Obbiettivo:

1) Obiettivo e requisiti dell'esercizio (da mettere a inizio report)

L'obiettivo è **creare una regola firewall su pfSense** che **blocchi l'accesso alla DVWA** ospitata su Metasploitable dalla macchina Kali e che, di conseguenza, **renda inefficace lo scan** verso quel servizio. Un requisito fondamentale è che **Kali e Metasploitable siano su reti diverse**, quindi pfSense deve gestire **almeno due reti interne** (oltre alla WAN) tramite una **nuova interfaccia** abilitata e configurata dalla WebGUI.

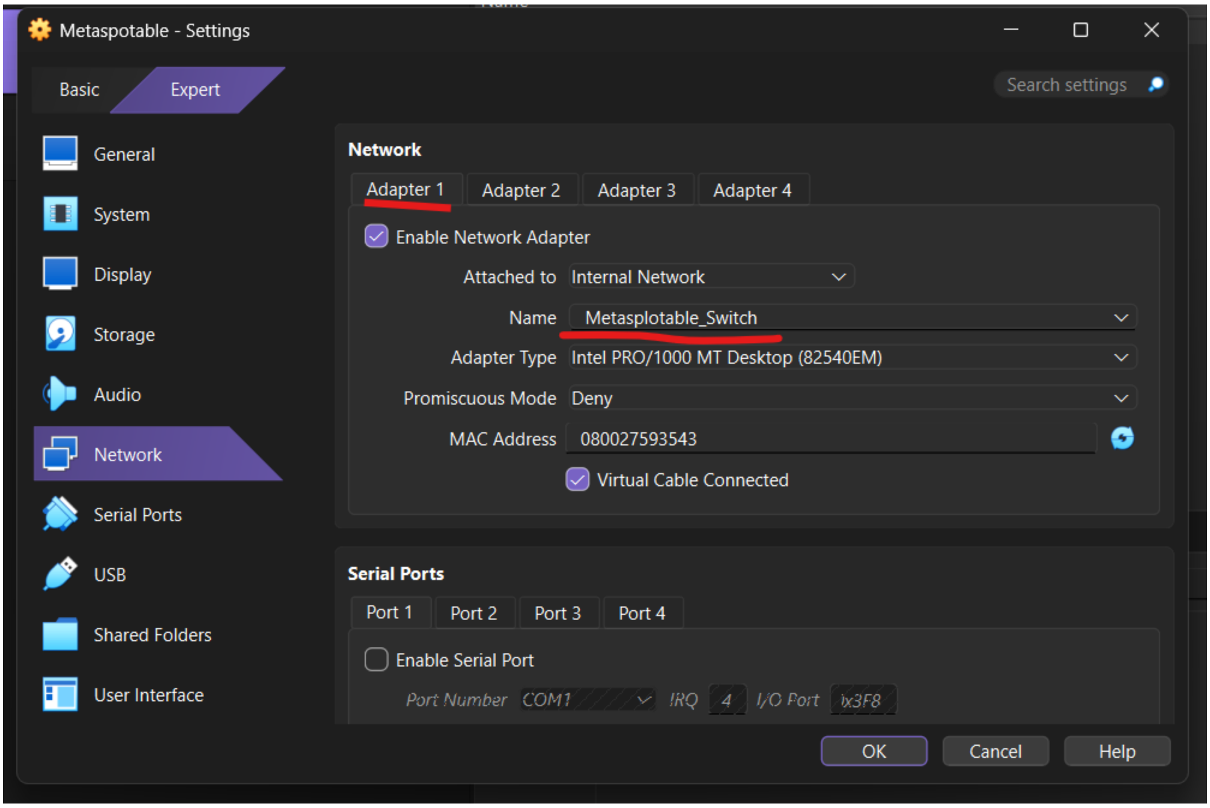
Configurazione Network delle tre macchine Virtuali

Ho realizzato una topologia a **3 macchine virtuali**:

- **pfSense** come router/firewall centrale (punto di controllo del traffico tra reti)
- **Kali Linux** (attaccante / scanner)
- **Metasploitable2** che ospita **DVWA** (target)

La separazione in reti diverse è importante perché, se Kali e Metasploitable fossero nella **stessa subnet**, il traffico passerebbe in locale (L2) e il firewall non vedrebbe/filtrerebbe correttamente quel traffico. Separandole, invece, ogni pacchetto Kali → Metasploitable è costretto a passare dal routing di pfSense, e quindi può essere filtrato tramite regole.

