Master's Projects Agenda

Idea: Develop a secure network for a new small business.

- Design a network map / firewall setup & wifi chart.
- Design an Active Directory Server that deploys a file share to the 5 windows business virtual machines.
- Let the server control DHCP & DNS (not the firewall).
- Route all virtual machine DNS through the server.
- Setup group policies to limit users control of the machines.
- create a cyber security support plan.
- develop a customer Written Information Security Plan.
- develop a disaster recovery plan.
- setup backups for the workstations & server and design a plan for power outage.

Network Map:

1. **Internet Connection:**
   - Create a bridged network adapter for each VM to connect to the host's physical network.
   - Ensure that the host machine has a stable and secure internet connection.
2. **Utilize a Business-Grade Router/Firewall:**
   - Set up a VM with a dedicated firewall/router operating system (e.g., pfSense, OPNsense).
   - Connect this VM to two network adapters—one for WAN and one for LAN.

Firewall Setup:

1. **Stateful Inspection Firewall:**
   - Configure the firewall VM to perform stateful packet inspection.
   - Define rules to allow necessary services (HTTP, HTTPS, DNS, etc.) for business operations.
   - Block unnecessary ports and services.
2. **Define and Enforce Rules:**
   - Set up firewall rules to control incoming and outgoing traffic.
   - Regularly review and update firewall rules based on security requirements.

WiFi Chart:

1. **Secure WiFi Network with WPA3 Encryption:**
   - Set up a VM with a wireless adapter to act as a virtual access point.
   - Configure WPA3 encryption for the WiFi network.
2. **Separate Guest and Internal Networks:**
   - Create two virtual networks on VirtualBox—one for internal use and one for guests.
   - Assign the internal network to the VMs that need access to the main business network.
   - Assign the guest network to the virtual wireless adapter for guest access.
3. **Regularly Update WiFi Passwords:**
   - Implement a policy to periodically update WiFi passwords for enhanced security.
4. **MAC Address Filtering:**

- Configure MAC address filtering on the virtual access point to restrict access to known devices.
- Maintain a whitelist of authorized MAC addresses.

Additional Tips for VirtualBox Setup:

1. **Network Adapter Configuration:**
   - For each VM, configure network adapters as needed (Bridged, NAT, Internal Network) based on your network design.
2. **Internet Connectivity for VMs:**
   - Ensure that VMs have internet access by configuring the firewall/router VM to share its internet connection with the LAN.
3. **Testing:**
   - Thoroughly test the network setup to ensure proper connectivity and security measures.

Active Directory Server:

1. **Deploy a Windows Server as the Active Directory Domain Controller:**
   - Install a new VM in VirtualBox and choose the Windows Server operating system.
   - Follow the installation wizard to set up Windows Server.
   - Configure a static IP address for the VM.
2. **Configure DNS and DHCP services on the server:**
   - Open the "Server Manager" and add the "Active Directory Domain Services" role.
   - Promote the server to a domain controller and follow the wizard to install DNS.
   - Optionally, install the DHCP role and configure it to provide IP addresses to clients.

File Share:

1. **Create File Shares:**
   - Open "Server Manager" and go to "File and Storage Services" -> "Shares."
   - Create new shares for user data, following the wizard.
2. **Implement Access Controls:**
   - Right-click on the folder you shared, go to "Properties," and then the "Security" tab.
   - Set appropriate permissions for user groups, ensuring that only authorized users have access.
   - You can configure NTFS permissions and share permissions based on your security requirements.

Group Policies:

1. **Enforce Group Policies:**
   - Open "Group Policy Management" from "Server Manager."
   - Create new Group Policy Objects (GPOs) for different purposes (e.g., security, software installation).
   - Link the GPOs to the appropriate Organizational Units (OUs).
2. **Control User Permissions:**

- Use GPOs to control user permissions by configuring settings in the "User Configuration" section.
- Set restrictions on user accounts, control access to specific resources, and configure user desktop environments.

3. **Software Installations:**
   - Use the "Software Installation" setting in GPOs to deploy software to user machines.
   - Specify MSI packages for deployment.
4. **USB Usage Restrictions:**
   - Use Group Policies to restrict USB usage.
   - Navigate to "Computer Configuration" -> "Policies" -> "Administrative Templates" -> "System" -> "Removable Storage Access" and configure the relevant settings.
5. **Login Hours and Other Security-Sensitive Settings:**
   - Navigate to "Account Policies" and configure settings like login hours, password policies, etc.
   - Set security options in "Computer Configuration" for system-wide settings.

