Active Directory Lab

NJIT Information and Cybersecurity Club

Presented by Jimmy Silva

Topics Covered

1. What is Active Directory?
2. Active Directory Structure
3. Kerberos Authentication
4. Kerberos Attack Vectors
5. Additional Resources

Active Directory | AD

What is Active Directory and why is it used?

What is Active Directory / AD?

Active Directory is a centralized directory service used to manage large scale networks and control different resources, like user accounts, endpoint devices, and services.

Key Protocols of AD:

- ***LDAP** (Lightweight Directory Access Protocol)
- ***Kerberos** (Authentication and Authorization)
- **SMB** (Group Policy Updating and Communication)
- **NTP** (Time Synchronization)

Active Directory Structure

Incoming Information Bomb...

Logical and Physical Definitions:

Domain: Core unit of the logical structure for AD

Schema: Set of definitions of object types and attributes

Forest: (Set of Trees) → **Tree** (Set of Domains) → **Domain** (Logical Container)

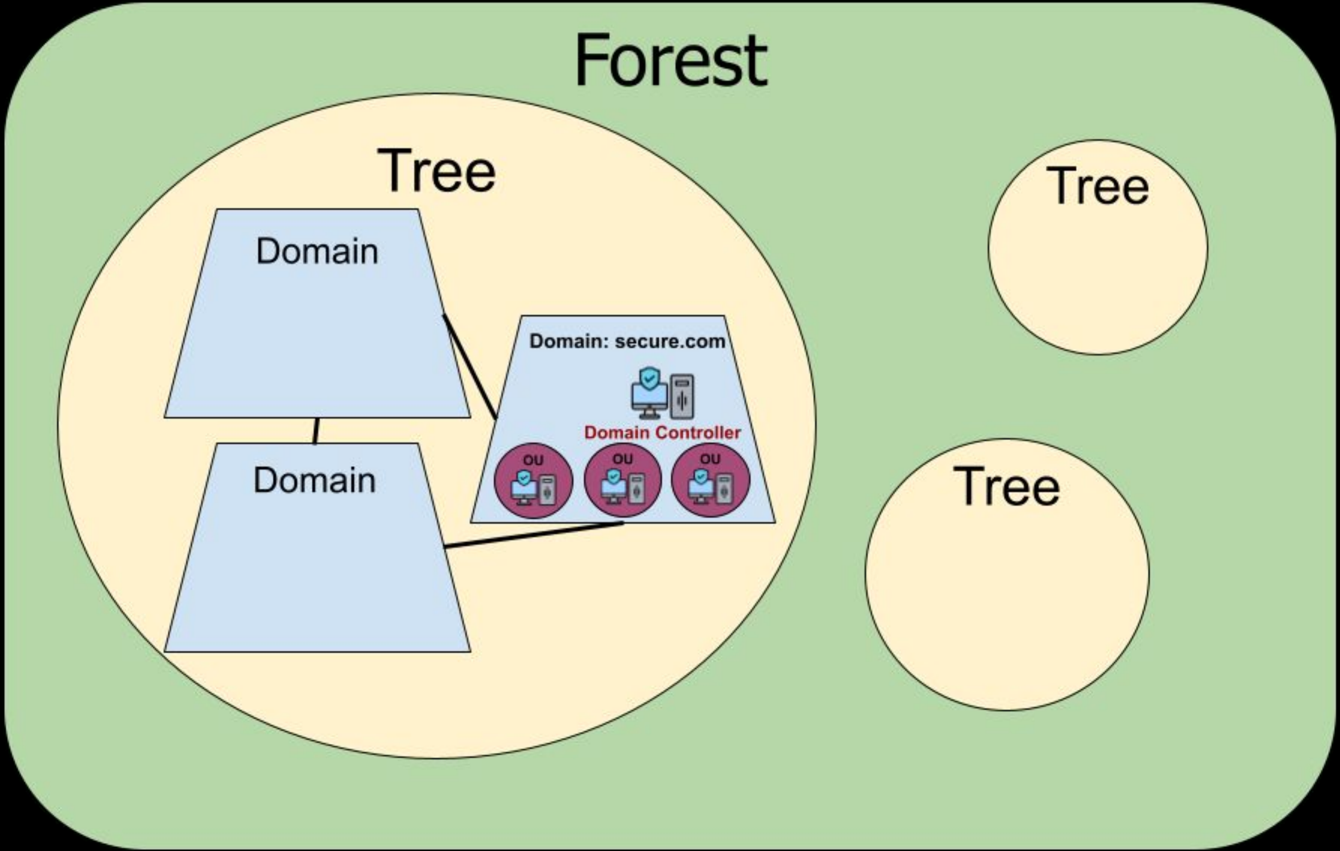
Users: Accounts that grant AD access and permissions

Organizational Units (OU): Defined groups that organize users.

