

REPORT S3L5

OBIETTIVO ESERCIZIO : creare una regola firewall che blocca l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

CONFIGURAZIONE RETE







La rete è stata configurata con le seguenti interfacce su pfSense

WAN : 192.168.43.30

LAN (Kali network) : 192.168.50.1 (gateway Kali)

OPT1 (Target Metasploitable) : 192.168.30.1 (gateway Metasploitable)

La macchina Metasploitable è stata configurata con IP statico 192.168.30.10

Interfaces   			
 WAN	↑	10Gbase-T <full-duplex>	192.168.43.30
 KALI	↑	10Gbase-T <full-duplex>	192.168.50.1
 METASPLOITABLE	↑	1000baseT <full-duplex>	192.168.30.1

VERIFICA CONNETTIVITÀ STATO INIZIALE

Prima dell'applicazione delle restrizioni firewall, è stato verificato che la comunicazione tra la rete LAN (Kali) e la rete OPT1 (Metasploitable) fosse completamente aperta.

TEST PING

È stato effettuato un test ping

dalla Kali (192.168.50.151)

verso il target

Metasploitable (192.168.30.10).

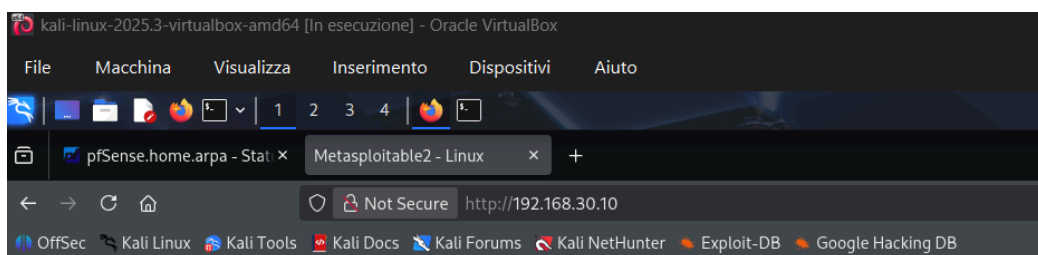
```
(kali@kali)-[~]
$ ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=1 ttl=63 time=10.7 ms
64 bytes from 192.168.30.10: icmp_seq=2 ttl=63 time=5.44 ms
64 bytes from 192.168.30.10: icmp_seq=3 ttl=63 time=5.95 ms
64 bytes from 192.168.30.10: icmp_seq=4 ttl=63 time=5.23 ms
64 bytes from 192.168.30.10: icmp_seq=5 ttl=63 time=4.85 ms
64 bytes from 192.168.30.10: icmp_seq=6 ttl=63 time=5.33 ms
64 bytes from 192.168.30.10: icmp_seq=7 ttl=63 time=5.36 ms
64 bytes from 192.168.30.10: icmp_seq=8 ttl=63 time=5.44 ms
64 bytes from 192.168.30.10: icmp_seq=9 ttl=63 time=4.23 ms
64 bytes from 192.168.30.10: icmp_seq=10 ttl=63 time=4.80 ms
64 bytes from 192.168.30.10: icmp_seq=11 ttl=63 time=5.36 ms
64 bytes from 192.168.30.10: icmp_seq=12 ttl=63 time=4.90 ms
64 bytes from 192.168.30.10: icmp_seq=13 ttl=63 time=5.37 ms
64 bytes from 192.168.30.10: icmp_seq=14 ttl=63 time=4.22 ms
64 bytes from 192.168.30.10: icmp_seq=15 ttl=63 time=5.49 ms
64 bytes from 192.168.30.10: icmp_seq=16 ttl=63 time=6.11 ms
64 bytes from 192.168.30.10: icmp_seq=17 ttl=63 time=5.07 ms
64 bytes from 192.168.30.10: icmp_seq=18 ttl=63 time=5.12 ms
64 bytes from 192.168.30.10: icmp_seq=19 ttl=63 time=5.67 ms
64 bytes from 192.168.30.10: icmp_seq=20 ttl=63 time=4.24 ms
64 bytes from 192.168.30.10: icmp_seq=21 ttl=63 time=6.23 ms
64 bytes from 192.168.30.10: icmp_seq=22 ttl=63 time=5.39 ms
64 bytes from 192.168.30.10: icmp_seq=23 ttl=63 time=6.11 ms
^C
— 192.168.30.10 ping statistics —
23 packets transmitted, 23 received, 0% packet loss, time 22281ms
rtt min/avg/max/mdev = 4.221/5.501/10.652/1.228 ms
```

TEST HTTP WEB

È stato verificato l'accesso

al server web Metasploitable

tramite browser su kali.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

CONFIGURAZIONE REGOLE FIREWALL

È stata creata una regola specifica sull'interfaccia LAN Kali per intercettare il traffico.

INTERFACCE WAN E OPT1(METASPLOITABLE)

Le configurazioni non sono state modificate restrittivamente per questo test.

pfSense
COMMUNITY EDITION

System ▾Interfaces ▾Firewall ▾Services ▾VPN ▾Status ▾Diagnostics ▾Help ▾

⌂

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / WAN

📊📋?

