

CREAZIONE POLICY PFSENSE

1.RICHIESTE

- vm di pfSense dove si vedono le 3 schede di rete e gli ip associati
- 3 screenshot del pannello di pfSense dal browser della kali:
- Firewall rules WAN,
- Firewall rules LAN,
- Firewall rules OPT1,
- browser della Kali che apre la pagina servita della Metasploitable2 (prima dell'applicazione della regola),
- browser della Kali che non riesce più ad aprire la pagina servita della Metasploitable2 (dopo l'applicazione della regola),
- terminale della Kali che riesce a pingare la Metasploitable2 (prima dell'applicazione della regola),
- terminale della Kali che continua a riuscire a pingare la Metasploitable (dopo l'applicazione della regola)

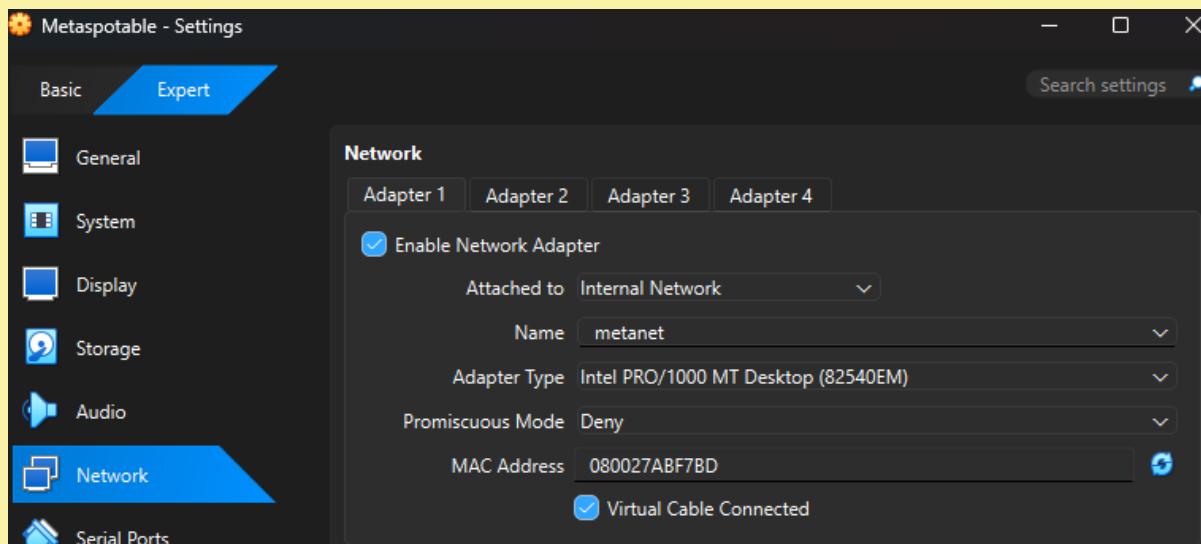
2.SPIEGAZIONE OBIETTIVO

L'obiettivo è di **bloccare** l'accesso al sito della **Metasploitable** e **DVWA** attraverso una regola **Firewall**(un software o hardware capace di filtrare il traffico dei dati, mantenendo la connessione sicura)ma nello stesso tempo, ricevere risposta dalla macchina attraverso il **ping**

