

ESERCITAZIONE

13/12/24

CONSEGNA 1

creare una regola firewall che blocchi l'accesso alla DVWA della MV Metasploitable da parte della MV kali Linux e ne impedisca lo scan delle porte.

ANALISI DELLA CONSEGNA

per adempiere alla consegna andremo prima a configurare un'ulteriore interfaccia di rete per la nostra macchina pf sense (FIREWALL) e successivamente procederemo a verificare, prima, l'esistenza di traffico tra le due MV e poi a bloccare lo stesso sulla porta inerente la DVWA

1.1

cominciamo creando la nostra interfaccia di rete, dal menu RETE di virtualbox, procediamo così:

Impostazioni di ricerca

Rete

Scheda 1 Scheda 2 Scheda 3 Scheda 4

☒ Abilita scheda di rete

Connessa a: Rete interna

Nome: intnet2

Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)

Modalità promiscua: Nega

Indirizzo MAC: 080027B51BF5

☒ Cavo connesso

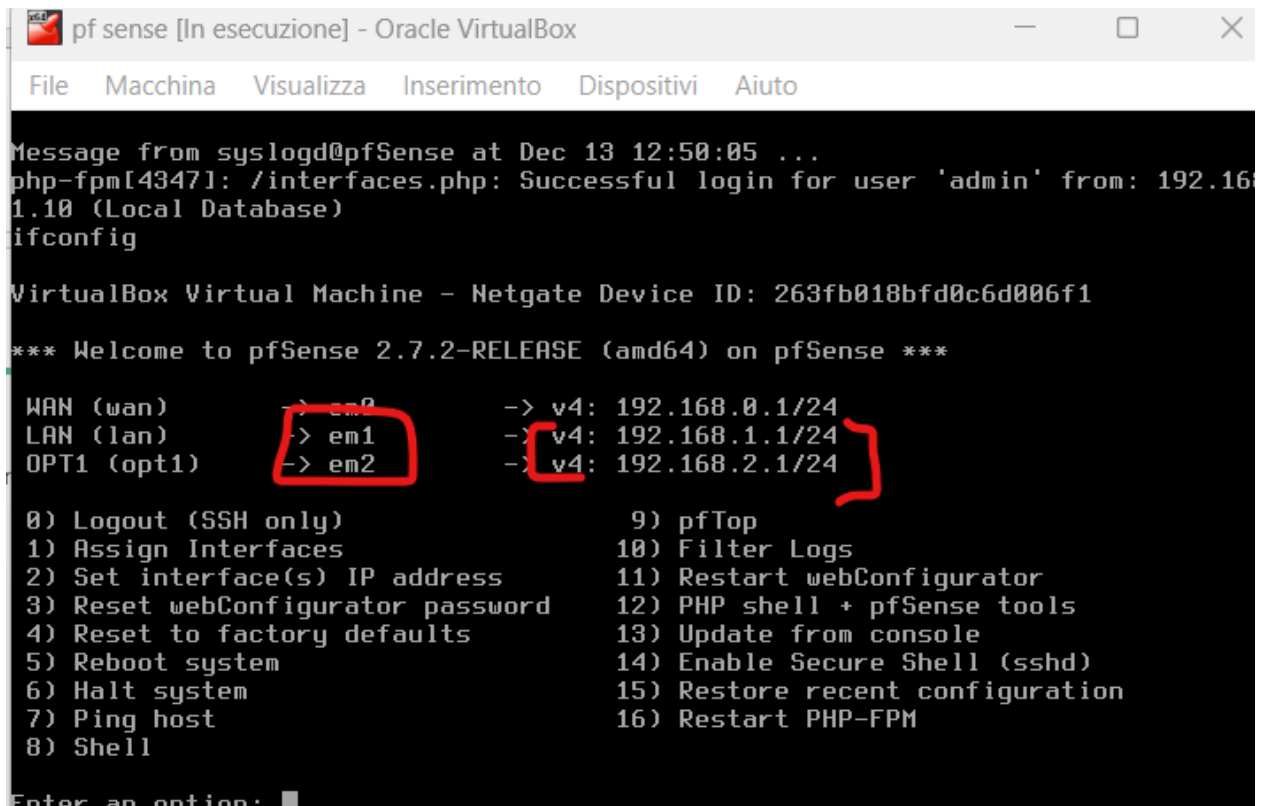
Porte seriali

Porta 1 Porta 2 Porta 3 Porta 4

OK Annulla Aiuto

assegniamo un nome qualunque (intnet2) e configuriamo come rete interna, ci servirà per inserirvi la nostra macchina metasploitable connessa alla seconda rete Lan.