Floating

WAN

KALI

METASPLOITABLE

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙️
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️

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.

⬆️ Add

⬇️ Add

🗑️ Delete

🔄 Toggle

📋 Copy

💾 Save

+ Separator

pfSense
COMMUNITY EDITION

System ▾Interfaces ▾Firewall ▾Services ▾VPN ▾Status ▾Diagnostics ▾Help ▾

⌂

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / METASPLOITABLE

📊📋?

Floating

WAN

KALI

METASPLOITABLE

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/3 KIB	IPv4 *	*	*	*	*	*	none			📌🔍📋🔄🗑️✖️

⬆️ Add

⬇️ Add

🗑️ Delete

🔄 Toggle

📋 Copy

💾 Save

+ Separator

INTERFACCIA KALI CON REGOLA DI BLOCCO

È stata inserita una nuova regola in cima alla lista con le seguenti caratteristiche:

- Action : Block
- Protocol : TCP
- Sources : Kali subnets
- Destination : Host 192.168.30.10
- Destination port Range : From HTTP (80) : To HTTP (80)

Questa configurazione blocca solamente il protocollo TCP sulla porta web, lasciando inalterato il protocollo ICMP usato dal ping.

Warning

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / KALI

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Floating

WAN

KALI

METASPLOITABLE

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/594 KiB	*	*	*	KALI Address	80	*	*		Anti-Lockout Rule	<div></div>
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	KALI subnets	*	192.168.30.10	80 (HTTP)	*	none		blocco sito di meta	<div></div>
<input type="checkbox"/>	✓ 2/1.52 MiB	IPv4 *	KALI subnets	*	*	*	*	none		Default allow LAN to any rule	<div></div>
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	KALI subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	<div></div>

↑ Add

↓ Add

Delete

Toggle

Copy

Save

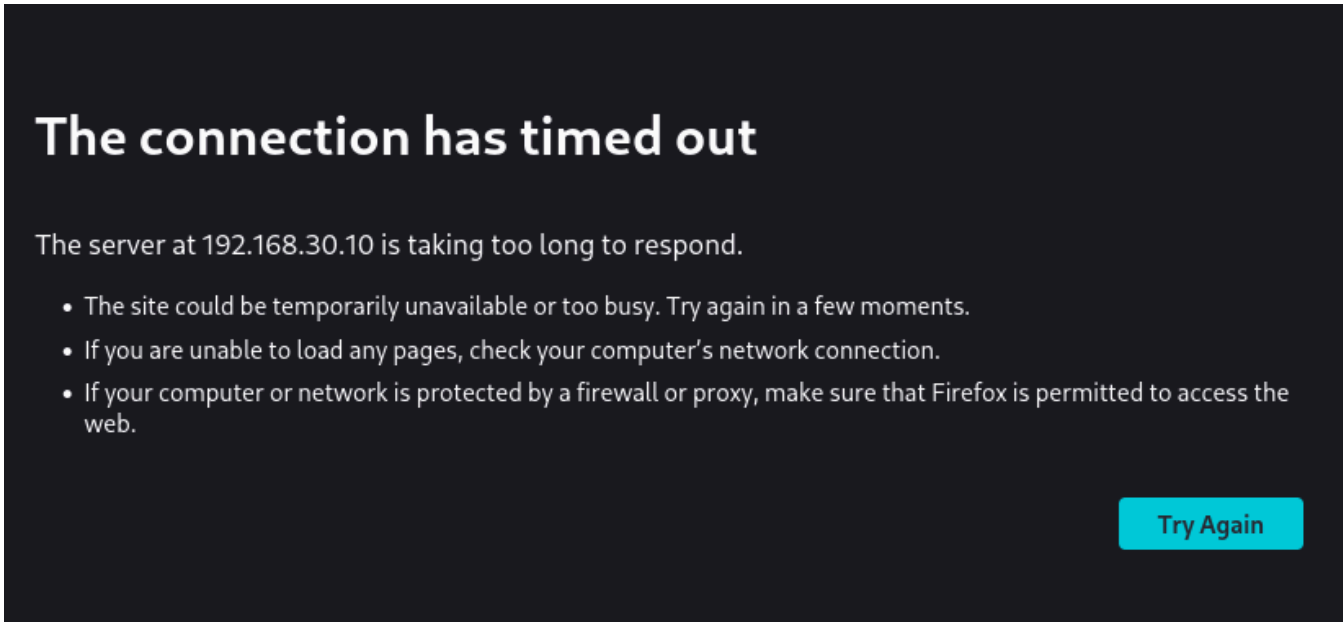
+ Separator

VERIFICA STATO FINALE

Dopo l'applicazione della regola, sono stati ripetuti i test per verificare l'efficacia del firewall.

TEST HTTP (WEB)

Grazie alla regola, se ora si tenta di accedere al sito <http://192.168.30.10>, il browser non riesce a stabilire una connessione, confermando che il traffico TCP sulla porta 80 è stato filtrato correttamente.



TEST ICMP (PING)

Nonostante il blocco web, il comando per lo stesso indirizzo IP(192.168.30.10) funziona comunque.

Questo dimostra che il blocco è selettivo cioè solo TCP e non totale.

