Unveiling the Active Directory Security: A comprehensive analysis

Journal:	*IEEE Security & Privacy*
Manuscript ID	Draft
Manuscript Type:	Tutorial/Survey
Date Submitted by the Author:	n/a
Complete List of Authors:	jhaldiyal, alok; UPES, Dadwani, Yash; Barclays India Shekhar, Sagar ; TIAA Global Business Services
Keywords:	Information Security, Application Security, Active Directory

Unveiling the Active Directory Security: A comprehensive analysis

Alok Jhaldiyal[*1], Sagar Shekhar [2], Yash Dadwani [3]

Author 1 (* Corresponding Author)

Name: Mr. Alok Jhaldiyal

Email: ajhaldiyal@ddn.upes.ac.in

Affiliation: Assistant Professor (Selection Grade), School of Computer Science, UPES, Dehradun

Author 2

Name: Mr. Yash Dadwani

Email: yashmeetdadwani07@gmail.com

Affiliation: Software Development Engineer, Barclays India

Author 3

Name: Mr. Sagar Shekhar

Email: sagar.shekhar99@gmail.com

Affiliation: SOC Analyst, TIAA GBS India

Abstract

Active Directory (AD) is a service by Microsoft that makes it easier for the clients to centrally manage their workstations and servers in the system using its unique hierarchical structure. This unique structural environment helps them to provide wide range of services that also includes storing the sensitive data of objects presiding over a network. These services have gained widespread usage and popularity, making it a target for several attackers who disguise themselves as the legitimate Domain Administrator accounts and thus gain the access of the highest privileged accounts on the AD environment. As AD works as a centralized management system, thus it helps to organize many people and provide them the access control. The attacks that take place against Active Directory have changed over the years and these attacks target the large number of features and functions of AD and try to exploit them. In this research, we try to focus on processing different attack activities inside the AD environment and then we offer our perspectives on importance, impact, and the detection of these Active Directory attacks. We also review the attacks by outlining their steps. Additionally, we experimented few attacks and have provided some of techniques and solutions against these attacks.

Keywords

Information Security; Active Directory; SMB; Golden Ticket

Statements and Declarations

a) We do not analyse or generate any datasets, because our work proceeds in a simulated environment configured on a local machine.

b) The authors declare that the submitted article adheres to all standard compliance and ethical standards as laid down by the journal.

c) The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

d) The authors declare that they have no conflict of interest.

1. Introduction

Active Directory (AD) is a centralized managed software to organize and store information, thus granting access and rights based on that information. It hierarchically groups all the network's users, computers, and other entities on the network [1]. Many hackers focus on the AD for several kinds of attacks due to its centralized management of an organization's resources. These attacks often involve the exploitation of vulnerabilities in the AD environment, with reports of attackers that abuse Domain Administrator privileges [2]. AD is a highly desirable target for attackers, as obtaining the Domain Administrator privilege enables them to develop a backdoor that impersonates the "Golden Ticket" to gain long-term administrator privileges. Event logs are important for detecting and investigating attacks on the AD because they document an attacker's actions, such as misusing accounts and processes, etc. These logs usually detect abnormal processes and thus help improve system security. Security operators may blacklist these peculiar processes, but this requires ongoing maintenance of black or white lists, which frequently includes account information, process names, directory names of run processes, etc. Blacklists can also increase false detections because attackers frequently misuse lawful procedures. In contrast, whitelists might take much time to maintain and update regularly.

Active Directory can be used to offer several services such as authentication, user based services, policy administration and identity management. It is the most popular windows domain directory service implementation and is used throughout the windows environment. Services provided by Active Directory are as follows [1, 3, 4]:

i. Directory federation services allow multiple clients to log in using a single sign-on (SSO) to several web applications within a single session.
ii. Domain services provide various services related to managing domain names, facilitating user login and search functionalities, and mediating communication between users and domains. These services can include domain name servers and domain name registrars.
iii. Lightweight directory services are designed to support applications that are enabled by the Open (LDAP) protocol. These services store and retrieve information about network resources such as users, groups, and devices.
iv. Rights management is a set of technologies and processes used to protect digital content subject to copyright by implementing encryption techniques and access controls to restrict the unauthorized use and distribution of digital content.
v. Certificate Services are responsible for maintaining, issuing, and distributing secure certificates to authenticate the certificate holder's identity.
vi. DNS service provides the services of Domain Name Resolution.