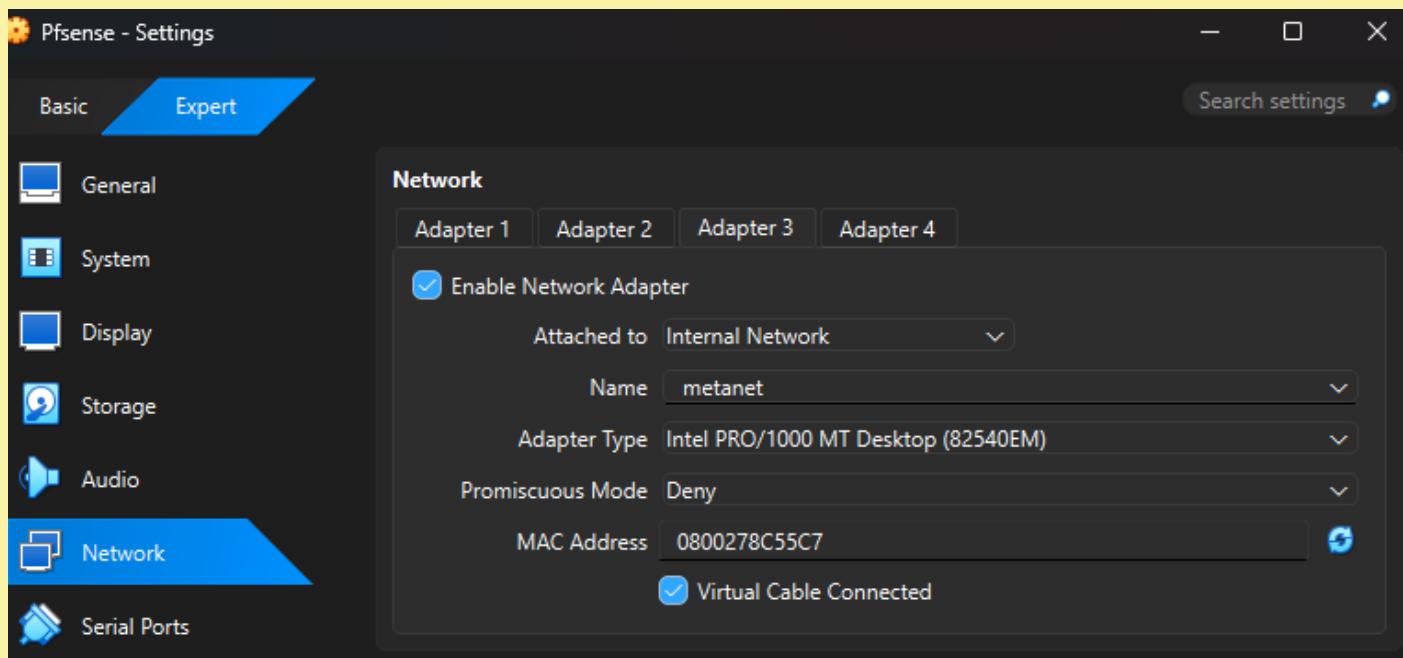
3.PASSAGGI

3.1 CONFIGURAZIONE

Il primo passaggio è quello di creare una terza interfaccia di rete per la **Metasploitable** , quindi apro le impostazioni Network e seleziono il tipo di rete in *Internal Network* e la chiamo “metanet”.



Successivamente apro la sezione *Network* della **Pfsense**, vado a configurare sull'Adapter 3 la "metanet".



Una volta fatto, apro la vm di Pfsense e la kali per accedere al sito della Pfsense, dove ho assegnato un'indirizzo IP statico a **OPT1**(Terza Interfaccia).

The screenshot shows the Pfsense web interface. In the top navigation bar, 'pfSense' and 'COMMUNITY EDITION' are visible. The left sidebar has 'System', 'Interfaces' (which is selected and highlighted in red), 'Assignments', 'WAN', 'LAN', and 'OPT1'. The 'Status' section is also present. The main content area is titled 'Static IPv4 Configuration'.

Under 'Static IPv4 Configuration':

- IPv4 Address**: 192.168.60.1 / 24.
- IP4 Upstream gateway**: None. A green button labeled '+ Add a new gateway' is next to it.

A note below explains the upstream gateway setting:

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](#).

Una volta assegnato, (“metanet”), torno sulla PfSense e vedo che è stata rilevata.

```
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.0.28/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0         -> v4: 192.168.60.1/24
```

Passo poi alla configurazione della Metasploitable abilitando il servizio di DHCP .

```
Configure IPv4 address OPT1 interface via DHCP? (y/n) n
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.60.100

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: 192.168.60.100
Enter the end address of the IPv4 client address range: 192.168.60.200
```

Di seguito apro la Metasploitable per vedere il suo indirizzo IP che consentirà di l'accesso al sito Metasploitable2 e di conseguenza al DVWA.

```
eth0: <BROADCAST,MULTICAST,UP,BROADCAST>
      link/ether 08:00:27:ab:f7:bc
      inet 192.168.60.100/24 brd 192.168.60.255
      inet6 fe80::a00:27ff:feab:f7
```

Torno sulla kali e faccio una prova per vedere se senza regola riesco ad accedere al sito e fare il ping.

The screenshot shows two browser windows side-by-side. The left window is DVWA (Damn Vulnerable Web App) at 192.168.60.100/dvwa. It displays a 'Welcome to Damn Vulnerable Web App!' page with various menu options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, and SQL Injection. Below the menu is a terminal window showing a ping command to 192.168.60.100. The right window is the Pfsense Firewall Rules interface at 10.0.2.15/firewall_rules.php?if=lan. It shows a table of rules with columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A warning message at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the table, a message says: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress."

