Chapter 10: Active Directory Usage & Hardening

In this laboratory exercise, the student will be introduced to the basic concepts of Active Directory and configure a domain, create group policy objects, and harden a domain controller.

10.1 Laboratory Exercise

Active Directory Usage & Hardening

10.1.1 Specifications

This lab exercise will be performed on Windows Server 2016, hereon referred to as **the Windows Server**. A trial version of Windows Server 2016 was used for development.

10.1.2 Learning Objectives

- Configure Windows Server
- Configure Active Directory
- Understand the Concept of Active Directory and Domain Controllers

10.1.3 Mapping to NIST Nice Framework

This laboratory exercise is intended to increase the student's familiarity with Active Directory and Group Policy. This exercise is skills application heavy. This laboratory exercise maps to the following KSAs from the NIST NICE Framework:

- Cybersecurity and Privacy Principles (K0004)
- Cyber Threats and Vulnerabilities (K0005)
- Test and Evaluation Processes (K0250)
- Recognize Types of Vulnerabilities (S0078)
- Apply Cybersecurity and Privacy Principles to Organizational Requirements (S0367)
- Apply Cybersecurity and Privacy Principles to Organizational Requirements (A0123)

10.1.4 Necessary Background and Expected Completion Time

This laboratory exercise can be completed by students with varying background and experience. The following categories should help identify approximately how much time (in minutes) will be necessary to complete the laboratory exercise, for a student meeting the criteria for the respective experience level.

- Beginner: A student in this category has little to no experience with the basics of active directory, group policy, and Windows Server.
- Intermediate: A student in this category is familiar with the basics of active directory, group policy, and Windows Server. This student may have hands-on experience using Windows Server.
- Advanced: A student in this category has experience with the basics of active directory, group policy, and Windows Server. This student also has hands-on experience using Windows Server, possibly a background as a systems administrator.

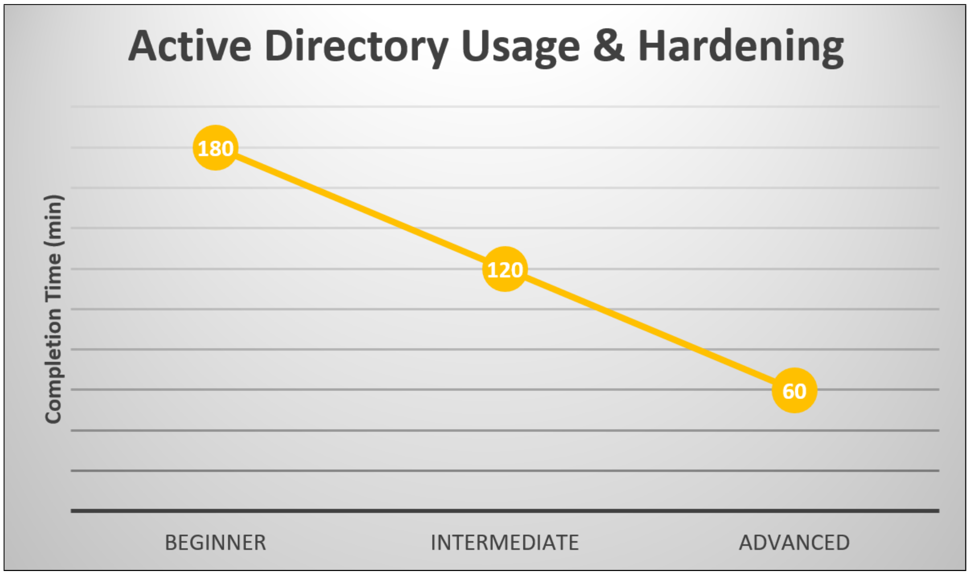

Figure 10.1: *Active Directory Usage & Hardening Laboratory Exercise Expected Completion Time (min)*

10.1.5 Configuration and Setup

The machine for this laboratory exercise does not require any custom configuration as the exercise requires the student to configure a Windows Server using Active Directory and Group Policies.

10.1.6 Challenges

Brief Introduction to Active Directory

Active Directory is a service typically found on Windows Server operating systems. Active Directory is a suite of configuration tools created by Microsoft which can be used to perform remote administration of systems [93]. Active Directory, short for the term *Active Directory Domain Services* [93], is a service which can be enabled on a Windows Server; when used to control and configure a group of machines, this server becomes known as a *Domain Controller* [93]. A domain controller can be used to remotely push policies, known as *Group Policies*, to all systems on the domain. In the following tasks, you will enable and configure Active Directory on a Windows Server, create Group Policy Objects, and perform a few basic domain controller hardening tasks.