Configurazione **Mtasploitable** Adapter1



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: Metasplotable_Switch

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027593543

☑ Virtual Cable Connected

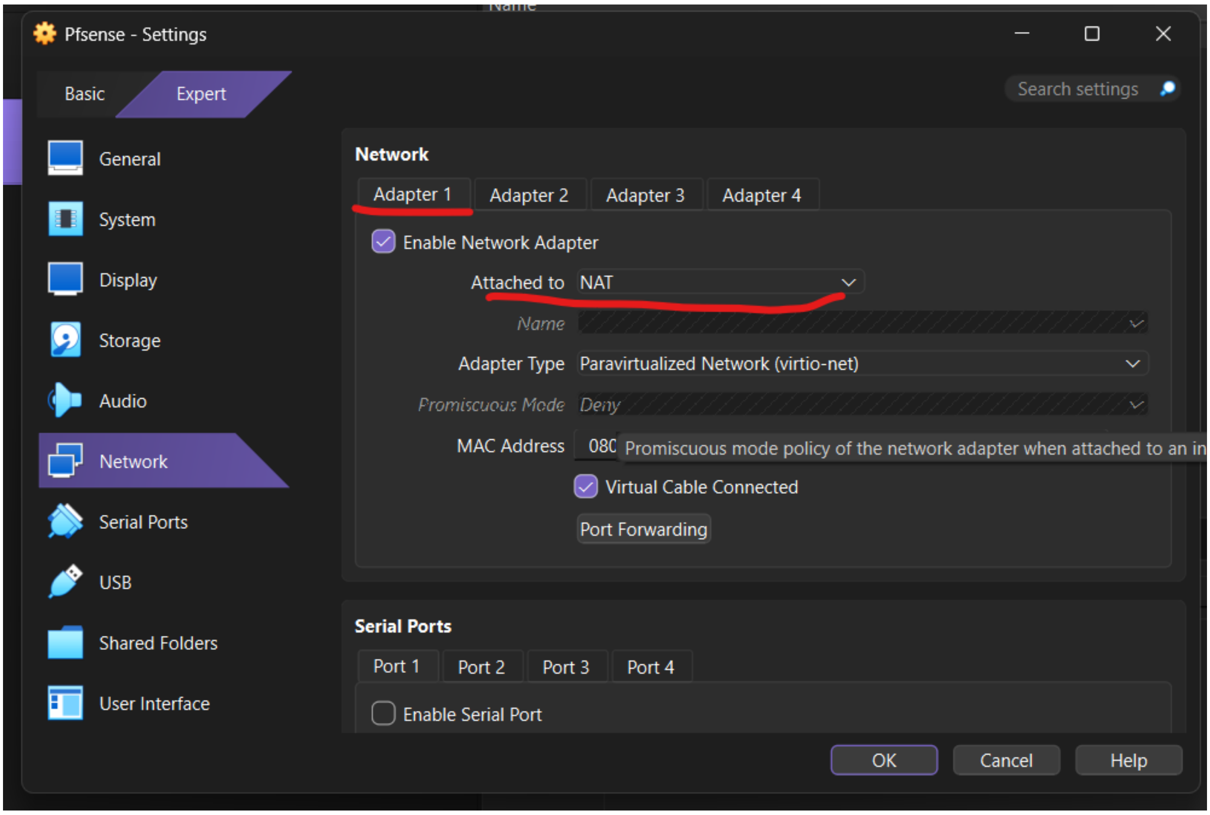
Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

☐ Enable Serial Port

Port Number: COM1 IRQ: 4 I/O Port: 0x3F8 pfSense è configurato con **3 schede di rete**: una per la WAN e due per le LAN interne (una verso Kali e una verso Metasploitable). Questo permette di creare due domini di broadcast separati e far sì che pfSense faccia da **gateway** tra le due reti interne.

Configurazione **PsSense** Adapter 01



Pfsense - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Paravirtualized Network (virtio-net)

