Active Directory Basics

redfoxsec.com/blog/active-directory-basics

Kunal Kumar

September 26, 2022

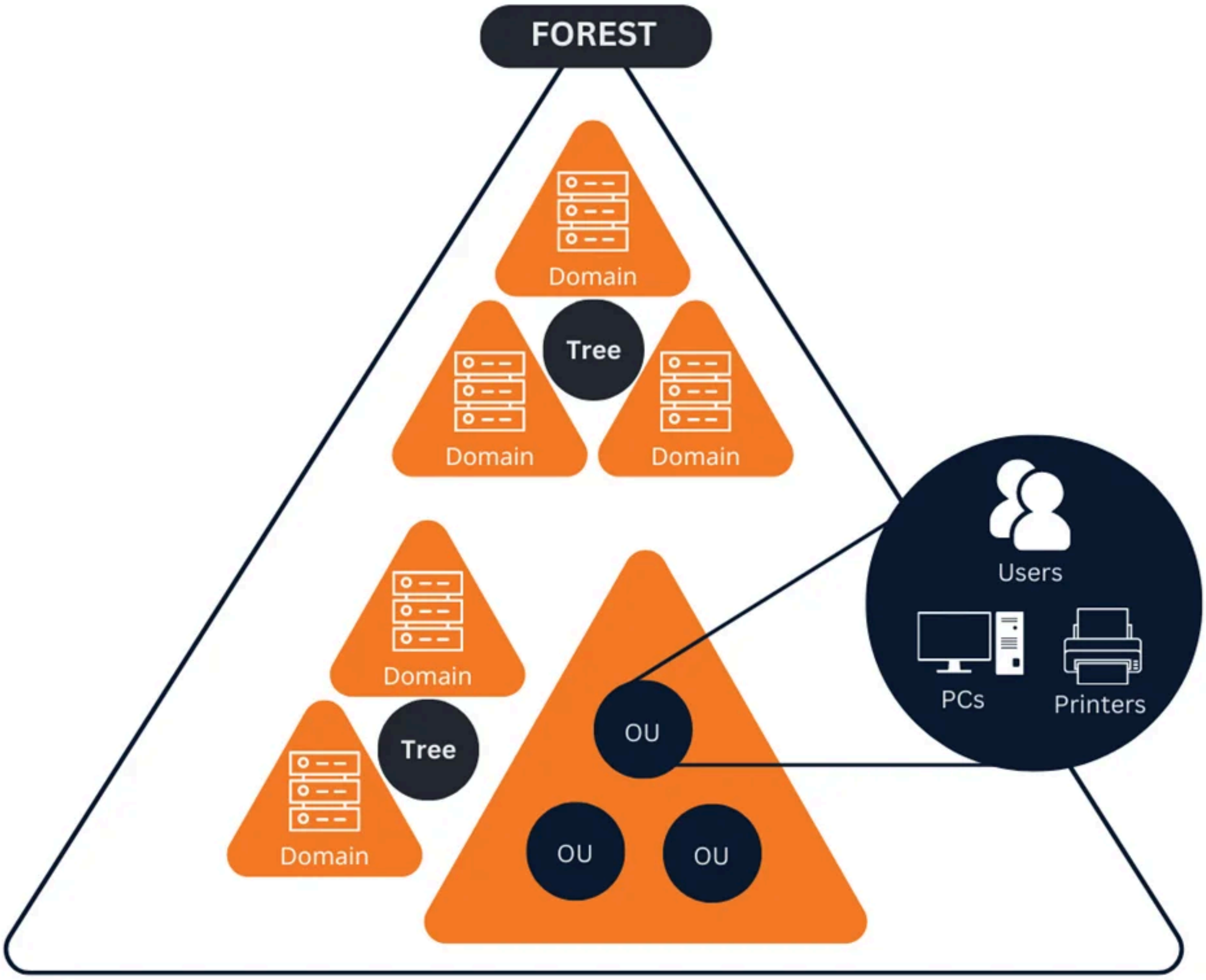
- September 26, 2022
- Active Directory
- Kunal Kumar

The number of resources such as users, databases, or servers managed in organizations poses questions about accountability as firms adjust to industry needs and norms. Additionally, the dispersed structure of managing the infrastructure and its procedures makes it challenging for enterprises to monitor employee activity. This makes it simpler for attackers to access the network's resources and leads to a significant loss of sensitive data. Windows started the Active Directory Domain Service in Windows Server 2000 and developed it until Windows Server 2012 to manage organizational resources in the network.

Active Directory is a central repository containing information related to all the resources in the organization's network, ranging from employees to devices, ensuring efficient information management. AD has a Windows server (Domain Controller), working in compatibility with the Windows Operating System to provide centralized management, scalability and security.

Active Directory uses a hierarchical, tiered layout of domains, trees, and forests to coordinate networked elements.

