PRACTICAL-4

AIM

Implementation of Windows/Linux security using firewall.

A. Block ICMP ping using OUTPUT chain and echo- reply.

B. Setup SPI Firewall that:

a. Allow all outgoing connection.

b. Block all unwanted incoming connection

THEORY

Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

ICMP

- The Internet Control Message Protocol (ICMP) is a protocol that devices within a network use to communicate problems with data transmission

SPI Firewall

- An SPI (stateful packet inspection) firewall protects you by examining incoming packets against existing connections.
- An SPI firewall can remember the attributes of each connection and use this info to determine the validity of a packet.
- It stores information it obtains by examining the packets and establishing rules. Thus, it sees the broader context of a packet, not only its contents.
- Due to this memory, the SPI firewall does not have to inspect every packet thoroughly, so it works faster than deep packet inspection (DPI).

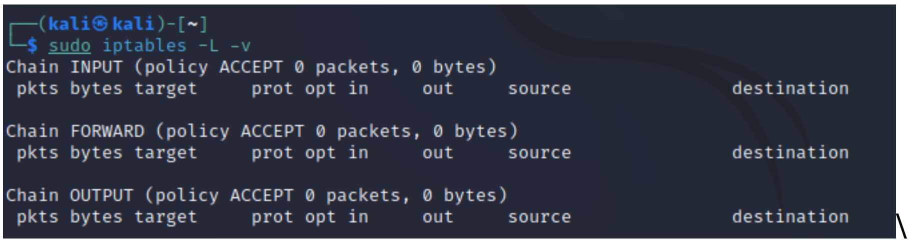
- The latter deconstructs the packets to check whether they are formed correctly and whether they include any malicious code.

- DPI is used for a wide variety of purposes including network management, security, data mining or internet censorship. It provides security at the expense of speed.

IMPLEMENTATION

Steps to block ICMP ping using output chain

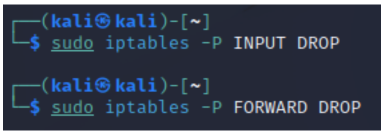
- To show the permission of iptables command.
  - sudo iptables -L -v



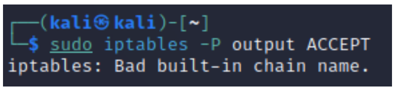
```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

\

- To enable Firewall perform the following.
  - sudo iptables -P INPUT DROP
  - sudo iptables -P FORWARD DROP
  - sudo iptables -P output ACCEPT

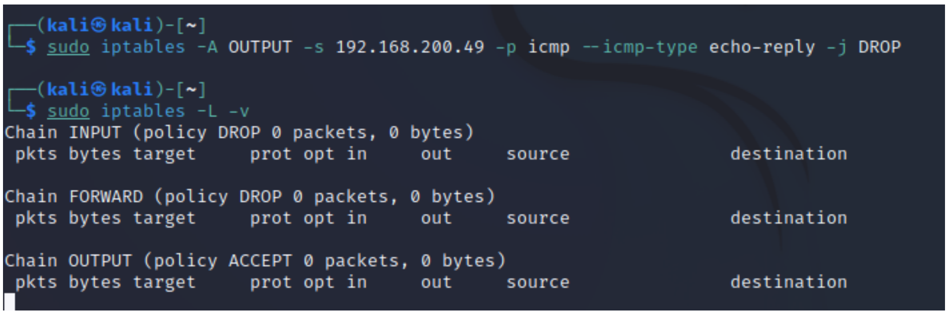


```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -P INPUT DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -P FORWARD DROP
```



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -P output ACCEPT
iptables: Bad built-in chain name.
```

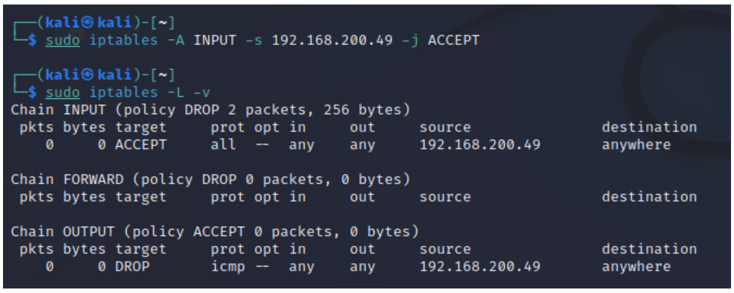
- To block ICMP ping, follow the commands:
  - sudo iptables -A OUTPUT -s 192.168.200.49 -p icmp --icmp-type echo-reply -j DROP



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A OUTPUT -s 192.168.200.49 -p icmp --icmp-type echo-reply -j DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

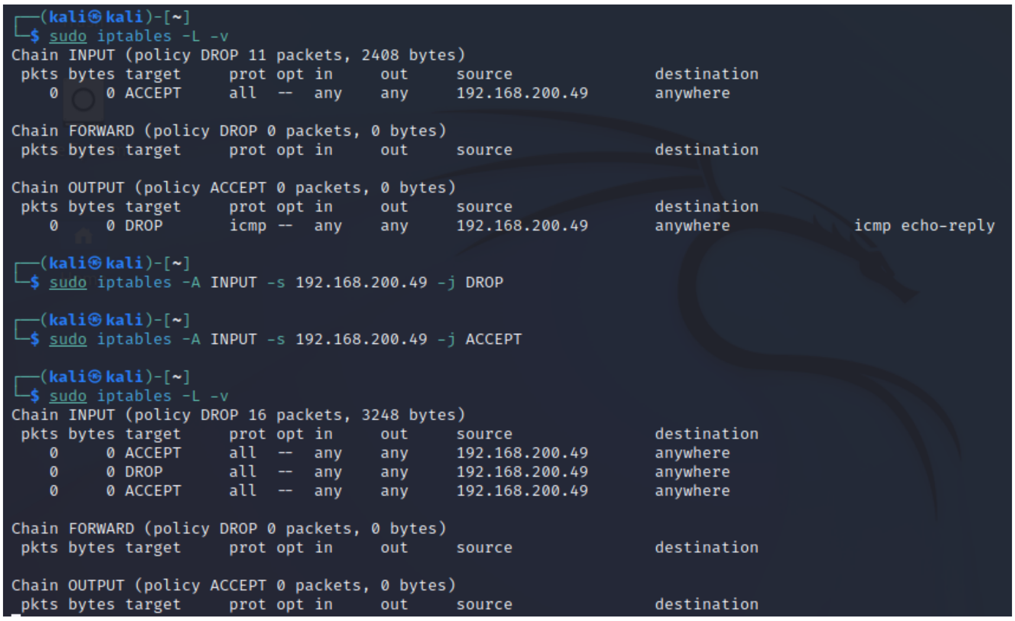
Allow all outgoing connections

- Perform the following commands:
    - sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy DROP 2 packets, 256 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    any     192.168.200.49       anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       icmp --  any    any     192.168.200.49       anywhere
```

Block all unwanted incoming connections



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy DROP 11 packets, 2408 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    any     192.168.200.49       anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       icmp --  any    any     192.168.200.49       anywhere             icmp echo-reply

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -s 192.168.200.49 -j DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy DROP 16 packets, 3248 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    any     192.168.200.49       anywhere
    0     0 DROP       all  --  any    any     192.168.200.49       anywhere
    0     0 ACCEPT     all  --  any    any     192.168.200.49       anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

CONCLUSION

- In this practical, I learnt how to block ICMP ping using output chain and echo-reply and how to setup SPI firewall.