In the name of God
Wednesday, February 2024
(tgt-tgs-krbtgt-hash)
AliReza ch

Titles

-Kerberos

-Pass the ticket

-Over pass the hash

-Kerberosting

-Golden ticket

-Silver ticket

-Skeleton key

About this mini **course** From CH
C:\whoami
Alireza ch

Hello,

Welcome! My name is Alireza CH, and I'd like to introduce you to one of the most important protocols: KERBEROS.

In this mini-course, I'll share more details about KERBEROS. Sometimes people aren't in a good mood, so if you have enough time, consider reading all the data and my experiences in this file. However, if you're short on time or not feeling your best, focus on the bold words.

I'll explain key topics using bold titles, such as the GOLDEN TICKET ATTACK. Additionally, pay attention to hints about detecting attacks—they often provide more details.

Thank you for reading this mini-course. Feel free to connect with me on LinkedIn anytime.

Best regards, Alireza CH

Farewell.

Kerberos :

Kerberos is a computer network security protocol that **authenticates service requests between two or more trusted hosts across an untrusted network, like the internet.**

It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users' identities.

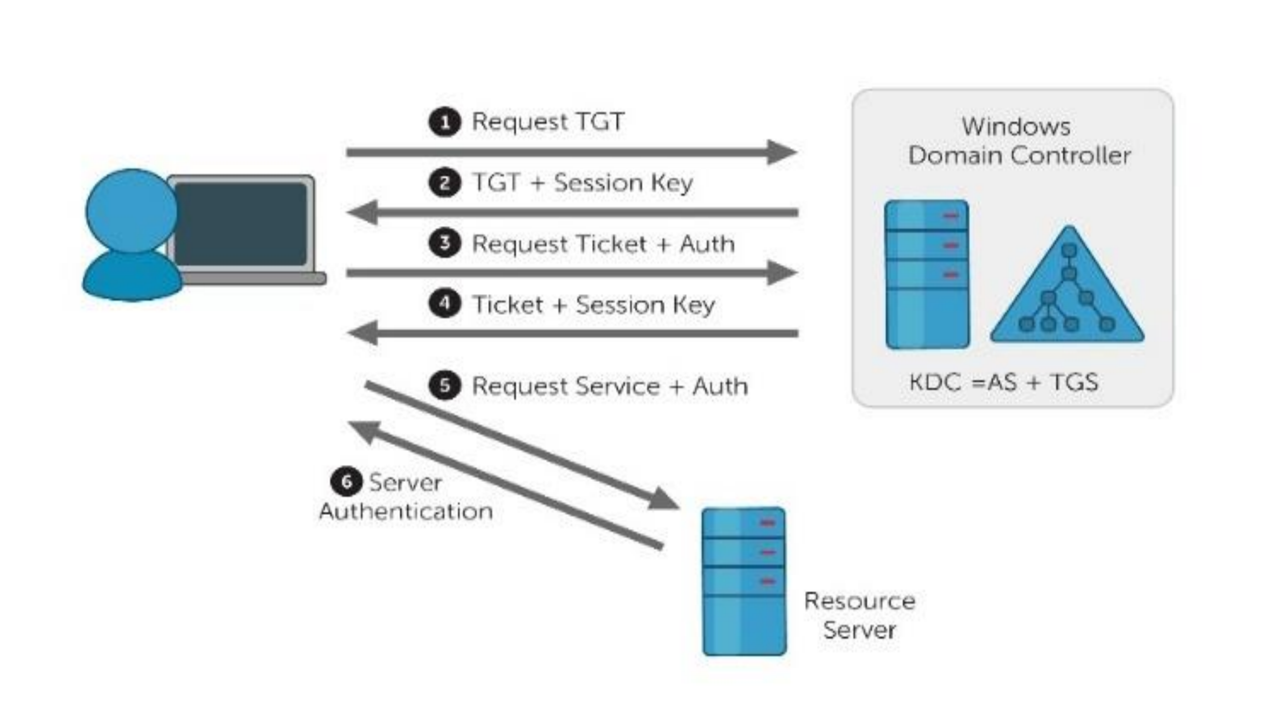
Kerberos :

What protocol does Kerberos use?

- **Kerberos** uses **symmetric key cryptography** and a key distribution center (KDC) **to authenticate and verify user identities**.