1.2



```
pf sense [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Message from syslogd@pfSense at Dec 13 12:50:05 ...
php-fpm[4347]: /interfaces.php: Successful login for user 'admin' from: 192.168.1.10 (Local Database)
ifconfig

VirtualBox Virtual Machine - Netgate Device ID: 263fb018bfd0c6d006f1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.0.1/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.1/24

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: █
```

avviamo pf sense e vediamo di configurare gli indirizzi IP delle due reti LAN, usiamo il comando

2) ASSIGN INTERFACES

e procediamo seguendo le istruzioni per l'inserimento manuale, in questo caso disattiviamo anche il dhcp. nella mia configurazione come si può vedere ho assegnato le porte come segue

WAN → EM0 → 192.168.0.1

LAN → EM1 → 192.168.1.1

OPT(nome default per lan2) → 192.168.2.1

1.3

Rete

Scheda 1 Scheda 2 Scheda 3 Scheda 4

☒ Abilita scheda di rete

Connessa a: Rete interna

Nome: intnet2

Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)

Modalità promiscua: Nega

Indirizzo MAC: 08002769E8F2

☒ Cavo connesso

procediamo andando a sistemare la scheda di rete di metasploitable su rete interna

(la stessa configurata per la nuova scheda pfsense)

tramite virtual box e poi ad assegnare gli indirizzi IPV4 statici rispettivamente a kali e metasploitable:

```
(kali@kali)-[/home/kali]
PS> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::2b3e:921a:2485:2557 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3070 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

assegno 192.168.1.10 per il primo client connesso alla lan 1 (KALI)

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:69:e8:f2
    →    inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe69:e8f2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3498 errors:0 dropped:0 overruns:0 frame:0
          TX packets:844 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:263039 (256.8 KB)  TX bytes:157053 (153.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Assegno 192.168.2.10 a metasploitable.

se abbiamo effettuato correttamente i passaggi ora avremo

KALI - IP 192.168.1.10 connesso alla LAN 192.168.1.1

META - IP 192.168.2.10 connesso alla LAN 192.168.2.1

1.4

possiamo effettuare dei ping verso la rispettiva lan dai due terminali per verificarne il funzionamento

notiamo però che metasploitable non comunica correttamente, andiamo quindi a verificare da GUI se il traffico viene o meno permesso e notiamo subito che non vi sono regole a permetterlo al momento, quindi, la aggiungiamo noi tramite 'add'

Action Pass
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 OPT1
Choose the interface from which packets must come to match this rule.

Protocol Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source ☐ Invert match Any Source Address /

Destination ☐ Invert match Any Destination Address /

per ora, siccome vogliamo per il momento solo verificare la connessione tra le macchine, possiamo permettere qualunque tipo di traffico quindi selezioniamo any ovunque.

facciamo però attenzione a selezionare PASS e l'interfaccia corretta (nel nostro caso OPT 1) con family ipv4 ovviamente e protocollo tcp

ora che abbiamo consentito il traffico della macchina verso la rete lan rilanciamo il ping da metasploitable verso 192.168.2.1 e otteniamo un riscontro positivo

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data:  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=11.7 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.891 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.467 ms  
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=1.13 ms
```

1.5

Ora, le macchine sono correttamente connesse alle rispettive reti LAN, ma non sono ancora in grado di comunicare tra di loro, se inviamo un ping da ad es. Kali verso 192.168.2.10 non otteniamo risposta, e questo è dovuto alla mancata configurazione di un gateway che possa permettere la trasmissione di dati tra LAN differenti.

