TASK 10

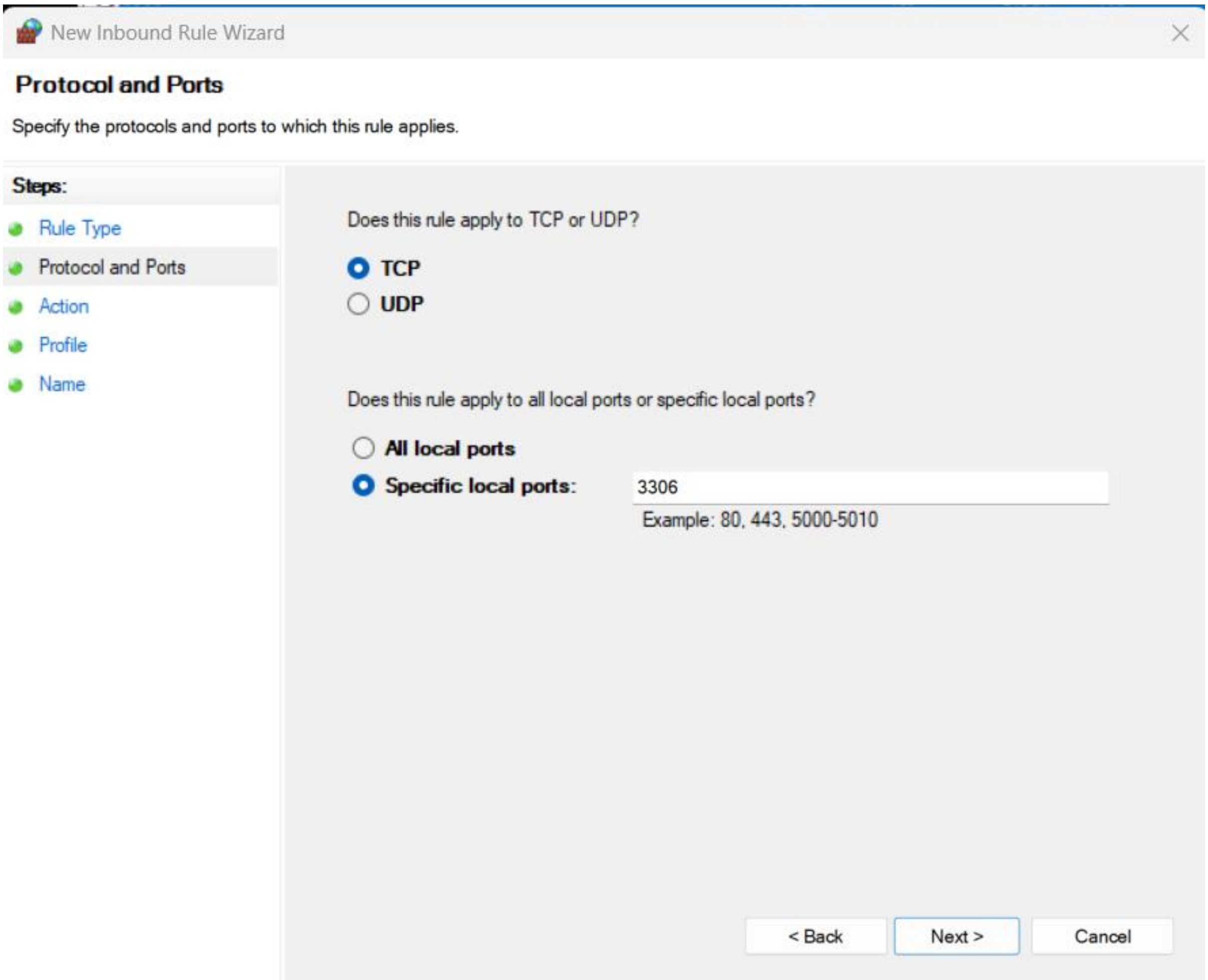
FIREWAL:

- Firewall is a concept of filtering and funnelling the network packets.
- It is a concept of monitoring and manging the incoming and outgoing traffic.
- It comes under both terms like software and hardware.
- Firewalls can be viewed as gated borders or gateways that manage the travel of permitted and prohibited web activity in a private network.

