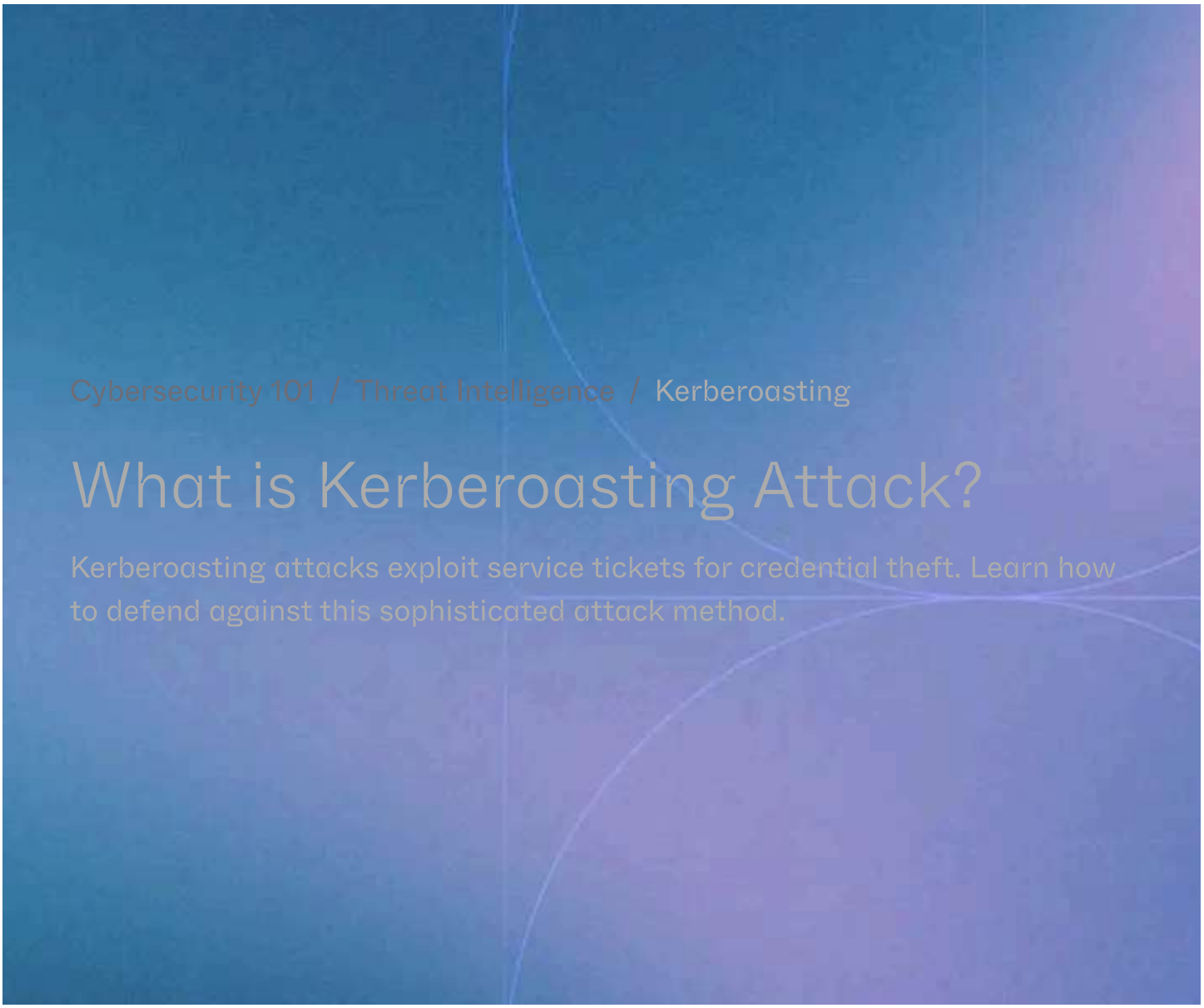
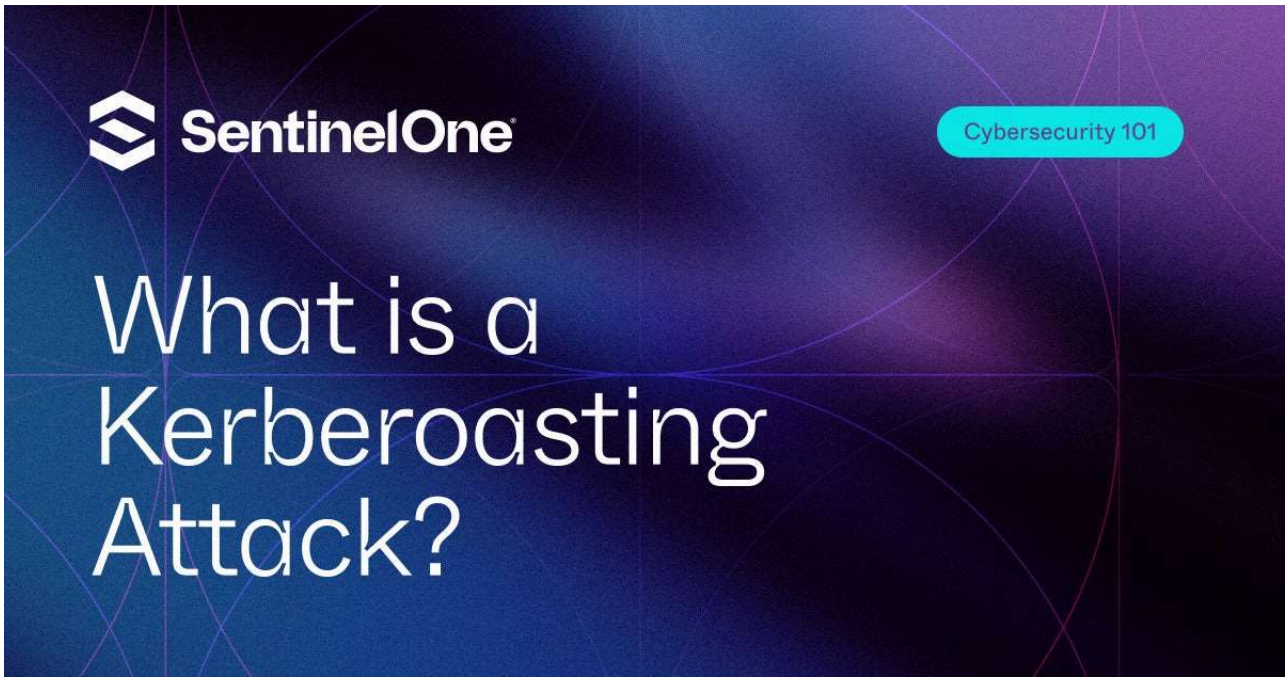