Promiscuous Mode: Deny

MAC Address: 080

Promiscuous mode policy of the network adapter when attached to an in

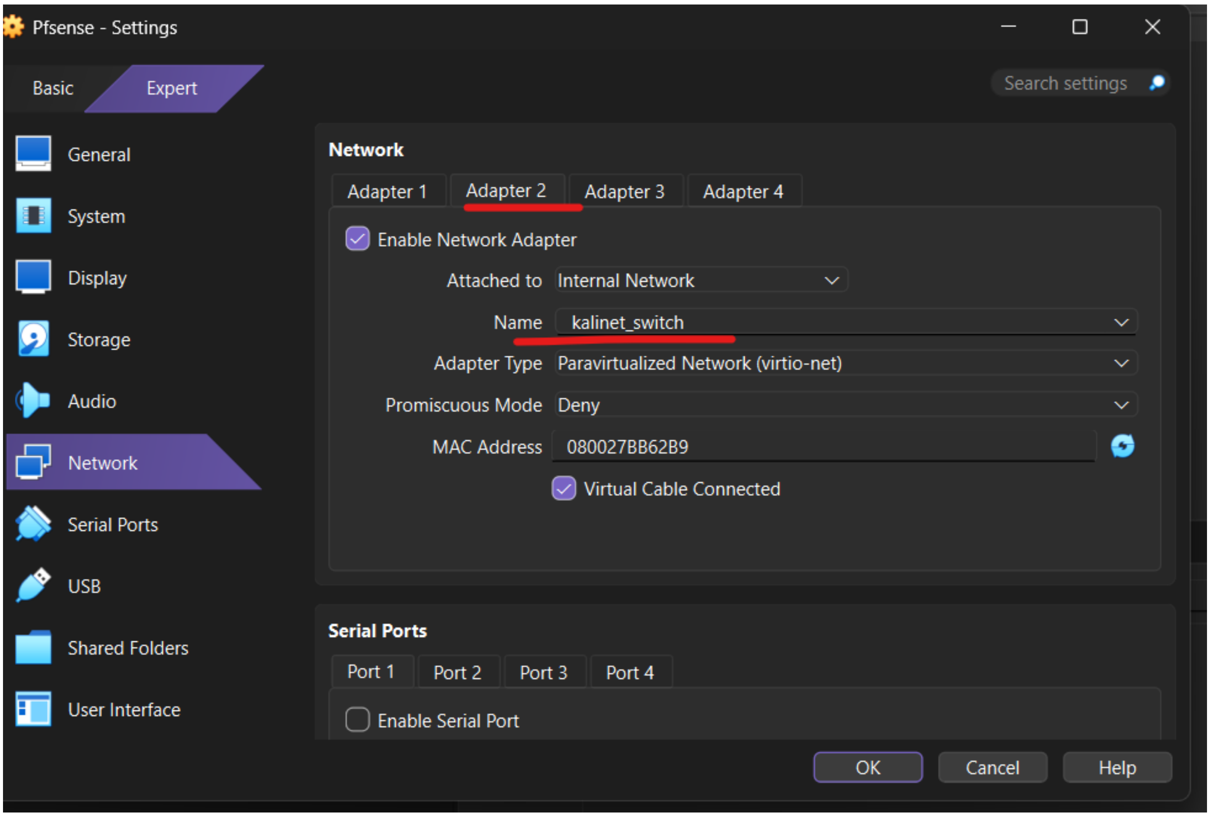
☑ Virtual Cable Connected

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

□ Enable Serial Port

Configurazione **PsSense** Adapter 02



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: kalinet_switch

Adapter Type: Paravirtualized Network (virtio-net)

