Active Directory Domain Services

Cybersecurity

Windows Administration and Hardening Day 3

7.3: Windows Admin - Active Directory

Class Preparation

1. Check into BCS
2. Update your git repository with `` `git pull` ``
3. Login to your Azure account and get setup for today. Instructions can be found:
    - *Repo folder: Activities/00_Windows_Lab*
    - *Slack #01-class-activities channel*

Homeworks Due

- Unit 6 (Bash): due Sunday November 8
- Unit 7 (Windows): due Sunday November 15

Upcoming Units

- Weeks 8 & 9: *Networking* (11/9 - 11/21)
- Week 10: Network Security

Schedule Notes

Thanksgiving Break - No Class

- Off: Wed 11/25 & Sat 11/28
- Return on Monday 11/30

Project 1 (Individual; Required)

- Mon 12/14 - Sat 12-19

Winter Break - No Class

- Last class on Sat 12/19
- Off: Mon 12/21 - Sat 1/02
- Return on Monday 1/04

Schedule Change

- Crypto delayed until after Winter Break

Class Objectives

By the end of today's class, you will be able to:

Set up an Active Directory server as a domain controller and join a Windows host to it.

Create domain organizational units, users, and groups.

Set up Group Policy Objects.

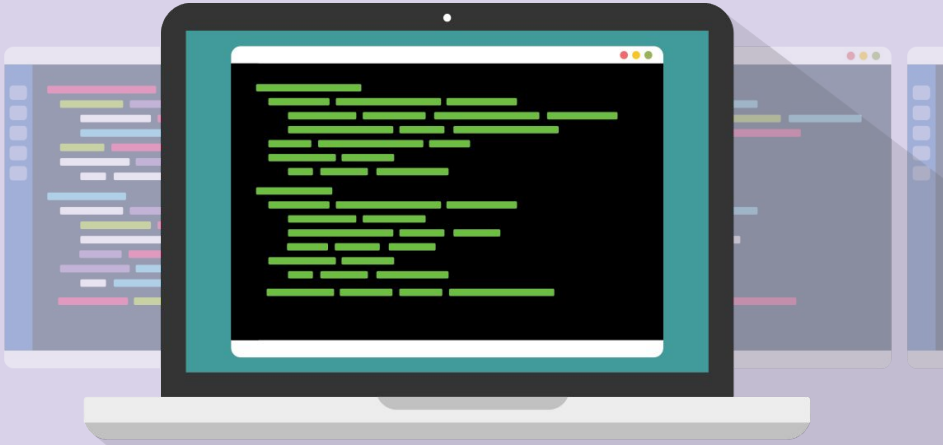
Today, we're going to learn how to manage the central databasing system for enterprise-scale Windows environments:

Active Directory Domain Services (AD)

Active Directory

Active Directory is the central databasing and management system for enterprise-scale Windows environments.

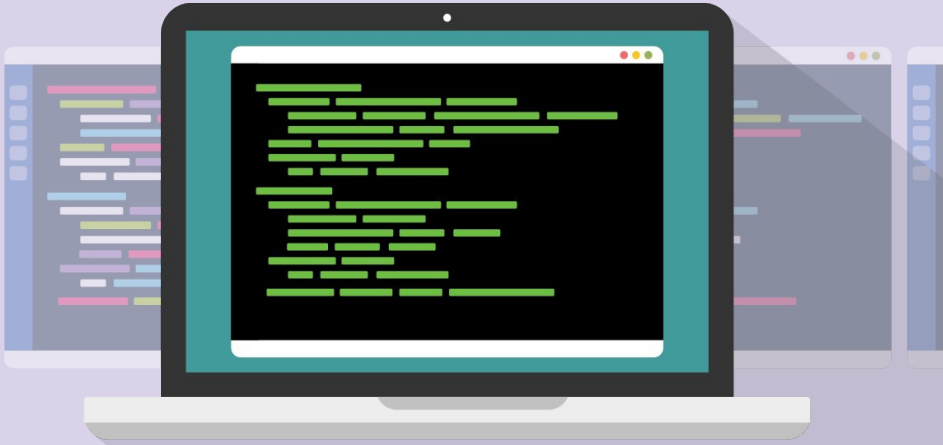
Having a strong understanding of Active Directory is crucial for anyone working in Windows-based system administration and security.



