Zero Trust Network Segmentation (Practical Task)

Objective

The goal of this task was to implement Zero Trust principles within a local network environment. This includes network segmentation and enforcing strict access control rules using iptables on Kali Linux.

Network Overview

The local network was segmented into three subnets:

• 192.168.10.0/24 — Department A

• 192.168.20.0/24 — Department B

• 192.168.30.0/24 — Department C

Each subnet represents a different trust zone.

Implementation Steps

Step 1: Allow Internal Access for Department A

Command used:

```
sudo iptables -A FORWARD -s 192.168.10.0/24 -j ACCEPT
```

Step 2: Block Department B from Accessing Department A

Commands used:

```
sudo iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.10.0/24 -j DROP

sudo iptables -A FORWARD -s 192.168.20.0/24 -j ACCEPT
```

Step 3: Block Department C from Accessing A and B

Commands used:

```
sudo iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.10.0/24 -j DROP
```

sudo iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.20.0/24 -j DROP

Step 4: Save Rules

Command used:

sudo iptables-save > zero-trust-rules.txt

Network Scanning (Verification)

Nmap was used to test the visibility of hosts in each segment:

nmap -sn 192.168.10.0/24

nmap -sn 192.168.20.0/24

nmap -sn 192.168.30.0/24

This confirmed that the segmentation was effective and that restricted communication paths were blocked.

Files Included

• zero-trust-rules.txt: Contains all applied firewall rules via iptables.

• Configuration screenshots: Proof of command execution and interface setup.

• This Word document: README explanation of setup and rules applied.

Conclusion

The configuration enforces Zero Trust principles by:
- Segmenting the internal network into trust zones.
- Applying strict firewall rules to control inter-department access.
- Minimizing lateral movement in the event of a breach.

This practical demonstration showcases how network-level policies can enhance security and reduce vulnerability in local environments.