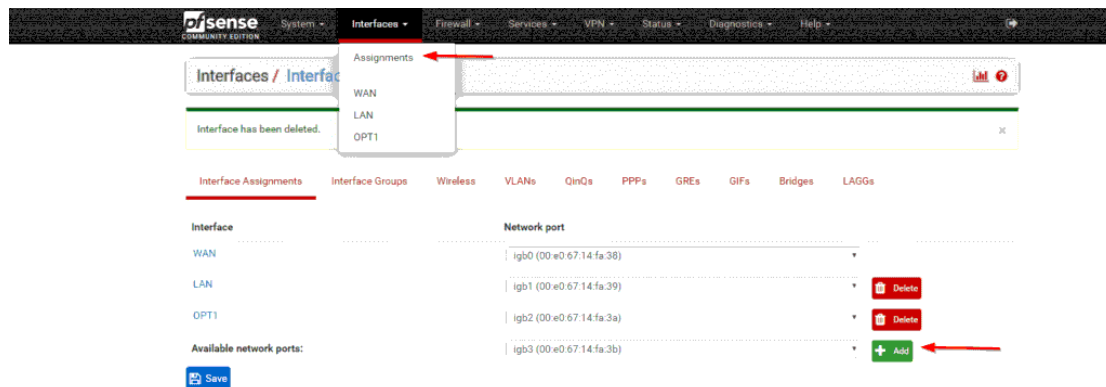


Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova 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.

La prima cosa da fare è aggiungere un'interfaccia di rete. Per gestire Kali Linux e Metasploitable su reti separate, è necessario aggiungere una nuova interfaccia di rete a Pfsense. Questo permette di separare le comunicazioni tra le due reti. Per farlo, sono entrato nell'interfaccia Web di Pfsense e sono andato su Interfaces poi Assignments. Qui ho cliccato su + Add per aggiungere una nuova interfaccia di rete e ho selezionato una delle interfacce fisiche disponibili. Una volta fatto, ho salvato le modifiche.



Dopo aver aggiunto l'interfaccia, l'ho configurata. Sono andato sull'interfaccia appena aggiunta e l'ho abilitata e le ho dato come nome Lan2. Poi ho configurato l'indirizzo IP della rete, in modo che fosse separata dalla rete di Metasploitable e Kali Linux.

https://192.168.1.1/interfaces.php?if=opt1

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Interfaces / LAN2 (em2)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN2 <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>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.</small>
Speed and Duplex	Default (no preference, typically autoselect) <small>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.</small>

Static IPv4 Configuration

IPv4 Address	192.168.50.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

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](#).

Successivamente, per impedire l'accesso alla DVWA su Metasploitable dalla mia macchina Kali Linux, ho creato una regola nel firewall di Pfense. Sono andato su firewall, poi su rules e ho selezionato la scheda corrispondente alla nuova interfaccia Lan2. Ho configurato la regola per bloccare il traffico TCP sulla porta 80 (che è quella utilizzata da DVWA), indicando come source la rete di Kali Linux e come destination quella di Metasploitable.

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address

The **Source Port Range** for a connection must be specified. The destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match

Destination Port Range (other)

From Custom

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

Come ultimo passaggio (che non sono riuscito a fare per problemi tecnici) bisogna controllare che effettivamente DVWA sia bloccato. Per farlo basta provare accedere alla DVWA da Kali Linux tramite browser e in teoria non dovrebbe connettersi oppure utilizzando il comando "nmap" per assicurarsi che la porta 80 di Metasploitable sia chiusa per Kali Linux.