Manuel Di Gangi

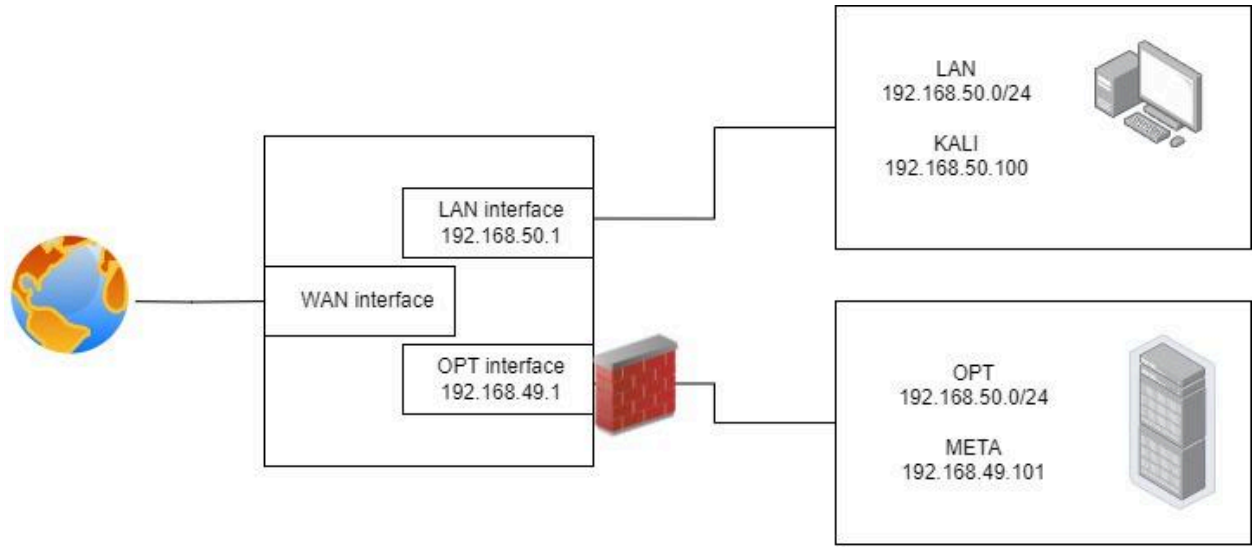
S5_L1

19 febbraio 2024

Traccia

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. 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.

Impostazione dell'ambiente

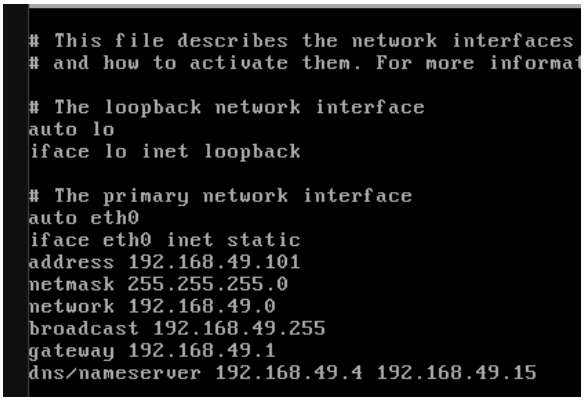


Impostazione di **PfSense**:

1. Installazione di PfSense
2. Impostazione delle interfacce di rete

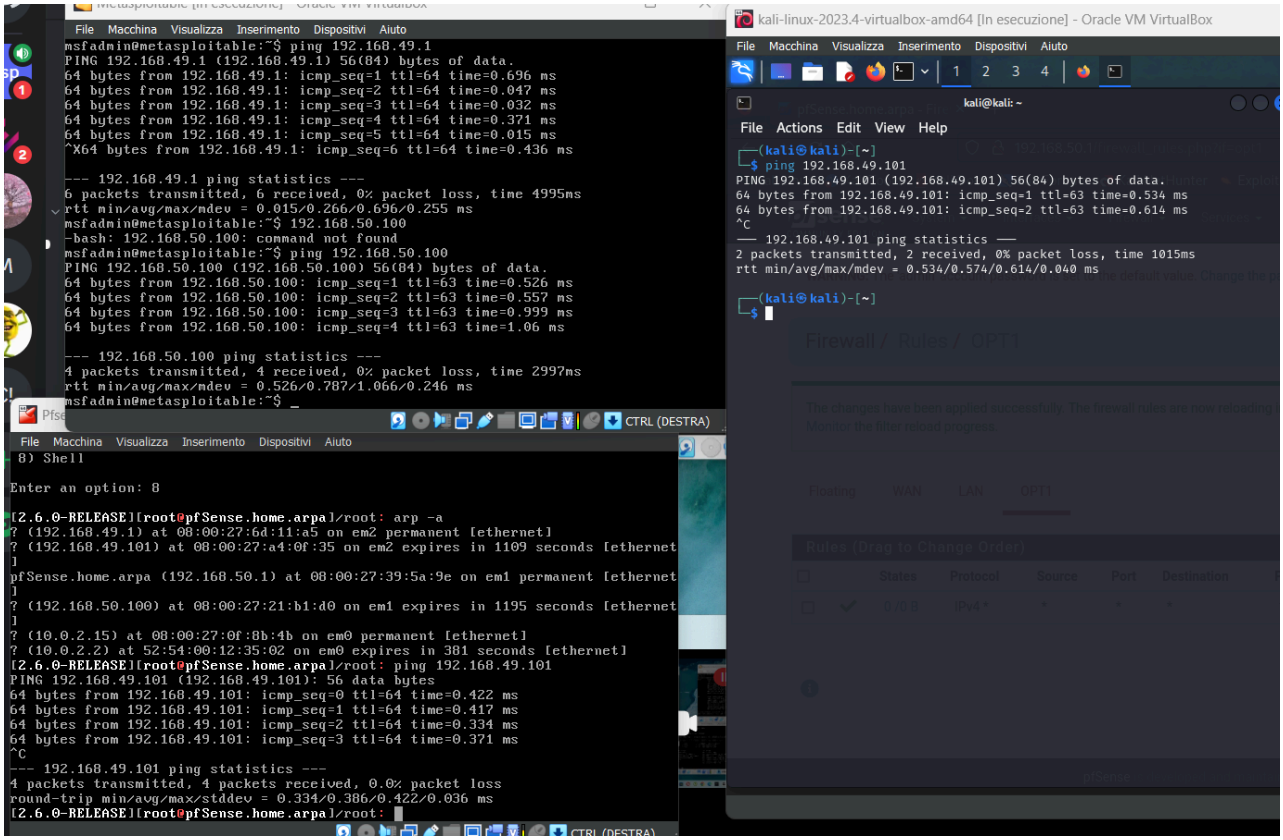
Impostazione di **Metasploitable**:

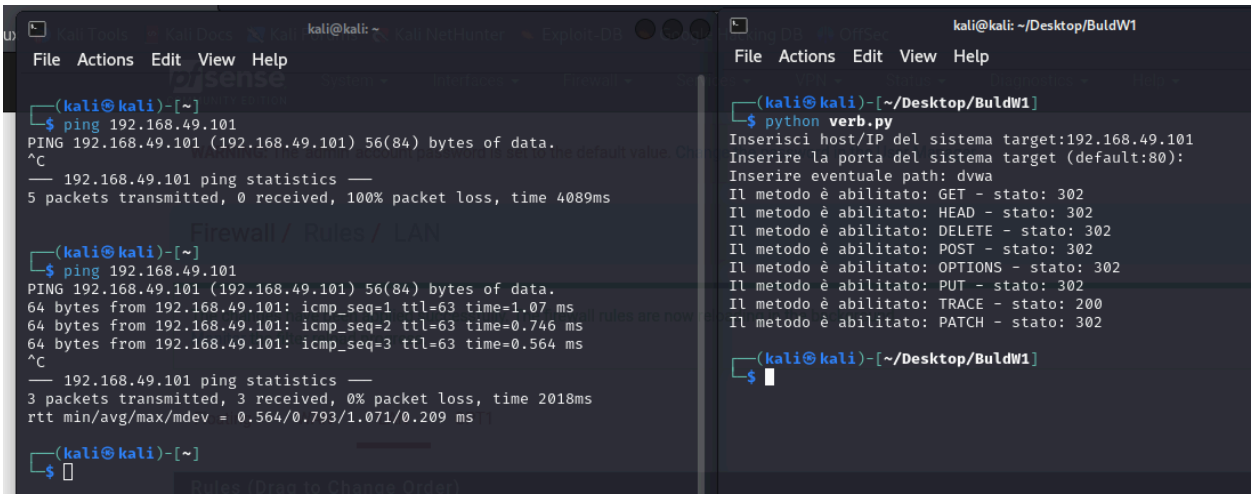
1. Modifica delle impostazioni della schede di rete
2. Riavvio servizi networking



Test funzionamento ambiente

Una volta terminato il settaggio dell'ambiente verifichiamo che le due macchine possano comunicare correttamente fra di loro. Come si può verificare dalle immagini seguenti, senza impostare alcuna restrizione le VM dialogano correttamente tra di loro, le richieste della Kali ricevono risposta ed entrambe le macchine si collegano ad internet.


