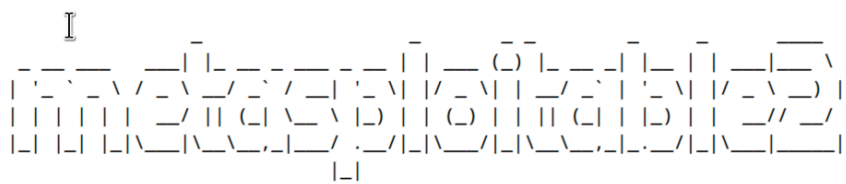


Pfsense rules



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](#)

```
$ ping 192.168.50.2
PING 192.168.50.2 (192.168.50.2) 56(84) bytes of data.
64 bytes from 192.168.50.2: icmp_seq=1 ttl=63 time=6.52 ms
64 bytes from 192.168.50.2: icmp_seq=2 ttl=63 time=4.25 ms
64 bytes from 192.168.50.2: icmp_seq=3 ttl=63 time=3.56 ms
^C
— 192.168.50.2 ping statistics —
 3 packets transmitted, 3 received, 0% packet loss, time=1000ms
 rtt min/avg/max/mdev = 3.56/4.25/6.52/1.50 ms
```

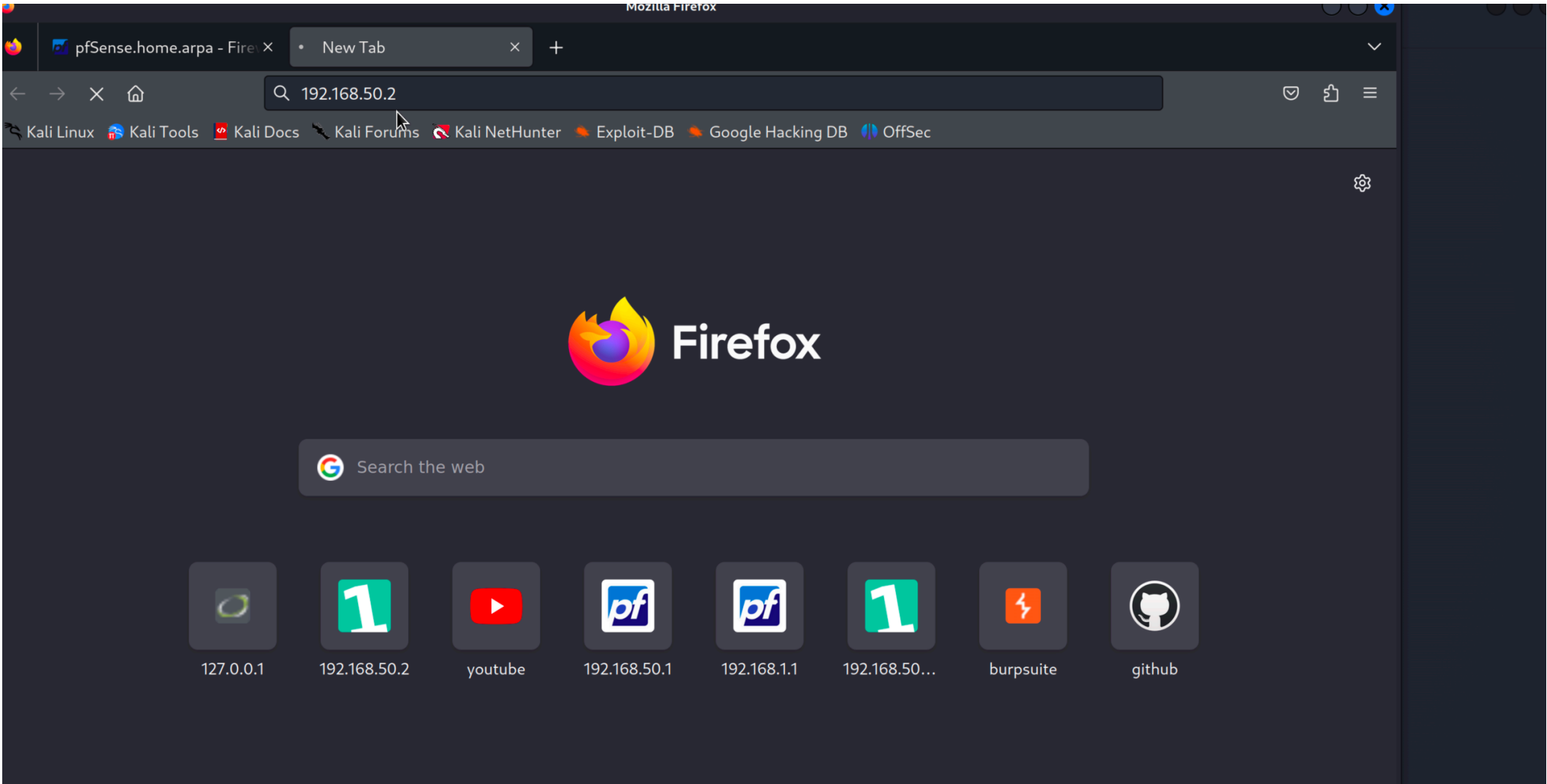
- In questa slide viene mostrata la raggiungibilità di metasploitable da parte di Kali sia su DVWA che tramite richiesta ping

FloatingWANLANOP11

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1/723 KiB	*	*	*	LAN Address	443 80	*	*	Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✖️	0/2 KiB	IPv4 TCP	192.168.1.2	*	192.168.50.2	80 (HTTP)	*	none	block DVWA scan to metasploitable	📌✎📄🕒🗑️
<input type="checkbox"/>	✓	0/3 KiB	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 rule	📌✎📄🕒🗑️✖️

- Ho creato una regola outbound su pfsense in modo tale che blocchi la richiesta HTTP da parte di Kali



71	74.203660951	172.20.10.2	224.0.0.251	MDNS	113	Standard query 0x0000 SRV HP LaserJet MFP M140w (DB6FAD)._ipps._tcp.local, 1
72	80.114385567	192.168.1.2	192.168.50.2	TCP	74	50926 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4100695964 T
73	80.364608555	192.168.1.2	192.168.50.2	TCP	74	50930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4100696215 T
74	81.138468118	192.168.1.2	192.168.50.2	TCP	74	[TCP Retransmission] 50926 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
75	81.394462093	192.168.1.2	192.168.50.2	TCP	74	[TCP Retransmission] 50930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
76	83.154480044	192.168.1.2	192.168.50.2	TCP	74	[TCP Retransmission] 50926 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
77	83.410471394	192.168.1.2	192.168.50.2	TCP	74	[TCP Retransmission] 50930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
78	85.138501582	VMware_b3:f3:7c	2a:17:9b:0f:cb:aa	ARP	42	Who has 192.168.1.1? Tell 192.168.1.2
79	85.140041895	2a:17:9b:0f:cb:aa	VMware_b3:f3:7c	ARP	60	192.168.1.1 is at 2a:17:9b:0f:cb:aa
80	85.366118520	192.168.1.2	192.168.50.2	TCP	74	50942 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4100701216 T
81	86.386507920	192.168.1.2	192.168.50.2	TCP	74	[TCP Retransmission] 50942 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
82	87.186571001	192.168.1.2	192.168.50.2	TCP	74	[TCP Retransmission] 50926 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P

- Il risultato è stato quello atteso così come evidenziato in Wireshark (non vi è risposta alla richiesta di connessione da parte di Kali)