



ESERCIZIO W9D4

Creazione Policy Pfsense

Mungiovì Fabio

TASK

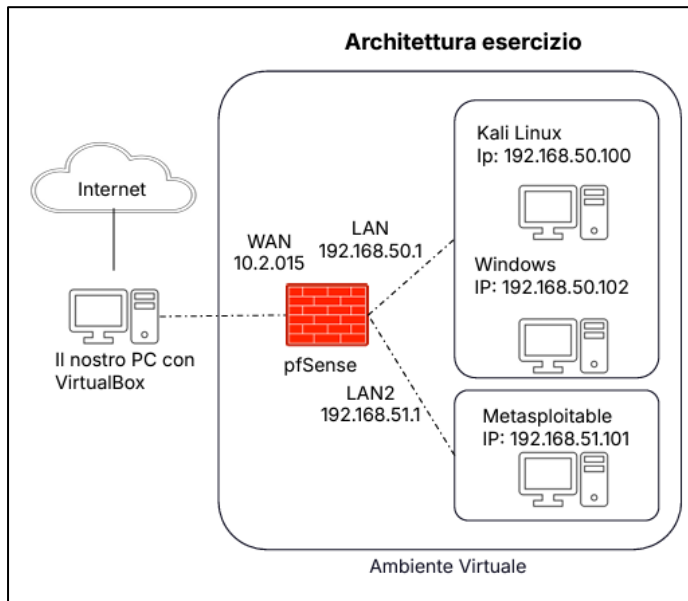
Creare tramite Pfsense, una regola firewall che blocchi l'accesso alla DVWA (su Metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, aggiungere quindi una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.




CONFIGURAZIONE

Andiamo innanzitutto a configurare il laboratorio, in modo da avere Metasploitable e Kali su due reti differenti.

L'obiettivo è raggiungere una configurazione come quella in figura.



Quindi, come prima cosa andiamo ad impostare dalle impostazioni della macchina virtuale di Pfsense, 3 interfacce di rete, 2 per le LAN e una per la WAN.

 Network Adapter	LAN Segment
 Network Adapter 2	NAT
 Network Adapter 3	LAN Segment

Le 2 LAN saranno collegate ognuna ad una sottorete interna.

La WAN sarà collegata in NAT con l'ambiente host.

Ora avviamo Pfsense, e da terminale, configuriamo le interfacce di rete e assegniamo gli IP desiderati.

```
WAN (wan)      -> em1      -> v4: 10.2.0.15/24
LAN (lan)      -> em0      -> v4: 192.168.50.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.51.1/24
```

Spostiamoci poi sui sistemi operativi e assegniamo anche a loro gli IP.

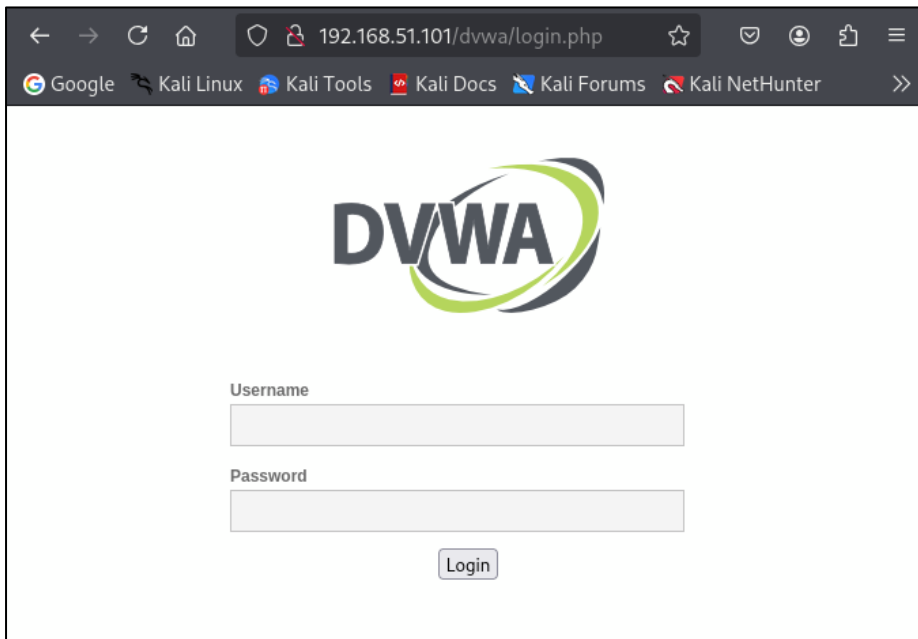
KALI = 192.168.50.100

Metasploitable = 192.168.51.101

ESECUZIONE

Da Kali ora avviamo il web browser, e nella barra degli indirizzi digitiamo l'IP di Metasploitable (192.168.51.101), e apriamo la pagina DVWA.