File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ ping 192.168.49.1
PING 192.168.49.1 (192.168.49.1) 56(84) bytes of data.
64 bytes from 192.168.49.1: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 192.168.49.1: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 192.168.49.1: icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from 192.168.49.1: icmp_seq=4 ttl=64 time=0.371 ms
64 bytes from 192.168.49.1: icmp_seq=5 ttl=64 time=0.015 ms
^X64 bytes from 192.168.49.1: icmp_seq=6 ttl=64 time=0.436 ms
--- 192.168.49.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4995ms
rtt min/avg/max/mdev = 0.015/0.266/0.696/0.255 ms
msfadmin@metasploitable:~$ 192.168.50.100
-bash: 192.168.50.100: command not found
msfadmin@metasploitable:~$ 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=63 time=0.526 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=0.557 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=0.999 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=1.06 ms
--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.526/0.787/1.066/0.246 ms
msfadmin@metasploitable:~$ _
CTRL (DESTRA)
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=0.534 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=0.614 ms
^C
--- 192.168.49.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.534/0.574/0.614/0.040 ms
(kali㉿kali)-[~]
$
File Macchina Visualizza Inserimento Dispositivi Aiuto
8) Shell
Enter an option: 8
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: arp -a
? (192.168.49.1) at 08:00:27:6d:11:a5 on em2 permanent [ethernet]
? (192.168.49.101) at 08:00:27:a4:0f:35 on em2 expires in 1109 seconds [ethernet]
pfSense.home.arpa (192.168.50.1) at 08:00:27:39:5a:9e on em1 permanent [ethernet]
? (192.168.50.100) at 08:00:27:21:b1:d0 on em1 expires in 1195 seconds [ethernet]
? (10.0.2.15) at 08:00:27:0f:8b:4b on em0 permanent [ethernet]
? (10.0.2.2) at 52:54:00:12:35:02 on em0 expires in 381 seconds [ethernet]
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101): 56 data bytes
64 bytes from 192.168.49.101: icmp_seq=0 ttl=64 time=0.422 ms
64 bytes from 192.168.49.101: icmp_seq=1 ttl=64 time=0.417 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=64 time=0.334 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=64 time=0.371 ms
^C
--- 192.168.49.101 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.334/0.386/0.422/0.036 ms
[2.6.0-RELEASE][root@pfSense.home.arpa]/root:
CTRL (DESTRA)


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
^C
--- 192.168.49.101 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4089ms
(kali㉿kali)-[~]
$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=1.07 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=0.746 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=0.564 ms
^C
--- 192.168.49.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.564/0.793/1.071/0.209 ms
(kali㉿kali)-[~]
$
kali@kali: ~/Desktop/BuldW1
File Actions Edit View Help
(kali㉿kali)-[~/Desktop/BuldW1]
$ python verb.py
Inserisci host/IP del sistema target:192.168.49.101
Inserire la porta del sistema target (default:80):
Inserire eventuale path: dvwa
Il metodo è abilitato: GET - stato: 302
Il metodo è abilitato: HEAD - stato: 302
Il metodo è abilitato: DELETE - stato: 302
Il metodo è abilitato: POST - stato: 302
Il metodo è abilitato: OPTIONS - stato: 302
Il metodo è abilitato: PUT - stato: 302
Il metodo è abilitato: TRACE - stato: 200
Il metodo è abilitato: PATCH - stato: 302
(kali㉿kali)-[~/Desktop/BuldW1]
$

Creazione delle **firewall rules**:

Creiamo una regola che blocca ogni richiesta destinata all'indirizzo 192.168.49.101 sulla porta 80. Eseguendo lo script del verb scanner sviluppato la settimana scorsa vediamo che questo non riceve alcuna risposta dal server, nemmeno un errore 404, costringendoci a terminare il programma. Questo comportamento di mancata risposta ci indica che il firewall ha bloccato le richieste. Nonostante ciò possiamo comunque pingare Meta in quanto abbiamo bloccato solamente i servizi HTTP sulla porta 80.