Promiscuous Mode: Deny

MAC Address: 080027BB62B9

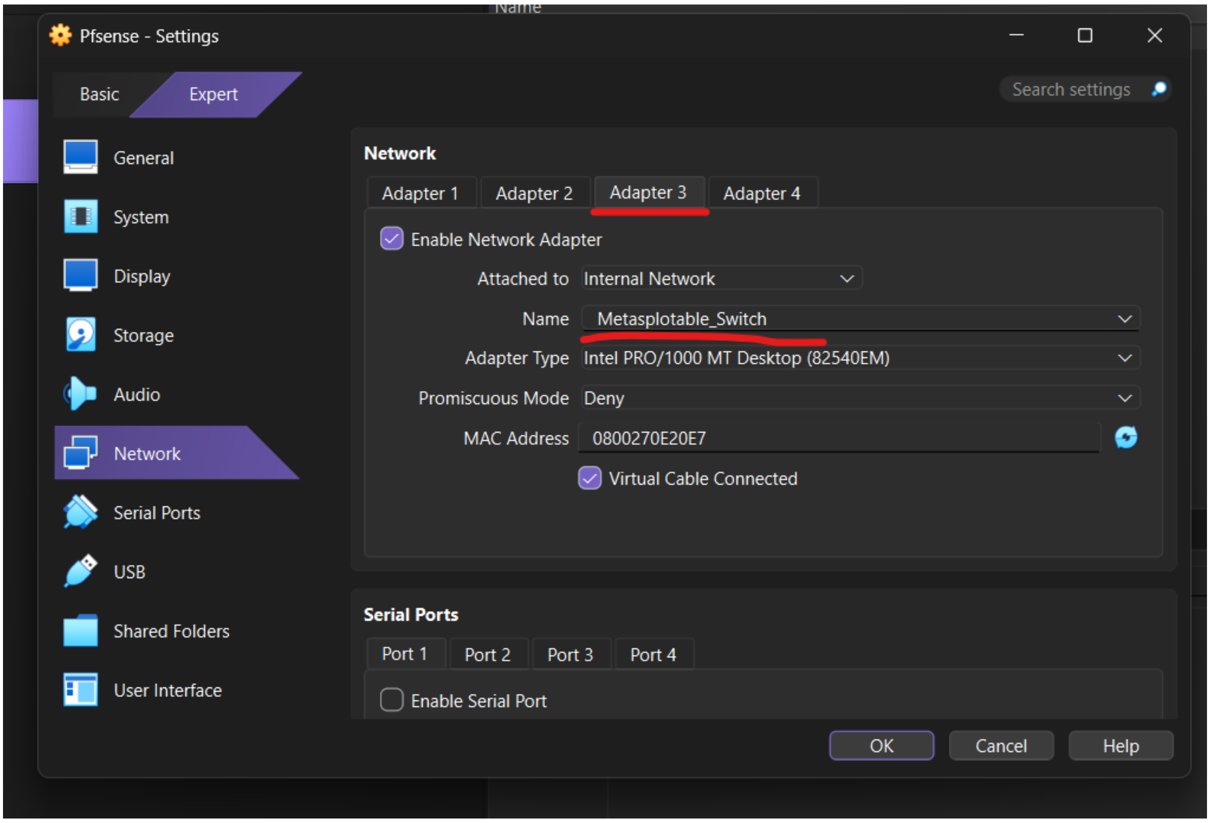
☑ Virtual Cable Connected

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

☐ Enable Serial Port

Configurazione **PsSense** Adapter 03



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: Metasplotable_Switch

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800270E20E7

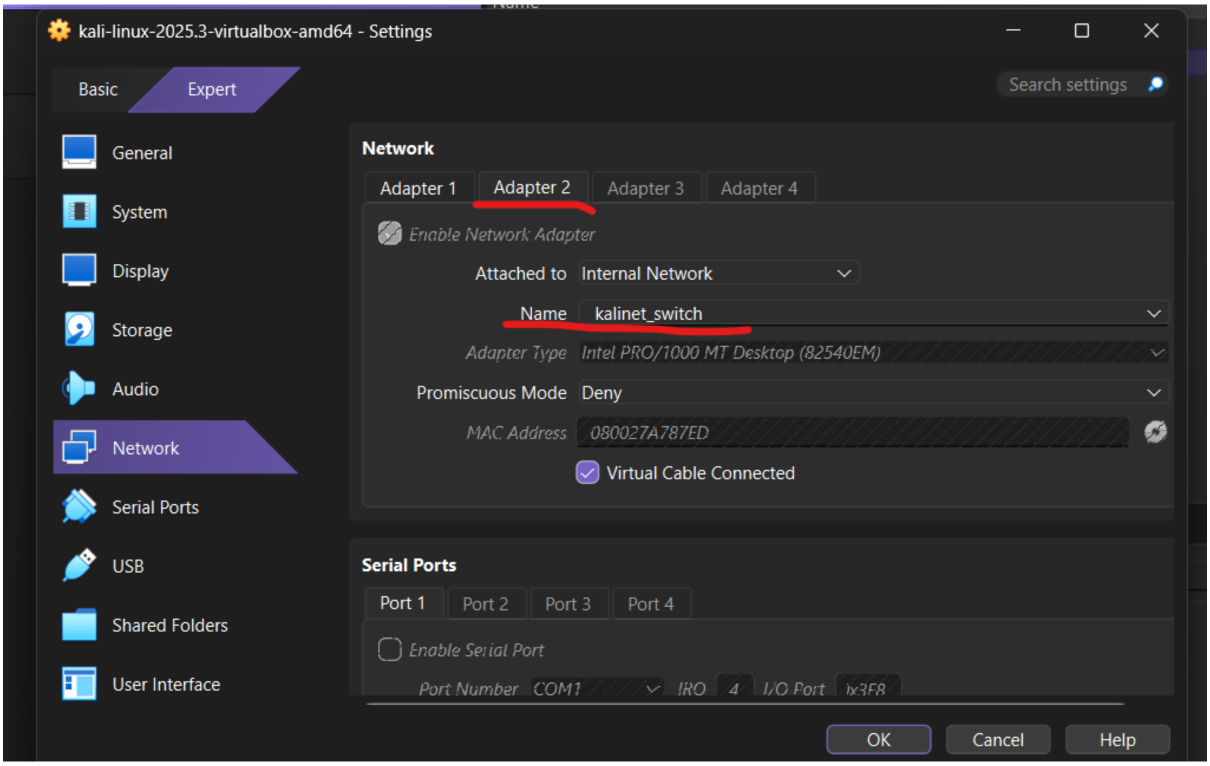
☑ Virtual Cable Connected

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

