IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TICKET FORGERY USING KERBEROASTING

[1]Dhruv Srivastava,

[1]Student

[1]Department of Electronics and Communications Engineering,
[1]R.V. College of Engineering, Bengaluru, India

Abstract: Kerberoasting, Golden Ticket, and Silver Ticket attacks represent significant threats to the security of Active Directory

environments, leveraging the vulnerabilities within the Kerberos authentication protocol. This project aims to explore these advanced attack techniques, their mechanisms, and their implications on enterprise security. Kerberoast ing is an attack method where attackers extract service account credentials from Kerberos tickets, which are then cracked offline to gain unauthorized access. This serves as a precursor to more severe exploits, such as Golden and Silver Ticket attacks. Golden Tickets allow attackers to forge Ticket Granting Tickets (TGTs) using the domain's Key Distribution Service account (krbtgt) hash, granting virtually unlimited access to any service or resource within the domain. This enables the attacker to impersonate any user, including domain administrators, leading to complete domain compromise. Conversely, Silver Tickets involve forging Ticket Granting Service (TGS) tickets for specific services, allowing attackers to access and control individual services without interacting with the domain controller, making detection significantly more

challenging. The project delves into the technical aspects of these attacks, the tools commonly used, such as Mimikatz, and the steps required to perform these exploits. Additionally, it discusses detection methods using tools like Wireshark and monitoring Kerberos traffic for anomalies. Preventive measures, including robust service account management, multi factor authentication, regular patching, and encryption practices, are also covered. This comprehensive analysis aims to equip cybersecurity professionals with the knowledge to detect, prevent, and mitigate the risks associated with Kerberoasting, Golden Tickets, and Silver Tickets, thereby enhancing the security posture of Active Directory environments.

***Index Terms* -** Component, formatting, style, styling, insert.

I. INTRODUCTION

Kerberos is an authentication protocol widely utilized for securing communication across untrusted networks, especially in distributed computing setups, was crafted by MIT. Its primary goal is to furnish robust authentication for

client-server interactions through the implementation of secret-key cryptography. This protocol serves to authenticate users or services operating within an exposed network environment susceptible to eavesdropping or replay attacks. Functioning via ticket-based mechanisms, Kerberos enables users to access network services without the need to transmit passwords openly. Its significance lies notably in enterprise settings, where it stands as a pivotal element in upholding the confidentiality, integrity, and genuineness of data exchanges amid clients and servers.

The three heads of the Kerberos protocol represent the following: (1), the client,(2) network resource(application server),(3)a key distribution center that acts as the Kerberos third party authentication service.

The Kerberos authentication protocol uses the following steps :

- Step 1: User login and request services on the host.This is also known as the Ticket Granting Service(TGS).
- Step 2: The Authentication Server verifies the users credentials and then gives Ticket Granting Ticket and a session key.
- Step 3: Decryption of message is done using the password and then sent to the TGS.
- Step 4: TGS decrypts the ticket sent by the user and authenticator verifies the request and then creates the ticket for requesting services from the services.
- Step 5: The user sends the Ticket and Authenticator to the Server
- Step 6: The server verifies the Ticket and authenticators then grant access to the service.

II.METHODOLOGY

The implementation was done by first setting up and Active Directory and a client machine on OracleVM .Here, the Active
Directory was assigned as the Domain Controller. After this, softwares such as Rubeus, Mimikatz, Splunk and Wireshark
were installed. In order to execute the Golden and Silver Ticket attacks, we used Mimikatz and Rubeus respectively.
A Golden Ticket attack is a type of advanced cyber attack that targets Active Directory (AD) environments, allowing attackers to gain unrestricted access to any resources within the network.
A Silver Ticket attack is another type of Kerberos attack in an Active Directory environment, similar to the Golden Ticket
attack but with different targets and impacts. While a Golden Ticket provides unrestricted access to the domain, a Silver Ticket focuses on gaining access to specific services.

