Active Directory and Its Security Attacks

Utkarsha Bamane [1], Sumitra Pundlik [2]

[1]MTech Student, Information and Technology (Cyber Security), MIT ADT University, Pune, Maharashtra, India
[2]Professor, Dept. of Information and Technology, MIT ADT University, Pune, Maharashtra, India

---***---

Abstract *Active Directory is Microsoft's developed hierarchical structure to provide services. Its services include storing the information about the objects which are present on the network. Network administrators have a key role as they will create and manage users and objects within the network. The active directory helps to organize a large number of users and provides access control at each level. Active directory works as a centralized management system as it can be used to manage all the elements of the network, including computers, groups, users, domains, security policies and any type of user-defined objects enabling the single sign-on (SSO) for the devices and application which are joined to the Active Directory domain.*

Key Words: Active Directory, Access control, Network, Single Sign-on (SSO), Centralized Management System.

1. INTRODUCTION

Active Directory is a directory service developed by Microsoft to manage the Windows domain network [5]. It is software to arrange, store information; provide access and permissions based on that information. It arranges all the Network's Users, Computers and other Objects into Logical, Hierarchical grouping [4]. The information is used to authenticate/authorize the Users, Computers and resources that are a part of the network. Active Directory lookout this by using Kerberos Authentication and Single Sign-On (SSO) [3]. Active Directory acts as a single repository for all of this user and computer-related information which makes it easier for user management. Active directory comes with windows server and it can be used to manage the entire organization.

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 [8]. As Active Directory manages the organization's resources it has become a common target for attackers. It can be exploited without ever attacking patchable exploits [1].

1.1. Components of Active Directory

While designing the infrastructure we need to consider both the components. Active Directory components consist of:

- Physical Components
- Logical Components

While designing the infrastructure we need to consider both the components. Logical components of the Active Directory structure can be changed at any given time consistent with the business requirement. But physical components are not easy to modify [10].

1.2. ACTIVE DIRECTORY OBJECTS

- **Users:** It contains information about the users. Enables the network resources access for the users [8].
- **Contacts:** Contains the contact information about the person associated with the company, for example, suppliers. It is used primarily to assign e-mail addresses or telephone numbers to external users [8].
- **Groups:** It is meant to represent groups that contain a collection of users, or computers, or contacts, or even other groups as members. It is used to simplify the administration of access control [8].
- **Computers:** It enables authentication and auditing of computer access to a resource on a network [8].
- **Printers:** It is used to simplify the process of locating and connecting to printers on the network [8].
- **Shared Folders:** It enables users to search for shared folders base on the properties [8].

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

2. ACTIVE DIRECTORY DOMAIN SERVICES

i. **Domain Services:** The domain service stores the centralized data and manages the communication between users and the domain controller. It is the primary functionality of Active Directory Domain Service [3] [9].

ii. **Certificate Services:** It allows Domain Controller to provide digital certificates, signature and public-key cryptography and is used to manage, generate and share certificates [3] [9].

iii. **Directory Federation Services:** It works based on the federated identity. It provides Single Sign-On (SSO) authentication for multiple applications in the same session so that user don't have to keep providing same credentials and also provide functionality that extends users SSO access to the application and systems outside the companies firewall[3] [9].

iv. **Lightweight Directory Service:** It supports cross-platform domain services, like any Linux computers present in the network [3] [9].

v. **Rights Management:** Rights management is used as a security tool to control information rights and data access policies [3] [9].

3. LITERATURE SURVEY

[Wataru Matsuda, 2018] This paper explains the Advance Persistent Threat (APT) attack on the organization's network and they have proposed a method for detecting attacks with the outlier detection using the machine learnings method of unsupervised learning which focuses on Event logs. The precision rate is high even if the Domain Administrator account is been compromised but there is also a chance for false-positive detection in the case of domain administrator as administrator commonly uses common that attackers use [1].

[Afnan Binduf, 2018] explained the Active Directory and the importance of using it. They have also covered different types of security vulnerabilities present in the active directory server and what measures can be taken to address the issue by going through the security aspects of the active directory. Alert feature, user authentication and many more different security features provided by the active directory are mentioned [2].

[Dr. Shwetav Sharad, 2019] This research paper tells about the role of Active Directory and its components. It gives you an overview of the services which are provided by the active directory and also about objects, trees, forests, domains, etc. which are included a logical structure. They have distinguished between two key feature of windows which is Workgroup and Domain [3].

[Nalini C Iyer, 2019] mentions the role of the administrator. List of the objectives on basis of which the active directory can be structured and methodology used. The main focus was on the topics like AD, Domain, Forest and structure [4].

[Purna Chandra Rao, 2015] has proposed an advanced new approach of active directory techniques. They have gone through the Active Directory architecture and how the FSMO role failure can impact the Active Directory functionality [5].