1. Configure the Windows Server to have the hostname `CYOTEE-DC`

2. Configure the Windows Server to have an IPv4 address of `192.168.7.20` and a default gateway of `192.168.7.1`.

3. Configure the Windows Server to use itself as its preferred DNS Server and do not set an alternate DNS server.

4. Configure the Windows Server to reflect your time zone.

5. Install Active Directory on the Windows Server.

6. Create a new domain `cyotee.local` in a new forest.

7. Configure the Forest Functional Level to Windows Server 2008.

8. Configure the Domain Functional Level to Windows Server 2008.

9. Ensure that the Windows Server is configured as a Global Catalog server.

10. Ensure that the Windows Server is configured as a DNS Server.

11. Configure DNS on the Windows Server to use the external DNS server with IPv4 address `192.168.7.30` as a forwarder.

12. Configure the Windows Server to not allow **root hints**.

13. Create the following Organizational Units in Active Directory.

    - Professors
    - Staff

14. Create the following three users in each of the Organizational Units. The username naming convention should be <firstname>.<lastname>@<domain>. Spaces or punctuation within a name should be omitted. Create a default password for each user (`Password123`) but require they change their password at the next login.

    - Professors

    - Emma Castillo
    - Jeanette Wise
    - Bernadette Rivera
  - Staff
    - Boyd Harmon
    - Jeremiah Houston
    - Adrian Miles

15. Create a new Security Group in each Organizational Unit with the same name as the Organizational Unit. The Security Group should be Global.

16. Add the three users in each Organizational Unit to the respective Security Group.

17. Create a Shared Folder for each Organizational Unit. The name of the Shared Folder should be the same as the name of the Organizational Unit with the word **Folder** appended to it (ex: StaffFolder). The only users who belong to the Organizational Unit should have access to the folder. The network path to the folder should be \server\share\<foldername>.

18. Create a new site called CYOTEE. Add the Windows Server to the new site.

19. Create a new Group Policy Object (GPO) and link it to the domain. The new GPO should match the following specification:

    - Name the GPO cyotee-pol.
    - Create a Folder Redirection policy to map the Documents folder to a network share on the Windows Server located at \\server\share\network-share.
    - Remove Run from the Start Menu.
    - Configure Control Panel to only start in icon view.
    - Block use of regedit.exe to mitigate against users editing the registry.
    - Disable the ability for users to access the command prompt.
    - Disable the ability for users to change the system time.

- Block use of `taskmgr.exe` to disable the ability for users to access the Task Manager.

20. Install the File Server Resource Manager role. Configure it according to the following specification:

    - Install the File Server Resource Manager on the Windows Server.
    - Create a text file in the user's `Desktop` directory containing the word *classified.*
    - Create a Classification Property called `Classified Property`.
    - Create a Classification Rule called **Classified Files** for files which contain the word *classified.*
    - Apply the Classified Files rule to the user's Desktop directory.
    - Verify whether or not the classification rule was applied properly by running the classification.

21. Create a File Screen which meets the following specifications:

    - Block all `.bat` and `.exe` files from running.
    - Apply the screen to the `My Documents` directory.
    - Generate an appropriate warning message.
    - Verify that the screen works by attempting to run a .bat file in the affected directory.

22. Reduce the Attack Surface by Removing Browsers

    One suggestion made in Microsoft's online documentation of Windows Server, in order to improve the security of domain controllers, is to remove all web browsers [94]. The article states:

> *"Browsing the Internet (or an infected intranet) from one of the most powerful computers in a Windows infrastructure using a highly privileged account (which are the only accounts permitted to log on locally to domain controllers by default) presents an extraordinary risk to an organization's security. Whether via a drive by download or by download of malware-infected "utilities," attackers can gain access to everything they need to completely compromise or destroy the Active Directory environment."*

Task: To mitigate against this risk, remove all web browsers from the domain controller (Windows Server).

23. Apply Principles of Least Privilege

    In Active Directory, there are three levels of administrators, namely: Built-In Admins (BA), Domain Admins (DA), and Enterprise Admins (EA). The BA group tends to have many users because they are thought to have less privileges than those in the DA and EA groups. This may be true, the base privileges granted to BA members is less than that of DA and EA members. This becomes irrelevant when noting that a member of any of the three groups can modify the membership of other groups, effectively gaining administrative control over all systems in the nested group [95]. It is suggested that administrative privileges only be granted to users who absolutely require the role to perform their tasking [96].

    Task: Reduce the number of administrators on a domain, including built-in administrators. Regularly monitor the administrators, as attackers will create domain admin accounts to gain control over a domain.

24. Hardening the Administrator Accounts

    Administrator accounts have increased privileges and can often be used to wreak havoc on a domain if compromised. Some suggestions for securing the administrator accounts include dual factor authentication and anti-delegation [95].

    Task 1: Require that administrator accounts need a smart card for logon.

    Task 2: Mark the administrator account as sensitive and cannot be delegated.