AD manages access and establishes security for network objects. It simplifies user management because it is a single repository for all user and computer-related information. It comes bundled with Windows Server and leverages to manage the entire organization. It is widely used for Identity Management Services (IMS), with 95% of Fortune 500 companies implementing it in their networks [5]. However, due to its role in managing an organization's resources, attackers can exploit it without relying on patchable exploits. Network administrators can build and administer a network's domains, users, and objects with AD. It uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

The majority of attacks against Active Directory tart by infecting just one PC in the environment before moving on to high-privileged users like domain admins [6]. Attackers typically use a variety of persistence strategies to prolong their presence in environments with high privileges. Using security measures to prevent and defend against cyber-attacks is more crucial in today's increasingly digital environment.

According to Kaspersky [7], a data intrusion costs enterprises USD 1.41M and businesses of various sizes USD 108 K. Consequently, the alarm for Active Directory security is rising considering these facts and figures, and numerous research projects have been offered to demonstrate the risk posed by the attacks of Active Directory and approaches to mitigate against them. This research paper's goal is to describe the methods for getting access to Active Directory systems and to offer mitigation techniques for identifying, minimizing, and preventing such assaults. We also carry out experimental research on four Active Directory attacks: LLMNR Poisoning attack, SMB Relay attack, Kerberoasting attack, and Golden Ticket attack

The rest of this paper is structured as follows. A quick introduction to the Active Directory components, objects, authentication, and threats is given in Section 2. Section 3 provides an examination of our experimental work. In Section 4, we provide the practical implementation of the attacks described in previous sections. Finally, conclusions and future work are presented in Section 5.

2. Background

2.1 Components of AD

The two components of the AD must be considered while designing its setup. These two components include logical and physical components. Depending on the business requirements, the logical components can be altered easily, whereas the physical ones are tough to modify [8].

The physical components include the Domain Controllers, Sites, and Global Catalog Server. The domain controllers are servers that manage and authenticate access to network resources. Sites are used to group domain controllers together based on their physical location and define the physical

topology of a network. The Global Catalog Server stores the partial copy of items in other domains in the same forest and the readable copy of items in its host domain.

On the other hand, the logical components include Forests, Domains, Domain trees, Organizational Units, and Trusts. Forests are collections of multiple trees that share a standard schema and configuration partition, whereas trees are collections of domains with a typical naming structure and a hierarchical relationship. Domains are used to manage and organize network resources and are typically structured around departmental or business unit lines. Organizational units aid in the smaller-scale grouping of items within the domain. Trusts allow resources in one domain to be accessed by users or computers in another domain.

2.2 AD Objects

i. USERS – This object type contains information about network users and enables access to network resources.
ii. CONTACTS – It provides the contact details for anyone connected to the business, such as suppliers. It typically assigns phone numbers or email addresses to external users.
iii. GROUPS – Groups represent collections of users, computers, contacts, or other groups as members, and it is applied to streamline access control administration.
iv. COMPUTERS – It allows for the authentication and auditing of computer access to a network resource.
v. PRINTERS – It is used to make finding and connecting to printers on a network easier.
vi. SHARED FOLDERS – This object type enables users to search for shared folders based on attributes.

2.3 Authentication in AD

Kerberos authentication system is primarily utilized in AD environments [9]. The Domain Controller in an AD environment uses authentication tickets known as Ticket Granting Tickets (TGT) and Service Tickets (ST) to process all authentications uniformly.

- Ticket-Granting Tickets (TGT): This type of ticket proves the user's authenticity. During the first authentication process, the client asks the Domain Controller for a TGT, which is then saved on the user's computer and reused until it expires. By default, the ticket expires after ten hours of its creation time.

- Service Ticket (ST): A ticket that permits the use of a service within the AD environment is known as a service ticket (ST). When users request access to a service, they request an ST from the Domain Controller and use the ticket to validate their identity to the service server.

2.4 Attacks Against AD

The general overview of the widespread attack methods against AD exploits the Kerberos authentication protocol. These are:

1) Intrusion [4, 10]: Attackers utilize various techniques to infect a computer with malware, including sending phishing emails with harmful attachments or tricking users into visiting malicious websites.
2) Steal Domain Administrator Privilege [11, 12]: After gaining control of a computer in the AD environment, the attacker tries to raise their level of access so that they can log into Domain Administrator accounts, for instance, by exploiting the vulnerabilities present in AD.
3) Attack performed using Golden Ticket [13, 14, 15]
    a. Create the Golden Ticket: The attacker creates the Golden Ticket after gaining Domain Administrator rights, which gives them permanent administrator rights.
    b. Attack using Golden Ticket: The Golden Ticket can then be used in an attack by the hacker to spread the infection or steal confidential data.