III.KERBEROASTING

Kerberoasting is a method aimed at acquiring the password hash of an Active Directory account associated with a Service Principal Name (SPN). In this attack, a domain user with authentication privileges requests a Kerberos ticket for a specific SPN. This ticket, encrypted with the hash of the service account password linked to the SPN, is then retrieved. Subsequently, the attacker engages in offline efforts to crack the password hash

1) Target Identification: The attacker identifies a target user account in the Active Directory that has SPNs
(Service Principal Names).The SPN represents MSSQL(Microsoft Structured Query Language)Server and Exchange Server.
that use kerberos authentication.
2) Requesting Service Tickets: Attacker requests TGS tickets from the KDC using a valid user account
3) Recovering Encrypted Service Tickets:Upon receiving the service tickets from the KDC.
4) Offline Brute Force Attack:Attacker attempts to brute force the tickets offline, since they are RC4 or AES encrypted.The
main aim is to obtain the plaintext password.
5) Privilege Escalation: Here, the compromised service account may have escalated privileges within the network . After
obtaining the plaintext password, the attacker can escalate the privileges and gain further access to critical resources.

IV.ENCRYPTION METHODS

RC4 (Rivest Cipher 4) and AES (Advanced Encryption Standard) are two widely used encryption algorithms with distinct
characteristics and applications. RC4 is a stream cipher designed by Ron Rivest in 1987, known for its simplicity and
speed. It encrypts data by generating a pseudo-random keystream and combining it with plaintext using bitwise XOR.
Despite its historical popularity in protocols like WEP and SSL/TLS, RC4 has been deemed insecure due to vulnera-

bilities that allow attackers to recover plaintext under certain conditions.

In contrast, AES, established as a standard by NIST in 2001, is a symmetric block cipher designed to replace older, less secure algorithms like DES. AES operates on fixed-size blocks of data (128 bits) and supports key lengths of 128, 192, or 256 bits. It employs a series of complex transformations, including substitution, permutation, and mixing, over multiple rounds to ensure robust security. AES is widely adopted for securing data in various applications, from encrypting sensitive files to securing communications in network protocols, due to its strong resistance to cryptographic attacks and its balance of performance and security.

A. RC4 Algorithm:

The algorithm starts with a key-scheduling algorithm (KSA) that initializes a permutation of all 256 possible byte values (the state array, S) based on a variable-length key. This is followed by the pseudo-random generation algorithm (PRGA), which updates the state array and produces a keystream byte for each byte of plaintext.

During the KSA, the state array is populated with values from 0 to 255 and shuffled using the provided key. The PRGA then enters a loop where it continues to modify the state array and selects bytes from it to form the keystream. Each the keystream byte is XORed with a byte of plaintext to create the ciphertext. Decryption is simply the reverse process, XORing the ciphertext with the same keystream to retrieve the original plaintext. Despite its historical significance and efficiency, RC4's vulnerabilities, particularly its susceptibility to certain attacks due to its predictable key scheduling, have led to its deprecation in favor of more secure algorithms.

B. AES Algorithm:

The Advanced Encryption Standard (AES) is a symmetric block cipher that encrypts data in fixed-size blocks of 128 bits using keys of 128, 192, or 256 bits. The encryption process involves several rounds of transformation steps, the number of which depends on the key length (10, 12, or 14 rounds for 128, 192, and 256-bit keys, respectively). Initially, the plaintext block is XORed with the first round key in the AddRoundKey step. Each subsequent round includes four steps: SubBytes (a non-linear substitution using a pre-defined S-box), ShiftRows (a row-wise permutation), MixColumns (a column- wise mixing operation using matrix multiplication), and another AddRoundKey. The final round omits the MixColumns step, ending with the AddRoundKey transformation. These operations ensure that the plaintext is thoroughly diffused and obscured, resulting in highly secure ciphertext. AES decryption reverses these steps using the inverse transformations, providing a robust and efficient encryption standard widely adopted for securing data.