☐ Enable Serial Port

Configurazione **Kali** Adapter 01



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ *Enable Network Adapter*

Attached to: Internal Network

Name: kalinet_switch

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027A787ED

☑ Virtual Cable Connected

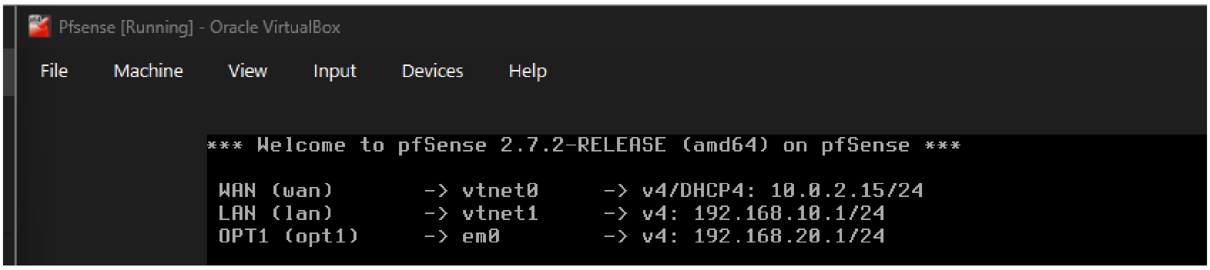
Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

□ *Enable Serial Port*

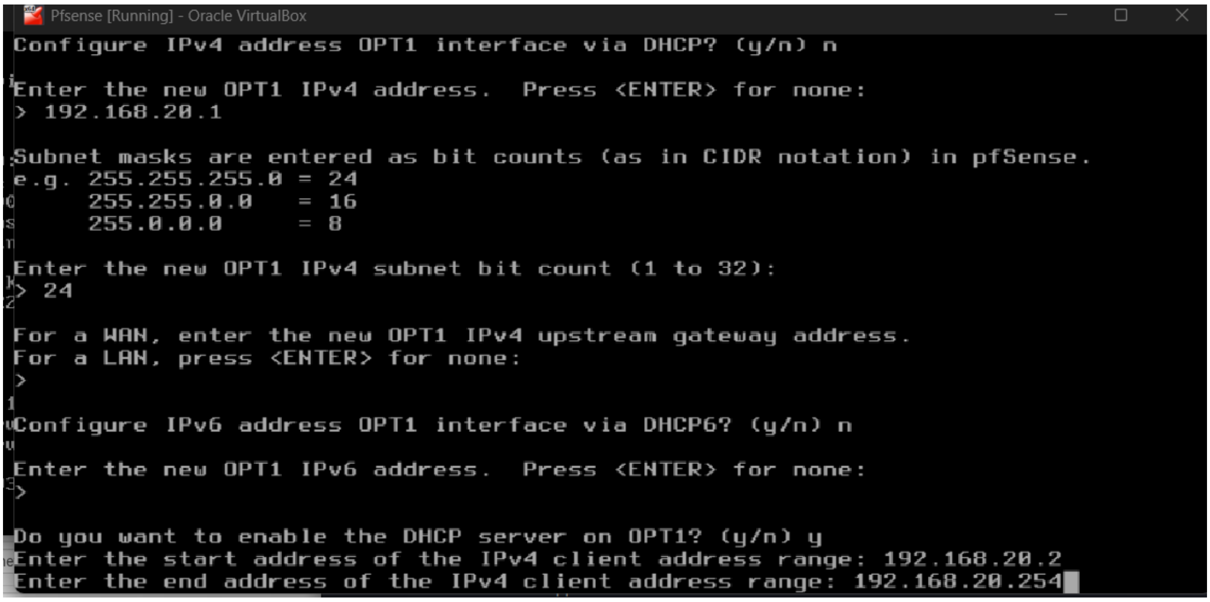
Port Number: COM1 IRQ: 4 I/O Port: 0x3F8