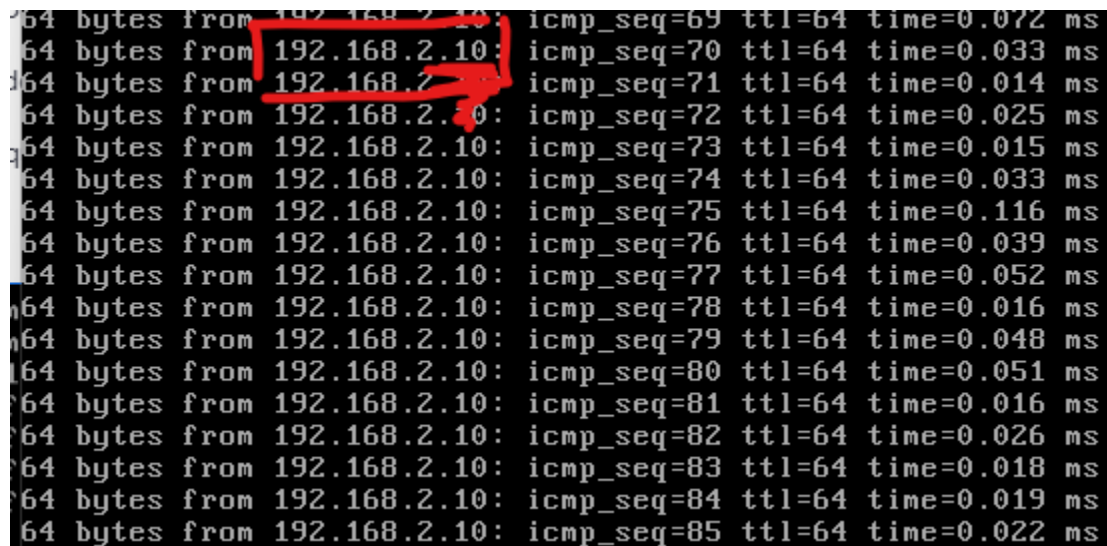
configuriamo il gateway per KALI con

```
sudo route add default gw 192.168.1.1
```

e su metasploitable con

```
sudo route add default gw 192.168.2.1
```

verifichiamo quindi se è ora possibile comunicare tra le due prima con un ping test:

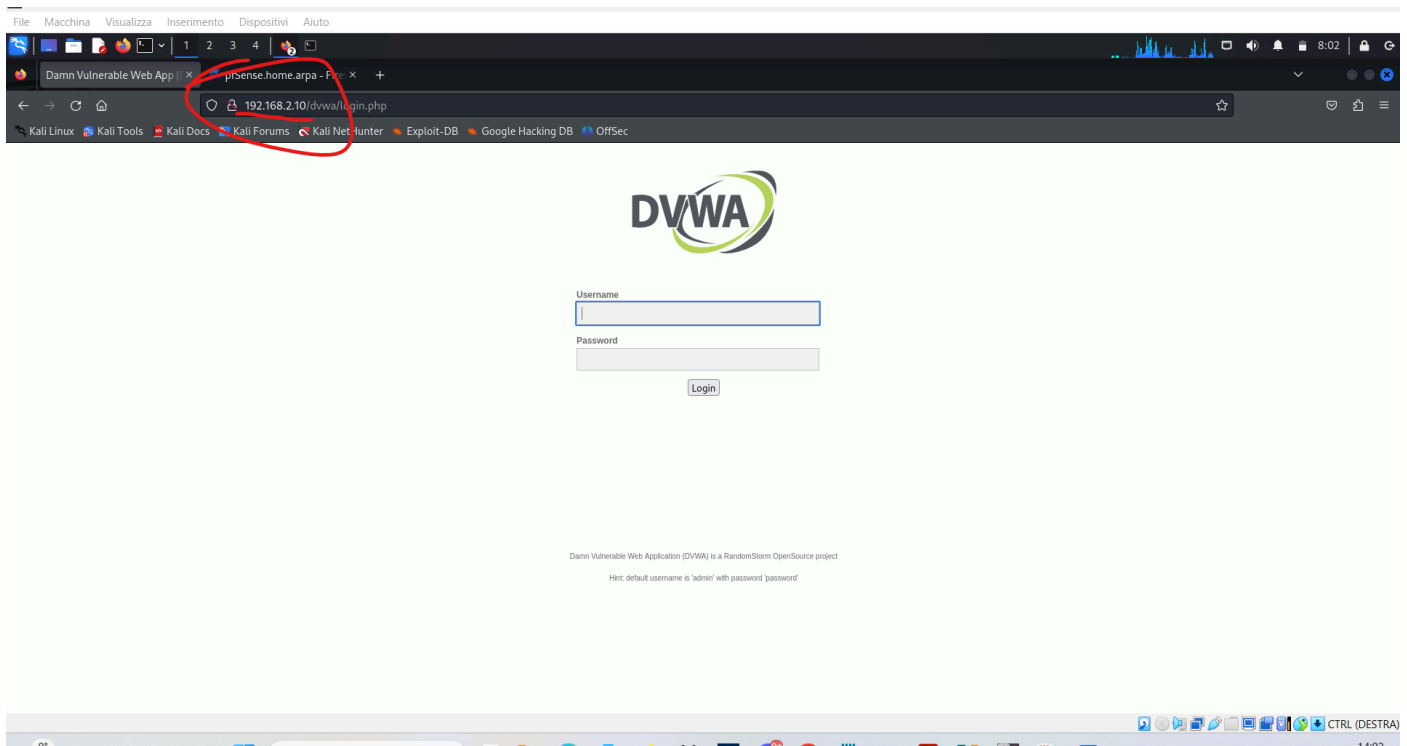


```
64 bytes from 192.168.2.10: icmp_seq=69 ttl=64 time=0.072 ms
64 bytes from 192.168.2.10: icmp_seq=70 ttl=64 time=0.033 ms
64 bytes from 192.168.2.10: icmp_seq=71 ttl=64 time=0.014 ms
64 bytes from 192.168.2.10: icmp_seq=72 ttl=64 time=0.025 ms
64 bytes from 192.168.2.10: icmp_seq=73 ttl=64 time=0.015 ms
64 bytes from 192.168.2.10: icmp_seq=74 ttl=64 time=0.033 ms
64 bytes from 192.168.2.10: icmp_seq=75 ttl=64 time=0.116 ms
64 bytes from 192.168.2.10: icmp_seq=76 ttl=64 time=0.039 ms
64 bytes from 192.168.2.10: icmp_seq=77 ttl=64 time=0.052 ms
64 bytes from 192.168.2.10: icmp_seq=78 ttl=64 time=0.016 ms
64 bytes from 192.168.2.10: icmp_seq=79 ttl=64 time=0.048 ms
64 bytes from 192.168.2.10: icmp_seq=80 ttl=64 time=0.051 ms
64 bytes from 192.168.2.10: icmp_seq=81 ttl=64 time=0.016 ms
64 bytes from 192.168.2.10: icmp_seq=82 ttl=64 time=0.026 ms
64 bytes from 192.168.2.10: icmp_seq=83 ttl=64 time=0.018 ms
64 bytes from 192.168.2.10: icmp_seq=84 ttl=64 time=0.019 ms
64 bytes from 192.168.2.10: icmp_seq=85 ttl=64 time=0.022 ms
```

