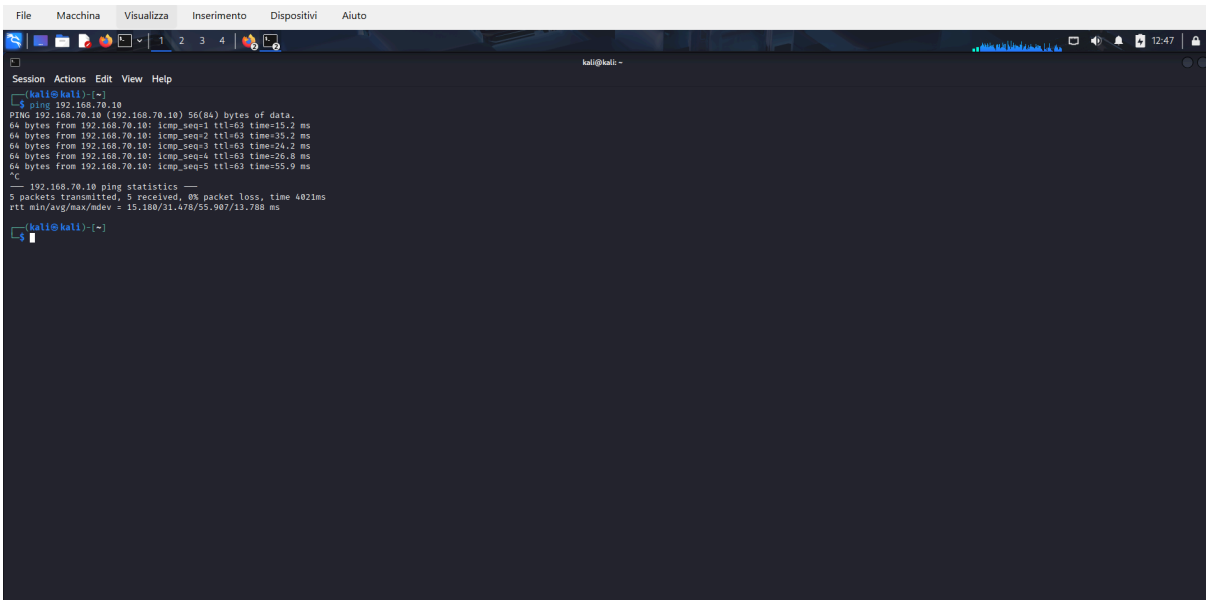
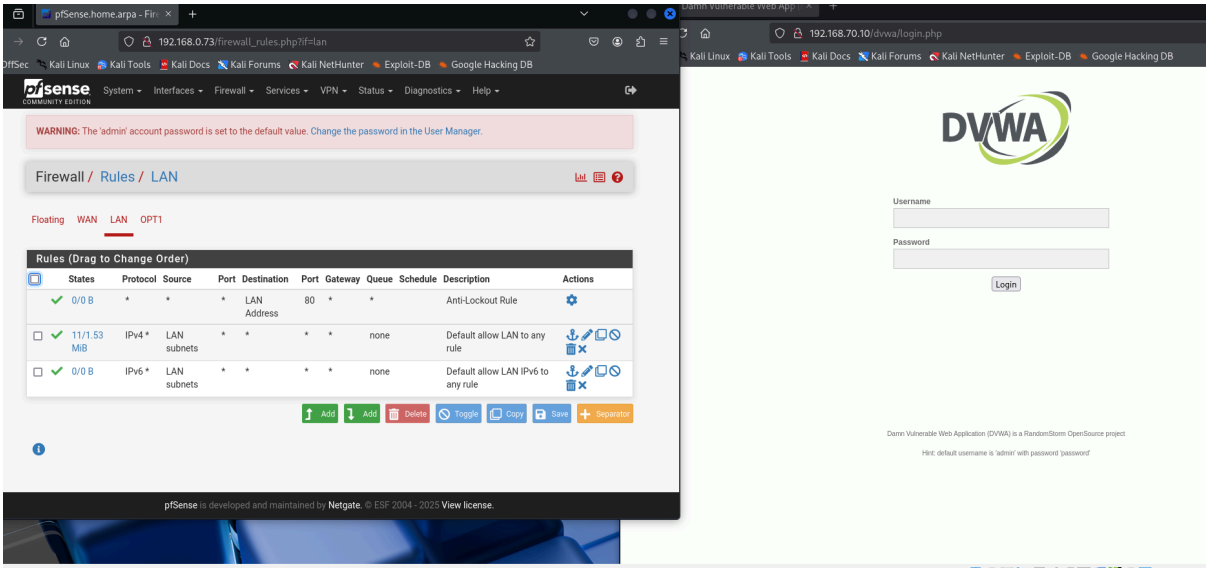
— 192.168.70.10 ping statistics —

5 packets transmitted, 5 received, 0% packet loss, time 4139ms

rtt min/avg/max/mdev = 2.151/10.579/25.149/8.406 ms

(kali@kali)-[~]

\$



192.168.0.73/firewall_rules.php?f=opt1

Kali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DB

pfSense

COMMUNITY EDITION

SystemInterfacesFirewallServicesVPNStatusDiagnosticsHelp

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / OPT1

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

FloatingWANLANOPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	↕ ✎ 🔄 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	↕ ✎ 🔄 🗑️ ✖

[↑ Add](#)[↓ Add](#)[🗑️ Delete](#)[🔄 Toggle](#)[📄 Copy](#)[💾 Save](#)[+ Separator](#)

Kali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DB

pfSense

COMMUNITY EDITION

SystemInterfacesFirewallServicesVPNStatusDiagnosticsHelp

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / WAN

FloatingWANLANOPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/26 KiB	*	RFC 1918 networks	*	*	*	*	*	Block private networks	⚙️
<input type="checkbox"/>	✗	0/1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	Block bogon networks	⚙️

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. [Click the button to add a new rule.](#)

[↑ Add](#)[↓ Add](#)[🗑️ Delete](#)[🔄 Toggle](#)[📄 Copy](#)[💾 Save](#)[+ Separator](#)