Attackers frequently try to gain Domain Administrator rights since it provides them complete control over the AD environment. Once they gain access, they manipulate a Ticket-Granting Ticket (TGT) with an authentic signature to generate a Golden Ticket. The Golden Ticket has a prolonged expiration time of up to ten years, allowing attackers to keep access even after changing their password. It is used to spoof any Administrator account. Furthermore, it can be challenging to distinguish between a malicious attack and a typical authentication because the Golden Ticket looks to be a legitimate authentication. Attackers can carry out their attacks using attack tools or built-in Windows commands.

3. Experimental Work and Analysis

In this section, we launched four AD attacks. To aid in quick detection and response in the event of an intrusion, these implementations are aimed to evaluate and identify any signatures of these attacks in

different event logs. The section is structured as follows: The lab setup and techniques are provided in Section 3.1, followed by a detailed discussion on the implementation of each os the the four attacks..

3.1 Lab Setup and Methodology

The software tools and components used in these practical labs are listed in:

VMWare (Hypervisor), Windows server 2019 (DC), Windows 10 (Host), Kali (Attacker Machine), Responder, NTLMrelayx, and, Mimikatz.

3.2 LLMNR Poisoning

In this experiment, as demonstrated in Figure 1, we assumed that an attacker conducts a man-in-the-middle attack using a responder tool. Usually, a DNS failure occurs when someone mistype the network drive address. The username, NTLM2 hash, and IP address of the client computer are all recorded by the responder tool. After obtaining the hash, the attacker can attempt to break it using a tool made specifically for this purpose, such as Hashcat. In the first step, we used the Responder tool to capture the hashes of the client's computer. It usually takes time to run, and once the responder is loaded, it is in the middle and waiting for any requests. Responder needs to run when the network has high traffic. In the next step, the client attempts to open a shared file but mistypes the network address. Post this event points to the IP address of the attacker rather than pointing to the correct domain controller's IP address, and thus an event of DNS failure occurs. Then, the user is informed that access to that domain is forbidden by the appearance of the Windows Security dialogue box. While this DNS Failure event was happening, the responder recorded the NTLMv2 hash, the IP address of the client's computer, and the username. In the final step, the attacker uses a tool known as Hashcat to crack the hashes. The attacker uses the -force flag to have Hashcat execute on a CPU rather than a GPU because his workstation is housed in a virtual environment. The attacker will be able to quickly decode the hashes if the passwords are weak and easy to guess. When a password is fourteen characters long and lacks both complexity and length, it is deemed weak. When the password is obtained in plain text, the attacker uses the account to gain access to a machine. Most firms and organizations still lack proper password policies and use LLMNR which makes them ideal targets for attackers looking to gain an early advantage.

