

Configurazione Firewall pfSense e Blocco DVWA

Introduzione

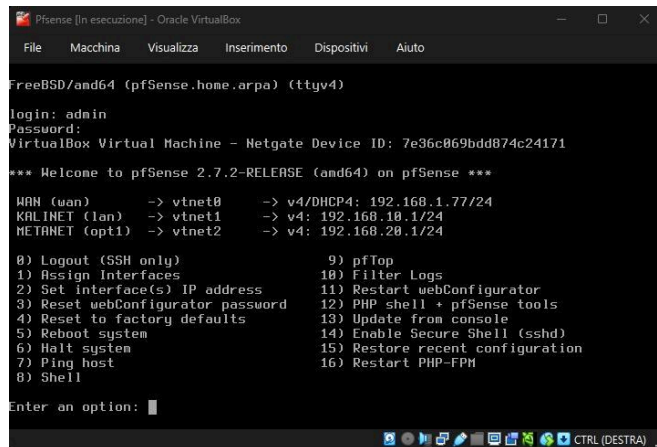
L'esercizio descrive la creazione di un firewall virtuale con pfSense in VirtualBox per controllare il traffico tra Kali Linux e Metasploitable2, mostrando sia il caso in cui l'accesso alla DVWA è bloccato sia quello in cui è consentito. Nel laboratorio sono presenti tre macchine virtuali: pfSense funge da router/firewall con tre interfacce (WAN, KALINET/LAN e METANET/OPT1).

Kali è collegata all'interfaccia KALINET -

Metasploitable2 all'interfaccia METANET.

L'obiettivo dell'esercitazione è creare regole firewall su pfSense per bloccare selettivamente le connessioni HTTP da Kali verso Metasploitable2 e verificare, tramite browser e ping, la differenza tra traffico filtrato e traffico consentito.

Di seguito la configurazione Pfsense :



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

FreeBSD/amd64 (pfSense.home.arpa) (ttyv4)
login: admin
Password:
VirtualBox Virtual Machine - Netgate Device ID: 7e36c869bdd874c24171

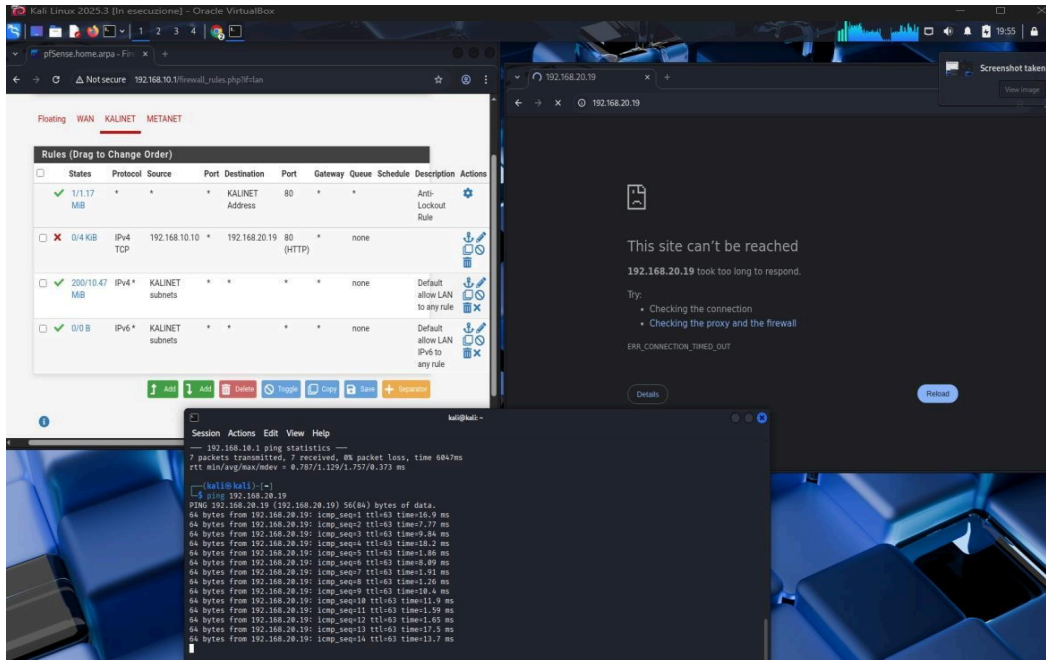
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.77/24
KALINET (lan)  -> vtnet1      -> v4: 192.168.10.1/24
METANET (opt1) -> vtnet2      -> v4: 192.168.20.1/24

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: 
```

Dopo aver salvato e applicato le regole del firewall, da Kali si testa la connettività verso Metasploitable2: il ping all'indirizzo 192.168.20.19 risponde regolarmente, perché la regola coinvolge solo il traffico TCP sulla porta 80, ma l'accesso HTTP dal browser produce "ERR_CONNECTION_TIMED_OUT". Questo comportamento dimostra che pfSense filtra il traffico a livello di porta: l'ICMP rimane consentito mentre le richieste HTTP vengono scartate dalla nuova regola di blocco.



Per ripristinare l'accesso alla DVWA è sufficiente disabilitare o cancellare la regola di blocco lasciando attiva soltanto la regola "Default allow LAN to any rule" sull'interfaccia KALINET. Una volta applicate le modifiche, ricaricando <http://192.168.20.19> dal browser di Kali compare la pagina iniziale di Metasploitable2, confermando che il traffico HTTP tra le due reti ora è nuovamente autorizzato.

