# Q1

**ALLOW:** This action permits the packet to pass through the firewall and reach its destination.

**REJECT:** When a packet matches the filtering rules with a reject action, the firewall prevents the packet from reaching its destination. It will also send an ICMP error packet.

**DROP:** Dropping a packet means the firewall silently discards the packet without sending any response to the sender.

**LOG:** log a message with a description of the packet.

**NAT:** modify network address information in packet headers while in transit, it includes actions such as SNAT, DNAT, MASQUERADE.

# Q2

**Open Ports:** If a port is open and accessible without any filtering, Nmap will report the port as "open." This means that Nmap successfully established a connection to the specified port.

**Closed Ports:** If a port is closed and accessible without any filtering, Nmap will report the port as "closed." This means that the port is reachable, but there is no active service listening on it. The host actively responds with a TCP RST packet indicating that the port is closed.

**Filtered Ports:** If a port is filtered, meaning a firewall or some other network filtering device is blocking access to the port, Nmap will report the port as "filtered." Nmap cannot determine whether the port is open or closed because it did not receive a response from the scanned host.

# Q3

Masquerading, is a technique used in Linux to allow multiple devices on a private network to share a single public IP address when connecting to the internet or other external networks, similar to 1: MANY NAT.

When a server from a private, internal network wants to communicate with a device on the internet, the server's private IP address is replaced with the public IP address of the router (or a gateway device) before the packet is sent out onto the internet. When the response comes back, the router uses the mapping

information It stored to route the response back to the appropriate server on the private network.

**Benefits:**

**IP Address Conservation:** Masquerading allows multiple devices within a private network to share a single public IP address.

It also helps with the scarcity of IPv4 addresses.

**Enhanced Security and Network Isolation:** Masquerading adds a layer of security by hiding the internal network structure. External entities see only the public IP address and are unaware of the individual devices on the internal network.

# Q4

Port forwarding allows unsolicited connections on particular ports that are otherwise inaccessible via a NAT firewall. As a result, computers outside your private network can connect to it. it is a process that permits you to receive network traffic through a port number of your choice and make it accessible for others on the internet.

**Benefits:**

**Remote Access:** port forwarding allows remote computers, to attach to a non-standard port of a selected computer that's hidden within a personal network.

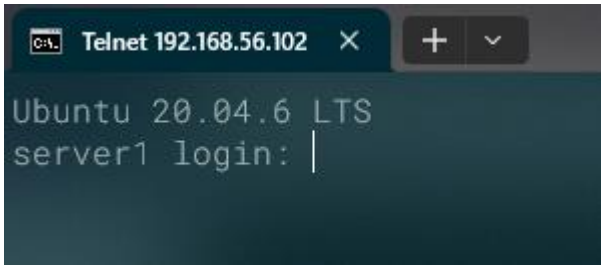
**Gaming:** Many online games require specific ports to be open for multiplayer or online gameplay.

**Extra Security:** Port forwarding provides you with an extra layer of online security, it is also used in VPNs.

# Q5

**telnet**

before:




Rule:

```
iptables -A INPUT -d 192.168.56.102 -s 192.168.0.0/16 -p tcp --dport 23 -j DROP
```

After:

```
C:\Users\Arshia>telnet 192.168.56.102
Connecting To 192.168.56.102...Could not open connection to the host, on port 23: Connect failed
```

**SYN limit**

Before:

```
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=80 flags=RA seq=28
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=80 flags=RA seq=29

--- 192.168.56.102 hping statistic ---
30 packets transmitted, 30 packets received, 0% packet loss
round-trip min/avg/max = 3.0/6.4/12.7 ms
```

Rule:

```
iptables -A INPUT -p tcp --syn -m limit --limit 20/minute -d 192.168.56.102  -j ACCEPT
```

```
iptables -A INPUT -p tcp --syn -d 192.168.56.102 -j DROP
```

test command:

```
hping3 -c 40 -S -p 80 192.168.56.102
```

after:

```
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=80 flags=RA seq=34
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=80 flags=RA seq=37

--- 192.168.56.102 hping statistic ---
40 packets transmitted, 17 packets received, 58% packet loss
round-trip min/avg/max = 0.5/4.7/9.2 ms
```

**http DNAT**

**I replaced the IPs in the question with IP of my machines**

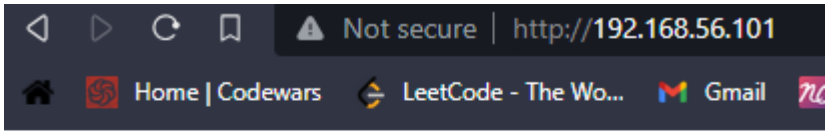
**I also used python's http.server module for a simple http service**

`sysctl -w net.ipv4.ip_forward=1`

`iptables -t nat -A PREROUTING -p tcp --dport 8080 -j DNAT --to-destination 192.168.56.101:80`

`iptables -t nat -A POSTROUTING -d 192.168.56.101 -p tcp --dport 80 -j SNAT –to-source 192.168.56.102`

main http server:

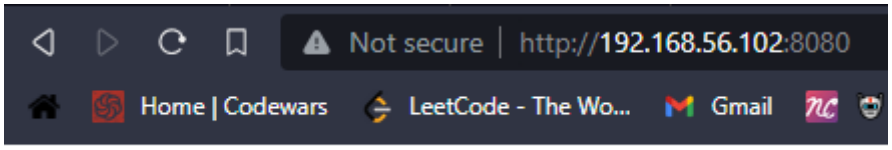



# Directory listing for /

---

---

Firewall server:




# Directory listing for /

---

---

**SNAT**

iptables -t nat -A POSTROUTING -o eth0 -s 192.168.56.102 -j SNAT --to-source 10.1.1.1

**DROP all packets from Firewall**

iptables -A OUTPUT -s 192.168.65.102 -j DROP

```
zero@server1:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.56.101 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1004ms
```

**FORWARD**

iptables -A FORWARD -d 192.168.179.120 -p tcp --dport 21 -j DROP