Active Directory

Security analysts, threat hunters, forensics experts, and incidence responders will all likely be required to know some Active Directory to be effective within their own organization or a client's.

Experts in penetration testing, threat intelligence, and malware reverse engineering will need to understand and leverage vulnerabilities to execute exploits in poorly implemented AD configurations.



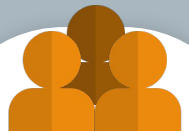
What is Active Directory?

What is AD?

Suppose a small startup with 20 employees receives a large amount of funding and adds 100 more employees to the company.

When the startup was small and scrappy, everyone helped each other out and had access to the same resources.

But for organizational and security reasons, the company now has to be stricter about resource access—ensuring everyone can access what they need, and not things they don't need.

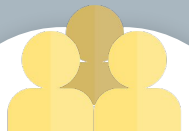


Accountants

need access to

IT Team

needs access to



Everyone

needs access to

Guests

should *not* have access to

Sensitive financial data

Networking components like switches and routers

Printers

Network

What is AD?

Resources are the files, networking components, and printers that users need permission to access. Permissions depend on roles and responsibilities within the company.

Security principals are the permissions and policies assigned to each set of users. They help us create specific controls for users, giving them only the access they need.

Security Principals

Accountants

need access to

IT Team

needs access to

Everyone

needs access to

Guests

should *not* have access to

Resources

Sensitive financial data

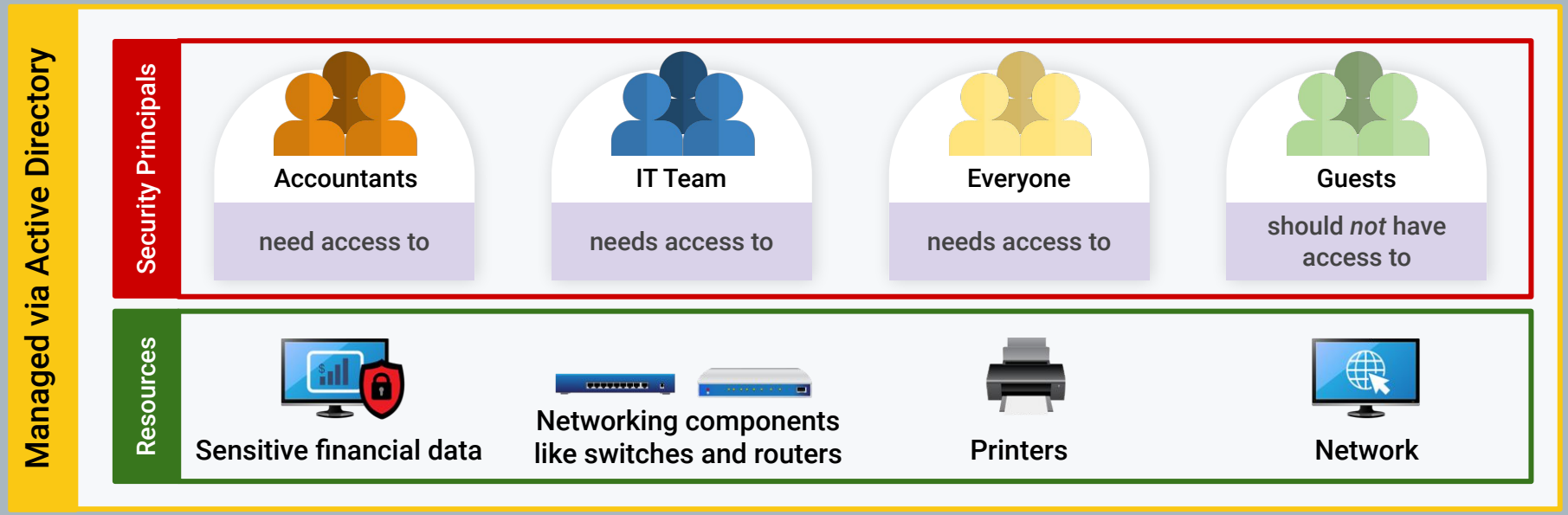
Networking components like switches and routers