e poi andando sull' IP di metasploitable tramite BROWSER:



possiamo cliccare su DVWA ora per andare a verificare se ci sono intoppi



e come vediamo l'accesso alla pagina ci viene concesso

1.6

ora procediamo col creare la nostra regola per impedire a kali di accedere a DVWA:

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 192.168.1.10 /

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 192.168.2.10 /

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.

Extra Options

torniamo sulla GUI da browser e accediamo alla sezione firewall - rules- LAN1

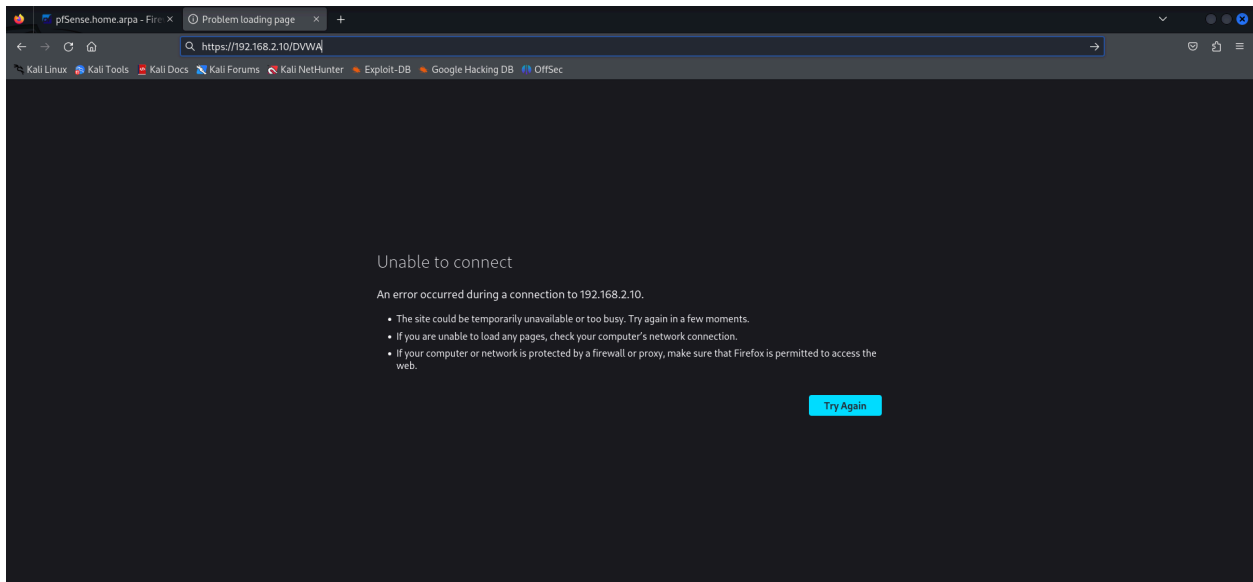
Clicchiamo su add e compiliamo come sopra:

inseriamo **BLOCK** per bloccare il traffico, selezioniamo l'interfaccia desiderata (LAN)

protocollo TCP perchè ci interessa solo bloccare il traffico http

e scegliamo la porta 80 che di default dovrebbe essere quella assegnata da metasploitable a DVWA

salviamo la nostra regola e procediamo ad effettuare la verifica, sempre tramite browser:



come possiamo notare ci è diventato impossibile visualizzare la pagina a causa del firewall impostato.

1.7

Possiamo inoltre verificarlo con la scansione delle porte da parte di kali verso metasploitable; nell'immagine sotto, possiamo confrontare due scan delle porte rilevanti effettuati uno **prima**, e uno **dopo** la regola posta su pfsense.

abbiamo usato il comando **nmap -F** che ci permette di vedere solo le porte comunemente più rilevanti

Come notiamo, tra la prima e la seconda scansione, la porta risulta "FILTERED" il che significa che non riusciamo a sapere se questa è effettivamente chiusa o aperta

```
File Actions Edit View Help
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

(kali@kali)-[~]
$ nmap -F 192.168.2.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 10:24 EST
Nmap scan report for 192.168.2.10
Host is up (0.0078s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    filtered http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

CONCLUSIONI: abbiamo impostato una regola per il firewall tramite pf sense, in modo da verificare la nostra capacità dell'utilizzo di pf sense al fine di escludere l'accesso di un determinato client a contenuti (in questo caso una porta specifica) di un'altra rete LAN. Questa Applicazione può essere molto utile in un'azienda per far sì che i dipendenti causino il minor numero possibile di danni, avendo accesso limitato, e che si possano mantenere riservate a determinate reti (o client) alcune delle porte disponibili per ovvie ragioni di sicurezza.

inoltre oscurare lo status di una porta la mette maggiormente in sicurezza da attacchi esterni e/O interni di qual sorta.

ESERCIZIO BONUS:

bloccare il traffico telnet da kali verso metasploitable

2.1

verifichiamo innanzitutto la presenza di traffico telnet autorizzato da kalia metasploitable

```
(kali㉿kali)-[~]  
$ telnet 192.168.2.10  
Trying 192.168.2.10 ...  
Connected to 192.168.2.10.  
Escape character is '^]'.  
  
metasploitable  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: 
```

2.2

per bloccare il traffico telnet ci serviremo dello stesso strumento utilizzato in precedenza su pf sense per bloccare il traffico verso DVWA, ma questa volta utilizzeremo la porta telnet (23) come oggetto del nostro blocco, procediamo:

The screenshot shows a firewall rule configuration page. Red arrows point to the following fields:

- Action:** Set to "Block". A red arrow points to the label "Action".
- Disabled:** The checkbox "Disable this rule" is unchecked.
- Interface:** Set to "LAN".
- Address Family:** Set to "IPv4". A red arrow points to the label "Address Family".
- Protocol:** Set to "TCP". A red arrow points to the label "Protocol".

Source Section:

- Source:** Set to "Address or Alias".
- Source Port Range:** Set to "any". A red arrow points to the "Source Port Range" label.

Destination Section:

- Destination:** Set to "Address or Alias".
- Destination Port Range:** Set to "Telnet (23)". A red arrow points to the "Destination Port Range" label.

seguiamo le indicazioni segnate nell'immagine e salviamo la nostra regola.

2.3

ora ri-eseguiamo la prova come in precedenza

```
(kali㉿kali)-[~]  
$ telnet 192.168.2.10  
Trying 192.168.2.10 ...  
telnet: Unable to connect to remote host: Connection timed out  
  
(kali㉿kali)-[~]  
$
```

e vediamo infatti che la porta telnet non ci consente più l'accesso.

Daniele Balani