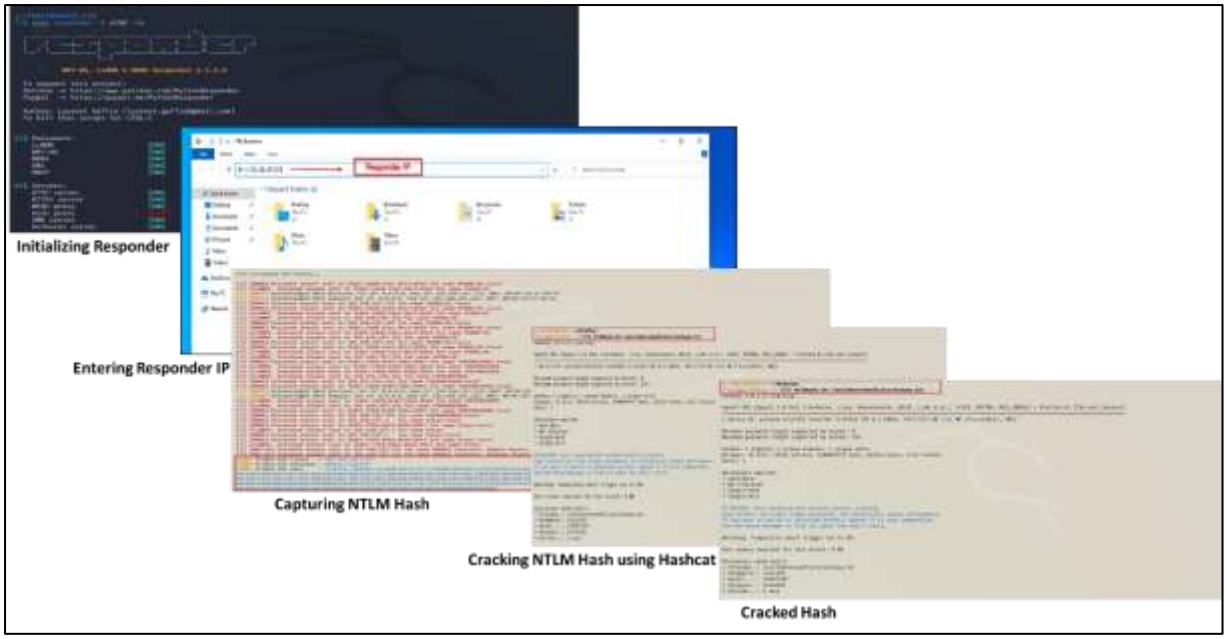

Figure 1: Implementation of LLMNR poisoning attack

3.3 SMB Relay Attack

A successful SMB Relay attack requires two conditions: First, the target machine's SMB signing must be disabled; second, the attacker must have administrator access to the target machine. In this attack, the attacker relays the hashes to another machine on the same network rather than offline cracking the captured hashes. To simulate this attack, we first run the nmap scan to check which hosts have the SMB signing disabled as can be seen in figure 2. On any workstation, message signing is disabled by default; however, it is enabled and necessary on Domain Controller by default. As the domain controller is a server, the attacker is unable to relay through it. Whenever the message signing is enabled but not necessary for some client IP addresses then those IP addresses are seized by the attacker and recorded in the targets.txt file and are free to launch a relay assault on them. In the next step, the attacker alters the configuration file of the responder by disabling both SMB and HTTP. Thus, here the responder acts as a listener in this sense and refrains from responding to these services. Then, the attacker launches a responder to wait for a response. The attacker sets up a relay using the ntlmrelayx tool (present in the impacket) along with the target list.

