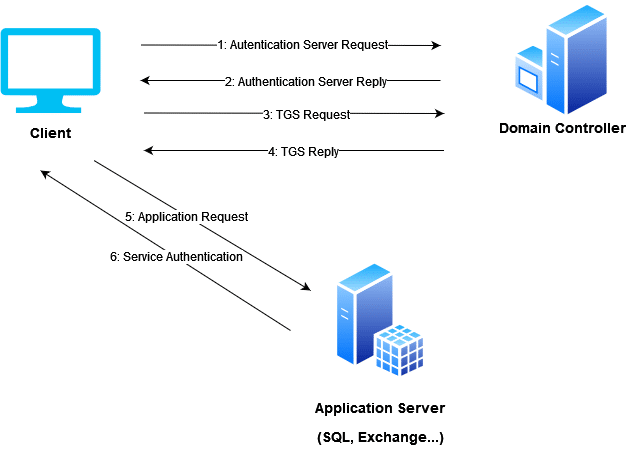
**[Research and document common Active Directory attacks (Kerberoasting, DCSync, Golden Ticket, etc.)](https://github.com/Nourhene13/projet-pfe-AD/issues/1)**

**Active Directory (AD)** is a directory service developed by Microsoft that is used to manage the permissions and access to resources within a network. AD stores information about objects such as users, computers, and groups, and provides services such as authentication, authorization, and management of network resources. It is widely used in organizations to ensure centralized control over network management.

**Kerberoasting Attack**

****

**What’s Kerberoasting:**

Kerberoasting is a form of attack that targets the **Kerberos authentication protocol** used by Active Directory. The main objective of the attack is to obtain **service account credentials** by exploiting how service tickets are encrypted in the Kerberos system.

**2. How Does Kerberoasting Work?**

1. **Initial Authentication**:
   * The attacker must already have access to the target network, meaning they are **authenticated** either as a regular user or through another form of access (e.g., compromised credentials or privilege escalation).
2. **Requesting Service Tickets**:
   * The attacker requests a **service ticket** for any service that uses a service account, such as a database or web server.
   * The service ticket is encrypted with the **password hash** of the service account.
3. **Cracking the Service Ticket**:
   * Once the attacker has obtained the service ticket, they can attempt to crack the encrypted ticket using **brute-force** techniques. The process of cracking involves trying multiple possible passwords to match the encrypted ticket.
   * This step typically happens **offline**, meaning the attacker doesn't need to interact with the server directly, allowing them to try many combinations without detection.
4. **Obtaining the Password**:
   * Once the attacker successfully decrypts the ticket, they obtain the service account's **clear-text password**.
5. **Exploiting the Password**:
   * The attacker can now use the service account’s password to access critical systems, escalate privileges, and perform malicious actions such as accessing sensitive data, modifying configurations, or using the service account for lateral movement in the network.

**4. Impact of Kerberoasting**

The Kerberoasting attack can have significant consequences, including:

* **Unauthorized Access**: Attackers gain access to service accounts, potentially including high-privilege accounts.
* **Privilege Escalation**: Once attackers control service accounts, they may escalate their privileges to administrative levels, gaining control over the network.
* **Lateral Movement**: With the cracked password, attackers can move laterally within the network to compromise additional systems and services.
* **Sensitive Data Exposure**: If the service accounts have access to sensitive data, attackers can exfiltrate or modify that information.

**5. Defending Against Kerberoasting**

To defend against Kerberoasting attacks, organizations should implement the following mitigation strategies:

**1. Enforce Strong Password Policies**

* **Complex Passwords**: Service accounts should have **complex and strong passwords** that are difficult for attackers to crack. This includes using a mix of uppercase and lowercase letters, numbers, and special characters.
* **Long Passwords**: Longer passwords are harder to brute-force. Using a password length of at least **20 characters** is recommended for service accounts.

**2. Use Managed Service Accounts (MSAs)**

* **MSAs** are **automatically managed** by Active Directory and do not rely on traditional passwords. This eliminates the risk of cracking the service account password, as there is no password to crack.
* MSAs are designed to rotate passwords automatically and securely, reducing the risk of exposure.

