

Progetto 15-12-2024

Emanuele Scopelliti

Creazione policy su Pfsense

Lo scopo del progetto consiste nel creare regole sulla nostra macchina Firewall pfsense


In modo da poter bloccare gli attacchi o i controlli dalla macchina Metasploitable2 verso la macchina KALI


Il progetto richiede di aver configurato ed attivato su macchina virtuale le seguenti macchine tutte con IPv4 con IP Statico


Kali con rete impostata su rete interna


Strumenti


Metasploitable2 con rete impostata su rete interna

**kali-linux-2024.3-virtualbox-amd64**
In esecuzione

**MetaSploitable2**
In esecuzione

**Windows 7 Test**
Spenta

**Windows 10 Test**
Spenta

**pfSense**
In esecuzione

Generale
Nome: MetaSploitable2
Sistema operativo: Linux 2.6 / 3.x / 4.x / 5.x (32-bit)

Sistema
Memoria di base: 512 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM

Schermo
Memoria video: 16 MB
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

Archiviazione
Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: Metasploitable.vmdk (Normale, 8,00 GB)

Audio
Driver host: Predefinita
Controller: ICH AC97


Rete
Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet meta')


Pfsense la nostra macchina firewall con tre reti per questioni di necessità dei flussi


Io ho configurato la scheda di rete 1 su Nat


La scheda 2 su rete interna


La scheda 3 su rete interna


**Strumenti**

**kali-linux-2024.3-virtualbox-amd64**
In esecuzione

**MetaSploitable2**
In esecuzione

**Windows 7 Test**
Spenta

**Windows 10 Test**
Spenta

**pfSense**
In esecuzione

Generale
Nome: pfsense
Sistema operativo: FreeBSD (64-bit)

Sistema
Memoria di base: 2048 MB
Processori: 2
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata

Schermo
Memoria video: 25 MB
Fattore di scala: 1.50
Scheda grafica: VBoxVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

Archiviazione
Controller: IDE
Dispositivo IDE primario 0: pfsense-disk001.vdi (Normale, 4,00 GB)
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto

Audio
Driver host: Predefinita
Controller: ICH AC97

Rete
Scheda 1: Intel PRO/1000 T Server (NAT)
Scheda 2: Rete paravirtualizzata (Rete interna, 'intnet')
Scheda 3: Intel PRO/1000 MT Desktop (Rete interna, 'intnet rete 3')

Inizialmente Meta era configurato in IPv6 di default ma con i seguenti comandi l'ho impostato in IPv4 statico

```
sudo nano /etc/network/interfaces
```

```
auto eth0
```

```
iface eth0 inet static
```

```
address 192.168.1.100
```

```
netmask 255.255.255.0
```

```
gateway 192.168.1.1
```

le configurazioni di rete solo le seguenti per ogni Macchina Virtuale:

Pfsense

Wan 10.0.2.15/24

Lan 192.168.50.1 /24

Terza rete OPT1 192.168.2.48/24

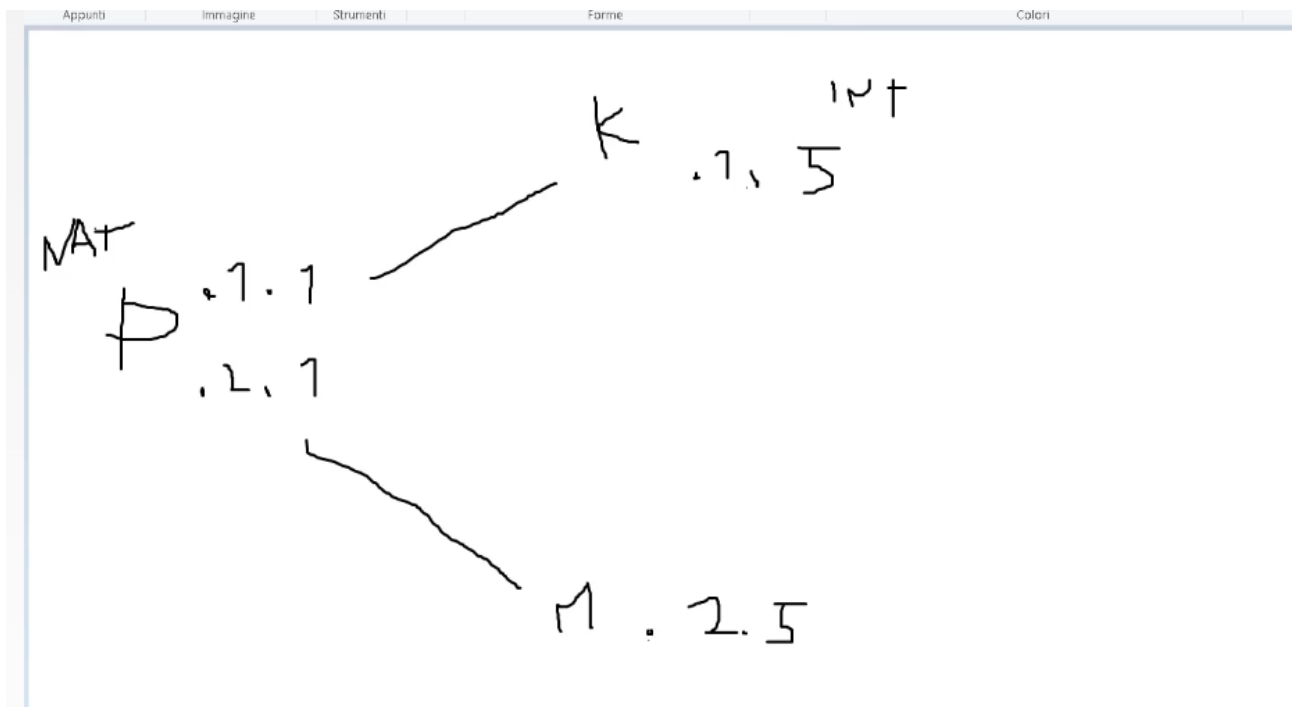
Kali

Lan 192.168.50.151 (il terzo Ottetto è lo stesso della seconda rete di Pfsense)

Meta

Lan 192.168.2.24 (il terzo Ottetto è lo stesso della terza rete di Pfsense)

La configurazione delle schede di rete è stata eseguita seguendo questo schema spiegato durante la lezione:



A questo punto verifico le impostazioni di rete delle macchine virtuali:

Pfsense

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 30d3400deef6988b280b
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0   -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em1      -> v4: 192.168.2.48/24

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
```

Kali

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.151 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::6c4b:1ded:98e0:6842 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 9629 bytes 7852639 (7.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5821 bytes 690850 (674.6 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 40 bytes 3904 (3.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 3904 (3.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Meta

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:34:6b:09
          inet addr:192.168.2.24  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe34:6b09/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:403 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:50938 (49.7 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:707 errors:0 dropped:0 overruns:0 frame:0
          TX packets:707 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:229863 (224.4 KB)  TX bytes:229863 (224.4 KB)
```

Inserimento delle regole nel Firewall di Pfsense da Kali con l'utilizzo di interfaccia grafica, attraverso il collegamento da Kali tramite Ip statico verso Pfsense:

Firewall / Rules / Edit

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 Address or Alias 192.168.50.151 /

[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 Address or Alias 192.168.2.24 /

Destination Port Range HTTP (80) From Custom To HTTP (80) Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1734271653
Created	12/15/24 14:07:33 by admin@192.168.50.151 (Local Database)
Updated	12/15/24 14:07:33 by admin@192.168.50.151 (Local Database)

[Save](#)

Blocco!

Source: IP di Kali

Destinazione: Metasploit con blocco della porta 80 (http non sicuro)

Verifica tramite Ping da kali a Meta è libera può essere effettuata perché la connessione è possibile in uscita

Ma invece da Meta a Kali quindi in ingresso è completamente bloccata

Da KALI verso Meta TEST:

```
(kali㉿kali)-[~]  
$ ping 192.168.2.48  
PING 192.168.2.48 (192.168.2.48) 56(84) bytes of data.  
64 bytes from 192.168.2.48: icmp_seq=1 ttl=64 time=0.942 ms  
64 bytes from 192.168.2.48: icmp_seq=2 ttl=64 time=0.590 ms  
64 bytes from 192.168.2.48: icmp_seq=3 ttl=64 time=0.675 ms  
64 bytes from 192.168.2.48: icmp_seq=4 ttl=64 time=0.495 ms  
64 bytes from 192.168.2.48: icmp_seq=5 ttl=64 time=0.466 ms  
64 bytes from 192.168.2.48: icmp_seq=6 ttl=64 time=0.643 ms  
64 bytes from 192.168.2.48: icmp_seq=7 ttl=64 time=1.66 ms  
64 bytes from 192.168.2.48: icmp_seq=8 ttl=64 time=0.587 ms  
64 bytes from 192.168.2.48: icmp_seq=9 ttl=64 time=0.511 ms  
64 bytes from 192.168.2.48: icmp_seq=10 ttl=64 time=0.738 ms  
64 bytes from 192.168.2.48: icmp_seq=11 ttl=64 time=1.70 ms  
64 bytes from 192.168.2.48: icmp_seq=12 ttl=64 time=1.72 ms  
64 bytes from 192.168.2.48: icmp_seq=13 ttl=64 time=1.34 ms  
64 bytes from 192.168.2.48: icmp_seq=14 ttl=64 time=1.09 ms  
64 bytes from 192.168.2.48: icmp_seq=15 ttl=64 time=1.48 ms  
64 bytes from 192.168.2.48: icmp_seq=16 ttl=64 time=0.889 ms  
64 bytes from 192.168.2.48: icmp_seq=17 ttl=64 time=0.874 ms
```