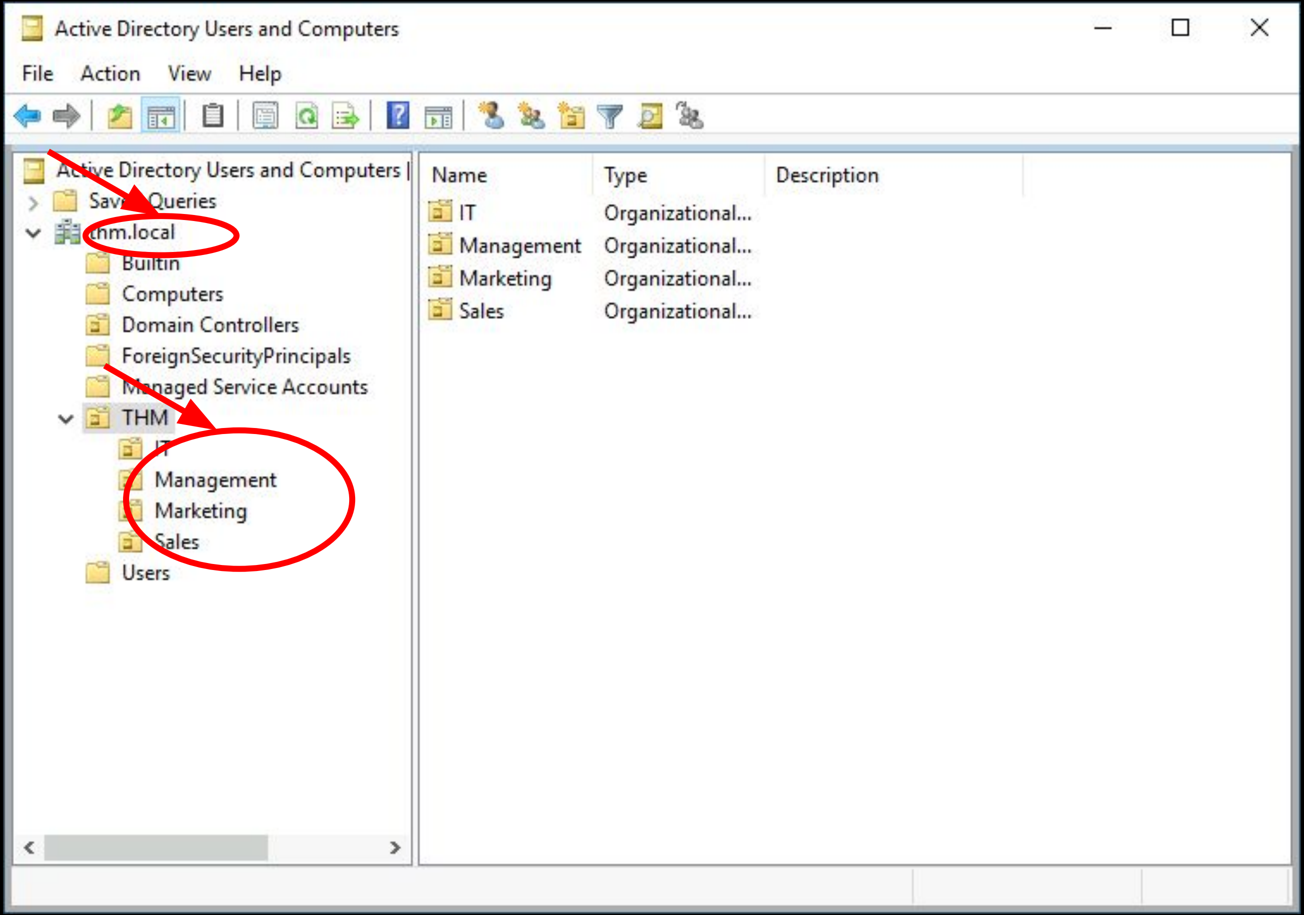
Security Groups: Groups that define permissions and resource access.

Domain Controller: AD server that reflects changes in the directory system.