V.SETTING UP ACTIVE DIRECTORY

Setting up an Active Directory (AD) environment on Oracle VM involves several steps, including configuring a domain controller (DC) and a client machine, followed by the installation of essential software for monitoring and security testing.

Begin by creating two virtual machines (VMs) on Oracle VM:one for the domain controller and one for the client. Install Windows Server on the DC VM and promote it to a domain controller by installing the Active Directory Domain Services (AD DS) role and configuring a new domain. On the client VM,install a Windows operating system and join it to the domain created on the DC. Next, install essential software tools such as Rubeus, Mimikatz, Wireshark, and Splunk. Rubeus and Mimikatz are crucial for performing security assessments and testing Kerberos-related vulnerabilities. Wireshark, a network protocol analyzer, helps in monitoring and analyzing network traffic. Splunk can be installed to collect and analyze logs, providing insights into network and security events. This setup creates a robust environment for learning, testing, and monitoring AD security and network operations.

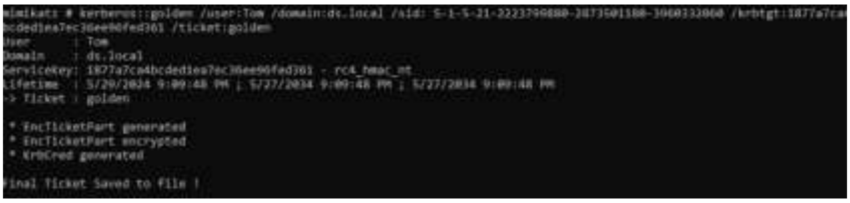
A. Tools and Software Used

- **Oracle VM:** Oracle VM is a virtualization solution provided by Oracle Corporation. It allows users to create and manage virtualized environments on x86 and SPARC-based systems.Users can create multiple VMs on OracleVM Server to run different operating systems and applications. Each VM is isolated from the others and has its own virtual hardware resources, including CPU,memory, storage, and network interfaces.
- **Microsoft Windows Server:** Microsoft Windows Server is a server operating system developed by Microsoft Corporation. It is designed to provide various server oriented functionalities, including file and print services, web services, application hosting, directory services, and more.
- **Rubeus:** Rubeus is a powerful tool for Windows Active Directory environments, primarily used for Kerberos based attacks and manipulation.
- **Mimikatz:** Mimikatz is a powerful post-exploitation tool commonly used in penetration testing, red teaming, and security research.
- **Splunk:** Splunk is a leading platform for analyzing and monitoring machine-generated data in real-time. It collects, indexes, and correlates data from various sources, allowing organizations to gain insights, troubleshoot issues, detect anomalies, and make data-driven decisions.
- **Wireshark:** Wireshark is a powerful and widely-used network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network.
- **MSSQL:** MSSQL is a Relational Database Management System developed by Microsoft.

VI.GOLDEN AND SILVER TICKET KERBEROASTING

A. Golden Ticket:

- The attacker gains administrative access to a domain controller or obtains the necessary credentials to extract the necessary information from the domain controller.
- The attacker extracts the password hash (NTLM hash) of the KRBTGT account from the domain controller’s Active Directory database. The KRBTGT account is a privileged account used by the Key Distribution Center (KDC) to encrypt TGTs for users during the authentication process.
- Using the extracted KRBTGT hash, the attacker generates a forged TGT with arbitrary user credentials and a desired ticket lifetime. The forged TGT is encrypted using the KRBTGT account’s password hash, making it indistinguishable from a legitimate TGT.