Dato il corretto funzionamento, decido di andare sulla sezione “**Firewall/Rules**” del sito di Pfsense per implementare la regola sul Firewall .

The screenshot shows the Pfsense Firewall Rules section. On the left, there's a sidebar with 'Aliases', 'NAT', and 'Rules'. The main area has tabs for 'Floating', 'WAN', 'LAN', and 'OPT1'. The 'LAN' tab is currently selected, showing a table of rules. One rule is visible: '0/0 B * LAN subnets * * * * * * none'. The 'Actions' column for this rule contains icons for edit, copy, and delete.

Sono presenti tre sezioni: WAN, LAN, OPT1 .

The screenshot shows the Pfsense Firewall Rules section with the 'LAN' tab selected. The main area displays a table of rules under the heading 'Rules (Drag to Change Order)'. There are two rules listed: '0/789 * RFC 1918 networks' and '0/0 B * Reserved Not assigned by IANA'. The 'Actions' column for the first rule contains icons for edit, copy, and delete. The 'Actions' column for the second rule also contains icons for edit, copy, and delete.

The screenshot shows the Pfsense Firewall Rules section with the 'LAN' tab selected. The main area displays a table of rules under the heading 'Rules (Drag to Change Order)'. There are three rules listed: '0/454 * * * LAN Address 80 * * Anti-Lockout Rule', '0/627 IPv4 * LAN subnets * * * * * none Default allow LAN to any rule', and '0/0 B IPv6 * LAN subnets * * * * * none Default allow LAN IPv6 to any rule'. The 'Actions' column for the first rule contains icons for edit, copy, and delete. The 'Actions' column for the second rule also contains icons for edit, copy, and delete. The 'Actions' column for the third rule also contains icons for edit, copy, and delete.

Ho scelto di implementare la regola nella **LAN** perché il pacchetto viene spedito dalla **kali** e all'arrivo nel **punto d'ingresso** del **Firewall**, la regola **negherà la destinazione(Metasploitable)** e **scarterà i pacchetti**.

Quindi dico di bloccare(**Block**) i pacchetti(**TCP**) che partono dalla Kali(**Source Address:192.168.50.10**) la cui destinazione è la Metasploitable(**Destination Address:192.168.60.100**) dalla porta 80(**HTTP**) alla 443(**HTTPS**).

Fatto ciò, sono passato alla prova della regola quindi bloccare l'accesso al sito ma mantenendo una connessione per il **ping**.

The connection has timed out

The server at 192.168.60.100 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

Session Actions Edit View Help

(kali㉿kali)-[~]

```
ping 192.168.60.100
PING 192.168.60.100 (192.168.60.100) 56(84) bytes of data.
64 bytes from 192.168.60.100: icmp_seq=1 ttl=63 time=3.71 ms
64 bytes from 192.168.60.100: icmp_seq=2 ttl=63 time=2.79 ms
64 bytes from 192.168.60.100: icmp_seq=3 ttl=63 time=3.62 ms
64 bytes from 192.168.60.100: icmp_seq=4 ttl=63 time=3.94 ms
```

Firewall / Rules / LAN

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

Floating WAN LAN OPT1

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action
✓ 2/394 KB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0/0 B	IPv4 TCP	192.168.50.10	*	192.168.60.100	80 - 443			none		
✓ 16/6.91 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	

Add Add Delete Toggle Copy Save Separator

Mi sono assicurato di aver bloccato solo quel sito aprendo una scheda Amazon con la regola attiva e come mostrato in foto,c'è un corretto funzionamento di quest'ultima.

Amazon.it consumer electronics + https://www.amazon.it/?tag=goitab-21&ref=pd_sl_781ozcfkw6_e&

Holiday films and gifts? We got it wrapped up

Very giftable deals Top Deal Shop gifts for everyone

Cookies and advertising choices

In addition, if you agree, we'll also use cookies to complement your shopping experience across the Amazon stores as described in our [Cookie notice](#). Your choice applies to using first-party and third-party advertising cookies on this service. Cookies store or access standard device information such as a unique identifier. The [102 third parties](#) who use cookies on this service do so for their purposes of displaying and measuring personalised ads, generating audience insights, and developing and improving products.

Accept Decline Customise

Firewall / Rules / LAN

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

Floating WAN LAN OPT1

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action
✓ 2/394 KB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0/0 B	IPv4 TCP	192.168.50.10	*	192.168.60.100	80 - 443			none		
✓ 16/6.91 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	

Add Add Delete Toggle Copy Save Separator