Active Directory Structure



Active Directory Structure Continued

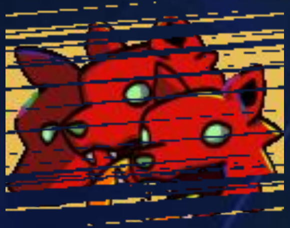


- Active Directory Users and Computers
  - Saved Queries
  - thm.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - THM
      - IT
      - Management
      - Marketing
      - Sales
    - Users

Name	Type	Description
IT	Organizational...	
Management	Organizational...	
Marketing	Organizational...	
Sales	Organizational...	

Kerberos Authentication

How does Kerberos works in AD?



Principle

Resource

KDC

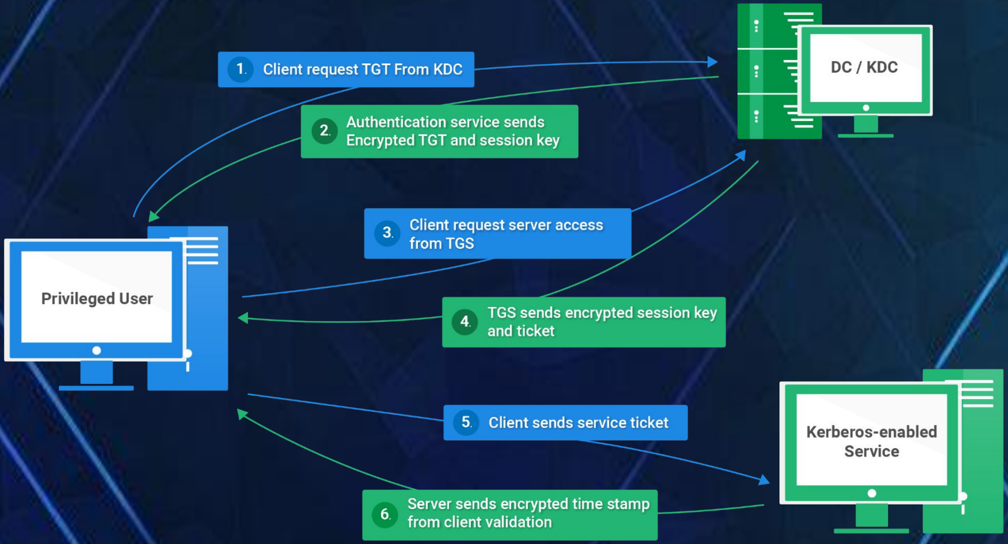
Kerberos Authentication

One of the biggest benefits of Active Directory services is its ability to provide **authentication** and verification of **users/hosts** within the domain.

Pros:

Strong Encryption Techniques

Safer Ticket Authentication


DC / KDC
1. Client request TGT From KDC
2. Authentication service sends Encrypted TGT and session key
Privileged User
3. Client request server access from TGS
4. TGS sends encrypted session key and ticket
5. Client sends service ticket
Kerberos-enabled Service
6. Server sends encrypted time stamp from client validation

Kerberos Authentication 101

1: Client requests **TGT** **(Ticket-Granting Ticket)** from the **KDC** **(Key Distribution Center)**

2: **KDC** verifies credentials, sends back *encrypted* **TGT** and Session Key.

3: Client will store **TGT**, if the session *expires*, do *steps 1-2* again

4: When the Client *requests* a resource, it will send it's **TGT** to the **TGS** **(Ticket Granting Server)**

5: **TGS** will verify the **TGT**, if valid, the **TGS** will send an <u>*encrypted session key*</u> for that resource

