**PROJECT 1 - INFRASTRUCTURE SECURITY**

**Active Directory Setup Report**

Madhuchandra Sethunath

**Objective:**

The goal of this project was to improve the security and management of the IT infrastructure by setting up a centralized Active Directory (AD) domain using Windows Server 2022. This would simplify user management, enforce strong security policies, and align with best practices like NIST and CIS standards. Ultimately, this move was aimed at reducing security risks and improving operational efficiency.

**Project Overview:**

This project set out to implement Active Directory (AD) as a solution for centralizing domain management, making user administration easier, and strengthening the overall security across the network. By using Windows Server 2022, Active Directory, and Group Policy Management Console (GPMC), I was able to organize users, enforce security policies, and ensure compliance with industry standards, making IT management much smoother.

**1. Setting Up Active Directory:**

To kick things off, I deployed Windows Server 2022 as the domain controller, which would serve as the central point for managing users, security, and network resources.

Steps:

1. Installed Windows Server 2022 on the designated server machine.
2. Configured the network settings, including IP and DNS.
3. Installed the Active Directory Domain Services (AD DS) role using Server Manager.
4. Promoted the server to a Domain Controller and created a new domain: mydomain.local

By doing this, the server was set up as the central hub for user and resource management within the domain.

**2. Client Configuration:**

Once the domain controller was in place, I needed to connect the client machines (running Windows 10) to the domain. This ensures that all users could be managed centrally, and security policies would apply to all client machines.

Steps:

1. On Windows 2022 server, I added A Windows 10 machine object under computers folder.
2. I also changed the adapter settings (to connect to the intended dns of windows server 2022) of windows 10.
3. Then the domain name was connected through advanced system settings.

Once done, the machines were successfully connected to the domain and could be managed via Active Directory Users and Computers (ADUC).

**3. Organizing Users:**

To keep things clean and manageable, I created Organizational Units (OUs) like "Executives" and "Research", and within these, I set up role-based groups.

Steps:

1. Using ADUC, I created two OUs: one for Executives and one for Research.
2. Created appropriate security groups within each OU, such as Executives Group and Research Group.
3. Assigned the correct permissions to these groups based on the roles.

By organizing users into these OUs, I could easily manage access, security policies, and group-based permissions for different roles.

**4. User Management:**

The next step was creating user accounts and adding them to their respective groups. This ensured that each user had access to the resources they needed, and security settings were applied correctly.

Steps:

1. Created individual user accounts (melanie and tony) in ADUC for users in the Executives and Research groups.
2. Assigned users to their respective groups, like placing executive users in the Executives Group.
3. Tested the login functionality by signing in with a few accounts to make sure everything worked.
4. I also ensured connectivity between windows 10 and windows 2022 server by implementing ping in the cmd.

This step ensured that all user access was properly configured, and users could log in without issues.

**5. Implementing Security Policies:**

To ensure strong security practices, I applied several security policies using Group Policy Objects (GPOs), including password settings, login hours, and audit logging. These policies were aligned with NIST and CIS standards.

Steps:

1. **Password Policies**:
   * Enforced strong password complexity and set minimum length requirements.
   * Configured password expiration and history policies.
2. **Login Hours**:
   * Restricted login hours for to ensure users could only access the network at specified times.
3. **Audit Logging**:
   * Enabled logging for login attempts, account changes, and policy modifications. Configurations were set for deciding success and failure for each of them. Some were excluded to avoid traffic in audit logging.
4. **Account Lockout Policies**:
   * Set limits for failed login attempts to prevent brute force attacks.

These security measures were applied through GPMC to ensure compliance with industry standards.

**6. Compliance and Reporting:**

After configuring the security policies, it was essential to verify that they were applied correctly. I used the Resultant Set of Policy (RSoP) tool to generate reports and ensure compliance with NIST and CIS guidelines.

Steps:

1. Ran the gpresult /h command in Command Prompt to generate the RSoP report in HTML format.
2. Reviewed the generated report to ensure the correct policies were applied and aligned with the security standards, confirming no configurations were missed.

This step provided confidence that the policies were correctly implemented and aligned with the organization's security goals.

**7. Testing and Validation:**

The last step was to verify that everything was working as expected. I validated user access, checked security logs, and reviewed the audit trails to ensure that the security settings were properly enforced.

Steps:

1. **User Access**: Logged in with 2 test accounts (madhu and mike) to make sure the policies worked and that users had the right access. I was able to log in with credentials of mike. Permissions of folders and files were checked. Madhu’s login attempt was blocked as it violated the logon timing.
2. **Security Logs**: Used **Event Viewer** to monitor any failed login attempts or unusual activities.

During the security monitoring process, I reviewed the following key event logs to validate the effectiveness of security policies and user activity:

* **Account Logon Events:**
  + Event ID 4624 (Successful logon): Verified successful logon events to confirm user authentication and system access.
* **Object Access:**
  + Event ID 4663 (Object access): Monitored access to sensitive objects and resources to ensure compliance with access control policies.
* **Account Management:**
  + Event ID 4720 (User account creation): Reviewed user account creation events to confirm that new accounts were created according to security policies.

1. **Audit Compliance**:

As of 12/13/2024, the domain controller’s security configuration was reviewed and found to demonstrate strong adherence to NIST and CIS benchmarks. Key highlights include:

* **Policy Management:**
  + Successful application of the Default Domain Controllers Policy
  + No errors detected during the policy refresh
  + Comprehensive security coverage across critical infrastructure
* **Audit and Security Controls:**
  + Full compliance with Group Policy Infrastructure
  + Audit Policy Configuration implemented and validated
  + Properly configured registry security
  + Overall security settings meet baseline requirements

The following were the conclusions drawn from the comparison with gudelines:

* Consistent domain controller configuration
* No unauthorized policy modifications detected
* Structured security policy management

Thus, it was substantially aligned with industry security standards.

This final step helped verify that the entire system was secure, compliant, and functioning as intended.

**Conclusion:**

The project was a success in setting up a centralized Active Directory domain with Windows Server 2022. By creating OUs, organizing users into groups, enforcing security policies, and validating compliance with industry standards like NIST and CIS, the security and manageability of the organization's IT infrastructure was significantly improved.

**References:**

* Microsoft Documentation on Active Directory and Group Policy.
* NIST and CIS Security Standards.

Please refer to the attached screenshots and RSoP report for a detailed view of each process.