PSense 3 schede di rete e gli ip associati:



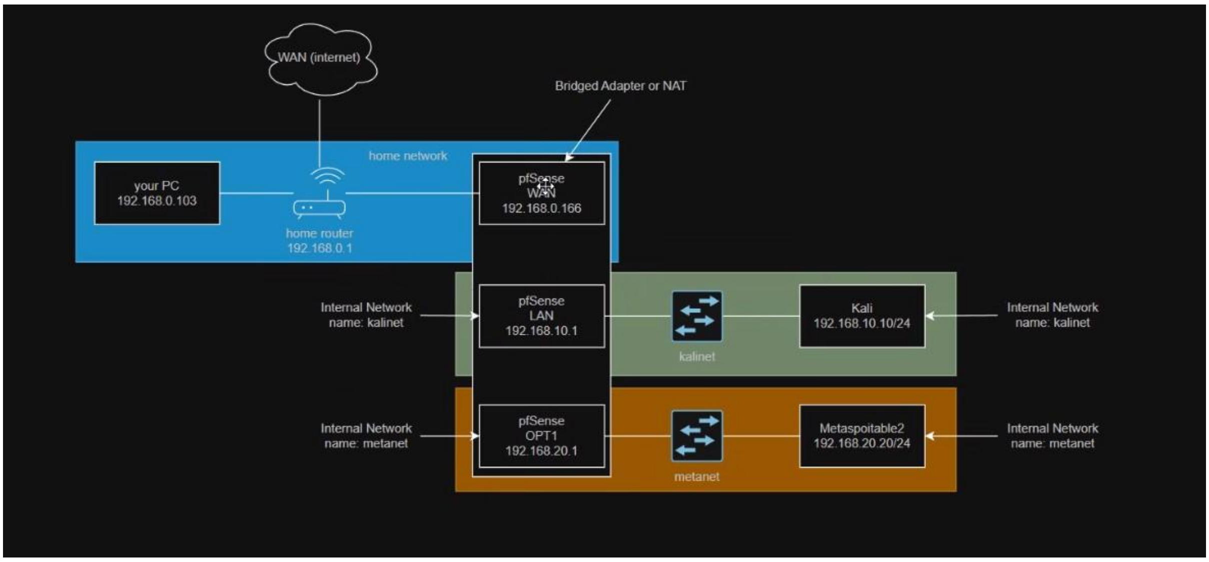
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.10.1/24
 OPT1 (opt1)     -> em0        -> v4: 192.168.20.1/24
```

PfSense Configuration gateway range
Network 1:
Start Address Range: 192.268.10.2
End Address Rage: 192.268.10.254
Network 2:
Start Address Range: 192.268.20.2
End Address Rage: 192.268.20.254

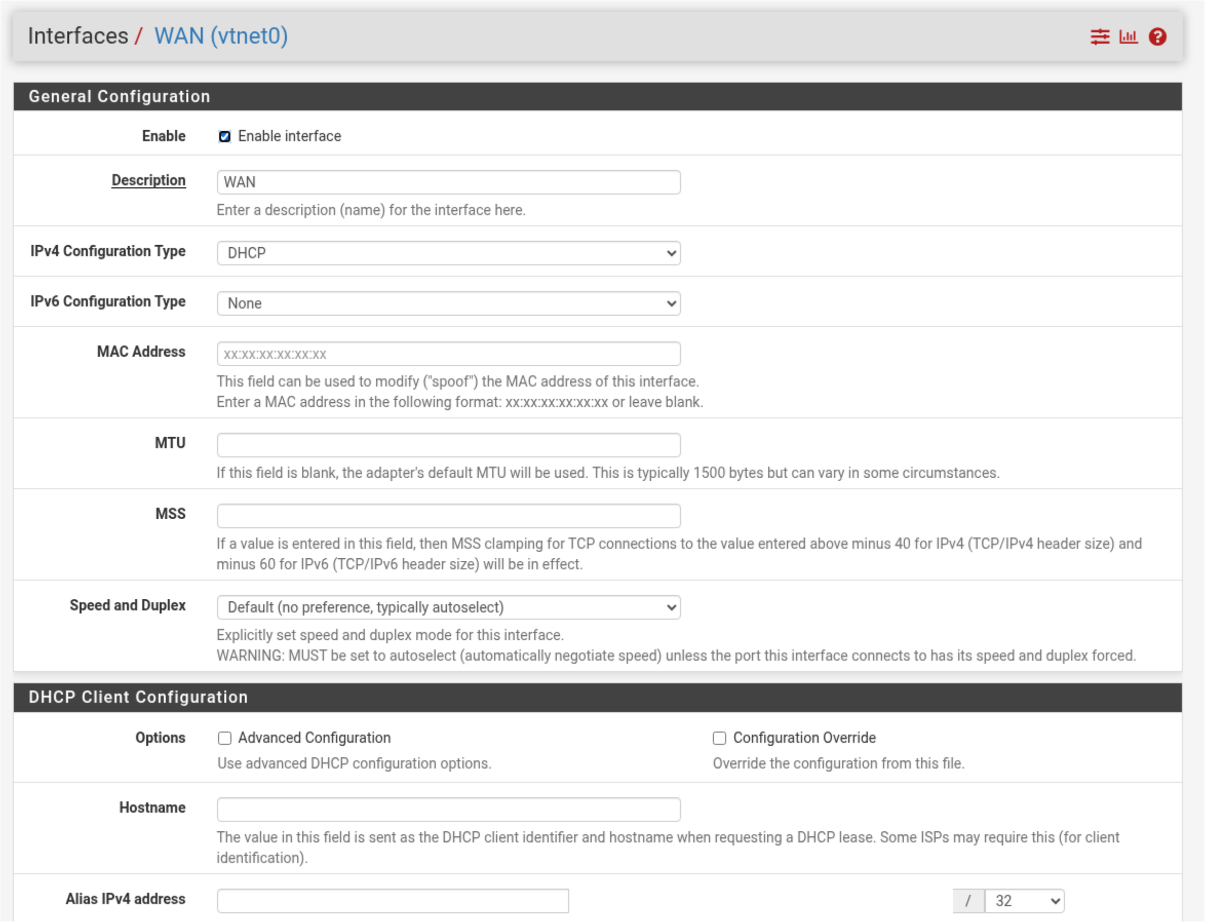