Printers

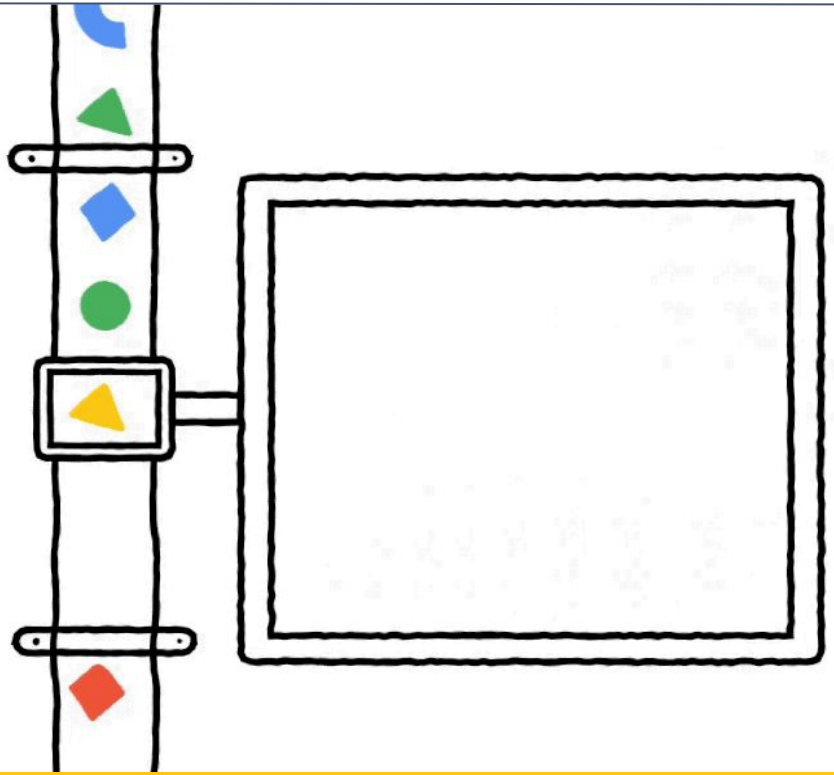
Network

What is AD?

Microsoft's **Active Directory** is the system we use to manage these resources *and* security principals.



What Exactly is AD?



Active Directory is all the services that work together to manage **authentication** and **authorization** within a Windows Server network.

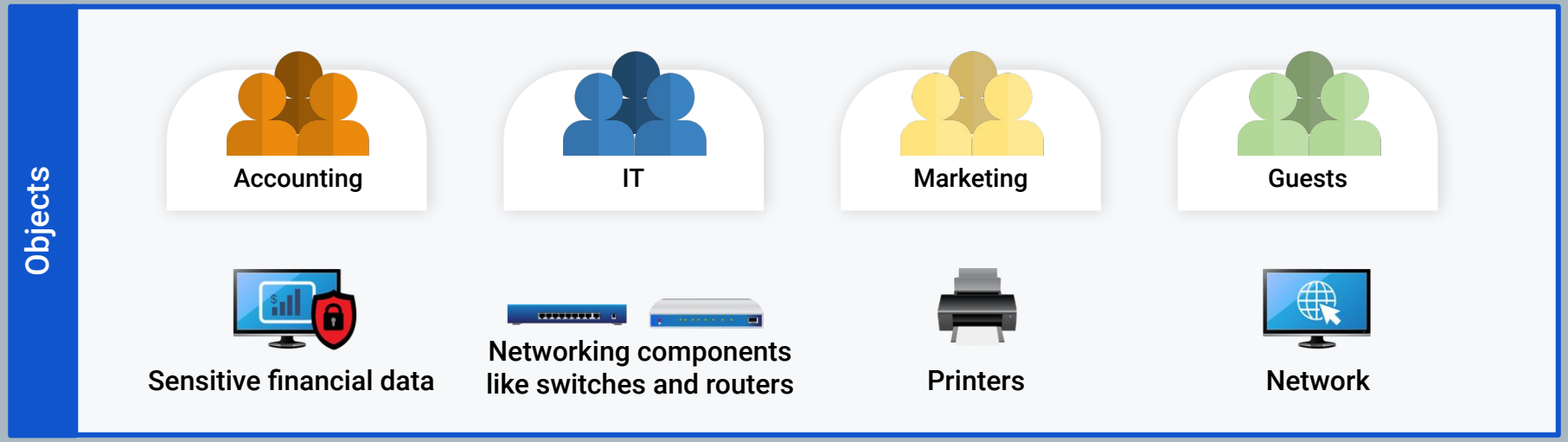
- **Authentication** allows users to prove their identity using a password, token, or biometric key.
- **Authorization** provides or denies users permission to material.

