Day 52

Exploitation Analyst

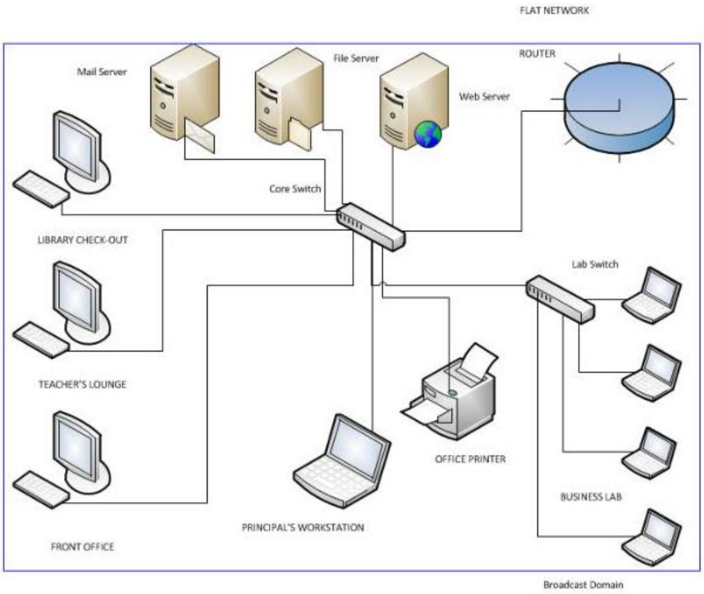
Network segmentation use case:

What is simple flat network?

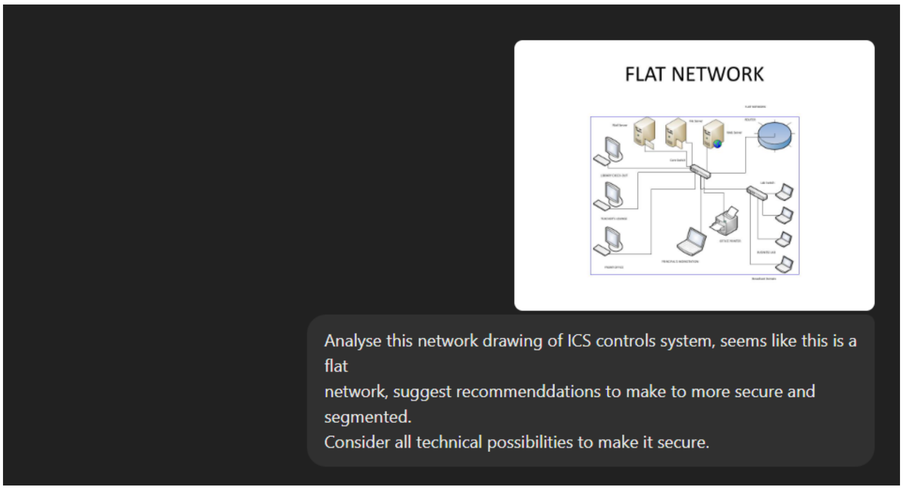
A simple flat network is when all devices—like computers, servers, and printers—are connected together in one big group with no separation.

- Easy to set up and manage when the network is small.
- Not very secure, because if one device is compromised, the attacker can reach all others.
- Becomes difficult to manage as more devices are added.

In cybersecurity, flat networks are avoided by creating segments (smaller groups) so that an attack in one group does not spread to the whole network.



Analysing using ChatGPT:



Analyse this network drawing of ICS controls system, seems like this is a flat
network, suggest recommenddations to make to more secure and segmented.
Consider all technical possibilities to make it secure.

Prompt:

Analyse this network drawing of ICS controls system, seems like this is a flat network, suggest recommendations to make to more secure and segmented. Consider all technical possibilities to make it secure.