Cyber Security Support Plan:

1. **Regular Updates:**
   - Establish a routine for applying security patches and updates.
2. **Employee Training:**
   - Conduct regular cybersecurity awareness training for employees.
3. **Antivirus and Anti-Malware:**
   - Install and maintain up-to-date antivirus and anti-malware software.
4. **Incident Response Plan:**
   - Develop an incident response plan to address security breaches promptly.

Written Information Security Plan:

1. **Data Classification:**
   - Define and classify types of data based on sensitivity.
2. **Access Controls:**
   - Clearly define access control policies for different levels of data.
3. **Physical Security:**
   - Implement physical security measures for servers and networking equipment.

Disaster Recovery Plan:

1. **Backup Strategy:**
   - Regularly back up critical data to an offsite location.
   - Test the backup and restore procedures periodically.
2. **Redundancy:**
   - Implement redundancy for critical systems to minimize downtime.

Power Outage Plan:

1. **Uninterruptible Power Supply (UPS):**
   - Install UPS devices for critical systems to provide temporary power during outages.

2. **Generator:**
   - Consider a generator for more extended power outages.

Virtual Machines (VMs):

- Windows VM (VM1)
- Linux VM (VM2)
- Mac VM (VM3)
- Five Windows Business VMs (VM4-VM8)

Network Setup:

- Use VirtualBox networking options (e.g., NAT, Bridged, Internal Network) to simulate a secure network.
- Connect each VM to the internal network for communication.
- Configure the firewall on a dedicated VM or use the built-in firewall settings in each VM's OS.

Network Map / Firewall Setup & WiFi Chart:

- VM with firewall software (e.g., pfSense, OPNsense) acting as the network gateway.
- Virtual WiFi adapter for wireless connections (if needed).
- Map out the network connections, specifying IP addresses and subnets.

Active Directory Server:

- Windows Server VM (VM9) with Active Directory installed.
- Configure DNS and DHCP on the Active Directory server.
- Create a file share on the server for the business VMs.

Group Policies:

- Use Group Policy on the Active Directory server to enforce restrictions.
- Limit user control, set password policies, and control software installations.

Cyber Security Support Plan:

- Install antivirus software on each VM.
- Regularly update and patch all operating systems.
- Implement intrusion detection and prevention systems.

Written Information Security Plan (WISP):

- Document security policies, procedures, and guidelines.
- Outline roles and responsibilities for security.
- Define incident response procedures.

Disaster Recovery Plan:

- Regularly backup critical data and configurations.

- Create a plan for data restoration in case of data loss.
- Implement off-site backup storage for redundancy.

Backup Strategy:

- Use backup software (e.g., Veeam) on the server and workstations.
- Regularly backup data and configurations.
- Store backups on a separate virtual disk or external storage.

Power Outage Plan:

- Configure UPS (Uninterruptible Power Supply) for the server.
- Implement automatic shutdown procedures during power outages.
- Document procedures for recovering from unexpected shutdowns.

Example: For VM1

1. Creating the Windows VM (VM1):

- Install VirtualBox on your host machine.
- Create a new VM in VirtualBox and install Windows as the guest OS.
- Allocate appropriate resources (CPU, RAM, storage) based on your requirements.

2. Networking Configuration:

- Connect VM1 to the internal network for communication with other VMs.
- Choose a network adapter type (e.g., Intel PRO/1000) that suits your setup.
- Optionally, set up a second adapter for internet access (NAT or Bridged).

3. Windows OS Configuration:

- Install the necessary Windows updates and security patches.
- Set a static IP address for VM1 or configure DHCP if handled by the AD server.

4. Security Configuration:

- Enable the Windows Firewall and configure rules based on your network setup.
- Install and update antivirus software.
- Consider using BitLocker for disk encryption if sensitive data is involved.

5. Domain Join:

- Join VM1 to the Active Directory domain controlled by VM9 (the AD server).

- Ensure that DNS points to the Active Directory server for name resolution.

6. Group Policy Configuration:

- Use Group Policy to enforce security settings on VM1.
- Implement policies for password complexity, account lockout, etc.
- Apply restrictions based on user roles.

7. File Share Access:

- Access the file share provided by the Active Directory server (VM9).
- Set up mapped network drives for easy access to shared resources.

8. Backup Configuration:

- Install backup software on VM1 (e.g., Windows Backup or third-party tools).
- Schedule regular backups of important data to the server or external storage.

9. Power Management:

- Adjust power settings on VM1 to ensure optimal performance and energy efficiency.
- If using a laptop, configure power options to suit the business needs.

10. Monitoring and Logging:

- Enable Windows event logging for security monitoring.
- Regularly review logs for any unusual activities.

11. Applications and Software:

- Install necessary business applications on VM1.
- Keep all software up to date to mitigate security vulnerabilities.