Active Directory and Its Security Testing

Rahul Banik, Sankha Subhra Debnath,

Department of Computer Science and Engineering, Techno College of Engineering Agartala

Abstract: Active Directory is Microsoft's developed Service delivery through a hierarchical system. One of its functions is the storage of data about things that are connected to the network. Since they will establish and manage users and items within the network, network administrators play a crucial role. An extensive user base may be organized using the active directory. which also offers access control at every level. As it can be used to manage all network components, including computers, groups, users, domains security policies, and any kind of user-defined objects. This article also briefly discusses the methodologies used in Vulnerability Assessment and Penetration Testing (VAPT), a security measure deployed by the banking industry to defend infrastructure from attacks in the online realm. An information security audit's presence enhances the likelihood that important security measures will be adopted, thwarting these assaults or significantly reducing cyberattacks. The primary gold of this article is to raise awareness of cyber security and its relevance at all levels of the financial industry.

Index Terms: Active Directory(AD), AD service, Information security, VAPT, Centralized Management System.

1. Introduction

Microsoft created Active Directory as a directory service to control the Windows domain network. The Active Directory provides knowledge about object access management and sets for security view aspects. AD domain has the services to store data concerning the network resource across a website. Active Directory, a Windows server has long-face complications like the authentication and authorization model needed to break down a network into domains. and generally, an unpredictable system ways that of trust. AD uses protocols like LDAP, Kerberos version, and DNS version. Active Directory is most commonly used for identity Management Services in the world 95% of the Fortune 1000 companies implement the Active Directory in their network.

An audit structure might be a collection of papers that outline the audit technique's strategy, and the expected audit results. the process for managing risks, and risk assessment as well. Additionally, the audit structure should provide detailed instructions on how to construct a certain audit plan.

2. Active Directory Objects

The core of any Windows Domain is the Active Directory Domain Services(AD DS). This service acts as a catalog that holds the information of all the "objects" that exist on your network.

2.1. Users

Users are one of the most common object types in Active Directory. Users are one of the objects known as security principals, meaning that they can be authenticated by the domain and can be assigned privileges over resources like files or printers. You could say that a security principal is an object that can act upon resources in the network.

Users can be used to represent two types of entities:

- **People:** users will generally represent persons in your organization that need to access the network, like employees
- **Service:** You can also define users to be used by services like IIS or MSSQL. Each and every service needs a user

to function, however, service users vary from ordinary users in that they only have access to the resources required to execute their particular service.

Each object contains:
GUID- 128 bit Globally Unique Identifier
SID– Security Identifier for every Security Principal object.

3. Security Group

if you are familiar with Windows, you presumably already know that user groups may be created so that several users can be assigned access permissions to a single collection of files or other resources. Adding users to an existing group will instantly give them access to all of the group's rights, making management easier. Security principals are therefore capable of controlling network resources.

- **Domain Admins:** Users of this group have administrative privileges over the entire domain. By default, they can administer any computer on the domain, including the DCs.
- **Server Operators:** Users in this group can administer Domain Controllers. They cannot change any administrative group memberships
- **Backup:** Users in this group are allowed to access any file, ignoring their permissions. They are used to perform backups of data on computers.
- **Account Operators:** Users in this group can create or modify other accounts in the domain
- **Domain Users:** Includes all existing user account in the domain
- **Domain Computer:** Includes all existing computers in the domain
- **Domain Controllers:** Includes all existing DCs on the

4. Active Directory Domain Services

I.**Domain Services:** The Domain service controls communication between users and the domain controller and saves the centralized data. It is the Active Directory Domain Service's major role.

II.**Certificate Services:** It is used to manage, create, and distribute certificates and enables Domain Controller to deliver digital certificates, signature, and public-key cryptography

III.**Directory Federation Services:** It operates via federated identities.In order to avoid having to repeatedly enter the same credentials, it offers Single Sign-On(SSO) authentication for different apps in the same session. It also offers functionality that extends users' SSO access to applications and systems outside of the computer firewall

IV.**Lightweight Directory Service :** It supports cross-platform domain services, like Linux computers present in the network

V.**Risk Management:** Rights management is used as a security tool to control information rights and data access policies

5. Methodology

Active Directory protocol requirements, first approach Like any system, LDAP allows users to search for and find certain objects. All credentials for Windows domains are kept on the Domain Controllers. Every time a user attempts to log in to the service using their domain credentials, the service must ask the Domain Controller to confirm that they are accurate. For network authentication in Windows domains, two protocols are available:

- **Kerberos:** Used by any recent version of Windows. This is the default protocol in any recent domain.
- **NetNTLM:** Legacy authentication protocol kept for compatibility purposes.