Author: SentinelOne
Updated: July 15, 2025

Kerberoasting is an attack method that targets service accounts in Active Directory. This guide explores how Kerberoasting works, its potential impact, and effective prevention strategies.

implementing strong password policies. Understanding Kerberoasting is essential for organizations to safeguard their Active Directory environments.




## What is a Kerberoasting Attack?

Kerberoasting is a cyber attack targeting the Kerberos authentication protocol, commonly used in Windows networks to securely authenticate users and devices. In a Kerberoasting attack, an attacker uses specialized tools to extract encrypted Kerberos tickets from a network and then attempts to crack the encryption to gain access to sensitive information or network resources.

Before digging deeper into Kerberoasting attacks and how they work, one should understand the architecture of service accounts.

- Service account passwords are the same length and do not expire.

of highly privileged groups like Domain Admins providing full admin rights to AD.

- Cracking the service account passwords enables attackers to exploit the Kerberos mechanism and compromise the entire AD domain.

### What is the Kerberos authentication protocol?

Kerberos is an authentication protocol commonly used in Windows networks to securely authenticate users and devices. The Kerberos protocol uses tickets to securely authenticate users and devices without transmitting plaintext passwords over the network. These tickets are encrypted using a secret key shared between the user and the authentication server. In a Kerberoasting attack, the attacker can extract these encrypted tickets from the network and then use brute-force or dictionary-based attacks to try and crack the encryption and gain access to the sensitive information or resources that the ticket grants access to.

Kerberoasting involves exploiting service tickets to steal credentials. Learn more about advanced threat detection with Singularity XDR.

### Why are Kerberoasting Attacks Prevalent?

Kerberoasting attacks are prevalent because they can be difficult to detect and prevent. The Kerberos protocol is designed to be secure and efficient, but it relies on the secrecy of the secret keys that are used to encrypt and decrypt the tickets in the authentication process. If an attacker can obtain these secret keys, they can use them to extract and decrypt the tickets, which can then be used to gain access to sensitive information or

networks. This makes Windows networks a particularly attractive target for attackers, as a successful Kerberoasting attack on an enterprise network can potentially provide the attacker with access to a large number of sensitive resources and information.

