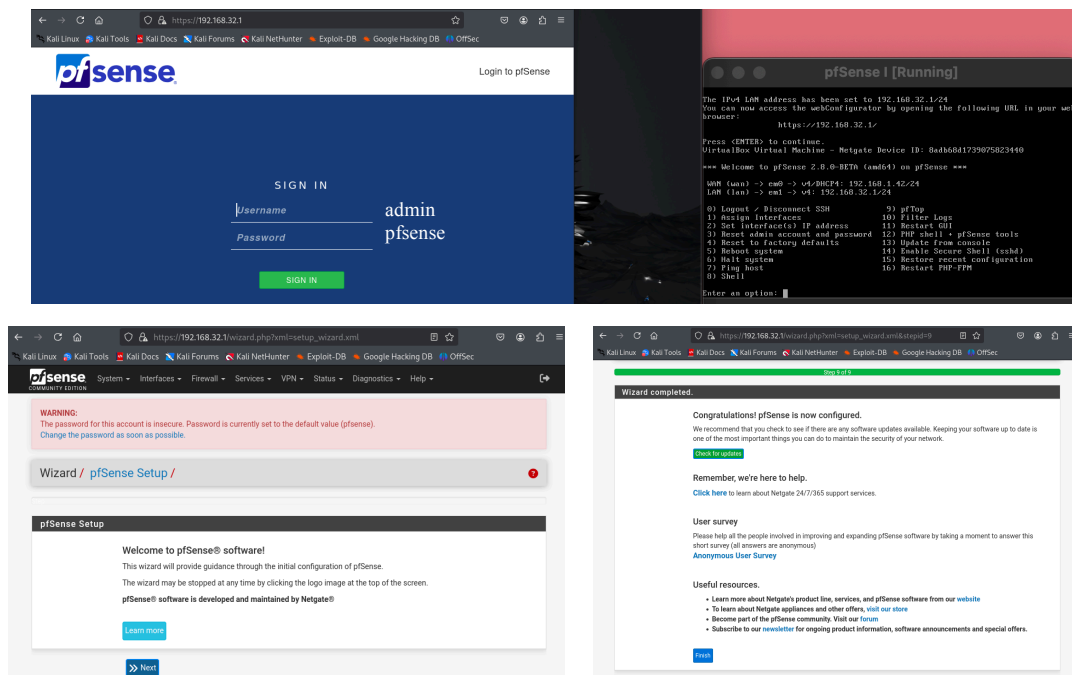


INSTALLAZIONE PFSENSE

1. Scaricare l'immagine Iso da "https://www.pfsense.org/download/"
2. Creare una nuova macchina virtuale su VirtualBox
3. Impostare le schede di rete:
 - Pfsense:
 - 1) Scheda con bridge
 - 2) Rete interna "intnet"
 - 3) Rete interna "pfsense"
 - Kali: 192.168.32.100
 - 1) Rete interna "intnet"
 - Metasploitable 2: 192.168.33.101
 - 1) Rete interna "pfsense"
4. Accendere la VM e configurarla
5. Accedere al sito di pfsense e cliccare su NEXT, poi su RELOAD ed infine su FINISH



6. Dal sito di Pfsense, andare su INTERFACES → ASSIGNMENTS e creare una LAN2 con IPv4 192.168.33.1/24 (oltre alla LAN con IPv4 192.168.32.1/24)

General Configuration

☒ Enable interface

Description

Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: 00:00:00:00:00:00 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

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

IPv4 Subnetmask

7. Dal sito di PfSense, andare su SERVICES → DHCP SERVER → LAN2 e compilare come segue

Deny Unknown Clients: Allow all clients

Ignore Denied Clients: ☐ Ignore denied clients rather than reject

Ignore Client Identifiers: ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

Primary Address Pool

Subnet: 192.168.33.0/24

Subnet Range: 192.168.33.1 - 192.168.33.254

Address Pool Range: 192.168.33.100 (From) to 192.168.33.200 (To)

+ Add Address Pool

Server Options

8. Avviare la VM Metasploitable 2 e tramite il comando `sudo nano /etc/network/interfaces`, scriviamo quanto segue

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
address 192.168.33.101
netmask 255.255.255.0
network 192.168.33.0
broadcast 192.168.33.255
gateway 192.168.33.1
```

9. Creare una nuova regola che blocchi il traffico sulla porta 80 da Kali a Meta, andando su FIREWALL → RULES → EDIT e compilando come segue

Firewall / Rules / Edit

Edit Firewall Rule

Action: Block

Disabled: ☐ Disable this rule

Interface: LAN

Address Family: IPv4

Protocol: TCP

Source: ☐ Invert match, Address or Alias, 192.168.32.100

Destination: ☐ Invert match, Address or Alias, 192.168.33.101

Destination Port Range: HTTP (80) From Custom To Custom

Extra Options: ☒ Log packets that are handled by this rule