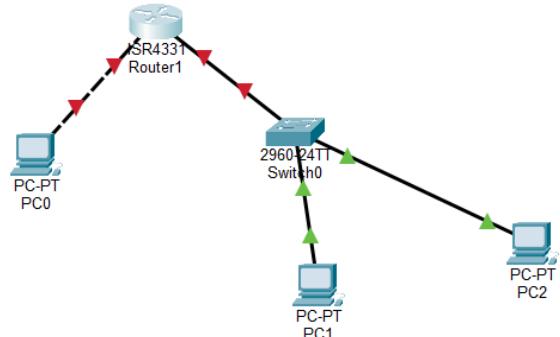


CREAZIONE POLICY PFSENSE

OBIETTIVO DELLA RETE

L'obiettivo è creare una policy di blocco con un firewall nella rete sottostante composta da un apparecchio Linux e un computer Metasploitable collegati in 2 reti interne differenti alla macchina PfSense quest'ultima sarà collegata sia alle reti interne differenti sia al router di internet.



In questo caso PfSense funge anche da switch che collega collegando così tutte le reti tra loro, infatti contiene 3 schede dei 3 collegamenti, la WAN con il router il che gli fornisce un indirizzo ip tramite il protocollo DHCP del router, che prevede l'assegnazione dell'IP automatica, mentre per le reti interne si definiscono manualmente e sono LAN con l'ip della macchina Kali e OPT1 con l'ip della Metasploitable.

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.12/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.20.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
```

COLLEGAMENTO

Tramite il browser della Kali possiamo accedere al pannello della PfSense, possiamo controllare da quest'ultima le configurazioni della rete e di tutti i suoi computer collegati ad essa.

Floating **WAN** LAN OPT1

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/15 KiB	*	RFC 1918 networks	*	*	*	*	*	Block private networks		
<input checked="" type="checkbox"/>	0/700 B	*	Reserved	*	*	*	*	*	Block bogon networks		

No rules are currently defined for this interface

Floating **WAN** **LAN** OPT1

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	1/505 KiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule		
<input checked="" type="checkbox"/>	0/3 KiB	IPv4 TCP	192.168.50.10	*	192.168.20.10	80 (HTTP)	*	none			
<input checked="" type="checkbox"/>	6/344 KiB	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule		
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule		

Add Add Delete Toggle Copy Save Separator

The screenshot shows the Pfsense Firewall Rules interface. At the top, there are tabs for Floating, WAN, LAN, and OPT1, with LAN selected. Below the tabs is a table header with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A message in the center states: "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." At the bottom are several action buttons: Add (green), Add (orange), Delete (red), Toggle (blue), Copy (light blue), Save (blue), and Separator (orange).

Infatti sempre tramite per testare il collegamento proviamo ad accedere, sempre tramite browser di Kali, sia alla pagina servita della Metasploitable, che a quella della Pfsense prova del fatto che nella rete siano tutti collegati tra loro,

The screenshot compares two web-based interfaces. On the left is the Damn Vulnerable Web Application (DVWA) interface, showing a menu with Home, Instructions, Setup, Brut Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area displays the DVWA logo and a welcome message: "Welcome to Damn Vulnerable Web App!". It includes sections for "WARNING!", "Disclaimer", and "General Instructions". On the right is the pfSense Firewall Rules interface, showing a table of rules. The first rule is checked and set to allow traffic from LAN to LAN port 80. The second rule is unchecked and set to allow traffic from LAN subnets to LAN port 80. The third rule is unchecked and set to allow traffic from LAN subnets to LAN port 80. Action buttons at the bottom include Add (green), Add (orange), Delete (red), Toggle (blue), Copy (light blue), Save (blue), and Separator (orange).

dopo aver testato il collegamento di livello 7 della IO, ovvero tramite applicativo, testiamo il collegamento a livello base tramite ping della macchina in questo caso il ping partirà dal terminale della Kali, collegata solo a Pfsense e dovrà raggiungere Metasploitable, che anch'essa è collegata solo alla Pfsense.

The screenshot shows a terminal window with a black background and white text. The session starts with the prompt "(kali㉿kali)-[~]". The user runs the command "\$ ping 192.168.20.10". The output shows four ICMP echo requests being sent to the target IP address. The last line of output is "rtt min/avg/max/mdev = 0.480/0.741/1.058/0.214 ms". The session ends with the prompt "[~]".

Questa dimostrazione prova che tutta la rete sia collegata come da progetto.

POLICY DI BLOCCO PFSENSE

L'obiettivo è quello di mettere un blocco di firewall del protocollo HTTP dalla macchina Kali alla Metasploitable e quindi bloccare solamente la rete web tramite quest'ultimo protocollo.

Tramite browser Kali andiamo nell'area dedicata ai firewall alla scheda della Kali quindi al collegamento LAN dove possiamo creare un blocco.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/62 KIB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	
✗ 0/3 KIB	IPv4 TCP	192.168.50.10	*	192.168.20.10	80 (HTTP)	*	none			
✗ 4/432 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	

Più il firewall si colloca in alto e più ha priorità di esecuzione, nel settaggio del andiamo a specificare che non si tratta di una respinta dell'accesso, che verrebbe notificato, ma di un blocco che semplicemente non fa accede, senza che ci venga inviata alcuna prova di accesso, specificando sia l'IP della Kali, ovvero l'ip di partenza, che l'IP della Metasploitable, quindi l'ip di arrivo, e settiamo unicamente il protocollo http con la porta 80, ricordando di posizionare il blocco nella rete interna.

Questa operazione farà sì che il browser della macchina Kali non sia più in grado di collegarsi con l'HTTP alla macchina Metasploitable, quindi quest'ultima non potrà più raggiungere l'indirizzo web.

```
(kali㉿kali)-[~]
$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=19.6 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=0.614 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=0.571 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=0.540 ms
^C
--- 192.168.20.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3030ms
rtt min/avg/max/mdev = 0.540/0.533/19.608/8.241 ms

(kali㉿kali)-[~]
$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=3.03 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=0.462 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=1.44 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=0.585 ms
64 bytes from 192.168.20.10: icmp_seq=5 ttl=63 time=0.482 ms
64 bytes from 192.168.20.10: icmp_seq=6 ttl=63 time=1.12 ms
^C
--- 192.168.20.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5091ms
rtt min/avg/max/mdev = 0.462/1.185/3.030/0.898 ms

(kali㉿kali)-[~]
```

Secondo ping dopo l'esecuzione del firewall

Ma comunque il collegamento della rete interna tra le due macchine continua, il blocco è unicamente per il protocollo HTTP quindi tramite ping possiamo provare che le macchine restano collegate tra loro e che la rete non ha avuto ripercussioni come da obiettivo del nostro firewall eseguito in modo corretto.