Remember the principle of least privilege from the Linux SysAdmin units?

What Exactly is AD?

Active Directory understands an organization's resources and security principals as objects.

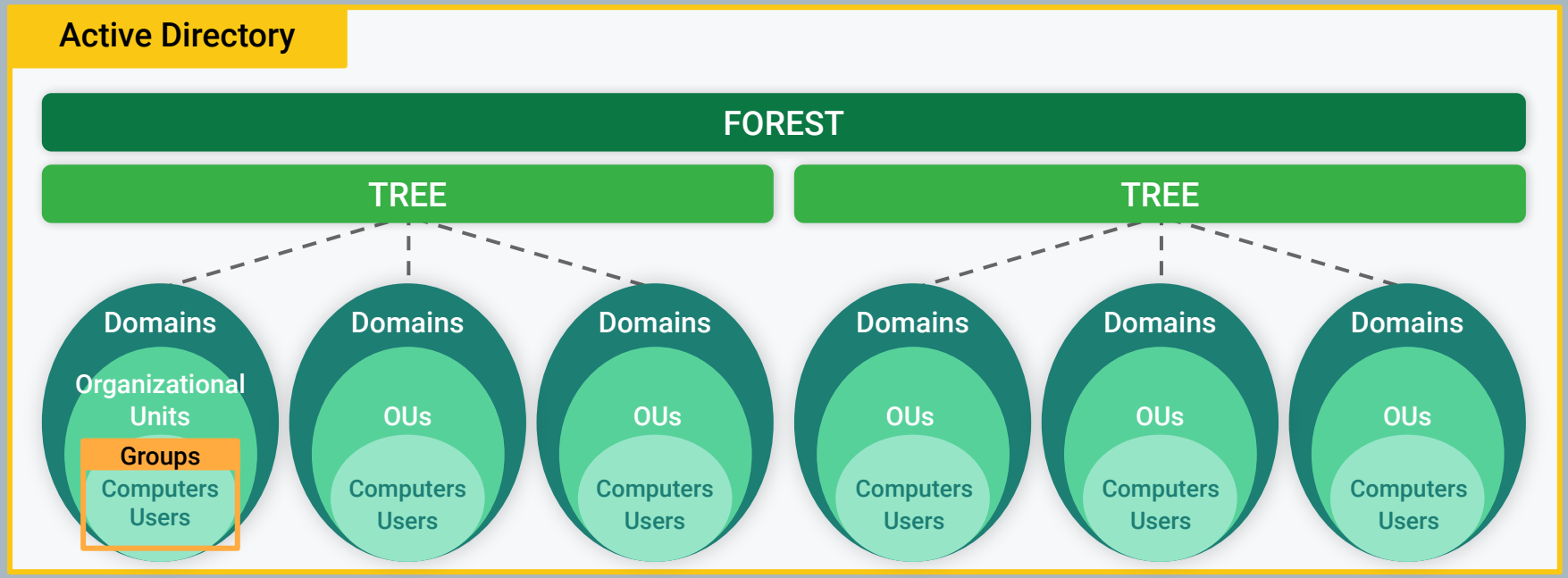
Objects are the users, groups, and computers, *and* the file shares, network printers, and other resources that users need to access.



AD Architecture

Active Directory has a hierarchical structure of organizational units, users, machines, groups, domains, trees, and forests.

Structure of Active Directory:



AD Authentication

AD uses the following authentication protocols:

LDAP (Lightweight Directory Access Protocol)

A standardized protocol for adding, deleting, and editing objects. If Active Directory is a journal of information, LDAP is the pencil and eraser.

Kerberos

A ticket-based authentication protocol, now the default authentication protocol for Windows Server domains. Provides direct encrypted sessions between users and networked resources.

NTLM (New Technology LAN Manager)

An authentication protocol that has become outdated because of pass the hash attacks.

We'll learn more about protocols in our Networking units, and will discuss these specific protocols during our Pentesting units.