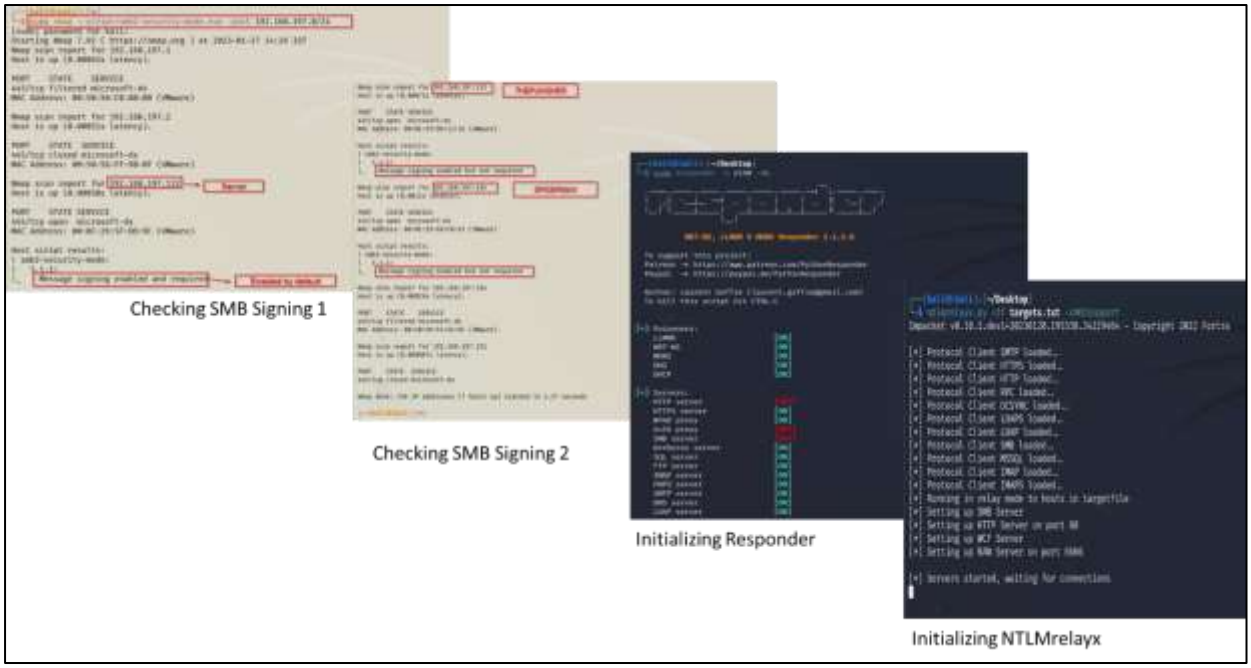

Figure 2: SMB Relay Attack and NTLMrelayx Initialization

An event of DNS failure occurs when the client enters the attacker's IP address instead of the domain controller's IP address. As the client is the administrator of this computer, therefore, the local SAM hashes have been dumped and thus now the attacker can copy these hashes, try cracking them offline, and finally will succeed in getting the SMB interactive shell. Post the initialization of NTLMrelay the various steps are performed as cam be seen in figure 3 that finally exposes files. The attacker goes to the shares folder and finds several directories and then lists the files included in those folders. In order to extend his influence over the administrator folder and subsequently this machine, he uses the ADMIN$ folder, where he can add files and obtain files.

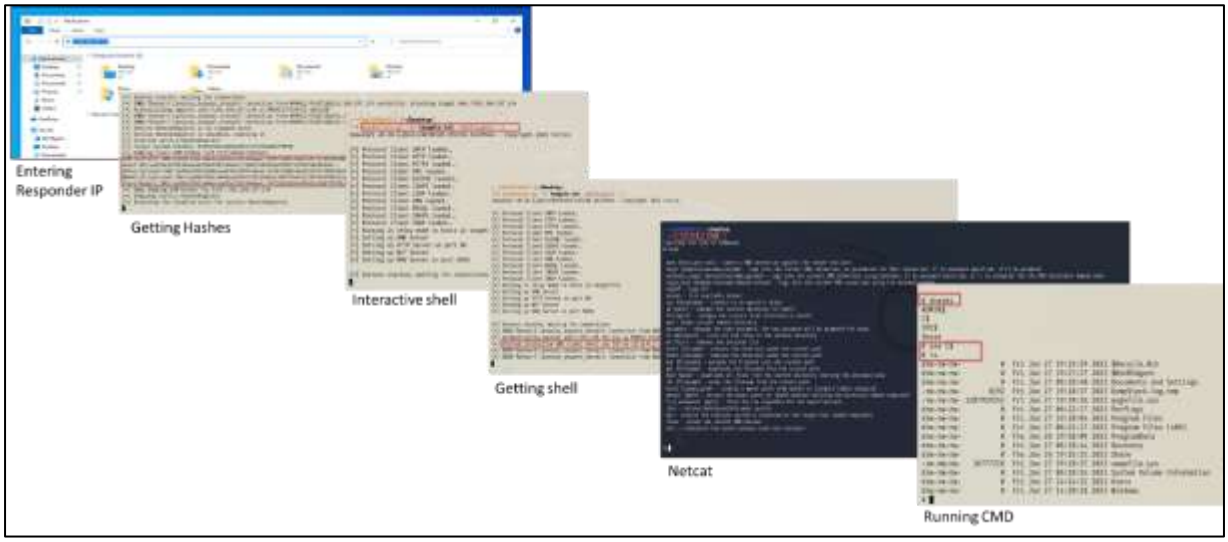

Figure 3: Part 1 - SMB Relay Attack final steps

3.4 Kerberoasting Walkthrough

An FTP server was installed on the client machine, and its server was launched using a domain admin account to imitate this attack. The name of the service was then entered as the account's SPN value. The attack started using the Get-NetUser-SPN command from Powerview to search the domain for users with the SPN attribute. After that, the attacker uses a GetUserSPNs.py script in order to request a service ticket. The TGS is then copied and saved into the serviceticket.txt file. Afterward, an offline crack is done for the TGS using Hashcat to get the admin password. Though, in order to crack this ticket, the attacker needs to locate the appropriate module. After cracking the ticket, the attacker finally gains the shell access and then dumps the SAM hashes. After the successful simulation of this attack, we can notice that there were no helpful logs on the workstation or domain controller that could have pointed to a privilege escalation attack because the Kerberoasting attack is a type of password-cracking attack.

This is because after breaking into the service account, the attacker can log in routinely without exhibiting any unusual behavior, making it more difficult to identify these kinds of attacks. To lessen the attack surface for this assault, it is advised to use complicated and lengthy passwords for service accounts and to restrict the privileges of these accounts.