**3. Regularly Rotate Service Account Passwords**

* **Password Rotation**: Service account passwords should be changed regularly to make it more difficult for attackers to crack and reuse old tickets.
* **Automated Password Management**: Utilize tools like **Group Managed Service Accounts (gMSA)** or other password management solutions to automate the process of rotating passwords securely.

**4. Monitor for Unusual Behavior**

* **Monitor Kerberos Service Ticket Requests**: Keep an eye on unusual service ticket requests, especially from users who don't typically access certain services or applications.
* **Event Log Analysis**: Analyze **Kerberos event logs** to detect suspicious ticket requests and potential attacks in real time.

**5. Implement Least Privilege Access**

* Service accounts should have the **minimum necessary privileges** required to perform their tasks. This reduces the impact of a potential compromise, as attackers will have limited access to critical resources.

**6. Utilize Ticket Lifetimes and Expiration**

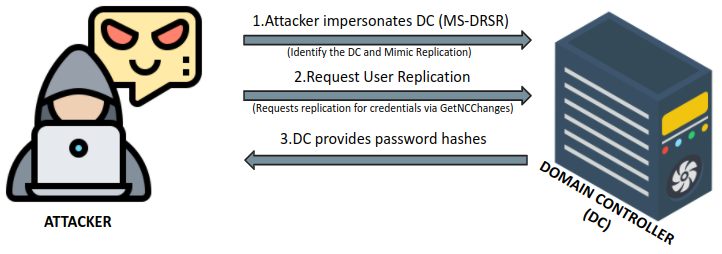
* **Shorten Ticket Lifetime**: Kerberos tickets should have a **short expiration time** to minimize the window of opportunity for attackers to crack them.
* **Enforce Ticket Expiration**: Use policies that force the **expiration** and renewal of tickets at regular intervals.

**6. Tools for Kerberoasting Detection**

Several tools and techniques can help organizations identify and mitigate Kerberoasting attacks:

* **Kerberos Roasting Tools**: Tools like **Rubeus** and **Impacket** can be used by attackers to exploit Kerberoasting. Monitoring their usage in the network is essential for detection.
* **SIEM Systems**: Security Information and Event Management (SIEM) solutions like **Splunk**, **Wazuh**, or **Microsoft Sentinel** can be used to analyze logs and detect unusual behavior related to Kerberos authentication requests.
* **Security Auditing**: Use Windows auditing features to monitor and log service ticket requests and any unusual activity related to Kerberos authentication.

**DCSync Attack**



**1. What is DCSync?**

DCSync is a stealthy attack that allows an attacker to **replicate the behavior of a Domain Controller (DC)** and extract sensitive authentication data, including password hashes, from Active Directory. This attack is possible when an attacker gains **Replicating Directory Changes** permissions, allowing them to request sensitive credentials from AD without directly compromising a Domain Controller.

Unlike other attacks that require direct access to domain controllers, **DCSync enables attackers to retrieve credentials remotely**, making it highly dangerous and difficult to detect.

**2. How Does DCSync Work?**

**1. Gaining Initial Access:**

* The attacker must already have access to an account with **Replicating Directory Changes** privileges.
* This can be achieved through **privilege escalation**, compromised administrator credentials, or by gaining control over a user with elevated rights (such as members of Domain Admins, Enterprise Admins, or the Administrators group).

**2. Impersonating a Domain Controller:**

* Once the attacker has the necessary permissions, they use specialized tools (e.g., **Mimikatz**) to mimic a **Domain Controller** and request replication of Active Directory data.

**3. Extracting Password Hashes:**

* The attacker retrieves **NTLM password hashes** and **Kerberos keys** of domain accounts, including those of privileged users and administrators.
* This data can be used for further attacks, such as **Pass-the-Hash (PtH)**, **Pass-the-Ticket (PtT)**, or **Golden Ticket** attacks.

**4. Maintaining Persistence:**

* Since the attacker has access to authentication data, they can create **backdoors**, escalate privileges, or maintain access even if their initial point of entry is removed.
* This allows attackers to **persist indefinitely** in the network, making it extremely difficult to fully remove their presence.

