Module 16 Security threats and vulnerability

Types of vulnerabilities

- Technological Vulnerabilities → Intrinsical tech Vulnerabilities
- Configuration Vulnerabilities → Unsecure user accounts, misconfiguration of security policies, weak passwords
- Security policy vulnerabilities → Lack of authentication, lack of written policy.

Physical security

Hardware threats → Robo o destrucción del material

- Environmental → Temperature of humidity
- Electrical threats →
- Maintenance threats → No spare parts, poor cabling and poor labeling.

Malware

- Virus → Requires human interaction
- Worm → Replicates on their own, does not require human interaction.
- Trojan → Seem to be beneficious, require human interaction.

Network Attacks

- Reconissance → Mapping the network via tools like **nslookup and whois**
- Access Attacks → Unathorized manipulation of data.
- Denial of service → Disabling the corrupt network

Access Attacks

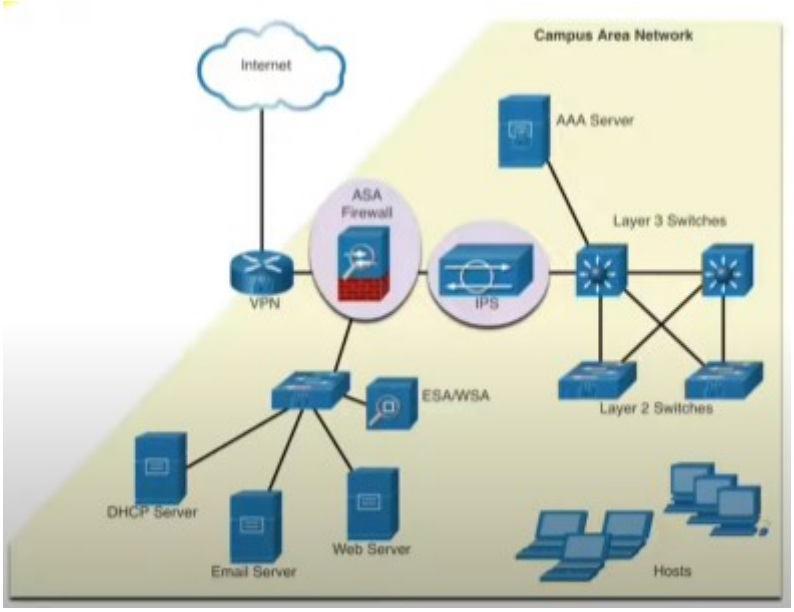
- Password Attacks
- Trust exploitation
- Port redirection
- MITM

Denial of service Attacks

Cheap easy and very destructive. The botnet is controlled from a **control node.**

Defense in depth

Layered defense approach



Backup

- Frequency
- Storage → Validation and test the recovery of the backup sollution
- Security → Preferably should be stored offsite
- Validation → Backups should be password protected.

Updates

It is really important that the end devices are updated and patched.

Authentication Authorization Accounting

- Authentication → Who is permitted to access the network.
- Authorization → What actions is the authenticated user is allowed to perform.
- Accounting → What actions has the user performed while in the network.

Network Attacks Mitigations

Types of firewalls

- Packet Filtering → Prevents or allows access based on IP and MAC
- Application Filtering → Prevents or allows access based on port numbers.
- URL Filtering

- Stateful Packet Inspection → Incomming packets must be requested from inside the network. If not the packet is prevented to enter the network.

Cisco Autosecure

This steps for securing the networks can be applied to any OS

- Default username and password must be changed immediatly.
- Access to system resources should be restriced only to those who are required to access them.
- Unnecesary services and applications should be uninstalled.
- Update any new hardware.

Password

- 8 – 10 characters.
- Mix Characters
- Change password often
- Do not write down password.
- Passfrace → Verbose passwords.

Enable SSH

1. Configure unique device hostname
2. Configure ID domain name
3. Generate key to encrypt ssh (360 – 2048) (Recommended 1024)
4. Verify and create a local Database Entry.
5. Authenticate against the local Database.
6. Enable VTY inbound.