A KDC involves three aspects:

A ticket-granting server (TGS) that connects the user with the service server (SS) A Kerberos database that **stores the password and identification of all verified users**.



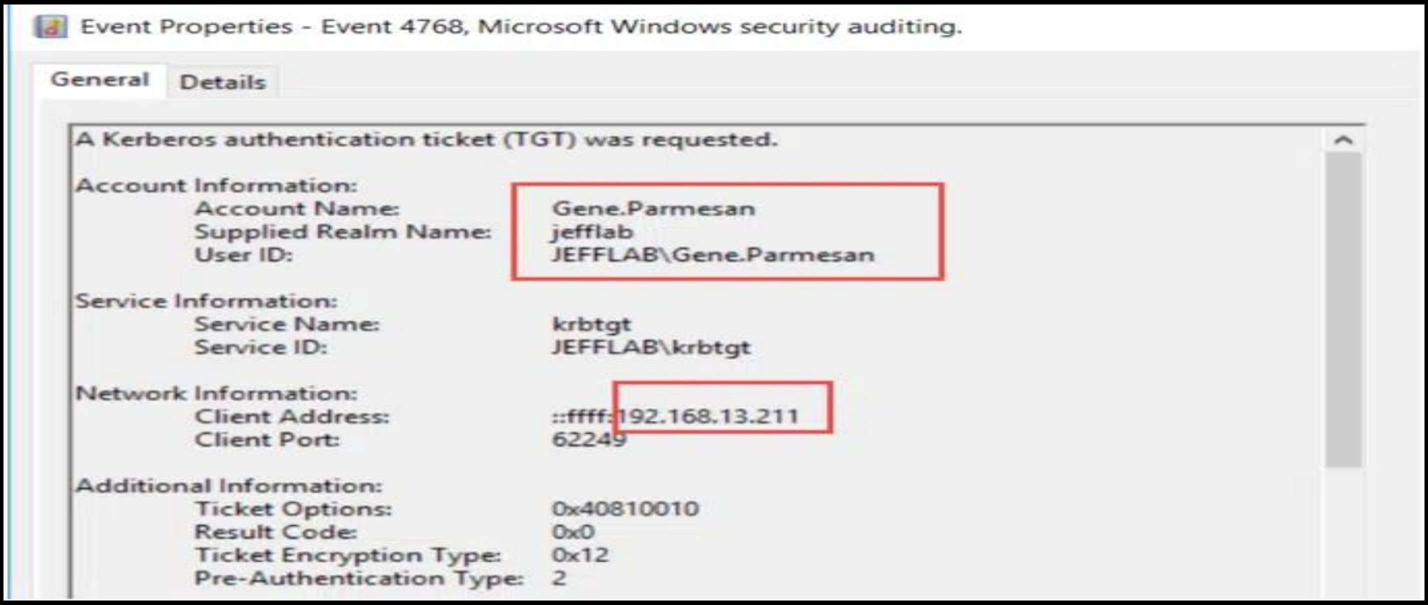
Pass - The - Ticket Attack

Pass the ticket (PtT) is a **method of authenticating to a system using Kerberos tickets without having access to an account's password**.

Kerberos authentication can be used as the first step to lateral movement to a remote system.

More details about pass-the-ticket attack

In a pass-the-ticket attack, **an attacker extracts a Kerberos Ticket Granting Ticket (TGT) from LSASS memory on a system** and then uses this valid ticket on another system to request Kerberos service tickets (TGS) **to gain access to network resources**.



Event Properties - Event 4768, Microsoft Windows security auditing.

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
          Account Name:              Gene.Parmesan
          Supplied Realm Name:       jefflab
          User ID:                   JEFFLAB\Gene.Parmesan

Service Information:
          Service Name:              krbtgt
          Service ID:                JEFFLAB\krbtgt

Network Information:
          Client Address:            ::ffff:192.168.13.211
          Client Port:               62249