**3. Impact of DCSync Attack**

DCSync attacks pose severe threats to organizations as they provide attackers with unrestricted access to critical systems:

* **Full Domain Compromise:** The attacker can retrieve password hashes for any user, including domain administrators, effectively **gaining complete control** over the Active Directory environment.
* **Lateral Movement & Privilege Escalation:** With access to administrator credentials, attackers can escalate their privileges and move laterally across the network.
* **Data Theft & Espionage:** Attackers can use harvested credentials to access **confidential data, email accounts, financial records, and critical business applications**.
* **Long-Term Persistence:** Even if security teams remove an attacker's initial access, **DCSync enables them to maintain hidden access** by creating new administrator accounts or backdoors.

**4. Defending Against DCSync Attacks**

To protect against **DCSync attacks**, organizations should implement the following security measures:

**1. Restrict Replication Permissions**

* Limit the **Replicating Directory Changes** privilege to only the necessary accounts.
* Regularly audit **Group Memberships** (e.g., Domain Admins, Enterprise Admins, Administrators) to ensure no unauthorized accounts have replication rights.

**2. Enable Least Privilege Access**

* Ensure that **only legitimate Domain Controllers** can request directory replication.
* Reduce unnecessary **domain-wide administrative privileges**.

**3. Implement Multi-Factor Authentication (MFA)**

* Require **MFA** for all **privileged accounts**, making it harder for attackers to use stolen credentials.

**4. Monitor and Detect Suspicious Behavior**

* Use **SIEM (Security Information and Event Management) tools** to monitor directory replication requests.
* Monitor logs for **event IDs 4662 and 4742**, which indicate **directory replication requests**.
* Track **unusual login activities** from accounts that do not typically perform replication tasks.

**5. Implement Strong Password & Hash Protection Policies**

* Enforce **long and complex passwords** for domain administrator accounts.
* Regularly rotate **KRBTGT** passwords to mitigate **Golden Ticket** persistence risks.

**6. Disable Unnecessary NTLM Authentication**

* Restrict NTLM authentication and enforce **Kerberos-only** authentication for secure environments.
* Use **Windows Defender Credential Guard** to prevent attackers from using stolen credentials.

**5. Tools for DCSync Detection**

Several tools can help detect and prevent **DCSync** attacks:

* **Mimikatz** – Often used by attackers to perform DCSync attacks. Monitoring for its usage is critical.
* **Event Logs (4662, 4742, 4624, 4672)** – Can reveal unauthorized replication requests and privilege escalations.
* **SIEM Solutions (Splunk, Wazuh, Microsoft Sentinel)** – Help detect abnormal authentication patterns and replication activities.
* **BloodHound** – Used by attackers to identify accounts with replication rights; security teams can use it for auditing.
* **LDAP Queries** – To monitor which accounts have **Replicating Directory Changes** permissions.

**Golden Ticket Attack**

****

**1. What is a Golden Ticket Attack?**

A **Golden Ticket attack** is a type of Kerberos attack where an attacker forges valid Kerberos Ticket Granting Tickets (TGTs), granting them unrestricted access to any system in the Active Directory domain. The attack is named after the fictional *Golden Ticket* from *Charlie and the Chocolate Factory* because it provides the attacker with unlimited access.

**2. How Does a Golden Ticket Attack Work?**

The attack exploits weaknesses in how Kerberos handles authentication within Active Directory. Here’s how it works:

**1. Obtain Domain Administrator Access**

* To carry out a Golden Ticket attack, the attacker needs **Domain Admin (DA) or Enterprise Admin privileges** or must compromise the **KRBTGT account**, which is responsible for encrypting Kerberos tickets.

**2. Extract the KRBTGT Hash**

* The attacker extracts the **NTLM hash** of the **KRBTGT** account using tools like **Mimikatz**.
* The KRBTGT account is critical because **all Kerberos tickets in the domain are signed using its hash**.

**3. Forge a Golden Ticket**

* Using the extracted hash, the attacker creates a **forged Ticket Granting Ticket (TGT)** with any user credentials they choose.
* The TGT is signed with the **valid** KRBTGT hash, making it appear legitimate to the Kerberos system.

