Task 4 Security

Team Name: Horizon

Team Members:
Sohaila Ibrahim **52-21225** T-14
Hanya Abdo **52-20226** T-17
Nada Elbehery **52-8973** T-15
Omar Azzam **52-3187** T-14

Rule 1: Allow Web Server (192.168.1.2) to Access Web DB (192.168.1.3) via MySQL

iptables Command (On Web Database):

```
sudo iptables -A INPUT -p tcp -s 192.168.1.2 --dport 3306 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
sudo iptables -A OUTPUT -p tcp -d 192.168.1.2 --dport 3306 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 3306 -j DROP
```

Rule 2: Restrict Access to the Accounting DB (192.168.1.4) to Finance Subnet (192.168.2.0/24)

Where to Apply the Rule: On Router

```
# Allow Finance to access Accounting DB (MySQL)
sudo iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.1.4 -p tcp --dport 3306 -j ACCEPT

# Drop all other access to Accounting DBs MySQL
sudo iptables -A FORWARD -d 192.168.1.4 -p tcp --dport 3306 -j DROP
```

On the Accounting DB machine (192.168.1.4):

```
# Allow Finance subnet to access port 3306 (MySQL)
sudo iptables -A INPUT -p tcp -s 192.168.2.0/24 --dport 3306 -j ACCEPT

# Block all other access to port 3306
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP

sudo iptables -A OUTPUT -p tcp -d 192.168.2.0/24 --dport 3306 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 3306 -j DROP
```

Rule 3: Allow External Users to Access Web Server via HTTP/HTTPS Only

Where to Apply the Rule: On the Router

iptables Rules:

```
# Allow HTTP from external subnet
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 80 -j ACCEPT

# Allow HTTPS from external subnet
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 443 -j ACCEPT

# Drop all other traffic from external subnet to the web server
sudo iptables -A FORWARD -s 203.0.113.0/24 -j DROP
```

Rule 4: Allow Outbound Ping; Block Inbound Ping

Applied on: Router and Internal Hosts
iptables Rules (On the Router):

```
sudo iptables -A FORWARD -s 192.168.4.0/16 -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -A FORWARD -d 192.168.4.0/16 -p icmp --icmp-type echo-reply -j ACCEPT
```

On Each Internal Host:

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Explanation: Outbound ping (ICMP echo requests) is allowed for connectivity testing. Inbound ping is blocked to prevent reconnaissance and ICMP-based DDoS.

Rule 5: Only the IT Department Can Use SSH

Requirement: Only subnet `192.168.4.0/24` can access port 22.
Where to Apply the Rule: On Each Internal SSH-Enabled Machine

```
# Allow SSH from IT department
sudo iptables -A INPUT -p tcp -s 192.168.4.0/24 --dport 22 -j ACCEPT

# Block SSH from everywhere else
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

ON Router

```
sudo iptables -A FORWARD -p tcp -s 192.168.4.0/24 --dport 22 -j ACCEPT
```

Rule 6: Prevent Network from Being Transit Point for Unauthorized Traffic

Where to Apply: On the Router (192.168.1.1)
iptables Rule:

```
# Reject forwarding with ICMP error for unmatched traffic
sudo iptables -A FORWARD -j REJECT --reject-with icmp-host-unreachable
```

Phase 2: Snort Rules

Snort Rule 1: Detect Spoofed Internal Source on External Interface

```
drop ip 192.168.0.0/16 any -> any any (
    msg:"[ALERT] Spoofed Internal Source on External Interface";
    interface:eth0;
    sid:1000001;
    rev:2;
)
```

Explanation: Detects internal IPs on external interface—indicating spoofing.

Snort Rule 2: Detect Repeated Failed Login Attempts on Web Server

```
alert tcp any any -> 192.168.1.2 80 (
    msg:"[ALERT] Possible Brute-Force Login Attempt";
    content:"POST";
    content:"/login";
    http_method;
    threshold:type threshold, track by_src, count 5, seconds 10;
    sid:1000002;
    rev:1;
)
```

Snort Rule 3: Detect Bandwidth Spikes (Flooding/DDoS) on Web Server

```
alert tcp any any -> 192.168.1.2 80 (
    msg:"High HTTP Traffic (Possible DDoS)";
    threshold:type both, track by_dst, count 1000, seconds 10;
    sid:100006;
    rev:1;
)
```

Firewall Rules to Drop Excessive Connections:

```
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 80 \
    -m connlimit --connlimit-above 50 --connlimit-mask 32 -j DROP

sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 443 \
    -m connlimit --connlimit-above 50 --connlimit-mask 32 -j DROP
```

Snort Rule 4: Detect Stealth Port Scans