Additional Information:
          Ticket Options:            0x40810010
          Result Code:               0x0
          Ticket Encryption Type:    0x12
          Pre-Authentication Type:   2
```

Splunk Query for detecting pass the hash attack :

- index=wineventlog EventCode = 4769 OR EventCode = 4768 OR EventCode = 4770 | stats count by Account_Name, Service_Name, Ticket_Encryption_Type, Client_Address| where count > some_threshold

Hint :

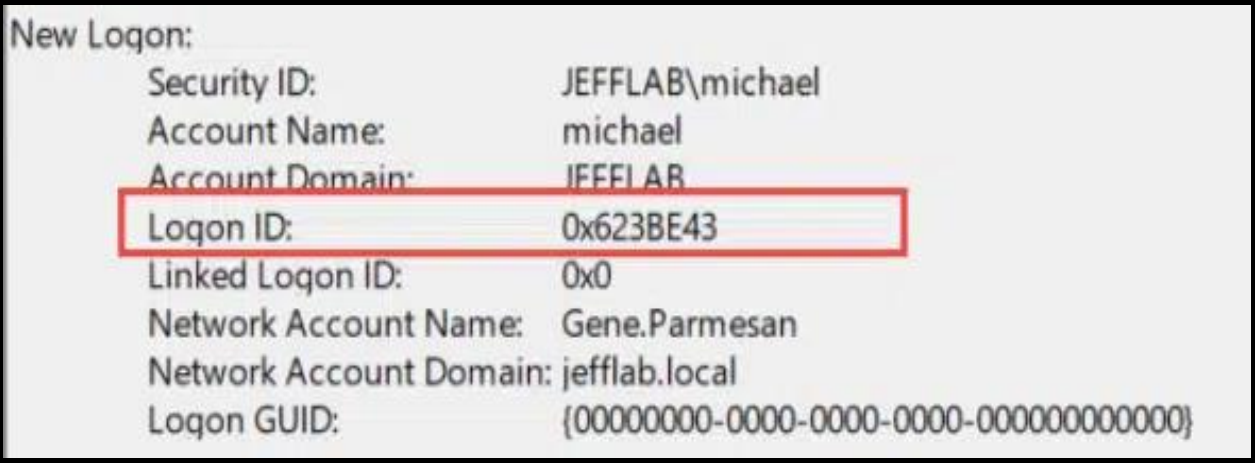
- This query searches for Windows event logs with EventCode 4624 (successful logon) and Logon_Type 3 (network logon). It also filters for authentication using the NTLM package and excludes logons from the specified domain. Finally, it groups the results by the account name and source network address.

Overpass- The - Hash

Overpass-the-hash is an attack that **enables an adversary to pass a user account's NTLM hash into the Kerberos authentication provider**. It combines pass-the-hash and pass-the-ticket techniques.

More details about pass-the-ticket and pass-the-hash

- One primary difference between pass-the-hash and pass-the-ticket is that Kerberos TGT tickets expire **(10 hours by default)**, whereas NTLM hashes change only when the user changes their password. So, a TGT ticket must be used within its lifetime, or it can be renewed for a longer period of time (7 days).