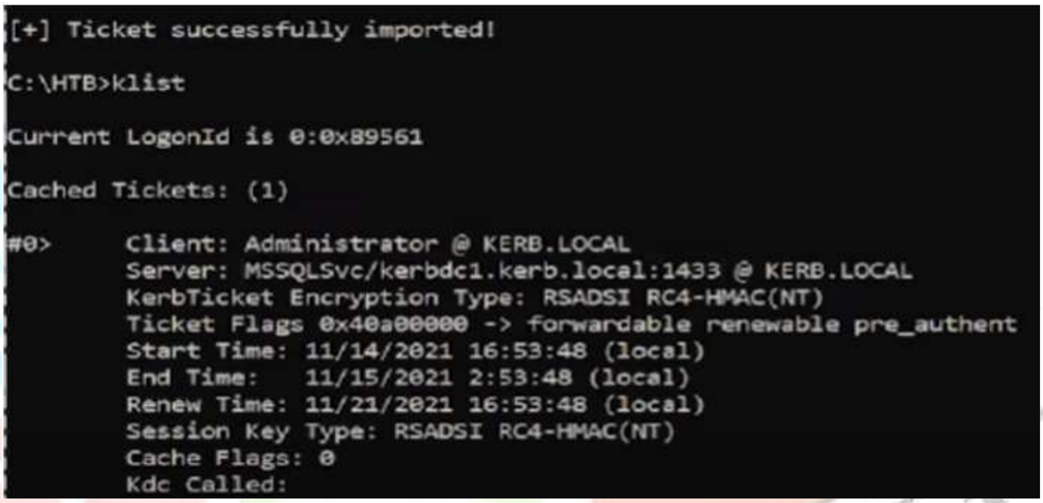


```
mimikatz # kerberos::golden /user:Tom /domain:ds.local /sid: S-1-5-21-2223799880-2873501588-3060332060 /krbtgt:1877a7ca
bcded1ea7ec36ee90fed361 /ticket:golden
User       : Tom
Domain     : ds.local
ServiceKey: 1877a7ca4bcded1ea7ec36ee90fed361 - rc4_hmac_nt
Lifetime   : 5/29/2024 9:09:48 PM ; 5/27/2034 9:09:48 PM ; 5/27/2034 9:09:48 PM
-> Ticket : golden

 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

Figure 1: golden ticket

B. *Silver Ticket:*

- The attacker enumerates the Active Directory environment to gather information about domain users, domain controllers, and service accounts
- Using Rubeus, perform a Kerberoasting attack by mentioning the domain and the users username and password,
- After entering the necessary details, we obtain the hashed value of the password. Hashcat or any other tool can be used to crack the password, in Silver Tickets, usually RC4 encryption is implemented, so, it is easy to crack the hash.
- This attack allows the attacker to access specific services or applications within the domain without needing to interact with the domain controller, making it more difficult to detect.



```
[+] Ticket successfully imported!

C:\HTB>klist

Current LogonId is 0:0x89561

Cached Tickets: (1)

#0>     Client: Administrator @ KERB.LOCAL
        Server: MSSQLSvc/kerbdc1.kerb.local:1433 @ KERB.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 11/14/2021 16:53:48 (local)
        End Time:   11/15/2021 2:53:48 (local)
        Renew Time: 11/21/2021 16:53:48 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:
```

Figure 2: silver ticket

VII. Results and Discussions

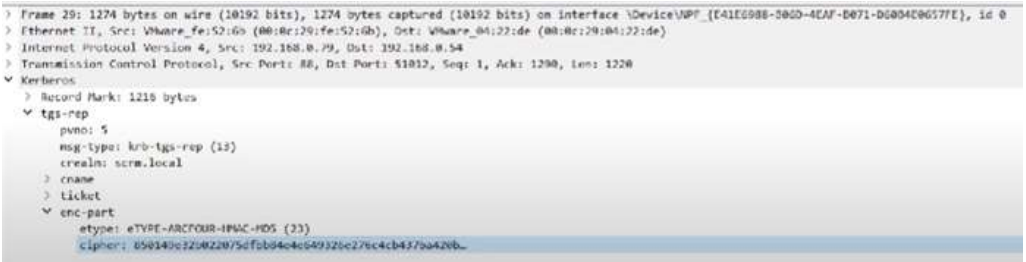
A. *Completion and Detection of Golden Ticket Attack*

- Here, we are given the confirmation that the Golden Ticket has been generated on the client system.
- After this, we utilize PsExec64 through which we are able to execute programs on remote systems.PsExec is a lightweight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software.
- After this, we are able to access the ”Command Prompt” of the Domain Controller through which we are able to access the files on the Domain Controller.

In order to detect the Golden Ticket on Wireshark, we follow these steps:

Capture Kerberos Traffic: Start Wireshark and begin capturing traffic on the network where the Kerberos authentication is taking place.

Inspect Ticket Granting Service (TGS) Requests: Here, we search for only TGS requests in wireshark in the packet capture.
These packets are used when a client requests access to a service using a TGT. Identify Suspicious Usernames.