While NetNTLM should be considered obsolete, most networks will have both protocols enabled. Let's take a deeper look at how each of these protocols works.

5.1. Authentication

Kerberos authentication is the default authentication protocol for any recent version of Windows. Tickets are given to users who log in to a service using Kerberos. Consider tickets as evidence of prior

authentication. Users who have tickets can use them to show a service that they have authenticated into the network previously and are thus permitted to access it.

When Kerberos is used for authentication, the following process happens:

1) The key Distribution Center (KDC), a service often placed on the Domain Controller responsible for producing Kerberos tickets on the network, receives the user's username and a timestamp encoded using a key obtained from their password.
The user can request more tickets to access particular services by sending a request in the form of a Ticket Granting Ticket(TGT), which the KDC will produce and deliver back. It can seem a little strange that you need a ticket to receive more tickets, but this arrangement enables users to seek service tickets without having to enter their login information each time they wish to use a service. The user receives a Session Key in addition to the TGT, which they will use to create the next requests.

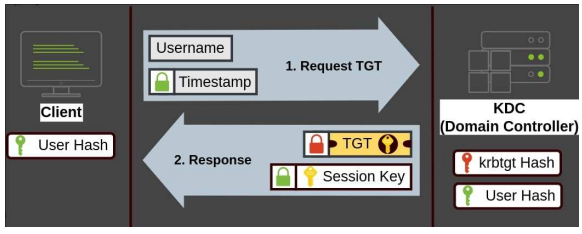

Fig. 1. Authentication Process 1

2) A user will utilize their TGT to request a Ticket Granting Service(TGS) from the KDC whenever they wish to connect to a network service, such as a sharing, website, or database. TGS are tickets that exclusively permit connection to the particular service for which they were designed. Users must transmit their username, a timestamp that has been encrypted with the session key, the TGS, and a Service and server name we want to access, in order to obtain a TGS.

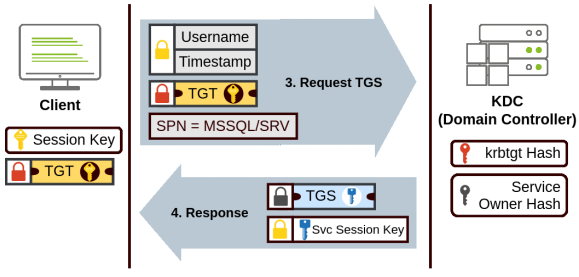

Fig. 2. Authentication Process 2

3) The TGs can then be sent to the desired service to authenticate and establish a connection. The service will use its configured account's password hash to decrypt the TGS and validate the Service Session Key.

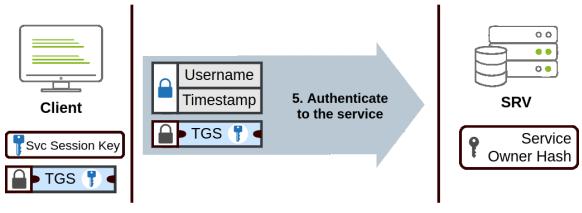

Fig. 3. Authentication Process 3

NetNTLM Authentication

- The client sends an authentication request to the server they want to access
- The server generates a random number and sends it as a challenge to the client.
- The client combines their NTLM password hash with the challenge to generate a response to the challenge and sends it back to the server for verification.

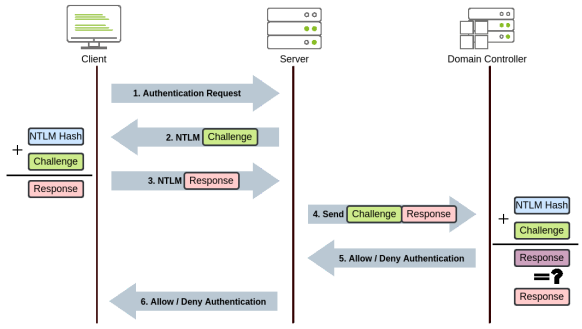

Fig. 4. Authentication Process

- The server forwards the challenge and the response to the Domain Controller for verification.
- The domain controller uses the challenge to recalculate the response and compares it to the original response sent by the client. if they both match, the client is authenticated; otherwise, access is denied. The Authentication result is sent back to the server.
- The server forwards the authentication result to the client

6. Vulnerability of Active Directory Servers

Many of these servers have numerous security flaws and vulnerabilities for which Microsoft is currently releasing security updates to repair them, organizations should pick and create the proper sort of Active Directory Server architecture. Remote Code Execution(RCE) and Denial of Service (DOS) attack is the major attack commonly found on an older version of Windows Server like Windows Server 2019 and Windows Server 2023, It is very important for organizations to use a newer version of the server and to update it as soon as Microsoft releases new updates.