Additionally, the attack can be carried out remotely without the need for the attacker to interact directly with the authentication server or the targeted network resources. This makes it difficult for defenders to identify and stop the attack before it is successful. Overall, the combination of these factors makes Kerberoasting attacks prevalent and potentially damaging organizations relying on the Kerberos protocol for secure authentication.

## How Kerberoasting Attacks Work

### 1. Account Authentication

In a Kerberoasting attack, the attacker first obtains the necessary permissions to request service tickets from the Kerberos authentication service. This can be done by compromising the account of a legitimate user who has the appropriate permissions. If the attacker is successful to gain access to the network resource that the ticket grants access to, without needing to know the actual password of the user or device that the ticket belongs to.

The Kerberoasting technique is an effective method for extracting service account credentials from AD as a regular user without sending any packets to the target system.



### 2. Kerberos Service Ticket

tickets from the Kerberos authentication service and then uses these tickets to try to crack the passwords of the accounts associated with those tickets. In this technique, an attacker can abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force attacks.

### 3. Password Cracking

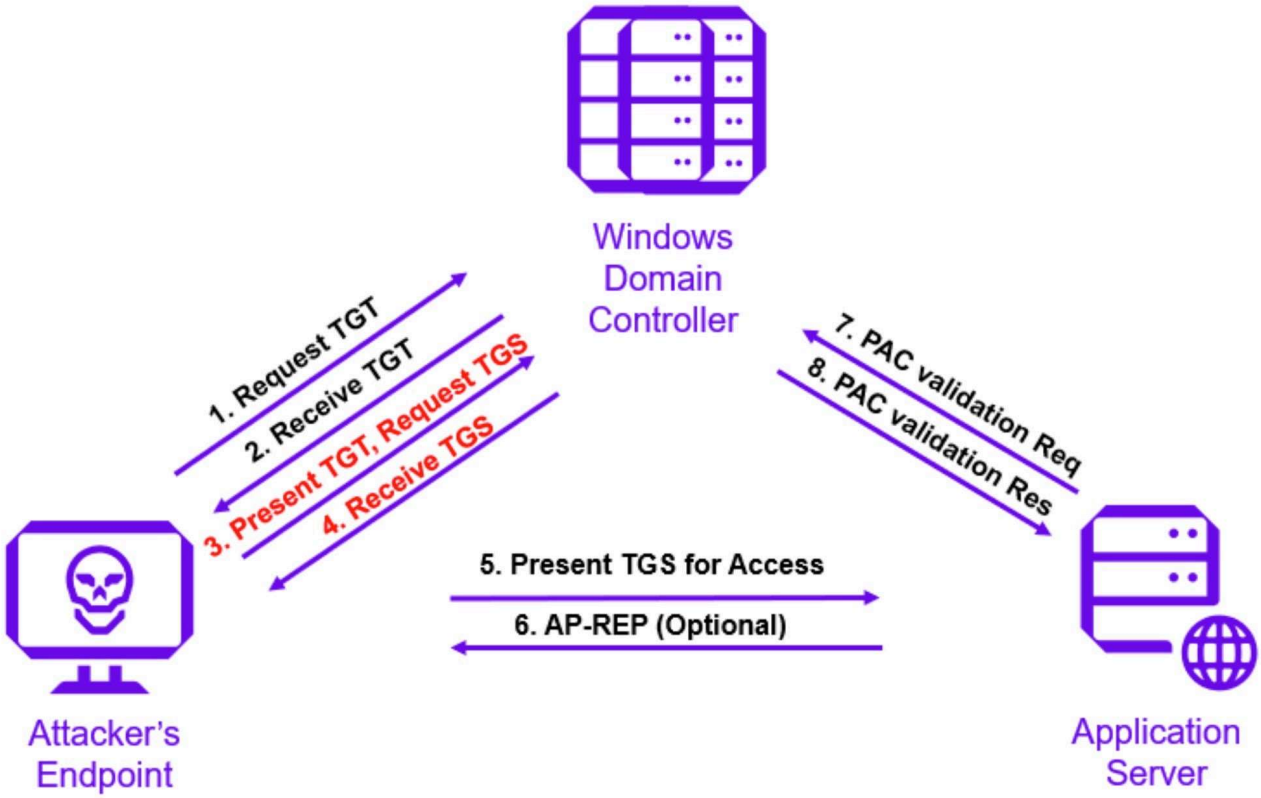
The attacker can obtain the service tickets by requesting them from the Kerberos authentication service using the accounts of legitimate users who have the appropriate permissions. Once the attacker has obtained the service tickets, they can use specialized tools to try to crack the passwords associated with those tickets. Attackers use the following process to crack a vulnerable service account password offline.

