**Week 2 & 3**

**Theory Content**

* 1. Encryption File System (EFS)

Diagram

Description automatically generated with medium confidence

* 1. Malware
* Malicious code intended to harm your environment

**Types of Malwares**

* Viruses
* Worms
* Trojan horses
* Ransomware (Locked out of system, ransom for access)
* Spyware
  1. Secure the Network

**Threats**

* DDOS attacks – Attacks availability of a server
* Malware – Virus, Worms, Trojans, Ransomware, Rootkits, Spyware
* Man-in-the-middle attacks – Intercept information to gather or manipulate information during transfer of it

**Mitigation**

* User education (Best protection)
* Mitigation of common network threats
  + DDoS-aware network application and services
  + Host-based firewalls
  + Antivirus software
  + Antimalware software
  + Secure communications
  1. IPsec
* Protocol suite that allows secure, encrypted communication between 2 computers

**Uses**

* Authenticate and encrypt host-to-host traffic
* Authenticate and encrypt traffic to specific servers
* Use L2TP/IPsec for VPN connections
* Site-to-Site tunnelling
* Enforce logical networks

**IPsec Rules vs Firewall Rules**

* Authenticate 2 computers before they begin comms VS FW allow traffic through but don’t authenticate or encrypt traffic
* Helps secure info being sent between 2 computers VS FW secure traffic only if a fw rules was previously configured
* IPsec uses key exchange, authentication, data integrity and data encryption (optionally)

**Configure IPsec**

* Use GPOs (Group policy objects) or firewall rules
* Predefined IPsec policies for the GPO method
  + Client (respond only)
  + Server (request security)
  + Secure Server (require security)

**1. Server Harderning**

**- Public Key Encryption**

**- Encrypting File System (EFS)**

**File encrpytion key = symmetric key (FEK) uses Public and Symmetric key encryption**

**Encrypt document with FEK**

**Create 3 copies of FEK**

**lock 1 using owner public key (DDF)**

**lock 1 using person who need access public key (DDF)**

**lock 1 using recovery agent public key (for when key is accidentally lost) (DRF)**

**- Malware Protection**

**2. Secure the Network**

**- Configure Windows Firewall and advanced security**

**Configure rules for both inbound and exbound. Eg, block ping from certain ip addresses/any ip address**

**- Implement IPSEC. Suite of protocols that allow secure encrypted communiccation between 2 computers**

**- Uses:**

**Authenticate and encrypte host-to-host traffic**

**Authenticate and encrypt traffic to specific servers**

**Use L2Tp for VPN connections**

**Site-to-site tunneling**

**Enforce logical networks**

**3. Secure File Services**

**- Use File Server Resource Manager**

**- Create Quotas (control how much is stored on ur file servers)**

**- File Screening (Control what types of data u can store on ur file server)**

**4. Manage Privileged Identities**

**- User rights (what task a user can complete, not = permission. Permission allows u to access a resource, right allows u to perform an action)**

**- Create taskpad (tool for nonadin users to use)**

**- Delegate privileges to users or groups**

**- Password policies Keep users account secure**

**- Account lockout policies Keep users account secure**

**5. Configure Advance Audit Policies**

**- Audit policy (Keep track of events in the domain, user logon/logoff)**

**- Manage Advanced audit policy (more options of how things can be configured on a granular level, more detailed)**