```
New Logon:
        Security ID:               JEFFLAB\michael
        Account Name:              michael
        Account Domain:            JEFFLAB
        Logon ID:                  0x623BE43
        Linked Logon ID:           0x0
        Network Account Name:      Gene.Parmesan
        Network Account Domain:    jefflab.local
        Logon GUID:                {00000000-0000-0000-0000-000000000000}
```

Splunk Query for detecting pass the hash attack:

- index=security EventCode=4624 OR EventCode=4625 | stats count by EventCode, Account_Name, Workstation_Name | where count > 10 AND EventCode=4624| table Account_Name, Workstation_Name, count

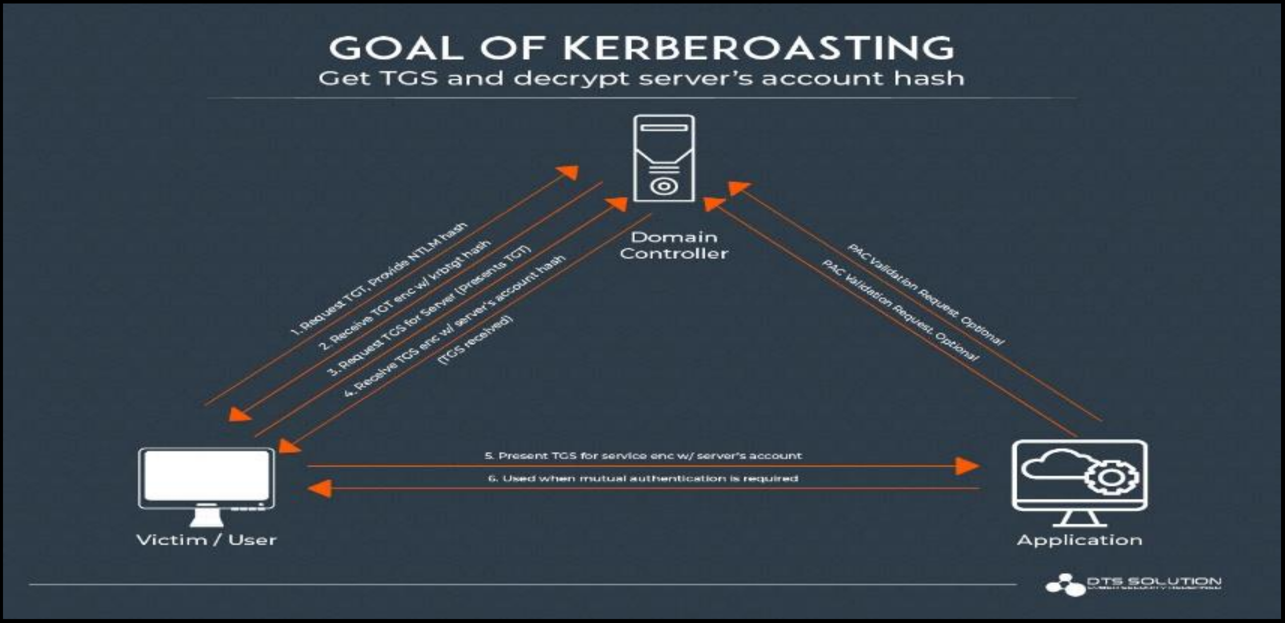
Hint:

- This query searches for Windows security events with EventCode 4624 (successful logon) or 4625 (failed logon) and then groups the results by the account name and workstation name. It then filters the results to only show events where the count is greater than 10 and the EventCode is 4624 (successful logon). This can help you identify accounts that are being used to log in from multiple workstations, which may indicate an Overpass-the-Hash attack.

Kerberoasting (Part 1)

Kerberoasting is a post-exploitation attack technique that attempts to obtain a password hash of an Active Directory account that has a Service Principal Name (“SPN”). In such an attack, an authenticated domain user requests a Kerberos ticket for an SPN.

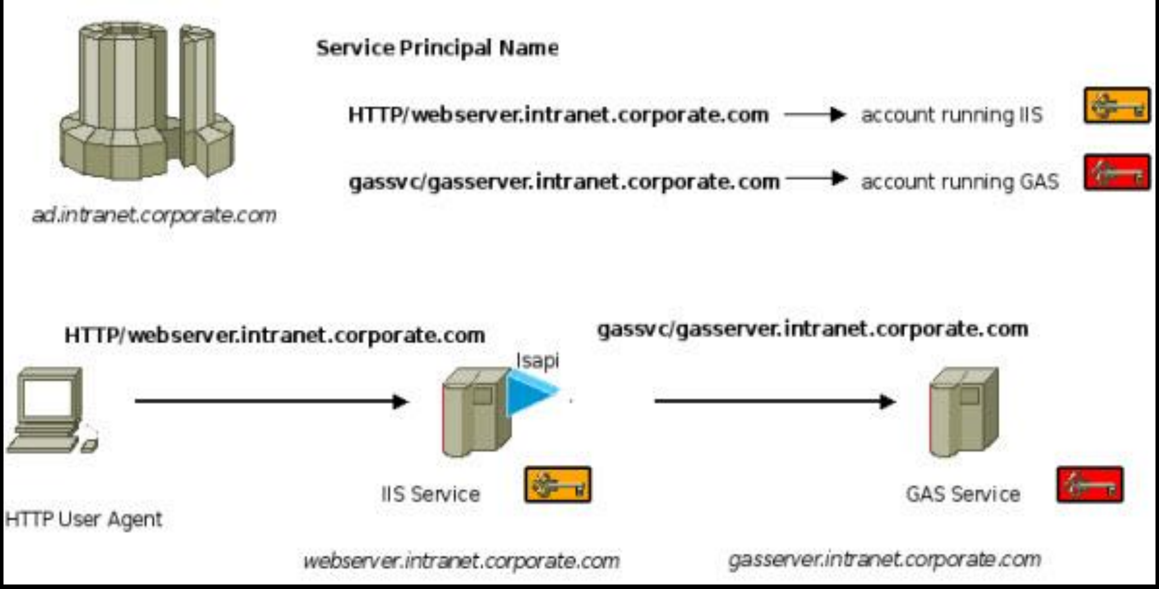
- **Kerberoasting** is a type of attack that **exploits a weakness in the Kerberos authentication protocol** used by Microsoft Active Directory.
  In a Kerberoasting attack, **an attacker targets a service account** that has **a Service Principal Name (SPN) set in Active Directory**.
  The attacker then requests a Kerberos ticket-granting ticket (TGT) for the targeted service account from the domain controller. Once the attacker has the TGT, they can use it to request a service ticket for the targeted service account's SPN.
  The service ticket contains an encrypted hash of the service account's password, which the attacker can then extract and crack offline.
