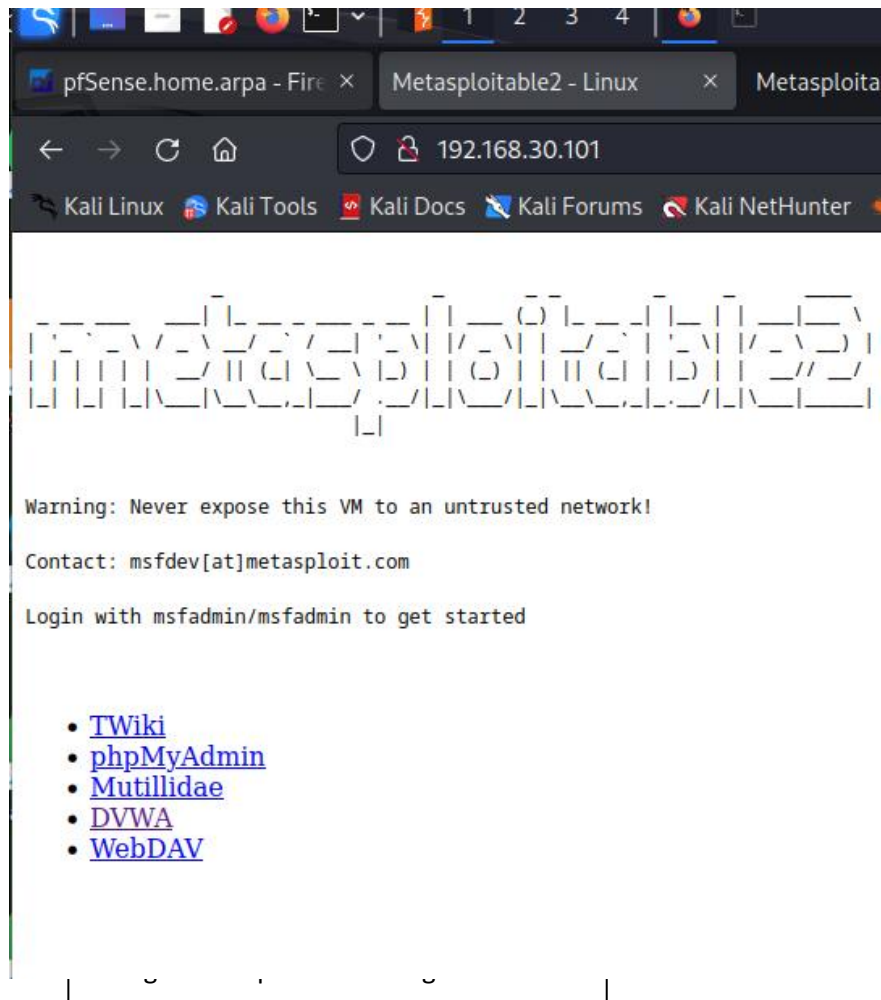


Esercizio 20-02

Traccia: utilizzare pfsense come firewall in NAT per permettere la comunicazione tra Kali e Metasploitable su due reti diverse, ma ponendo una regola nel firewall che vieti a Kali di accedere a DVWA inserendo l'IP di Metasploitable



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](#)



Regole del firewall di default

Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 1/2 KiB	IPv4 TCP	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 8 /1.69 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any	

```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=1.06 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=1.78 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=1.26 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=1.30 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 1.060/1.353/1.784/0.266 ms
msfadmin@metasploitable:~$
```

```
(kali@kali)-[~]
$ ping 192.168.30.101
PING 192.168.30.101 (192.168.30.101) 56(84) bytes of data:
64 bytes from 192.168.30.101: icmp_seq=1 ttl=63 time=1.25 ms
64 bytes from 192.168.30.101: icmp_seq=2 ttl=63 time=1.68 ms
64 bytes from 192.168.30.101: icmp_seq=3 ttl=63 time=2.11 ms
64 bytes from 192.168.30.101: icmp_seq=4 ttl=63 time=2.31 ms

^C
--- 192.168.30.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.245/1.836/2.308/0.409 ms
```

Dimostrazione della comunicazione tra le macchine con IP diversi

Floating WAN LAN LAN2

Aggiunta della regola per bloccare traffico tcp e udp da LAN (rete kali) verso LAN2 (rete meta)

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	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN address	*	LAN2 address	80 (HTTP)	*	none			
<input type="checkbox"/>	0/2 KiB	IPv4 TCP	*	*	*	*	*	none			
<input type="checkbox"/>	0/2 KiB	IPv4 TCP	*	*	*	*	*	none			
<input type="checkbox"/>	4 /1.69 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

CTRL (DEST)

pfSense.home.arpa - Fire... Metasploitable2 - Linux New Tab

192.168.30.100

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

Firefox

Search the web

Amazon Trivago 192.168.50... 192.168.40... 192.168.30... 127.0.0.1

Pagina del browser di Kali che non riesce a caricare l'indirizzo di Metasploitable