TYPES:

a) Network firewall
b) Host firewall

Blocking a port – Block inbound port 3306



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

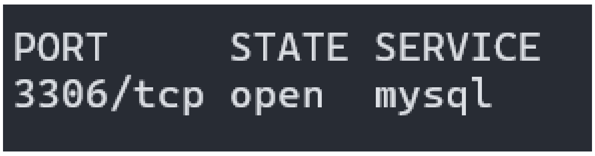
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 3306

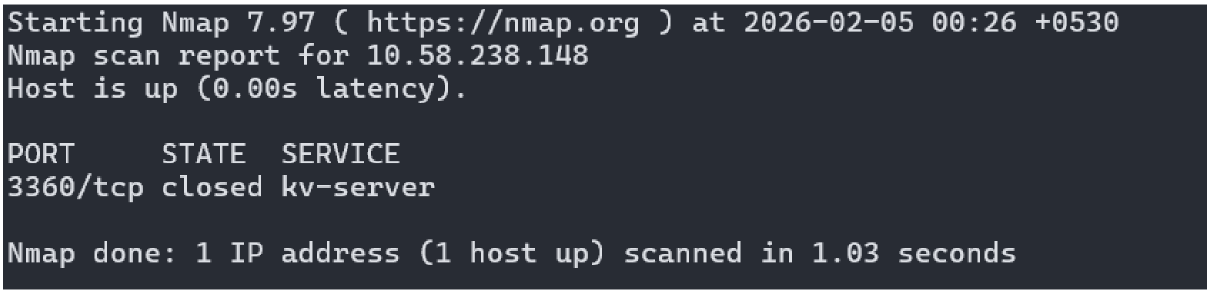
Example: 80, 443, 5000-5010

Blocking a port – by enrolling a new rule in inbound ports.



```
PORT     STATE SERVICE
3306/tcp open  mysql
```

To check whether the new rule is valid(working) or not:

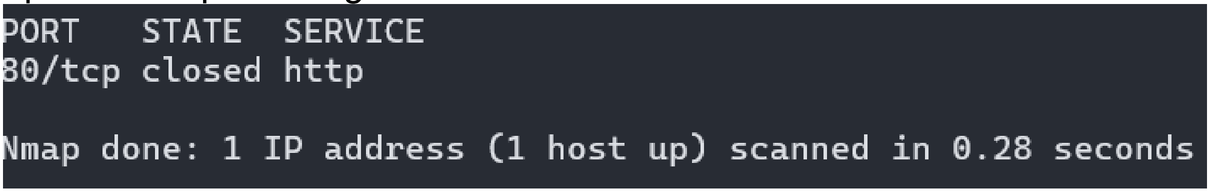


```
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-05 00:26 +0530
Nmap scan report for 10.58.238.148
Host is up (0.00s latency).

PORT     STATE  SERVICE
3360/tcp closed kv-server

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

- Using Nmap: nmap -p 3360 ip address
  It shows that the port is closed for inbound packets.

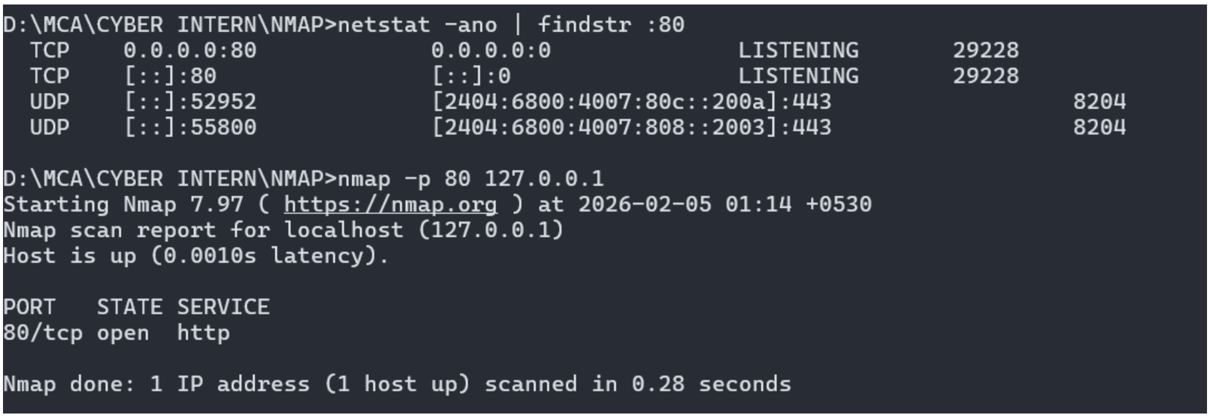
Enabling http port:

Mostly http port (80) is closed because of non secure transmission, so opened the port using firewall.



```
PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

After enabling an inbound firewall rule for TCP port 80, an HTTP service was started on the system. Netstat confirmed that the service was listening on port 80, and an Nmap scan verified that the port was accessible. This demonstrates the relationship between firewall rules and service availability.



```
D:\MCA\CYBER INTERN\NMAP>netstat -ano | findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       29228
  TCP    [::]:80                [::]:0                 LISTENING       29228
  UDP    [::]:52952             [2404:6800:4007:80c::200a]:443                  8204
  UDP    [::]:55800             [2404:6800:4007:808::2003]:443                  8204

D:\MCA\CYBER INTERN\NMAP>nmap -p 80 127.0.0.1
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-05 01:14 +0530
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0010s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```