```
> Frame 29: 1274 bytes on wire (10192 bits), 1274 bytes captured (10192 bits) on interface \Device\NPF_{E41E6988-506D-4EAF-B071-D6004E0657FE}, id 0
> Ethernet II, Src: VMware_fe:52:6b (00:0c:29:fe:52:6b), Dst: VMware_04:22:de (00:0c:29:04:22:de)
> Internet Protocol Version 4, Src: 192.168.0.79, Dst: 192.168.0.54
> Transmission Control Protocol, Src Port: 88, Dst Port: 51012, Seq: 1, Ack: 1290, Len: 1220
v Kerberos
  > Record Mark: 1216 bytes
  v tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: scrm.local
    > cname
    > ticket
    v enc-part
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        cipher: 050140e32b022075dfbb84e4e649326e276c4cb437ba420b…
```

Figure 3: detection of golden ticket on Wireshark

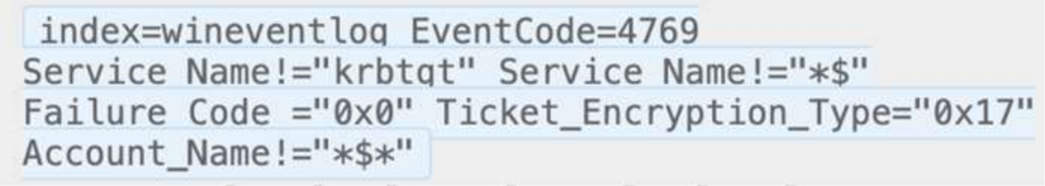
B. Completion and Detection of Silver Ticket Attack

- After performing the kerberoasting attack, we have to obtain the Domain Sid to obtain the Silver Ticket. This is done using LDAP Lightweight Directory Access Protocol (LDAP) is an application protocol used for accessing and managing directory information services over an IP network.
- We are able to obtain the ObjectSid, CN = KERBDC1 shows that the given data belongs to the Domain Controller.
- Once we obtain this, we are then able to go and enter the final query into Rubeus after which we generate the Silver Ticket.

In order to detect the Silver Ticket generation on Splunk, we follow the following steps:

We generate an alert. Here, the SPL Query searches for the event ID 4769.

Once we run the query, we get the following on the dashboard.This shows that all events related to the Event ID 4769 have been captured by Splunk.This helps in the detection of the Kerberos Silver Tickets.