- A **domain** is a group of objects, such as users, devices and services, that share the same AD database and have the same domain name system.
- A **tree** is one or more domains grouped. Trees can have trust relationships where a secure connection, or trust, is shared between the domains. Trust can be direct, where one domain can trust a second, and the second domain can trust a third and implicit, where the first domain can trust the third domain without needing explicit trust.
- A **forest** is a collection of multiple trees. A forest consists of shared catalogs, directory schemas, application information and domain configurations. The schema defines an object's class and attributes in a forest. Forest is the security boundary of an AD.
- **Organizational Units (OUs)** organize users, groups and devices. Each domain can contain its own OU. However, OUs cannot have separate namespaces, as each user or object in a domain must be unique.



Benefits of Active Directory

- It is used to manage resources and policies of the organizational network from a centralized space.
- It allows secure authentication by following the Kerberos protocol that is used in Windows Server 2000.
- It is highly scalable, thus enabling organizations to tackle growing needs by changing policy properties and user management.

Authentication

AD Authentication is a process that typically follows **Kerberos** protocol since Windows 2000, where users have to log in using their credentials to gain access to resources. Before Kerberos, the **NTLM** protocol was used to authenticate the users. NTLM is still present in all Windows devices for fallback and legacy uses.

The main difference between NTLM and Kerberos is in authentication mechanisms. NTLM relies on a three-way handshake between the client and the server for authentication. Kerberos uses a two-part process with a key distribution center and the service. Another huge difference is that NTLM uses password hashing (without salting), whereas Kerberos leverages encryption.

NTLM

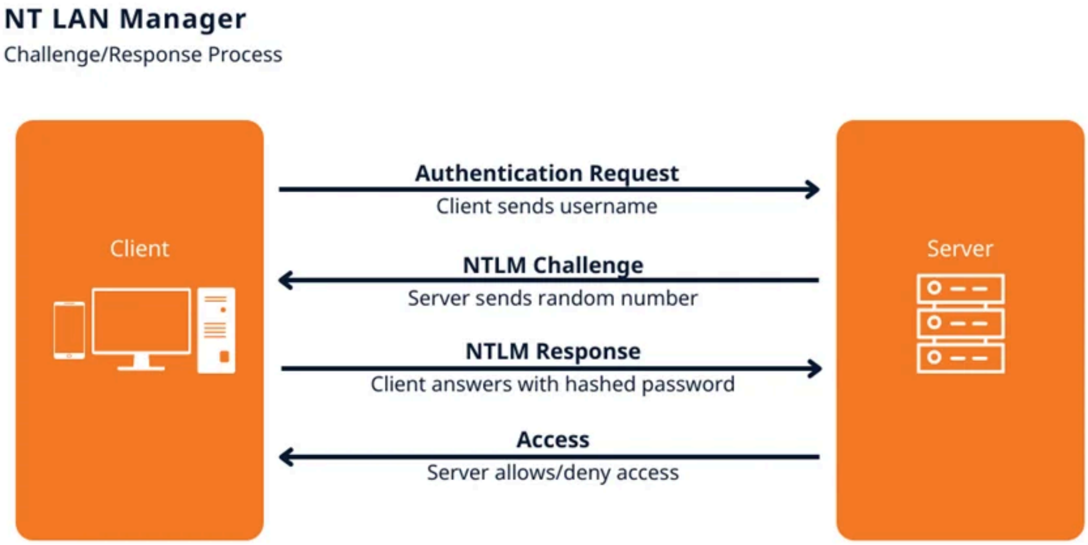
New Technology LAN Manager (NTLM) was the primary security protocol used to authenticate users' identities in AD before Windows 2000. NTLM can be used for authentication with the help of a challenge-response-based scheme. When the client requests access to a service, the service sends a challenge to the client, where the client has to perform a mathematical operation using its authentication token and then return the result to the service. The service will send the result to the Domain Controller (DC) for validation. If the DC confirms that the client's response is correct by verifying with its databases, the service allows access to the client.

Here is an outline of the NTLM authentication process once the user provides their credentials during logon:

1. The client sends the username to the server (in plaintext).
2. The server generates an 8-byte random number, called a challenge, and sends it to the client.
3. The client encrypts this challenge with the hash of the user's password and returns the result to the server. This is called the response.
4. The server sends the following to the domain controller:
    - username
    - challenge sent to the client
    - response received from the client

5. The domain controller uses the username to retrieve the hash of the user’s password from the Security Account Manager (SAM) database. It uses this password hash to encrypt the challenge sent from the server.

Eventually, the domain controller compares the encrypted challenge it computed to the response computed by the client. If they are identical, authentication is successful.