```
Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.20.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.20.2
Enter the end address of the IPv4 client address range: 192.168.20.254
```

Topologico Ottenuto:



Screenshot Firewall rules **WAN**:



Interfaces / WAN (vtnet0)

General Configuration

Enable ☑ Enable interface

Description WAN
Enter a description (name) for the interface here.

IPv4 Configuration Type DHCP

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

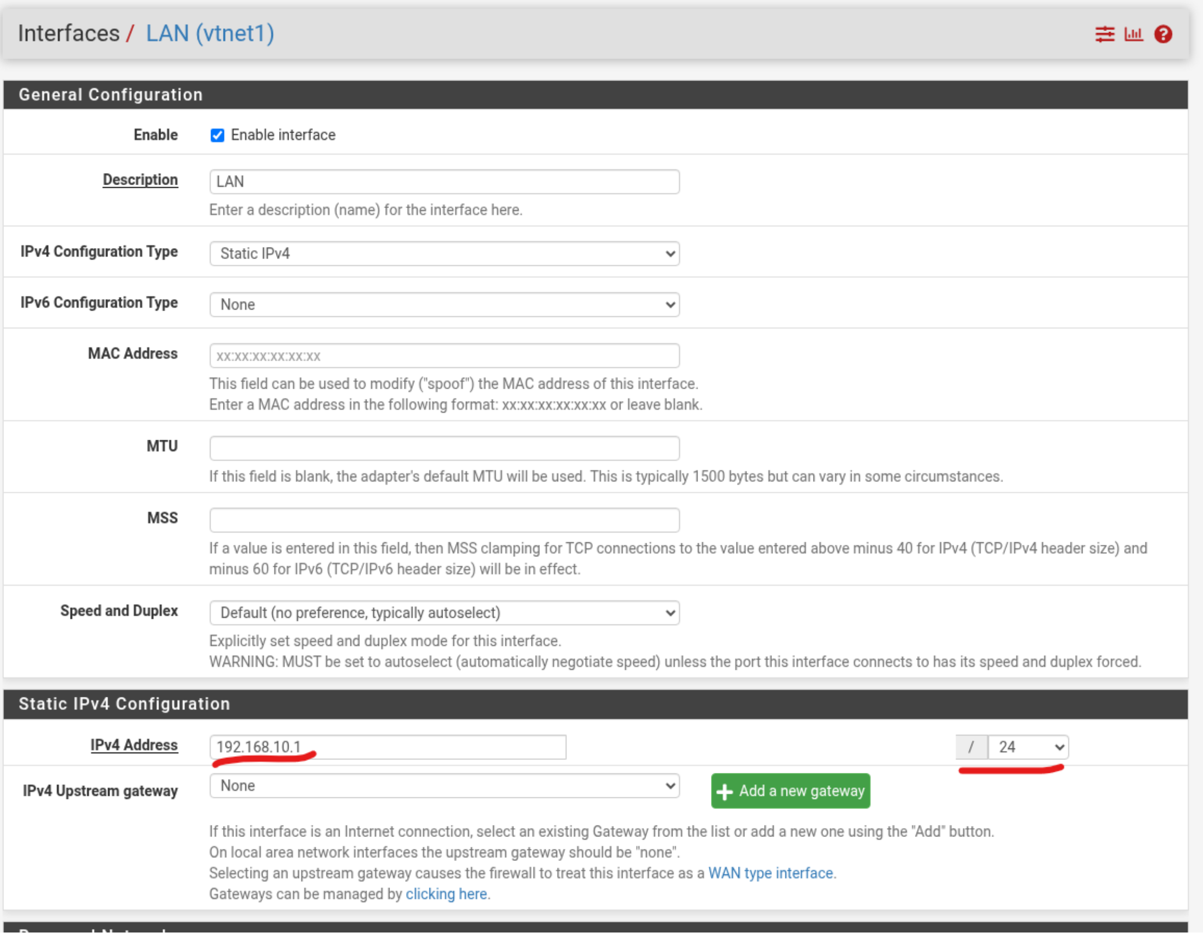
DHCP Client Configuration

Options □ Advanced Configuration
Use advanced DHCP configuration options.
□ Configuration Override
Override the configuration from this file.

Hostname
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Alias IPv4 address / 32

Screenshot Firewall rules LAN



Interfaces / LAN (vtnet1)

General Configuration

Enable ☑ Enable interface

Description LAN
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

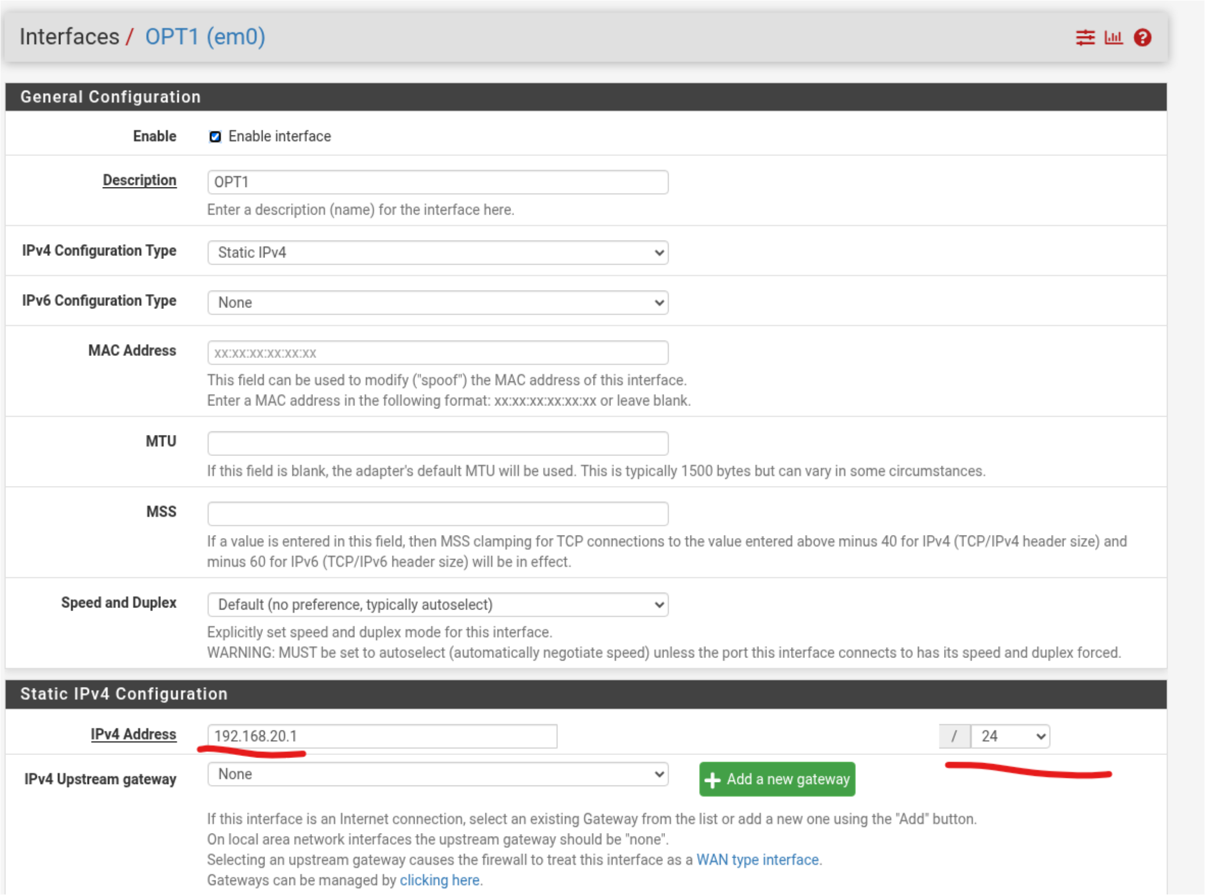
Static IPv4 Configuration

IPv4 Address 192.168.10.1 / 24

IPv4 Upstream gateway None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.

Screenshot Firewall rules **OPT1**



Interfaces / OPT1 (em0)

General Configuration

Enable: ☑ Enable interface

Description: OPT1
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

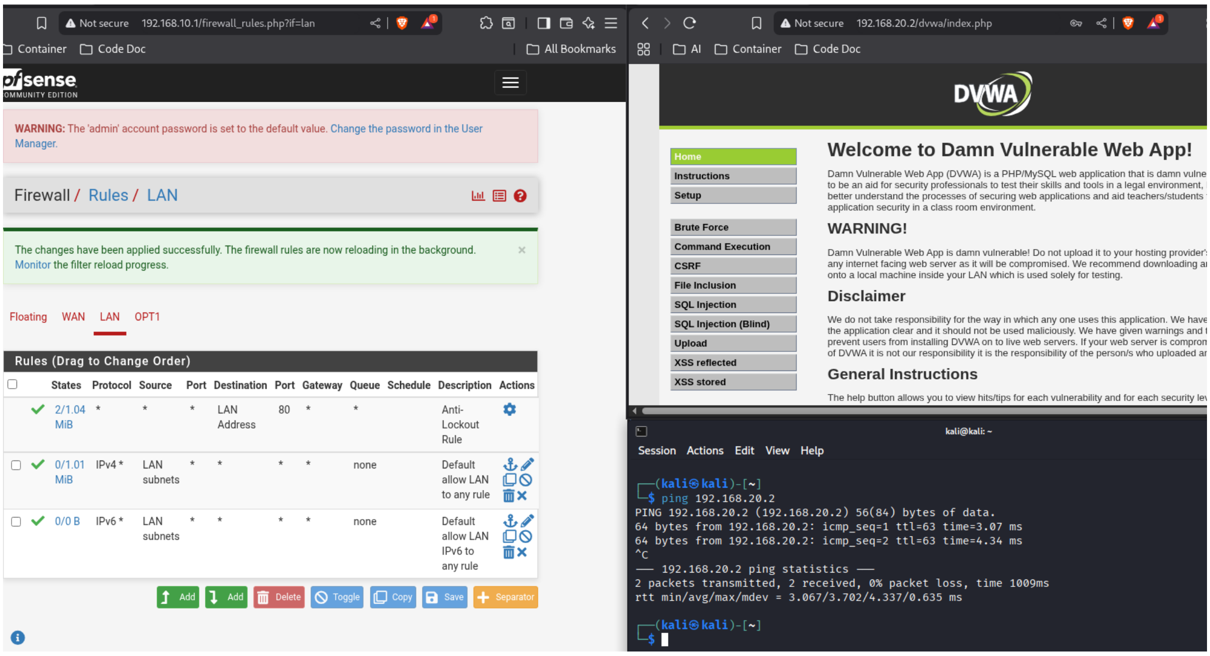
Static IPv4 Configuration

IPv4 Address: 192.168.20.1 / 24

IPv4 Upstream gateway: None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.

Screeenshot browser della Kali che apre la pagina DVWA servita dalla Metasploitable2 + il protocollo ICMP raggiungibile.



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

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	2/1.04 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□	✓	0/1.01 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	

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulne
to be an aid for security professionals to test their skills and tools in a legal environment,
better understand the processes of securing web applications and aid teachers/students
application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider'