```
alert tcp any any -> 192.168.0.0/16 any (
    msg:"Stealth Port Scan - Incomplete Connection Attempt";
    flow:stateless;
    flags:S;
    detection_filter: track by_src, count 5, seconds 3600;
    sid:100008;
    rev:1;
    metadata:policy security-ips;
)
```

Snort Rule 5: Detect SQL Injection Attempts

```
drop tcp any any -> 192.168.1.2 80 (
    msg:"[ALERT] SQL Injection Attempt - OR ’1’=’1";
    content:"’ OR ’1’=’1";
    nocase;
    sid:1000005;
    rev:1;
)

drop tcp any any -> 192.168.1.2 80 (
    msg:"[ALERT] SQL Injection Attempt - UNION keyword";
    content:"UNION";
    nocase;
    sid:1000006;
    rev:1;
)
```

Snort Rule 6: Alert on Contact with Competitor IP

```
alert ip 192.168.3.0/24 any -> 203.0.113.45 any (
    msg:"[ALERT] Marketing Access to Competitor IP";
    sid:1000007;
    rev:1;
)
```

Firewall Rules Summary by Device

Router (192.168.1.1)

```
sudo iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.1.4 -p tcp --dport 3306 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.1.4 -p tcp --dport 3306 -j DROP
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 80 -j ACCEPT
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 443 -j ACCEPT
sudo iptables -A FORWARD -s 203.0.113.0/24 -j DROP
sudo iptables -A FORWARD -s 192.168.4.0/16 -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -A FORWARD -d 192.168.4.0/16 -p icmp --icmp-type echo-reply -j ACCEPT
sudo iptables -A FORWARD -p tcp -s 192.168.4.0/24 --dport 22 -j ACCEPT
sudo iptables -A FORWARD -j REJECT --reject-with icmp-host-unreachable
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 80 -m connlimit
    --connlimit-above 50 --connlimit-mask 32 -j DROP
sudo iptables -A FORWARD -s 203.0.113.0/24 -d 192.168.1.2 -p tcp --dport 443 -m connlimit
    --connlimit-above 50 --connlimit-mask 32 -j DROP
```

Web DB (192.168.1.3)

```
sudo iptables -A INPUT -p tcp -s 192.168.1.2 --dport 3306 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
sudo iptables -A OUTPUT -p tcp -d 192.168.1.2 --dport 3306 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 3306 -j DROP
```

Accounting DB (192.168.1.4)

```
sudo iptables -A INPUT -p tcp -s 192.168.2.0/24 --dport 3306 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
sudo iptables -A OUTPUT -p tcp -d 192.168.2.0/24 --dport 3306 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 3306 -j DROP
```

Internal Hosts (192.168.x.x)

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
sudo iptables -A INPUT -p tcp -s 192.168.4.0/24 --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

Phase 2: Snort Rules

Rule ID	Snort Rule
1	drop ip 192.168.0.0/16 any → any any (msg:”[ALERT] Spoofed Internal Source on External Interface”; interface:eth0; sid:1000001; rev:2;)
2	alert tcp any any → 192.168.1.2 80 (msg:”[ALERT] Possible Brute-Force Login Attempt”; content:”POST”; content:”/login”; http$_{m}ethod; threshold : typethreshold, trackby_{s}rc, count5, seconds10; sid : 1000002; rev : 1; $)
3	alert tcp any any → 192.168.1.2 80 (msg:”High HTTP Traffic (Possible DDoS)”; threshold:type both, track by$_{d}st, count1000, seconds10; sid : 1000006; rev : 1; $)
4	alert tcp any any → 192.168.0.0/16 any (msg:”Stealth Port Scan - Incomplete Connection Attempt”; flow:stateless; flags:S; detection$_{f}ilter : trackby_{s}rc, count5, seconds3600; sid : 1000008; rev : 1; metadata : policysecurity - ips; $)
5	drop tcp any any → 192.168.1.2 80 (msg:”[ALERT] SQL Injection Attempt - OR ’1’=’1’”; content:”’ OR ’1’=’1”; nocase; sid:1000005; rev:1;) drop tcp any any → 192.168.1.2 80 (msg:”[ALERT] SQL Injection Attempt - UNION keyword”; content:”UNION”; nocase; sid:1000006; rev:1;)
6	alert ip 192.168.3.0/24 any → 203.0.113.45 any (msg:”[ALERT] Marketing Access to Competitor IP”; sid:1000007; rev:1;)