Kerberos Overview

Bob is attempting to access a networked file server:

1. Bob's Windows 10 machine sends a request to authenticate the **Key Distribution Center (KDC)**, seeking a **Ticket Granting Ticket (TGT)**.

   A KDC has a database of valid credentials, an **Authentication Server** and a **Ticket Granting Server.**

2. Once his credentials are verified, Bob receives a TGT that allows him to request access to resources.

   That TGT is cached and permits him to request more tickets for the current domain session.

3. When Bob attempts to access the file server, he sends the Ticket Granting Ticket to the Ticket Granting Server, requesting access to the file server.

4. The Key Distribution Center checks if the file server exists and if the TGT is valid. If it is, the KDC sends Bob an encrypted **service ticket** containing info he authenticated earlier, and a **session key**. Bob is then sent the encrypted service ticket and a copy of the session key.

Kerberos Overview

Bob is attempting to access a networked file server:

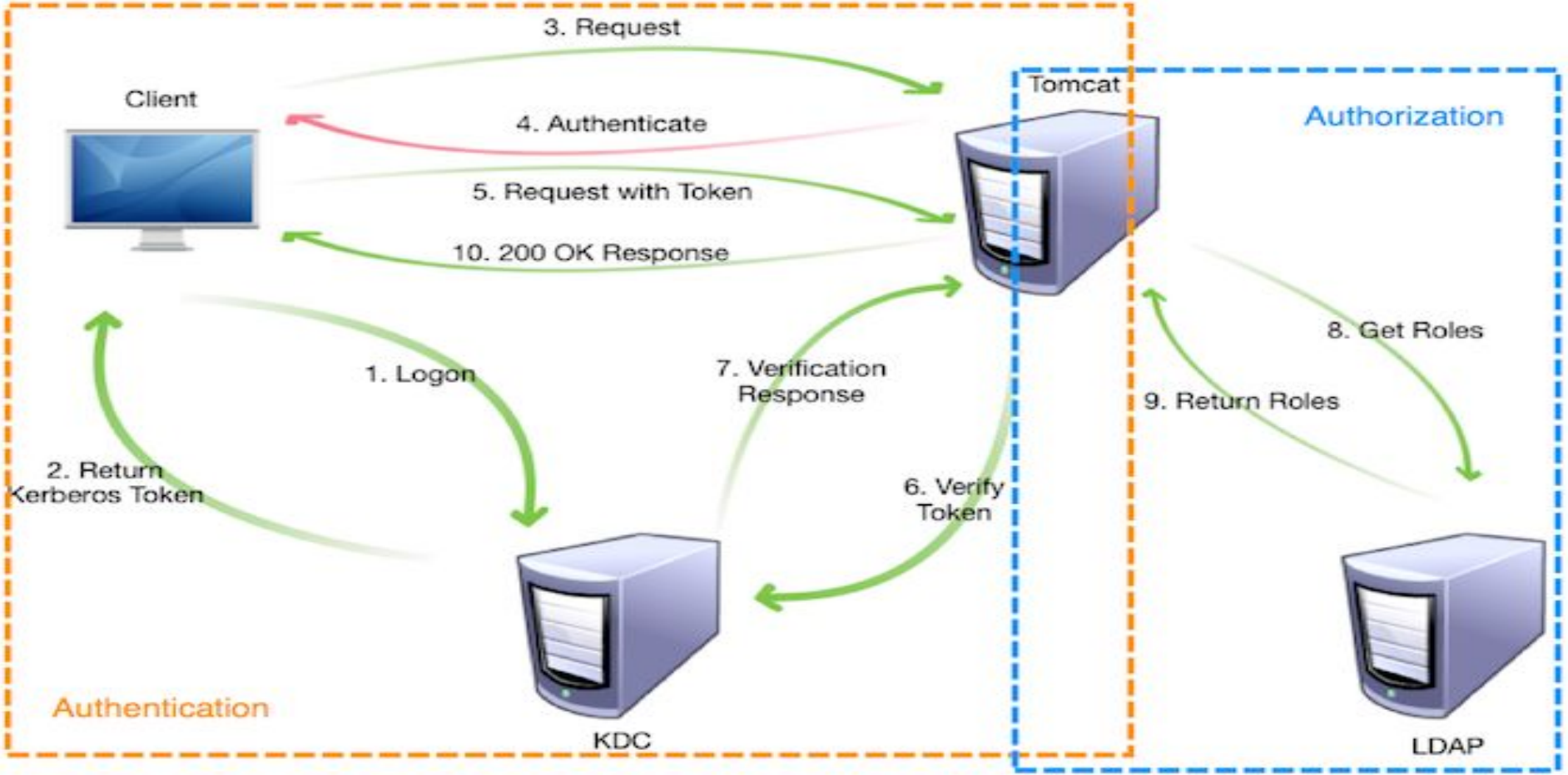
5 Bob then uses the session key to encrypt a new message containing his current information and send that, along with the service ticket, to the file server.