**4. Gain Full Access to the Domain**

* The forged TGT allows the attacker to **request service tickets (TGS)** for any service in the network.
* Since the ticket is valid, it bypasses security controls and provides **persistence**—the attacker can maintain domain access indefinitely.

**3. Impact of a Golden Ticket Attack**

A successful Golden Ticket attack is **devastating** because it gives an attacker full control over an Active Directory environment. The consequences include:

* **Unlimited Access** – Attackers can access **any** resource within the network.  
  **Persistence** – Even if the compromised user’s password is changed, the attack remains effective.  
  **Privilege Escalation** – Attackers can impersonate any user, including administrators.  
  **Lateral Movement** – Attackers can move through the network undetected, accessing multiple systems.  
  **Undetectable Exploitation** – Since the forged tickets appear valid, traditional security measures might not detect them.

**4. Defending Against Golden Ticket Attacks**

Because Golden Ticket attacks exploit a fundamental part of Kerberos authentication, **preventing and detecting them is critical**. Here’s how:

**1. Secure the KRBTGT Account**

* Regularly **rotate the KRBTGT account password** (at least twice in succession) to invalidate stolen hashes.
* Use **Group Managed Service Accounts (gMSA)** for securing critical service accounts.

**2. Implement Strong Privileged Access Management (PAM)**

* Restrict **Domain Admin (DA) access** to only a few necessary accounts.
* Use **Privileged Access Workstations (PAWs)** for administrative tasks to reduce exposure.

**3. Enable Logging & Monitoring**

* Monitor **Event ID 4769 (TGS requests)** for unusual activity.
* Use **SIEM solutions** (e.g., Splunk, Microsoft Sentinel, Wazuh) to detect anomalies.
* Look for **TGTs with long lifetimes**, as attackers often use extended ticket lifespans.

**4. Implement Least Privilege**

* Use **tiered administration** to limit DA access.
* Restrict **service accounts** from having unnecessary permissions.

**5. Deploy Endpoint Detection & Response (EDR) Solutions**

* Use EDR tools like **Microsoft Defender for Identity**, **CrowdStrike**, or **SentinelOne** to detect **Mimikatz** usage or unusual Kerberos authentication patterns.

**5. Tools for Golden Ticket Detection**

**1. Mimikatz**

* Attackers use **Mimikatz** to extract and forge Kerberos tickets.
* Security teams should **monitor for its execution** in logs and endpoint monitoring tools.

**2. Microsoft ATA / Defender for Identity**

* Detects **suspicious Kerberos activity**, such as forged ticket usage.

**3. SIEM Solutions (Splunk, Wazuh, Sentinel)**

* Can be configured to detect **anomalous TGT requests**.

**4. KList and Kerberos Logs**

* Use **klist.exe** to list active Kerberos tickets and look for unusually long TGT lifetimes.

**Other Kerberos Attacks**

Besides **Kerberoasting**, **Golden Ticket** and **DCSync** attacks, there are several other Kerberos-based attacks:

**1. Silver Ticket Attack**

* Similar to Golden Tickets but targets **service tickets (TGS)** instead of TGTs.
* Does not require KRBTGT hash but exploits individual **service accounts**.
* Harder to detect because TGS tickets are used **directly on the service**.

**2. Pass-the-Ticket (PtT) Attack**

* Attackers steal **legitimate Kerberos tickets** and reuse them to access resources.
* Exploited using tools like **Rubeus** and **Mimikatz**.

**3. Overpass-the-Hash (Pass-the-Key) Attack**

* An attacker **injects** stolen credentials into memory to request Kerberos tickets.
* Often used for **privilege escalation**.

**4. DCSync Attack**

* Attackers impersonate **Domain Controllers** to pull user credentials from Active Directory.
* Extracts **password hashes**, including **KRBTGT** for Golden Ticket attacks.

**5. AS-REP Roasting**

* Targets accounts **not requiring pre-authentication**.
* Extracts **encrypted AS-REP responses** to brute-force passwords offline.

**Conclusion**

The **Golden Ticket attack** is one of the most powerful attacks against Active Directory because it grants an attacker **persistent, unrestricted access**. Defending against it requires **strong password policies, monitoring, and privilege restrictions**.