Figure 4: Part 2 - Implementation of Kerberoasting Attack

3.5 Golden Ticket Attack

Users can use golden tickets, or TGTs, to give attackers access to resources. Attackers utilize these TGTs to obtain service tickets from the domain controller without verifying the accuracy of the

information in the TGT. The TGT is used in the Kerberos protocol to show the KDC (Kerberos Key Distribution Center) service on the domain controller that the user is authenticated to the DC. The password for the KRBTGT account is required to both encrypt and decrypt Kerberos tickets. Since the account name is the same across all domains and the password is rarely changed, it is a popular target for hackers. In this attack simulation as shown in figure 5, in order to create the Kerberos Golden Tickets, we need two things: The name and SID of the domain to which the KRBTGT account belongs as well as the password hash of the KRBTGT account. In the first step, we gained privileged access of the domain controller and after logging in remotely, we extracted the domain name, SID, and password hash using Mimikatz. Then, we copied the SID of the domain controller and NTLM hash. The attacker then used the parameters of the Mimikatz for creating the golden tickets. In this command, the /ptt (pass the ticket) trigger injects the golden ticket being created. In the next step, the created golden ticket is saved and further loaded via the *misc* command. This golden ticket is then passed to the next session or current session. This ticket is then used to access the client's computer by connecting to the domain controller and gaining access to all kinds of stored files.