6 The file server then decrypts the service ticket containing the session key, and uses that session key to decrypt the message from Bob that contains his current information.

7 Finally, the file server uses the session key to encrypt a new message to be sent to Bob containing information about the file server.

If Bob's existing copy of the session key properly decrypts the message, the file server is verified.

Kerberos Overview



Creating OUs, Users and Groups

Creating OUs, Users and Groups

Now that we've introduced Active Directory domain controller, we'll assign organizational units and groups.

Organizational units (OUs) are logical groupings of an organization's assets and accounts.

- For example, all of the computers in the sales department of our company should be grouped together in an organizational unit, which might be called `GC Users > Sales`.
- All of these computers would have the same policies, set by the group policies.

Creating OUs, Users and Groups

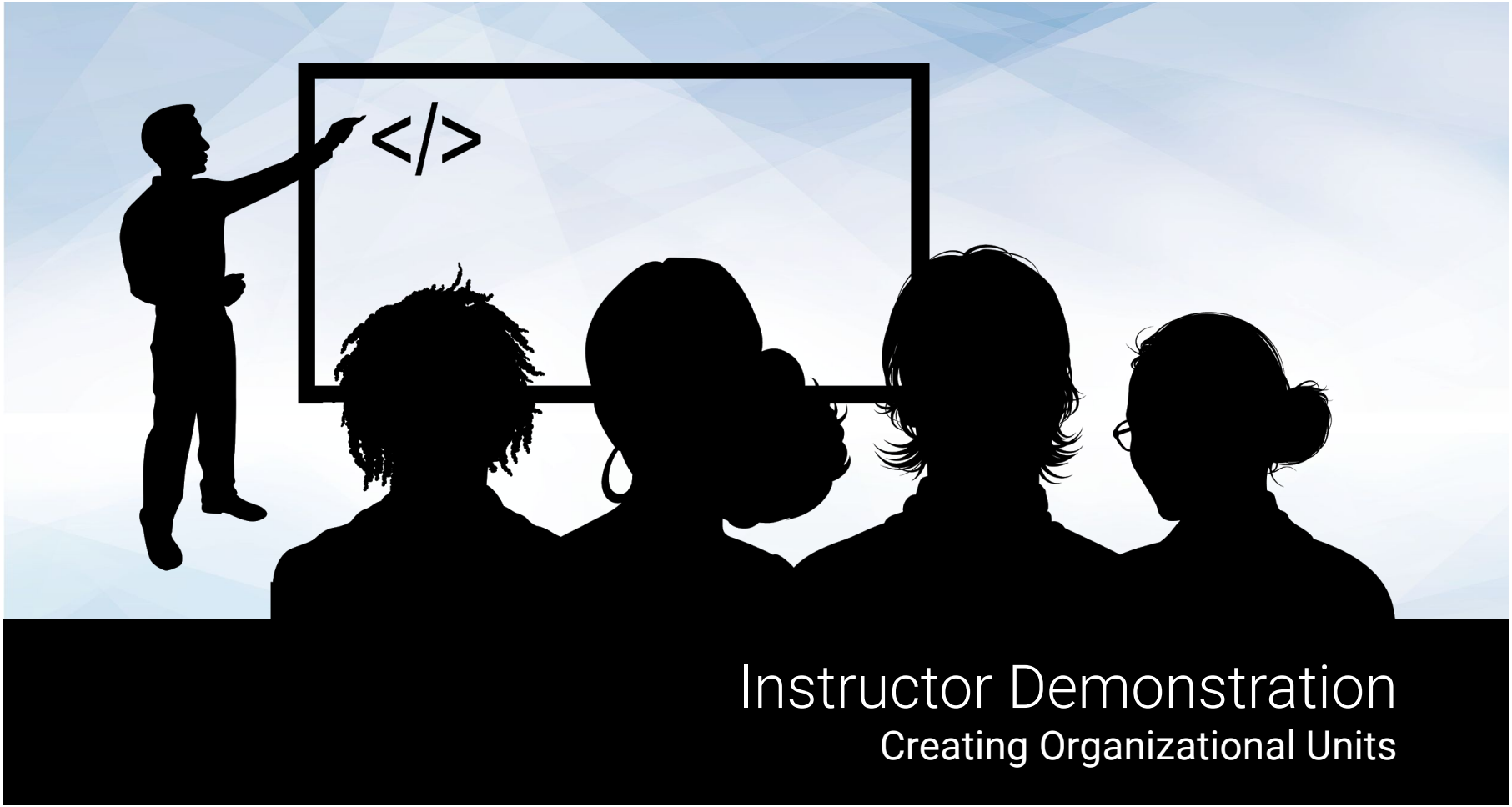
In the following demo, we will:

01 Create a new domain organizational unit called GC Users.

02 Create a sub-OU called Marketing.

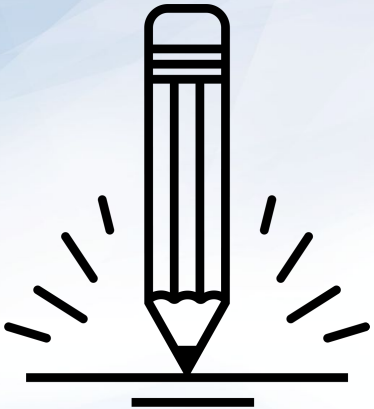
03 Create a user, Caroline, under the GC Users > Marketing OU.

04 Create a group, Marketing, under the GC Users > Marketing OU.



Instructor Demonstration

Creating Organizational Units



Activity: Creating Domain OUs, Users, and Groups

For this activity, you will set up users, groups, and organizational units for your recently created domain.

Suggested Time:
20 Minutes

Group Policy Objects

Now that we have OUs, groups, and users, we can create Group Policies that enforce the principle of least privilege.

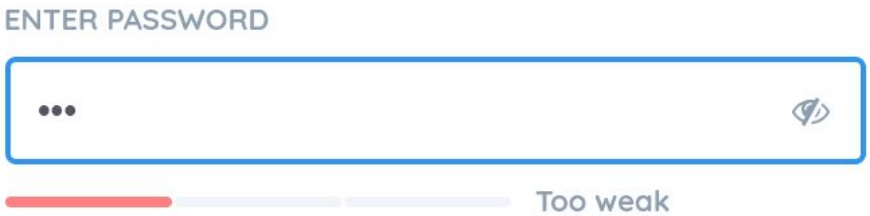
Group Policy Objects

Group Policy Objects (GPOs) are packages of policy settings that contain one or more group policy.

GPOs are the basis of AD's policy management.

For example, if we want to both:

1. Implement password complexity requirements for accountants.
2. Deploy some form of anti-malware software when they next log on.



We can combine these two policies into one GPO called **`Better Password and Anti-Malware Setup`** and apply it to all accountants in the OU.

Group Policy Object Demo

In the following demo, we want to remove access to the Control Panel:

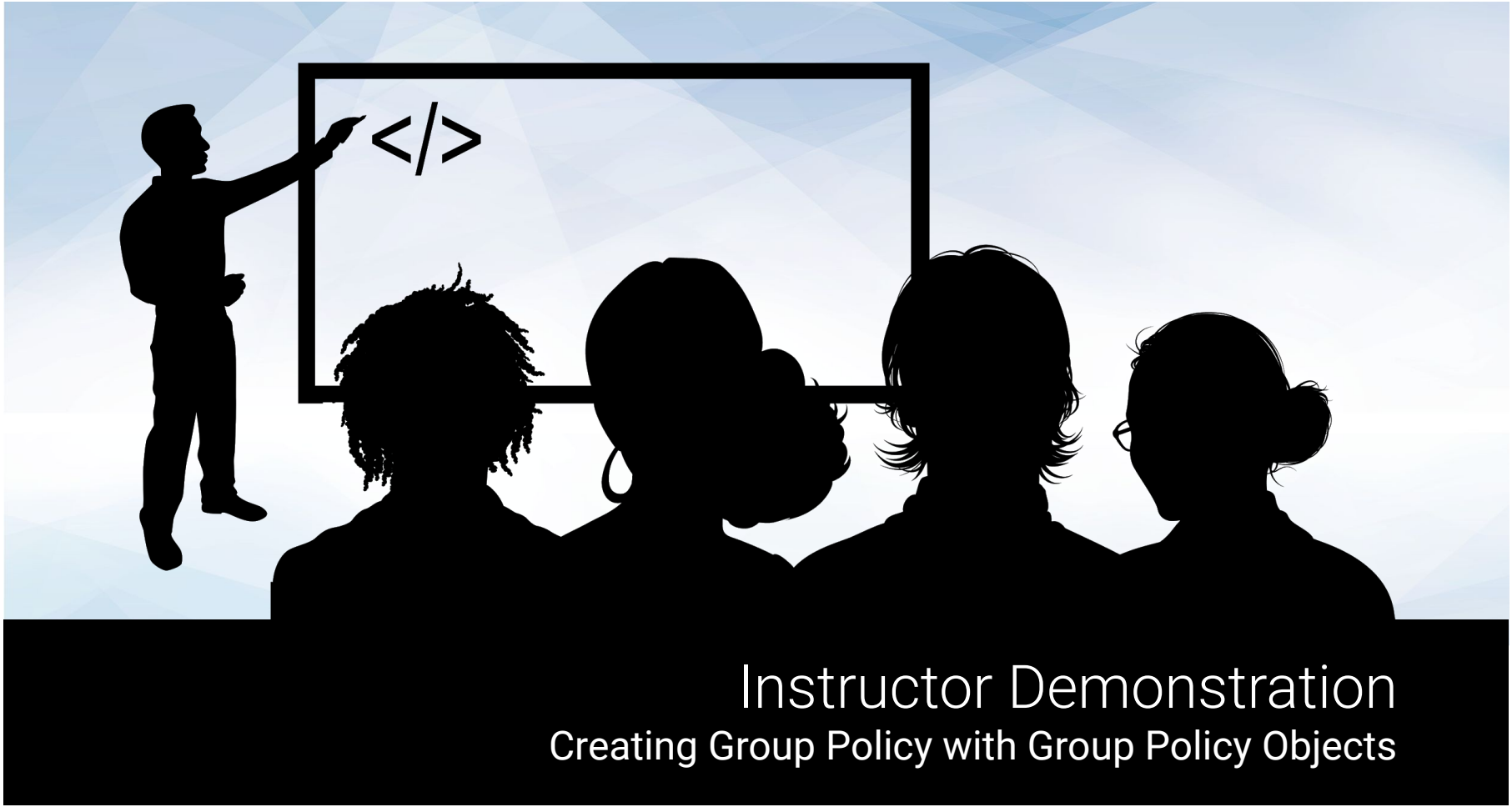
01 Create a Group Policy Object.

02 Edit the individual policies for our Group Policy Object.

03 Link the Group Policy Object to an organizational unit.

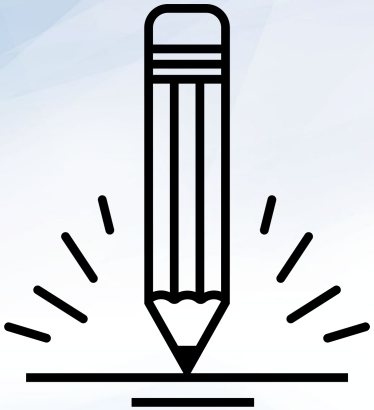
04 Within the Windows 10 machine, pull the latest Active Directory changes.

05 Verify if the GPO worked.



Instructor Demonstration

Creating Group Policy with Group Policy Objects



Activity: Creating Group Policy with Group Policy Objects

In this activity, you will create Group Policy Objects to enforce policies for users.

Suggested Time:
25 Minutes

⚠️ Shut Down Your Machines ⚠️

Everyone must shut down their Hyper-V virtual machines and Windows RDP Host Machine. You will need the remaining hours to complete your homework.