```
index=wineventlog EventCode=4769
Service Name!="krbtgt" Service Name!="*$"
Failure Code ="0x0" Ticket_Encryption_Type="0x17"
Account_Name!="*$*"
```

Figure 4: splunk query for detection of Silver Ticket

VIII. Inferences

Golden Ticket and Silver Ticket attacks highlight critical vulnerabilities in the Kerberos authentication protocol within
Active Directory environments. The primary inference is the need for stringent security measures to protect against these
sophisticated attacks. Golden Ticket attacks, with their ability to provide unrestricted domain-wide access by exploiting
the KRBTGT account, demonstrate the importance of regularly updating service account credentials and monitoring for
anomalous activities. Silver Ticket attacks, which target specific services, underscore the necessity of applying the principle of
least privilege and employing robust access controls to limit the impact of compromised accounts. These attacks emphasize the
urgency of implementing comprehensive security practices, including multi-factor authentication, regular security audits,
and advanced threat detection mechanisms, to safeguard against unauthorized access and potential data breaches.

IX. References

[1] David, S. Kerberoasting: Credential Theft Using Kerberos. International Journal Of Cyber Security. 10, 123-134 (2019)

[2] Smith, J. & Brown, A. Defending Against Kerberoasting Attacks: Techniques and Tools. Cyber Defense Review. 11, 45-58 (2020)

[3] Wang, L. & Zhang, M. Analysis of Kerberoasting Attack Vectors. Proceedings Of The International Conference On Cyber Security. pp. 87-95 (2021)

[4] Garcia, L. & Hernandez, M. Improving Detection of Kerberoasting Attacks in Real-Time. Journal Of Information Security. 14, 212-223 (2018)

[5] Kim, J. & Lee, S. Kerberos and Credential Theft: A Survey on Kerberoasting. Journal Of Network Security. 9, 301-312 (2022)

[6] Taylor, R. & Miller, E. Golden Ticket Attacks: Unrestricted Access inActive Directory. Proceedings Of The Conference On Information Security. pp. 101-112 (2017)

[7] Brown, A. & Smith, J. Understanding Golden Ticket Attacks and Defense Mechanisms. Cyber Security Journal. 13, 150-165 (2021)

[8] Chen, W. & Li, X. Mitigating the Risk of Golden Ticket Attacks in Enterprise Networks. International Conference On Network Security. pp.56-67 (2019)

[9] Jones, M. & Davis, S. Golden Ticket Exploits: Techniques and Counter-measures. Information Security Research. 16, 89-98 (2020)

[10] Johnson, P. & White, A. Active Directory Security: Addressing Golden Ticket Vulnerabilities. Journal Of Cyber Defense. 15, 275-289 (2022)

[11] Martinez, L. & Anderson, J. Silver Ticket Attacks: Targeted Service Exploits in Kerberos. Proceedings Of The Symposium On Information Assurance. pp. 134-145 (2018)

[12] Williams, D. & Moore, K. Understanding and Defending Against Silver Ticket Attacks. Network Security Journal. 12, 99-110 (2021)

[13] Lopez, M. & Wilson, E. Service Account Compromise and Silver Ticket Attacks. International Conference On Cybersecurity. pp. 78-89 (2020)

[14] Clark, S. & Harris, B. Mitigating Silver Ticket Attacks in Active Directory Environments. Journal Of Computer Security. 14, 200-213 (2019)[15] Gonzalez, J. & Perez, C. Silver Ticket Exploits: Techniques and Defen-sive Strategies. Information Security Review. 17, 65-78 (2022)

[16] Rodriguez, J. & Sanchez, L. Enhancing Detection of Kerberoasting Attacks Using Machine Learning. International Workshop On Cyber Threat Intelligence. pp. 90-101 (2021)

[17] Nguyen, T. & Hoang, D. Survey on Kerberoasting Attacks and Defense Mechanisms. Journal Of Network And Computer Applications. 19, 412-425 (2020)

[18] Patel, R. & Verma, N. Golden Ticket Attacks: Techniques and Case Studies. Proceedings Of The International Conference On Information Systems Security. pp. 122-133 (2019)

[19] Turner, R. & Scott, D. Securing Active Directory Against Silver Ticket Attacks. Journal Of Cybersecurity Technology. 10, 145-159 (2021)

[20] Evans, M. & Thompson, A. Machine Learning Techniques for Kerberoasting Detection. International Conference On Cybersecurity AndResilience. pp. 101-112 (2022)