  The reason this attack is possible is because service accounts with SPNs set in Active Directory have a special privilege that allows them to request Kerberos tickets on behalf of other users.
  This privilege is necessary for the service account to authenticate users who are accessing the service. However, it also means that if an attacker can obtain a TGT for the service account, they can use it to request a service ticket and extract the password hash.
  To prevent Kerberoasting attacks, it's important to regularly review and remove unnecessary SPNs from service accounts. Additionally, using strong, complex passwords for service accounts can make it more difficult for attackers to crack the password hash.


GOAL OF KERBEROASTING
Get TGS and decrypt server's account hash
Domain Controller
1. Request TGT, Provide NTLM hash
2. Receive TGT enc w/ krbtgt hash
3. Request TGS for Server (Presents TGT)
4. Receive TGS enc w/ server's account hash (TGS received)
PAC Validation Request, Optional
PAC Validation Request, Optional
5. Present TGS for service enc w/ server's account
6. Used when mutual authentication is required
Victim / User
Application
DTS SOLUTION

Kerberoasting (Part 1.5)

More details about Kerberoasting attack

- By cracking the password of a service account, the threat actors could gain access to sensitive systems and data within the network.
  Hint :
- A service principal name (SPN) is a unique identifier of a service instance. Kerberos authentication uses SPNs to associate a service instance with a service sign-in account. Doing so allows a client application to request service authentication for an account even if the client doesn't have the account name


Service Principal Name
HTTP/webserver.intranet.corporate.com
account running IIS
gassvc/gasserver.intranet.corporate.com
account running GAS
ad.intranet.corporate.com
HTTP/webserver.intranet.corporate.com
gassvc/gasserver.intranet.corporate.com
Isapi
HTTP User Agent
IIS Service
GAS Service
webserver.intranet.corporate.com
gasserver.intranet.corporate.com

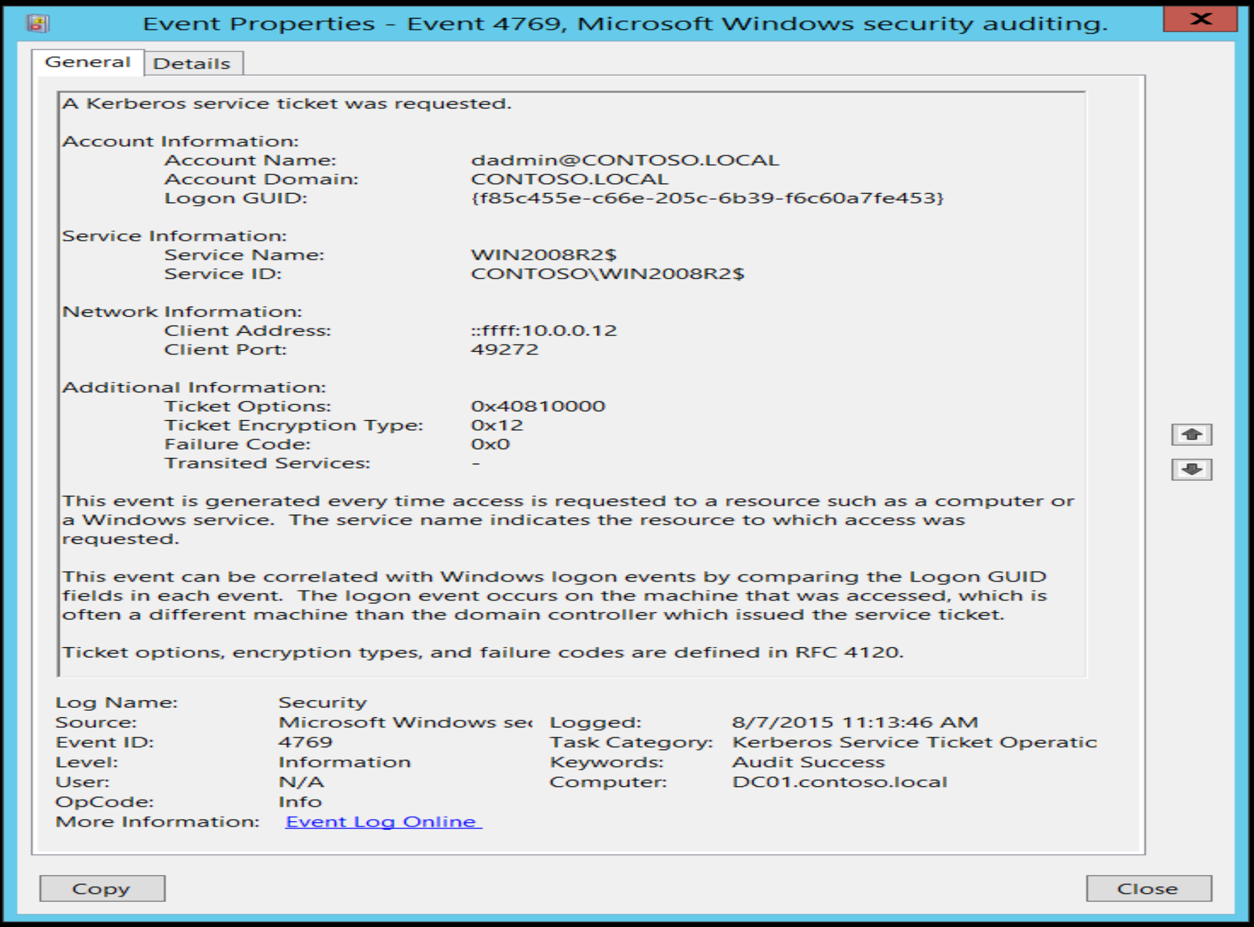
Kerberoasting (Part 2)

Splunk Query for detecting Kerberoasting attack:

- index=windows EventCode=4769 | search "Service Name"="krbtgt" | search "Ticket Encryption Type"="0x17" | stats count by Account_Name

Hint :

- This query searches for Windows security events with **EventCode 4769**, which indicates a Kerberos **service ticket request**. It then filters the results to only include requests for the krbtgt service account and tickets encrypted with RC4-HMAC encryption (0x17). Finally, it groups the results by the account name of the user requesting the ticket.
- Windows event ID **4769** is generated every time the Key Distribution Center (KDC) receives a Kerberos Ticket Granting Service (TGS) ticket request.



Event Properties - Event 4769, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A Kerberos service ticket was requested.

Account Information:
        Account Name:           dadmin@CONTOSO.LOCAL
        Account Domain:         CONTOSO.LOCAL
        Logon GUID:             {f85c455e-c66e-205c-6b39-f6c60a7fe453}

Service Information:
        Service Name:           WIN2008R2$
        Service ID:             CONTOSO\WIN2008R2$

Network Information:
        Client Address:         ::ffff:10.0.0.12
        Client Port:            49272

Additional Information:
        Ticket Options:         0x40810000
        Ticket Encryption Type: 0x12
        Failure Code:           0x0
        Transited Services:     -

This event is generated every time access is requested to a resource such as a computer or
a Windows service.  The service name indicates the resource to which access was
requested.

This event can be correlated with Windows logon events by comparing the Logon GUID
fields in each event.  The logon event occurs on the machine that was accessed, which is
often a different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.

Log Name:          Security
Source:            Microsoft Windows sec   Logged:          8/7/2015 11:13:46 AM
Event ID:          4769                    Task Category:   Kerberos Service Ticket Operatic
Level:             Information             Keywords:        Audit Success
User:              N/A                     Computer:        DC01.contoso.local
OpCode:            Info
More Information:  Event Log Online
```