Output:

1. Network Segmentation

- Divide the network into multiple VLANs (e.g., one for servers, one for office PCs, one for lab, one for printers).
- Use firewalls or layer-3 switches to control traffic between VLANs.
- Apply the principle of least privilege: only allow necessary communication (e.g., business lab should not directly talk to servers).

2. ICS / OT Security Zones

- Separate IT (business side) and OT (control side) networks with a firewall/DMZ.
- Place servers that need to communicate between IT and OT (like web or file servers) in a demilitarized zone (DMZ).
- Prevent direct internet access from control systems.

3. Access Control

- Use role-based access control (RBAC) to limit who can access servers, switches, and critical systems.
- Enforce network access control (NAC) so that only authorized devices can connect.

4. Monitoring and Logging

- Deploy IDS/IPS (Intrusion Detection/Prevention Systems) to monitor malicious traffic.
- Use SIEM (Security Information and Event Management) tools to collect and analyze logs.
- Enable NetFlow/sFlow on switches to detect unusual communication.

5. Segregate Critical Assets

- Mail, file, and web servers should not be directly reachable from all workstations. Put them behind an internal firewall.
- Printers and other non-critical devices should be isolated since they can be exploited.

6. Defense-in-Depth

- Use endpoint protection (antivirus, EDR) on all PCs and servers.
- Enable patch management for OS and applications.
- Use application whitelisting in ICS environments to block unauthorized software.

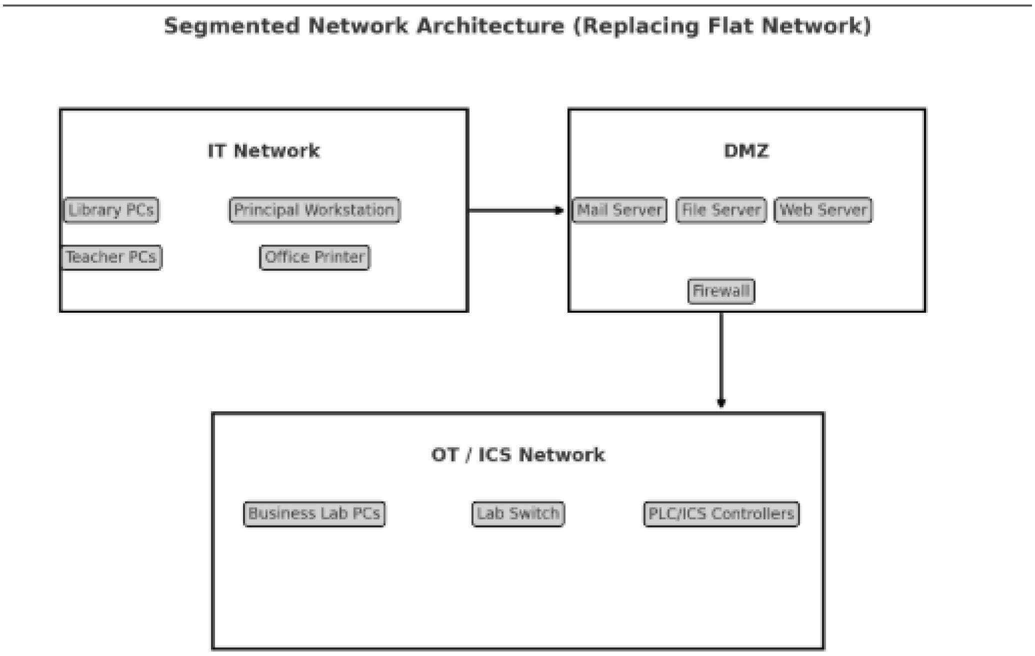
7. Secure Remote Access

- If remote maintenance is needed, use a VPN with MFA (multi-factor authentication).
- For vendors, give access through a jump server in the DMZ, not directly to the ICS network.

8. Redundancy and Fail-Safes

- Deploy redundant switches and firewalls to avoid single points of failure.

- Apply segmentation at Layer 2 and Layer 3 to ensure reliability and resilience.



--The End--