4. Vulnerabilities of Active Directory Servers

The organizations should choose and build the appropriate type of Active Directory Server architecture because many of these server have various types of vulnerabilities and security issues for which Microsoft is still making security updates to patch it. Denial of Service (DoS) attack and Remote code execution (RCE) is the major attacks commonly found on the older version of the Windows Server like Windows Server 2000, Windows Server 2003, and Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2. 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 [2].

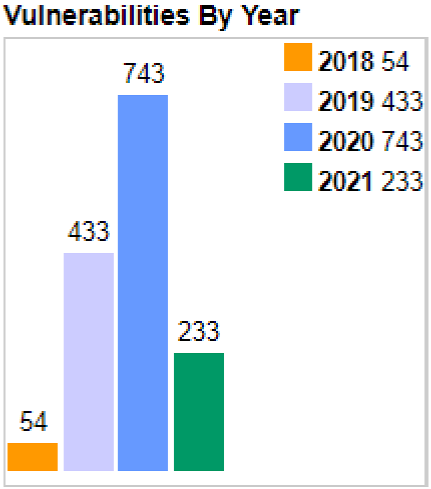

Fig -1: Analysis of vulnerabilities year-by-year

Figure 1 shows the exploit vulnerabilities increasing over time from 2018 to 2021. As technology is advancing so is the threat to systems. 223 vulnerabilities are found in 2021 till date. A total of 1463 vulnerabilities are found from 2018 till date [6].

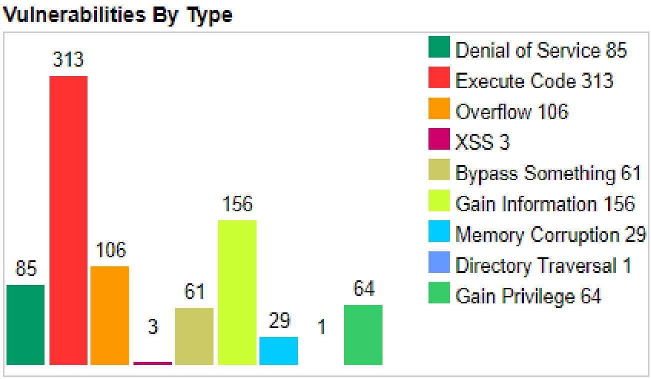

Fig -2: Analysis of vulnerabilities by the types

The above figure 2 shows the list of vulnerabilities found on Windows Server 2019. The most common majorly found vulnerabilities are code execution, information gathering and buffer overflow. Buffer overflow exploit allows the attacker to execute arbitrary code with network service privileges [7].

In 2020 the Kerberos security feature bypass vulnerability and windows task scheduler feature bypass vulnerability has a critical impact. It also mentions exploits related to denial of service attack and gaining access privileges. Cross-site-scripting (XSS) vulnerability exists in Windows Server 2019 Active Directory Federation Services (ADFS) that does not properly sanitize user inputs, therefore it is also known as 'Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability' [7].

6. CONCLUSIONS

Active directory is a commonly used solution for any company that wants to manage and control information and resources. Active directory is integrated into windows servers which have some vulnerabilities that could affect it in the organization. Active directory security can be enhanced by maintaining the security of the windows servers. There are many features in the active directory that might raise security concerns if not used properly. The active directory has built-in security measures that help in managing security in the organization. The environment should be secure properly where the active directory is placed, which is the responsibility of the company. While this paper discussed active directory as an important system for organization security, the scope will be to develop a case study for the active directory that can be presented in future papers to refine our findings. Implementation of an active directory based on the benchmark can be developed as a future scope.

REFERENCES

[1] Wataru Matsuda, “Detecting APT attacks against Active Directory using Machine Learning ” 2018 IEEE Conference on Applications, Information and Network Security (AINS) available- https://ieeexplore.ieee.org/document/8631486

[2] Afnan Binduf, “Active Directory and Related Aspects of Security” 2018 IEEE Conference available - https://ieeexplore.ieee.org/document/8593188

[3] Dr Shwetav Sharad, “Research Paper on Active Directory” International Research Journal of Engineering and Technology (IRJET) Volume: 06 Issue: 04, Apr 2019 available - https://www.irjet.net/archives/V6/i4/IRJET-V6I4761.pdf

[4] Nalini C Iyer, “Implementation of Active Directory for efficient management of network” ScienceDirect Procedia Computer Science 172 (2020) 112–114 available - https://www.sciencedirect.com/science/article/pii/S1877050920313399

[5] Purna Chandra Rao, “An Advanced approach of Active Directory Techniques” International Journal of Information and Technology (IJIT) – Volume 1 Issue 1, Mar-Apr 2015 available - http://www.ijitjournal.org/volume-1/issue-1/IJIT-V1I1P1.pdf

[6] https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor_id=26

[7] https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-50662/opbyp-1/Microsoft-Windows-Server-2019.html

[8] https://tcm-sec.com/

[9] https://www.varonis.com/blog/active-directory-domain-services/

[10] https://subscription.packtpub.com/book/networking_and_servers/9781787289352/1/ch01lvl1sec10/active-directory-components