NT LAN Manager
Challenge/Response Process
Client
Server
Authentication Request
Client sends username
NTLM Challenge
Server sends random number
NTLM Response
Client answers with hashed password
Access
Server allows/deny access

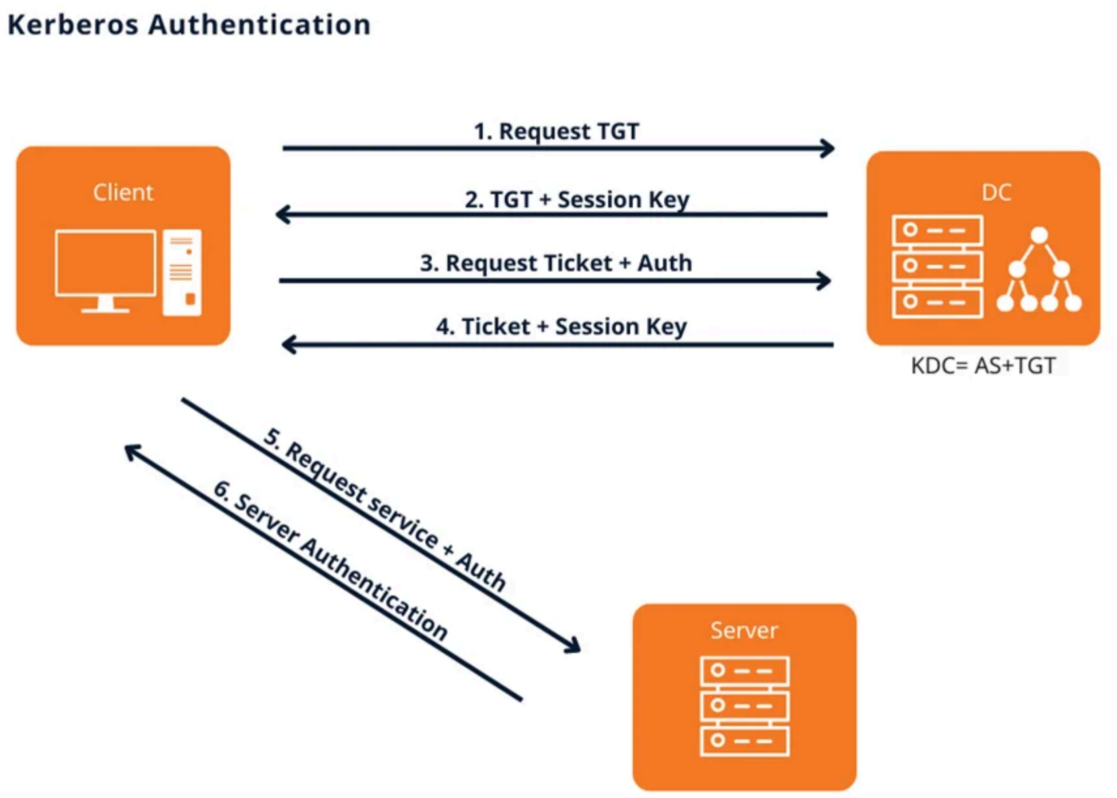
Kerberos

Kerberos provides a centralized authentication server that authenticates users to servers and vice-versa. In Kerberos, an authentication server and a database are used for client authentication. Kerberos runs as a third-party trusted server, the Key Distribution Center (KDC). Each user and service on the network is a principal.

There are two main components in the KDC:

- Authentication Server (AS): The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
- Ticket Granting Server (TGS): The Ticket Granting Server issues the ticket for the Server

Kerberos Overview:



1. A user logs in and requests a service from the host. This process starts with the client requesting the Ticket Granting Ticket (TGT) by passing the username as well as the Service Principal Name (SPN) encrypted with the user's NTLM hash to the Authentication Server (AS).
2. The KDC verifies the user's credentials by decrypting the data with the user's hash from its database. The AS supplies the ticket-granting-ticket (TGT) encrypted with the krbtgt hash along with the session key encrypted using the user's password hash.
3. The message is decrypted using the user's password hash, and then the encrypted TGT is sent to the Ticket Granting Server (TGS). The Ticket contains authenticators like usernames and network addresses.
4. The ticket is decrypted by the TGS using a krbtgt hash, and the authenticator verifies the request. Then it creates the ticket for requesting services from the Server, encrypts it with the service hash and sends it to the user.
5. The user sends the service ticket and session key to the Server.
6. The server verifies the Ticket and session and then generates access to the service. After this, the user can access the services.

You can watch this video for a deep dive into Kerberos. We will delve into Active Directory attacks in our upcoming blogs.

By partnering with Redfox Security, you'll get the best security and technical skills to execute a practical and thorough penetration test. Our offensive security experts have years of experience assisting organizations in protecting their digital assets through penetration testing services. To schedule a call with one of our technical specialists, call 1-800-917-0850 now.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. We proudly deliver robust security solutions with a combination of data-driven, research-based, and manual testing methodologies.

“Join us on our journey of growth and development by signing up for our comprehensive **courses** if you want to excel in cybersecurity.”

PreviousBlockchain 101
NextIPV6 DNS Takeover

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker’s Swiss Army Knife. Have You Heard About It?