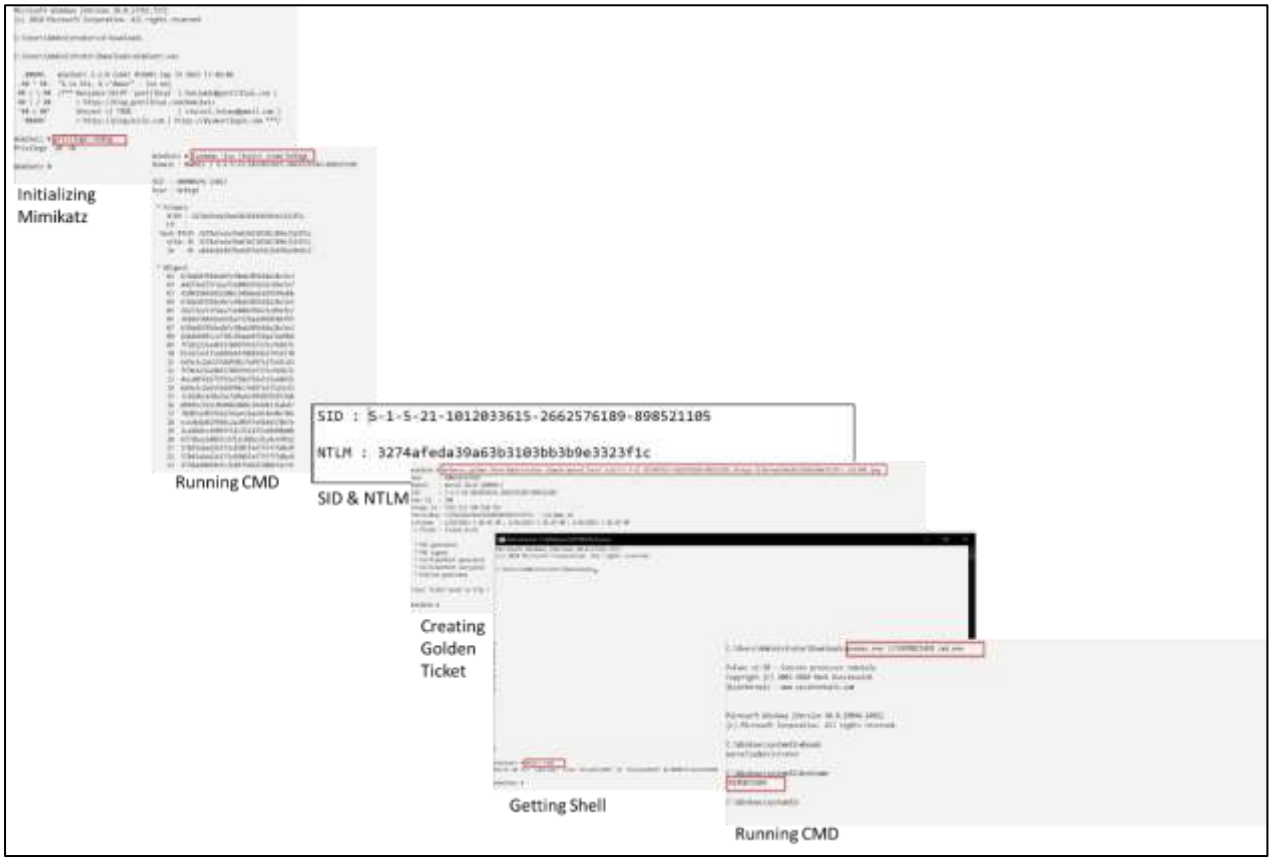

Figure 5: Generation of golden ticket and its execution

4. Mitigation Strategies of Security Attacks: -

4.1 LLMNR Poisoning Attack –

Implementing robust security measures is crucial to safeguard a network from LLMNR Poisoning attack. One such measure involves disabling LLMNR (Link-Local Multicast Name Resolution), a non-essential protocol that can be exploited by attackers. Disabling this protocol can prevent attackers from exploiting the name resolution process. This measure recommended unless it is necessary for specific network setups or applications. Additionally, utilizing DNS over HTTPS (DoH) which encrypts DNS traffic over HTTPS protocol, which adds an extra layer of security. It prevents eavesdropping, tampering, or interception of DNS traffic by attackers. By using DoH, the DNS queries are sent over a secure connection to a DNS server that supports DoH. Another effective technique is the implementation of DNSSEC, which provides a way to validate the authenticity and integrity of DNS responses. It uses digital signatures to verify that DNS records have not been tampered with. DNSSEC prevents attackers from spoofing DNS responses and redirecting users to malicious websites by ensuring the authenticity of DNS data. To enhance network segmentation and restrict unauthorized access, VLANs can be employed. VLANs (Virtual Local Area Networks) can be used to logically segment a network into smaller isolated networks. This helps prevent unauthorized access and limits the ability of attackers to eavesdrop on network traffic. Furthermore, deploying a firewall act as a barrier, filtering and monitoring network traffic based on established security rules, thereby preventing unauthorized access, and blocking malicious activity.

4.2 SMB Relay Attack –

Mitigating SMB Relay attacks requires a multi-faceted approach. Firstly, disabling SMBv1, an outdated and vulnerable protocol, helps prevent attackers from exploiting its weaknesses. By deactivating SMBv1, the potential attack surface is reduced. Secondly, utilizing SMB Signing is recommended as it digitally signs SMB packets, ensuring their integrity and authenticity. This prevents attackers from intercepting and modifying SMB traffic. Another effective strategy involves implementing Extended Protection for Authentication, an added layer of security for authentication protocols, including SMB. Enabling this feature bolsters defences Finally, implementing two-factor authentication adds an extra layer of protection by requiring an additional verification step, making it more challenging for attackers to gain unauthorized access even if they intercept authentication traffic. By employing these strategies collectively, organizations can significantly reduce the risk and impact of SMB Relay attacks, enhancing the overall security of their network against SMB Relay attacks. Additionally, network isolation plays a vital role in preventing the spread of SMB Relay attacks. By segregating critical systems from the rest of the network, the impact of an attack can be limited.

4.3 Kerberoasting Attack –

Mitigating Kerberoasting attacks requires a comprehensive approach to strengthen the security of the Kerberos authentication protocol. Firstly, employing strong passwords with complex combinations

serves as a fundamental defence, making it arduous for attackers to crack the encrypted hashes, even if obtained. Implementing password policies that enforce complexity and regular rotation further enhances password strength. Secondly, utilizing service accounts with non-expiring passwords for specific purposes can reduce the risk of Kerberoasting. These accounts have passwords that do not change regularly, limiting the opportunities for attackers to exploit them. Thirdly, adopting Group Managed Service Accounts (GMSA) automates password management for service accounts, mitigating the risk of Kerberoasting by ensuring more secure credential handling. Another effective strategy is to implement Kerberos Constrained Delegation. This feature restricts the scope of Kerberos authentication requests to specific services, preventing attackers from leveraging compromised accounts for broader attacks. Lastly, leveraging Privileged Access Management (PAM) solutions plays a pivotal role in enhancing security. PAM solutions enable better management and monitoring of privileged accounts and activities, reducing the risk of Kerberoasting by enforcing strict access controls and monitoring unauthorized access attempts. By implementing these multifaceted measures, organizations can fortify their defenses against Kerberoasting attacks and bolster the overall security of their systems and AD environment.