Sappiamo ora che la rete è configurata correttamente.



Collegiamoci ora, sempre da browser, invece all'indirizzo IP di Pfsense (192.168.50.1), così da poter entrare nella pagina di configurazione, dove andremo a creare la policy del firewall per bloccare la pagina della DVWA di Metasploitable.

Seguendo il path Firewall/Rules/LAN ci troveremo nella pagina delle regole del firewall, clicchiamo su aggiungi per impostarne una nuova.

Edit Firewall Rule	
Action	<div>Block</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>TCP</div> <div>Choose which IP protocol this rule should match.</div>

Nella parte superiore, impostiamo come da figura.

- Action = Block
Indica come viene gestito il traffico in questa regola, cioè bloccato
- Interface = LAN
L'interfaccia da dove arrivano i pacchetti
- Protocol = TCP
Scegliamo il protocollo da bloccare

Source

Source

☐ Invert match

Address or Alias

192.168.50.100

/

⚙️ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Address or Alias

192.168.51.101

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Nella seconda parte inseriamo gli IP della macchina fonte della regola (KALI) e la macchina di destinazione (Metasploitable), indicando solo la porta 80 da cui deve essere bloccato il traffico.

Salviamo e torniamo alla lista delle policy, dove ora dovremmo trovare quella appena creata.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 2/1.85 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0/3 KiB	IPv4 TCP	192.168.50.100	*	192.168.51.101	80 (HTTP)	*	none			📌✎📄🗑️
<input type="checkbox"/>	✓ 0/851 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	📌✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌✎📄🗑️✖️

Provando ora a collegarsi di nuovo all’IP di Metasploitable, noteremo subito che la pagina DVWA non verrà più caricata.

Come ulteriore conferma della funzionalità del firewall effettuiamo una scansione con il tool Nmap all’IP di meta, per vedere lo stato delle porte.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap 192.168.51.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 19:05 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try  
using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.51.101  
Host is up (0.0093s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE      SERVICE  
21/tcp    open       ftp  
22/tcp    open       ssh  
23/tcp    open       telnet  
25/tcp    open       smtp  
53/tcp    open       domain  
80/tcp    filtered  http  
111/tcp   open       rpcbind  
139/tcp   open       netbios-ssn  
445/tcp   open       microsoft-ds  
512/tcp   open       exec  
513/tcp   open       login  
514/tcp   open       shell  
1099/tcp  open       rmiregistry  
1524/tcp  open       ingreslock
```

Notiamo come la porta 80 risulti “filtered”, cioè bloccata dal firewall.

Analizzando i log di pfsense troveremo ancora conferma dell’esecuzione della regola impostata.

Last 500 Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	May 1 23:29:42	LAN	👤 Block DVWA from KALI (1746053598)	📌 192.168.50.100:56828	📌 192.168.51.101:80	TCP:S

Anche da Wireshark, intercettando i pacchetti, abbiamo la prova che la destinazione non ci sta rispondendo, ed il browser continua ad effettuare tentativi di connessione, senza ricevere alcuna risposta.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.51.101	TCP	74	60788 → 80 [SYN] Seq=0 Win=64240 Len=0 M
2	0.251006487	192.168.50.100	192.168.51.101	TCP	74	60802 → 80 [SYN] Seq=0 Win=64240 Len=0 M
3	1.012698845	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60788 → 80 [SYN] Se
4	1.268317650	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60802 → 80 [SYN] Se
5	2.040611671	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60788 → 80 [SYN] Se
6	2.292320654	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60802 → 80 [SYN] Se
7	3.060472415	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60788 → 80 [SYN] Se
8	3.316626398	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60802 → 80 [SYN] Se
9	4.085031606	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60788 → 80 [SYN] Se
10	4.340664551	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60802 → 80 [SYN] Se
11	5.108465083	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 60788 → 80 [SYN] Se
12	5.236151062	VMware_c2:64:9b	VMware_ba:6c:96	ARP	42	Who has 192.168.50.1? Tell 192.168.50.10
13	5.237835604	VMware_ba:6c:96	VMware_c2:64:9b	ARP	60	192.168.50.1 is at 00:0c:29:ba:6c:96