Quindi connessione libera e verificata

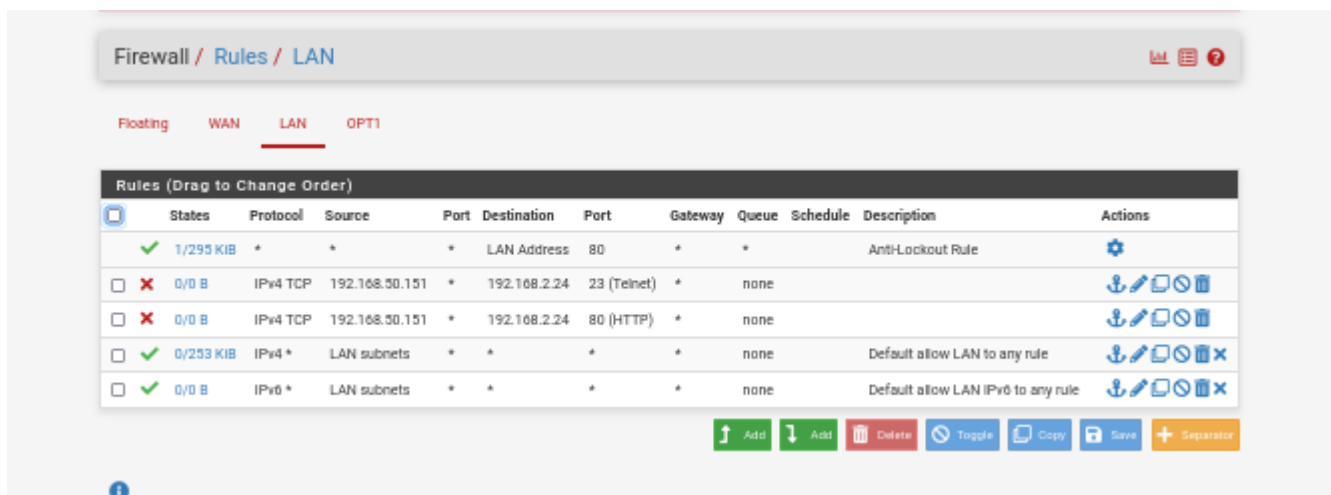
Meta verso KALI TEST:

```
msfadmin@metasploitable:~$ ping 192.168.50.151  
PING 192.168.50.151 (192.168.50.151) 56(84) bytes of data.  
From 192.168.2.24 icmp_seq=1 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=2 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=3 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=4 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=5 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=6 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=8 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=9 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=10 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=12 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=13 Destination Host Unreachable  
From 192.168.2.24 icmp_seq=14 Destination Host Unreachable  
  
--- 192.168.50.151 ping statistics ---  
14 packets transmitted, 0 received, +12 errors, 100% packet loss, time 13014ms  
, pipe 4  
msfadmin@metasploitable:~$
```

Connessione Bloccata

Bloccata la porta corrispondente di Telnet la 23

Save



Ping su telnet

TEST VERIFICA BLOCCO:

```

MetaSploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

collisions:0 txqueuelen:0
RX bytes:229863 (224.4 KB)  TX bytes:229863 (224.4 KB)

msfadmin@metasploitable:~$ ping 192.168.50.151
PING 192.168.50.151 (192.168.50.151) 56(84) bytes of data.
From 192.168.2.24 icmp_seq=1 Destination Host Unreachable
From 192.168.2.24 icmp_seq=2 Destination Host Unreachable
From 192.168.2.24 icmp_seq=3 Destination Host Unreachable
From 192.168.2.24 icmp_seq=4 Destination Host Unreachable
From 192.168.2.24 icmp_seq=5 Destination Host Unreachable
From 192.168.2.24 icmp_seq=6 Destination Host Unreachable
From 192.168.2.24 icmp_seq=8 Destination Host Unreachable
From 192.168.2.24 icmp_seq=9 Destination Host Unreachable
From 192.168.2.24 icmp_seq=10 Destination Host Unreachable
From 192.168.2.24 icmp_seq=12 Destination Host Unreachable
From 192.168.2.24 icmp_seq=13 Destination Host Unreachable
From 192.168.2.24 icmp_seq=14 Destination Host Unreachable

--- 192.168.50.151 ping statistics ---
14 packets transmitted, 0 received, +12 errors, 100% packet loss, time 13014ms
, pipe 4
msfadmin@metasploitable:~$ telnet 192.168.50.151
Trying 192.168.50.151...
telnet: Unable to connect to remote host: No route to host
msfadmin@metasploitable:~$ _

```