

Pfsense

ERNESTO ROBLES

kali & metaspitable

Sulla macchina kali è stato impostato
l'ip 192.168.1.60/24 con gateway 192.168.1.89
il quale è l'ip della lan PfSense

su metaspitable l'ip 192.168.50.100/24

```
(kali3@kali3)-[~]
$ sudo route
[sudo] password for kali3:
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.1.89 0.0.0.0 UG 0 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0

(kali3@kali3)-[~]
$ 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=64 time=0.665 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.257 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.398 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.425 ms
^C
--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3149ms
rtt min/avg/max/mdev = 0.257/0.436/0.665/0.146 ms

(kali3@kali3)-[~]
$ nmap -F 192.168.50.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 19:37 CEST
Nmap scan report for 192.168.50.100
Host is up (0.00076s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
```

Le tre interfacce presenti nel firewall
Pfsense sono:
wan 10.0.2.15/24
lan 192.168.1.89/24
lan2 192.168.50.100/24 (macchina
metasoitable)

```
firewall [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: dedd867ec05ce437a427

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.89/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.100/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Oct 23 17:33:47 ...
php-fpm[372]: /index.php: Successful login for user 'admin' from: 192.168.1.60 (
Local Database)
```

Viene impostata la regola di blocco che nega l'accesso alla dvwa da parte della macchina kali

Edit Firewall Rule

Action

Block

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.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

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

Single host or alias

192.168.50.100

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.

Wireshark interface showing a network capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane displays the details of the selected packet (No. 462), showing it is an ICMP Destination unreachable (Port unreachable) message.

No.	Time	Source	Destination	Protocol	Length	Info
449	253.400980943	192.168.1.60	34.117.237.239	TCP	76	[TCP Retransmission] 34104 → 443 [SYN] Seq=0 Win=64:
450	253.679916216	192.168.1.60	3.221.31.29	TCP	76	[TCP Retransmission] 44916 → 443 [SYN] Seq=0 Win=64:
451	253.679942489	192.168.1.60	34.117.237.239	TCP	76	[TCP Retransmission] 34110 → 443 [SYN] Seq=0 Win=64:
452	253.690227051	192.168.1.60	192.168.50.100	TCP	76	[TCP Retransmission] 36424 → 443 [SYN] Seq=0 Win=64:
453	255.430929853	192.168.1.60	34.117.237.239	TCP	76	[TCP Retransmission] 34104 → 443 [SYN] Seq=0 Win=64:
454	255.430950566	192.168.1.60	3.221.31.29	TCP	76	[TCP Retransmission] 44904 → 443 [SYN] Seq=0 Win=64:
455	255.430954456	192.168.1.60	192.168.50.100	TCP	76	[TCP Retransmission] 36420 → 443 [SYN] Seq=0 Win=64:
456	255.704298486	192.168.1.60	34.117.237.239	TCP	76	[TCP Retransmission] 34110 → 443 [SYN] Seq=0 Win=64:
457	255.704322739	192.168.1.60	3.221.31.29	TCP	76	[TCP Retransmission] 44916 → 443 [SYN] Seq=0 Win=64:
458	255.705348701	192.168.1.60	192.168.50.100	TCP	76	[TCP Retransmission] 36424 → 443 [SYN] Seq=0 Win=64:
459	256.901416897	SernetSu_0b:1f:b0		ARP	62	Who has 192.168.1.60? Tell 192.168.1.254
460	256.901431379	PcsCompu_1e:6a:2e		ARP	44	192.168.1.60 is at 08:00:27:1e:6a:2e
461	256.905091715	192.168.1.254	192.168.1.60	NBNS	94	Name query NBSTAT *<00><00><00><00><00><00><00><00>
462	256.905114311	192.168.1.60	192.168.1.254	ICMP	122	Destination unreachable (Port unreachable)
463	257.595046777	PcsCompu_1e:6a:2e		ARP	44	Who has 192.168.1.254? Tell 192.168.1.60
464	257.595110222	PcsCompu_1e:6a:2e		ARP	44	Who has 192.168.1.89? Tell 192.168.1.60
465	257.595592876	PcsCompu_52:8c:89		ARP	62	192.168.1.89 is at 08:00:27:52:8c:89
466	257.598415397	SernetSu_0b:1f:b0		ARP	62	192.168.1.254 is at a0:95:7f:0b:1f:b0

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bi
Linux cooked capture v1
Address Resolution Protocol (request)

any: <live capture in progress> Packets: 529 · Displayed: 529 (100.0%) Profile: Default

Con wireshark possiamo confermare come non ci sia alcuna risposta da parte della destinazione

✖	Oct 23 17:54:38	LAN	(1698083493)	  192.168.1.60:58686	  192.168.50.100:80	TCP:S
✖	Oct 23 17:54:38	LAN	(1698083493)	  192.168.1.60:38266	  192.168.50.100:443	TCP:S
✖	Oct 23 17:54:40	LAN	(1698083493)	  192.168.1.60:38278	  192.168.50.100:443	TCP:S
✖	Oct 23 17:54:40	LAN	(1698083493)	  192.168.1.60:58698	  192.168.50.100:80	TCP:S
...				 	 	

Il traffico da Kali viene effettivamente bloccato e possiamo vederlo grazie ai log

Dal browser si evidenzia come la dvwa non sia raggiungibile una volta digitato l'ip della macchina metasploitable

