

CONSEGNA:

Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a PfSense in modo tale da gestire una ulteriore rete.

SVOLGIMENTO:

Le macchine Kali Linux e Metasploitable sono su reti differenti come richiesto dalla consegna. Entrambe le reti sono settate su internal così che possano parlare solo con l'ambiente virtuale.

```
kali@kali: ~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 1777 bytes 1495381 (1.4 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1344 bytes 278067 (271.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
Metasploitable [Running]
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9c:24:72
          inet addr:192.168.2.99  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9c:2472/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2543 (2.4 KB) TX bytes:13509 (13.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56461 (55.1 KB) TX bytes:56461 (55.1 KB)

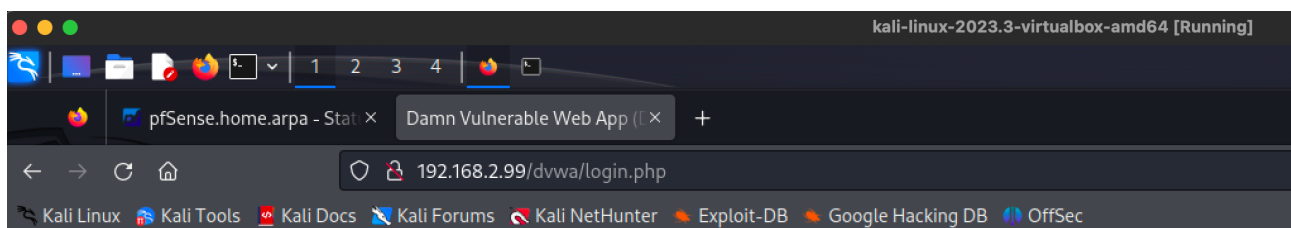
msfadmin@metasploitable:~$ _
```

Sulla macchina pfsense oltre che la scheda WAN ci sono abilitate due schede di rete LAN una per la rete 192.168.1.0/24 e una per la rete 192.168.2.0/24.

Non è stato sufficiente abilitare una nuova scheda di rete da VirtualBox ma si è dovuto abilitare l'interfaccia da pfsense raggiungendola prima dalla macchina Kali.

+++++

Dalla macchina Kali raggiungiamo il DVWA sulla macchina Metasploitable



Username

Password

Login

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.2.1	TCP	66	47220 → 80 [ACK] Seq=1 Ack=1 Win=899 Len=0 TSval=298146136
2	0.001448352	192.168.2.1	192.168.1.100	TCP	66	[TCP ACKed unseen segment] 80 → 47220 [ACK] Seq=1 Ack=2 Win=
3	0.255893682	192.168.1.100	192.168.2.1	TCP	66	47234 → 80 [ACK] Seq=1 Ack=1 Win=656 Len=0 TSval=2981461565
4	0.256377040	192.168.1.100	192.168.2.1	TCP	66	47254 → 80 [ACK] Seq=1 Ack=1 Win=524 Len=0 TSval=2981461565
5	0.257468712	192.168.2.1	192.168.1.100	TCP	66	[TCP ACKed unseen segment] 80 → 47254 [ACK] Seq=1 Ack=2 Win=514
6	0.257971921	192.168.2.1	192.168.1.100	TCP	66	[TCP ACKed unseen segment] 80 → 47234 [ACK] Seq=1 Ack=2 Win=514
7	1.538955773	192.168.1.100	192.168.1.1	TCP	66	48336 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=335367903
8	1.540359767	192.168.1.1	192.168.1.100	TCP	66	[TCP ACKed unseen segment] 80 → 48336 [ACK] Seq=1 Ack=2 Win=514
9	2.917944085	192.168.1.100	192.168.0.1	DNS	88	Standard query 0x23dd A contile.services.mozilla.com
10	3.001223915	192.168.0.1	192.168.1.100	DNS	104	Standard query response 0x23dd A contile.services.mozilla.com A 3
11	3.003043512	192.168.1.100	34.117.237.239	TCP	74	35686 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
12	3.003463861	192.168.1.100	192.168.2.1	TCP	74	45920 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2
13	3.004280349	192.168.2.1	192.168.1.100	TCP	74	80 → 45920 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=128
14	3.004353262	192.168.1.100	192.168.2.1	TCP	66	45920 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2981464313
15	3.004647877	192.168.1.100	192.168.2.1	HTTP	452	GET / HTTP/1.1
16	3.005604415	192.168.2.1	192.168.1.100	TCP	66	80 → 45920 [ACK] Seq=1 Ack=387 Win=65408 Len=0 TSval=3572912292

+++++

Creazione della regola

Firewall / Rules / LAN

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

Floating WAN **LAN** LAN1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/305 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	LAN1 subnets	*	*	none			
<input checked="" type="checkbox"/>	0/2.25 MiB	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

+++++

Dopo l'applicazione della regola che blocca le richieste dalla LAN alla LAN1 (da quella dove sta kali a quella dove sta meta) la DVWA non risulta più raggiungibile.
La regola funziona applicata alla LAN prima di quelle che lasciano passare il traffico.
La stessa regola non funziona se depositata sulla LAN1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.2.99	TCP	74	42552 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3744954806 TSecr=
2	0.250878498	192.168.1.100	192.168.2.99	TCP	74	42556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3744955057 TSecr=
3	1.018526801	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 42552 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
4	1.276661337	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 42556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
5	3.035187919	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 42552 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
6	3.291370970	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 42556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
7	5.252778356	192.168.1.100	192.168.2.99	TCP	74	44670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3744960059 TSecr=
8	6.265548339	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 44670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
9	7.066059993	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 42552 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
10	8.282196411	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 44670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
11	12.442525051	192.168.1.100	192.168.2.99	TCP	74	[TCP Retransmission] 44670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
12	13.467190663	PcsCompu_cb:7e:f5	PcsCompu_af:03:c2	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
13	13.468237898	PcsCompu_af:03:c2	PcsCompu_cb:7e:f5	ARP	60	192.168.1.1 is at 08:00:27:af:03:c2