4.4 Golden Ticket Attack –

Golden Ticket attacks pose a significant threat to AD environments, necessitating the implementation of effective mitigation strategies. Firstly, implementing a strong password policy is vital. This includes enforcing complex passwords, setting password expiration policies, and promoting the use of multi-factor authentication. These measures make it more challenging for attackers to obtain or crack credentials. Furthermore, minimizing Domain Admin access is crucial as Golden Ticket attacks rely on compromising such privileged accounts. By reducing the number of users with Domain Admin privileges, the attack surface is diminished. Thirdly, actively monitoring AD for suspicious activity can help detect and respond to Golden Ticket attacks promptly. Monitoring for unusual changes to the domain, abnormal authentication requests, and unusual usage patterns can raise alerts and enable timely investigation. Leveraging Managed Service Accounts (MSAs) strengthens security by providing unique and frequently changing passwords for service accounts, mitigating the risk of Golden Ticket attacks. By implementing these comprehensive mitigation strategies collectively, organizations can significantly reduce the risk of Golden Ticket attacks. Regular security assessments, patch management, and employee education on the importance of cybersecurity also contribute to a robust defense against such threats.

5. Conclusion and Future Work: -

Attacks on AD are much more dangerous and sophisticated, and they have the potential to damage the entire system. We discussed the characteristics of AD and its authentication in this paper. There was discussion of the most typical AD attacks. A summary of the current detection and mitigation techniques

was also given. In order to ensure the security and integrity of organisational networks, it is crucial to concentrate on preventing attacks against AD. Through this research, a number of efficient mitigation techniques for various attack types, including Golden Ticket attacks, Kerberoasting attacks, LLMNR Poisoning attacks and SMB Relay attacks, have been identified and suggested. These tactics include using Managed Service Accounts, limiting Domain Admin access, monitoring AD for suspicious activity, and setting strong password restrictions. But because cyber threats are constantly growing, it takes constant work to stay one step ahead of attackers. Thus, in our upcoming work, we intend to suggest and model fresh detection and mitigation techniques for various AD attacks by focusing on areas like User Education and Awareness, Security Automation, Zero Thrust Architecture and Integration with Threat Intelligence.

6. References

1. Desmond, B., Richards, J., Allen, R., & Lowe-Norris, A. G. (2008). *AD: Designing, Deploying, and Running AD*. " O'Reilly Media, Inc.".
2. Chadwick, D. (2005). Threat modelling for AD. In *Communications and Multimedia Security: 8 th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Sept. 15–18, 2004, Windermere, The Lake District, United Kingdom* (pp. 173-182). Springer US.
3. Dias, J. (2002). *A guide to microsoft AD (ad) design* (No. UCRL-MA-148650). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States).
4. Mokhtar, B. I., Jurcut, A. D., ElSayed, M. S., & Azer, M. A. (2022). AD Attacks—Steps, Types, and Signatures. *Electronics*, *11*(16), 2629.
5. DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016, November). Implementing zero trust cloud networks with transport access control and first packet authentication. In *2016 IEEE International Conference on Smart Cloud (SmartCloud)* (pp. 5-10). IEEE.
6. Wueest, C. (2014). Targeted attacks against the energy sector. *Symantec Security Response, Mountain View, CA*.
7. *Kaspersky. Kaspersky's 2019 IT Security Economics Report. Available online: https://go.kaspersky.com/rs/802-IJN-240/images/GL_Kaspersky_Report-IT-Security-Economics_report_2019.pdf (accessed on 01 September 2023).*
8. Clines, S., & Loughry, M. (2008). *AD for dummies*. John Wiley & Sons.
9. Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Gómez, N. G. (2021). On Attacking Kerberos Authentication Protocol in Windows AD Services: A Practical Survey. *IEEE Access*, *9*, 109289-109319.
10. Matsuda, W., Fujimoto, M., & Mitsunaga, T. (2018, November). Detecting apt attacks against AD using machine leaning. In *2018 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 60-65). IEEE.
11. Fujimoto, M., Matsuda, W., & Mitsunaga, T. (2018, November). Detecting abuse of domain administrator privilege using windows event log. In *2018 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 15-20). IEEE.
12. Grillenmeier, G. (2021). Protecting AD against modern threats. *Network Security*, *2021*(11), 15-17.
13. Soria-Machado, M., Abolins, D., Boldea, C., & Socha, K. (2014). Kerberos golden ticket protection. *Mitigating Pass-the-Ticket on AD, CERT-EU Security Whitepaper*, *7*, 2016.
14. Kotlaba, L., Buchovecká, S., & Lórencz, R. (2021, February). AD Kerberoasting Attack: Detection using Machine Learning Techniques. In *ICISSP* (pp. 376-383).
15. Grippo, T., & Kholidy, H. A. (2022). Detecting Forged Kerberos Tickets in an AD Environment. *arXiv preprint arXiv:2301.00044*.