Golden Ticket attack

The Golden Ticket attack is where a threat actor is granted almost **unlimited access to an organization's domain (devices, files, domain controllers, etc.)** by accessing user data stored in Active Directory.

- 1_The attacker gains access to the domain controller and extracts the domain's KRBTGT account password hash. This account is used by the Kerberos service to encrypt and sign TGTs.
- 2_The attacker uses the password hash to generate a forged TGT that has a very long lifetime (up to 10 years). This TGT is then stored in memory on the attacker's machine.
- 3_The attacker can now use the forged TGT to request service tickets for any account in the domain, including highly privileged accounts such as domain administrators.
- 4_The attacker can use the service tickets to access any resource in the domain, including sensitive data and systems.

What is the difference between pass the hash attack and golden ticket?

One primary difference between pass-the-hash and pass-the-ticket is that Kerberos TGT tickets expire (10 hours by default), whereas NTLM hashes change only when the user changes their password. So a TGT ticket must be used within its lifetime, or it can be renewed for a longer period of time (7 days).

Hint:

- It's difficult to estimate the exact probability of a Golden Ticket attack, as it depends on a variety of factors such as **the strength of the domain controller's security measures**, **the complexity of the KRBTGT account password, and the attacker's level of expertise**.
- However, it's important to note that **Golden Ticket attacks are a relatively advanced and sophisticated type of attack that require a high level of skill and knowledge to execute successfully**. Additionally, they typically require the attacker to have already gained access to the domain controller and extracted the KRBTGT account password hash, which is not a trivial task.
- That being said, it's still important to take steps to prevent Golden Ticket attacks, such as implementing **strong password policies**, **limiting access to domain controllers**, and **monitoring for suspicious activity**. By following best practices for securing domain controllers and staying vigilant for potential threats, you can help reduce the risk of a Golden Ticket attack.

Golden Ticket attack

Splunk Query for **detecting golden ticket attack**:

- index=windows EventCode=4769 "Ticket Options"="0x40810000" "Ticket Encryption Type"="0x17" | stats count by Account_Name

Hint :

This query searches for Windows security events with **EventCode 4769**, which indicates a Kerberos service ticket request. It then filters the results to only include requests with the "Ticket Options" **field set to 0x40810000**, which indicates a request for **a TGT** with a **very long lifetime (up to 10 years)**. It also filters the results to only include tickets encrypted with RC4-HMAC encryption (0x17). Finally, it groups the results by the account name of the user requesting the ticket.

This query can help identify potential Golden Ticket attacks by highlighting accounts that are requesting TGTs with a very long lifetime and encrypted with RC4-HMAC encryption, which are common characteristics of Golden Ticket attacks. However, it's important to note that this query may also capture legitimate TGT requests, so additional investigation may be necessary to confirm whether a Golden Ticket attack has occurred.

Silver Ticket

A **silver ticket** is a forged authentication ticket often created when an attacker **steals an account password**. Silver ticket attacks **use this authentication to forge ticket granting service ticket**. A Silver Ticket attack is a type of attack that targets the Kerberos authentication protocol in Windows Active Directory environments. It allows an attacker to generate a forged service ticket for a specific service, which can be used to gain access to that service and potentially escalate privileges.

- The attacker **gains access to a domain member machine** and extracts the service account password hash for the target service.
- The attacker **uses the password hash** to generate **a forged service ticket** for the target service. This ticket is then stored in memory on the attacker's machine.
- The attacker can now use **the forged service ticket to access the target service and potentially escalate privileges**.
- It's important to note that a **Silver Ticket attack requires the attacker to have already gained access to a domain member machine and extracted the service account password hash**, which is not a trivial task. Additionally, the attacker must have **knowledge of the service's SPN (Service Principal Name) and the associated service account password hash**.
- To prevent Silver Ticket attacks, it's important to follow **best practices for securing domain member machines, such as using strong passwords, limiting access to sensitive machines, and monitoring for suspicious activity**. Additionally, regularly rotating service account passwords and implementing multi-factor authentication can also help mitigate the risk of Silver Ticket attacks.

Hint :

Additionally, they typically require the attacker to have already **gained access to a domain member machine and extracted the service account password hash**, which is not a trivial task. That being said, it's still important to take steps to prevent Silver Ticket attacks, such as **implementing strong password policies**, **limiting access to sensitive machines**, and **monitoring for suspicious activity**.