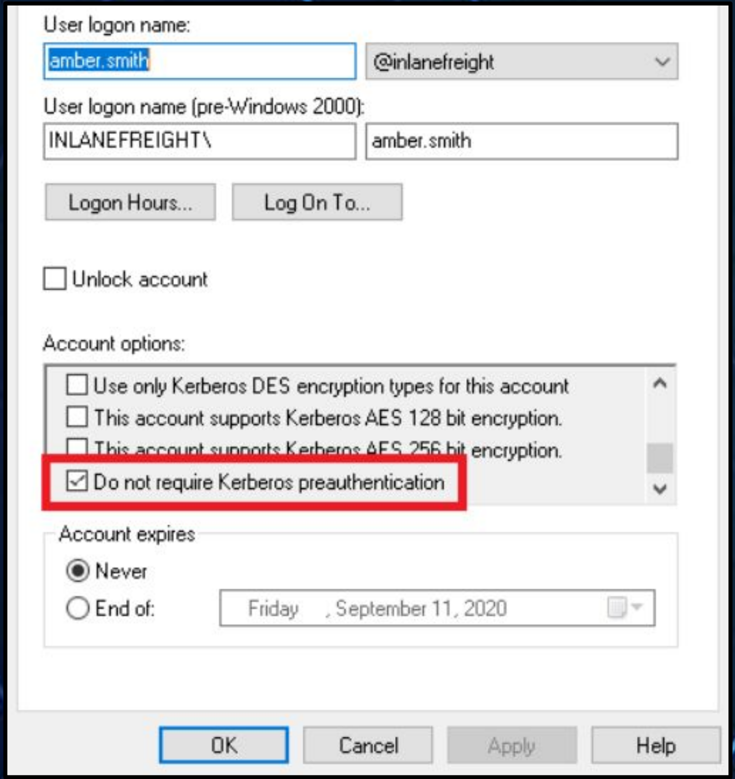
Kerberos Attacks

What are some common threat vectors in AD?

Common Kerberos Authentication Attack Vectors

AS-REQ Roasting: Without Kerberos *pre-authentication* properly configured, anyone can request authentication data for a user, which can be brute-forced offline.

Pass-the-Hash: If a endpoint machine/identity is *compromised*, any associated session keys can be used.



User logon name:

amber.smith @inlanefreight

User logon name (pre-Windows 2000):

INLANEFREIGHT\ amber.smith

□ Unlock account

Account options:

□ Use only Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.
□ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

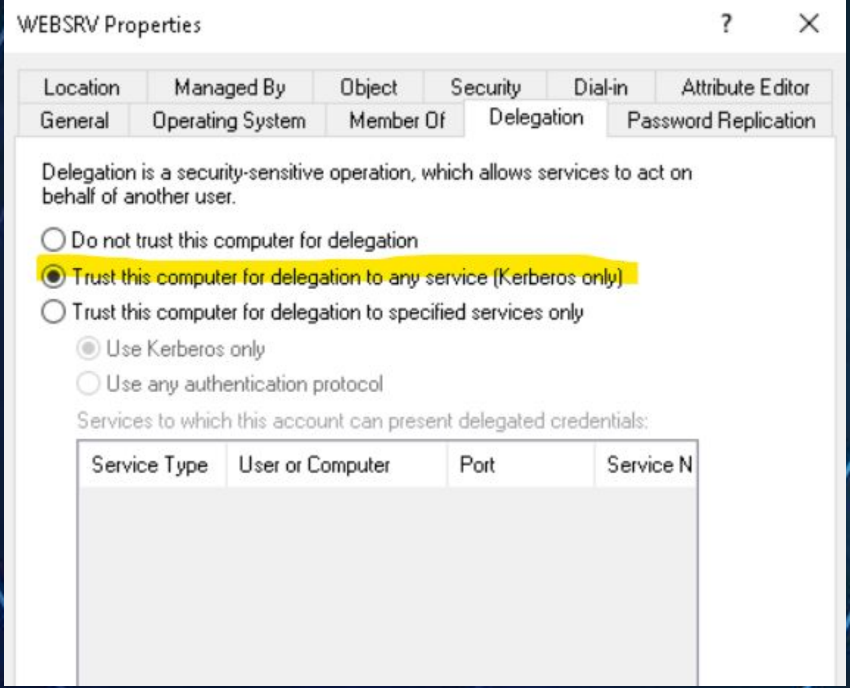
Account expires

● Never
○ End of: Friday , September 11, 2020

Common Kerberos Authentication Attack Vectors

Kerbroasting: Similar to *AS-REQ* roasting, but requires prior Kerberos authentication

Unconstrained Delegation: When a service is able to *impersonate* a user to access another service.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N

Common Kerberos Authentication Attack Vectors

Golden Ticket: Via *impersonating* Kerberos Ticket Granting Account (krbtgt), attackers can forge and sign TGT's to any services in AD!

Silver Ticket: Less powerful, instead the attack focuses on *forging TGS tickets*, which bypasses the domain controller completely

Additional Resources + Resources Used

Active Directory Basics - Try Hack Me

Microsoft Learning Path AD

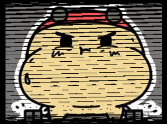
My Totally Awesome AD Write-Ups

Kerberos Attack Vectors 🔥

Active Directory Hardening Lab - Try Hack Me

Breaching Active Directory Lab - Try Hack Me

What Next?



NJIT Student? → try logging in on a domain computer with your email and open a wireshark capture. See how much you can spot as AD traffic!

Try some **TryHackMe** or **HackTheBox** Resources linked!

Download a Windows Server ISO and spin up a VM, try messing around with Group Policy!

Microsoft shares a lot of free resources on AD and their cloud version of AD (Microsoft Entra), take a look!