any internet facing web server as it will be compromised. We recommend downloading a
onto a local machine inside your LAN which is used solely for testing.

Disclaimer

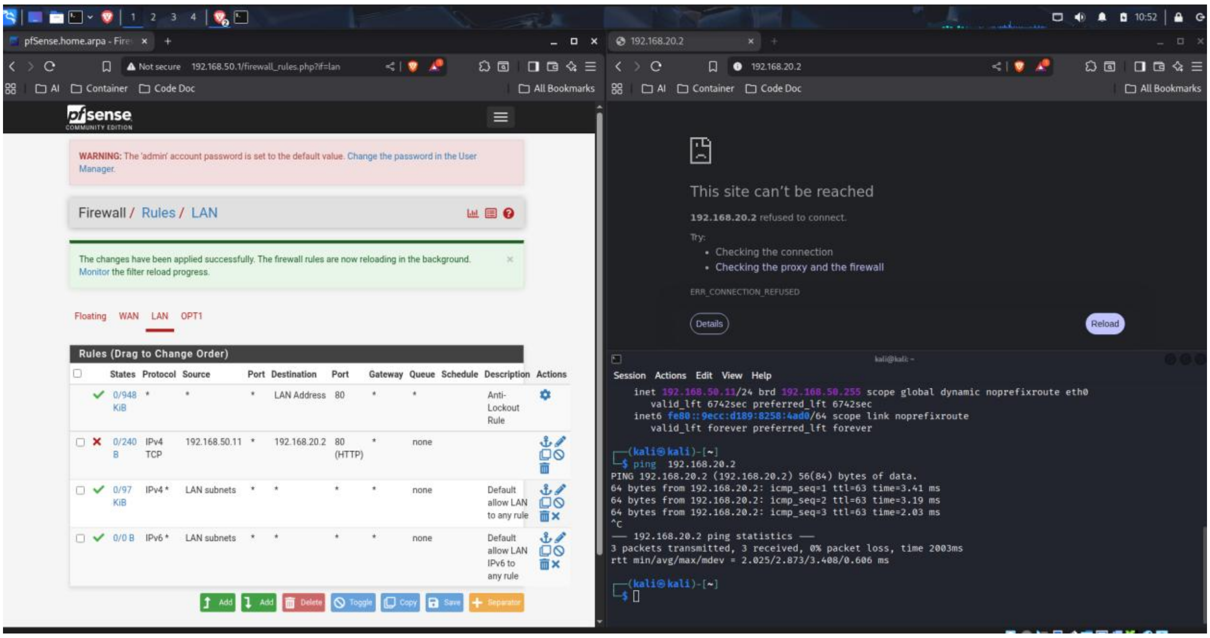
We do not take responsibility for the way in which any one uses this application. We have
the application clear and it should not be used maliciously. We have given warnings and
prevent users from installing DVWA on to live web servers. If your web server is compron
of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded a

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security le

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=3.07 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=4.34 ms
^C
—— 192.168.20.2 ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 3.067/3.702/4.337/0.635 ms

┌──(kali㉿kali)-[~]
└─$ 
```

Screeenshot browser della Kali che non riesce più ad aprire la pagina DVWA servita dalla Metasploitable2, sulla porta HTTP(80) del protocollo TCP (dopo l'applicazione della regola di block) + il protocollo ICMP ancora funzionante



pfSense.home.arpa - Fire
Not secure 192.168.50.1/firewall_rules.php?if=lan
AI
Container
Code Doc
All Bookmarks
pfsense COMMUNITY EDITION
192.168.20.2
10:52

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

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/948 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□	✗	0/240 B	IPv4 TCP	192.168.50.11	*	192.168.20.2	80 (HTTP)	*	none			
□	✓	0/97 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	

This site can't be reached

192.168.20.2 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

```
    inet 192.168.50.11/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
       valid_lft 6742sec preferred_lft 6742sec
    inet6 fe80::9ecc:d189:8258:4ad0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping  192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=3.41 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=3.19 ms
64 bytes from 192.168.20.2: icmp_seq=3 ttl=63 time=2.03 ms
^C
── 192.168.20.2 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.025/2.873/3.408/0.606 ms

┌──(kali㉿kali)-[~]
└─$ 
```