Silver Ticket

Splunk Query for **detecting Silver ticket attack** :

- index=windows EventCode=4769 "Ticket Options"="0x10000" "Ticket Encryption Type"="0x17" | stats count by Account_Name

Hint :

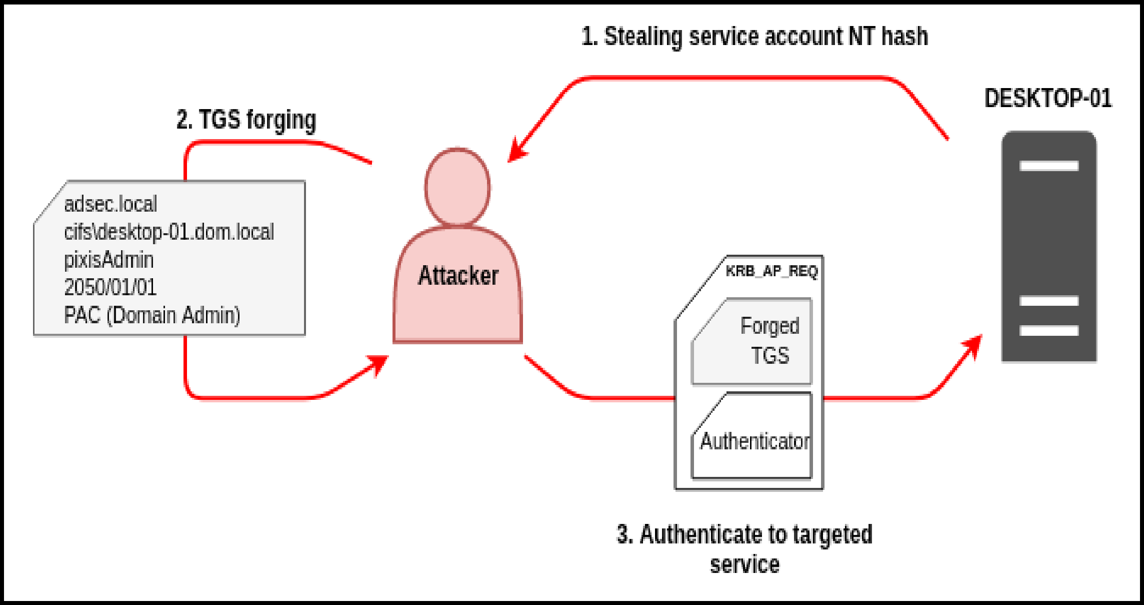
the encryption type 0x17 refers to RC4-HMAC encryption.

RC4-HMAC is a symmetric encryption algorithm that is **used to encrypt and sign Kerberos tickets**.

When a user requests a Kerberos ticket for a service, the ticket is encrypted with the service's **secret key using RC4-HMAC encryption**.

The ticket is then sent to the user, who can use it to authenticate to the service.

RC4-HMAC encryption is a relatively weak encryption algorithm that has known vulnerabilities and is no longer considered secure. As a result, it's recommended to use stronger encryption algorithms such as AES for Kerberos authentication. However, RC4-HMAC is still commonly used in many Windows Active Directory environments, which makes it a popular target for attackers.



Skeleton key attack

A Skeleton Key attack is a type of attack that **targets the Kerberos authentication protocol** in Windows Active Directory environments. It allows **an attacker to bypass authentication and gain access to any account in the domain using a single password**.

Here's how a Skeleton Key attack works:

- The attacker gains access to a domain controller and injects a malicious DLL into the LSASS process.
- The attacker uses the malicious DLL to intercept and modify Kerberos authentication requests. Specifically, the DLL modifies the authentication request to accept a specific password as valid for any account in the domain.
- The attacker can now use the password to authenticate as any user in the domain, including domain administrators.

It's important to note that a Skeleton Key attack requires the attacker to have already **gained access to a domain controller**, which is not a trivial task. Additionally, **the attacker** must have **knowledge of the domain's secret key**, which is used to encrypt and sign Kerberos tickets.

To prevent Skeleton Key attacks, it's important to follow best practices for securing domain controllers, such as limiting access to sensitive machines, implementing strong password policies, and monitoring for suspicious activity.

Splunk Query for detecting Silver ticket attack :

- index=windows EventCode=4624 Logon_Type=3 Account_Name!="*$" | stats count by Account_Name

Hint:

This query searches for Windows security events with **EventCode 4624**, which indicates a **successful logon event**. It then filters the results to only include logon events with **Logon_Type 3**, which indicates a network logon. It also filters the results to exclude logon events with account names that end with an asterisk, which is a common characteristic of Skeleton Key attacks. Finally, it groups the results by the account name of the user who logged on.

THE END