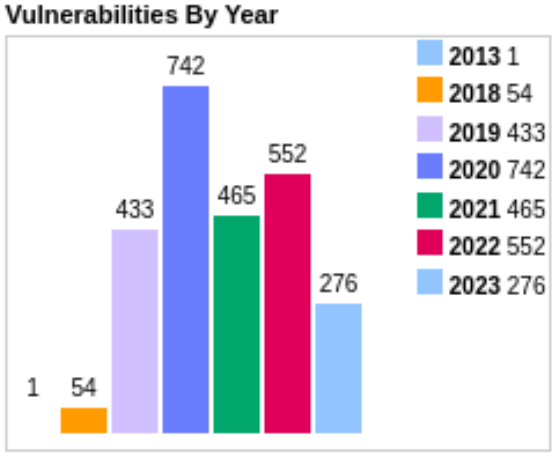

Fig. 5. Analysis of Vulnerabilities By Year

Figure 5 shows the exploit vulnerabilities increasing over time from 2013 to 2023. The threat to systems is growing as technology does as well.276 vulnerabilities have been discovered so far in 2021.

Figure 6 shows the list of vulnerabilities found on Windows Server 2022. The most common vulnerability is found in Code Execution, Denial of Service, and overflow

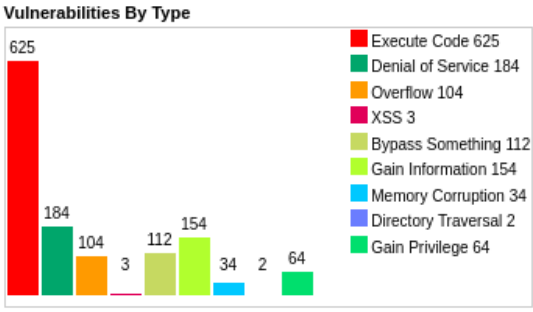

Fig. 6. Analysis of Vulnerabilities By Types

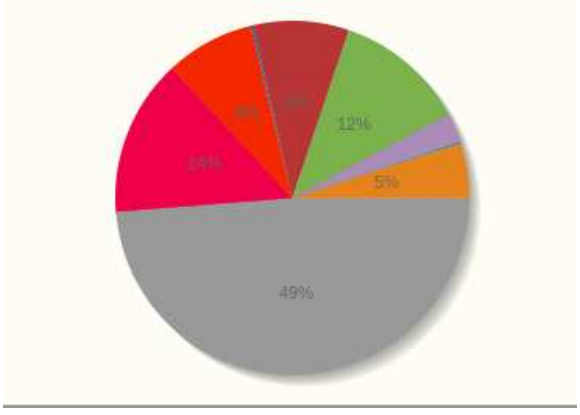

Fig. 7. Pie Chart

7. conclusions

Active Directory needs to undergo security testing in order for an organization's IT infrastructure to be available, secure, and of high integrity. Organizations may discover vulnerabilities, apply the required controls, and maintain a strong security posture by evaluating the many facets of AD security. To stay current with threats and maintain a robust defense against prospective assaults, security measures must be frequently reviewed and updated. The organization is in charge of ensuring that sure the environment is properly secured where the active directory is located. Although the active directory was addressed as a crucial system for organizational security, the focus of this work was to provide a case study for the active directory that could be used to further our analysis in subsequent studies. Future scopes might include developing an active directory implementation based on the benchmark.

References

[1] https://www.irjet.net/archives/V8/i7/IRJET-V8I7396.pdf, *2021*
[2] https://jespublication.com/upload/2020-1104136.pdf, *2020*
[3] https://tryhackme.com/room/winadbasics
[4] https://tryhackme.com/room/postexploit
[5] https://subscription.packtpub.com/book/networking-and-servers/9781787289352/pref
[6] https://tcm-sec.com/
[7] https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-50662/opbyp-1/Microsoft-Windows-Server-2019.html
[8] https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor_id=26