### 4. Attack Escalation

In a successful attack, the attacker can gain access to the accounts associated with the service tickets, allowing them to gain unauthorized access to sensitive information or to carry out other malicious activities. This can be a serious security threat to organizations that use the Kerberos authentication protocol. The first step is to discover Service Principal Names (SPNs). Attackers can easily find all SPNs of specific types using the Active Directory PowerShell module. The most useful SPN type that an attacker scan for is “SQL”. For example, the Get-ADObject cmdlet shown below discovers all SQL servers registered in Active Directory.

*“get-adobject -filter {serviceprincipalname -like “*sql*”} -*

authentication ticket (TGT) to request one or more Kerberos ticket-granting service (TGS) tickets for any Service Principal Name (SPN) from a domain controller (DC). Attackers take advantage of Microsoft's legacy support for Kerberos RC4 encryption (RC4_HMAC_MD5) since the NTLM password hash is used extensively with this encryption type. When requesting TGS tickets, attackers can force them to use RC4 encryption.




After identifying the target server, the attacker gets the list of SPNs associated with service accounts. They can use these service accounts to request Kerberos TGS service tickets from a domain controller (DC).

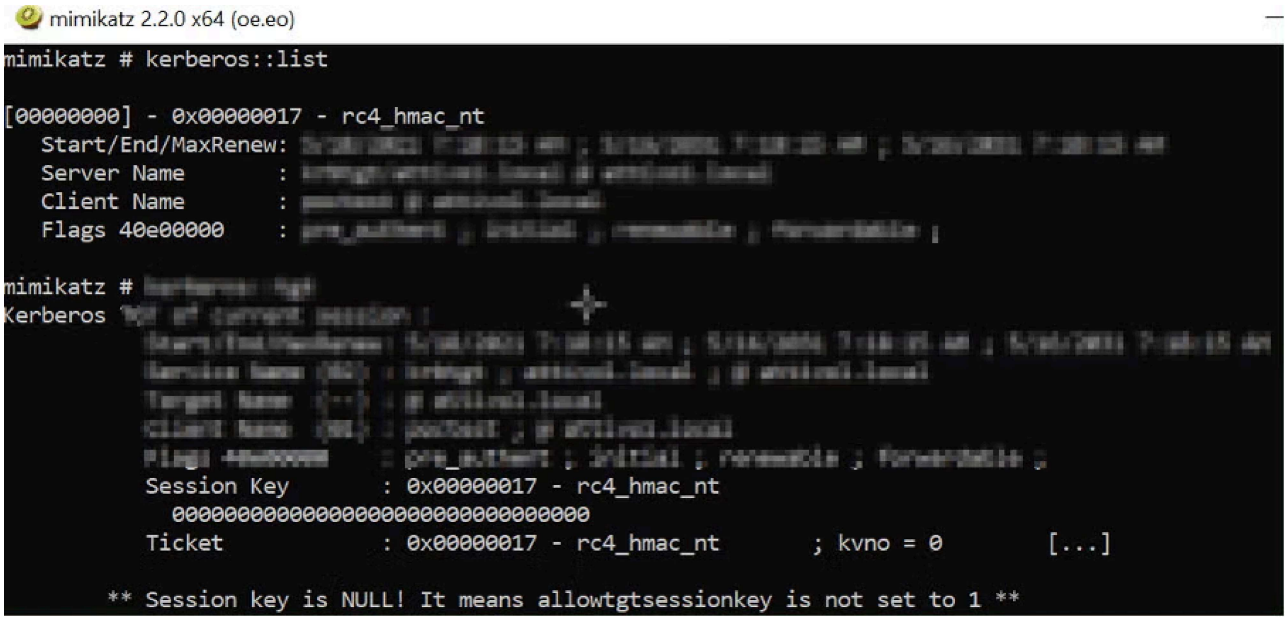
*"Add-Type -AssemblyName System.IdentityModel"*

*"New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken*



*ArgumentList*

*the RC4 encryption type.*




*Once the client receives the ticket, an attacker can export all Kerberos service tickets from the user's memory to a file without elevated rights.*

Overall, here are the steps that are commonly used in Kerberoasting attacks:

1. The attacker obtains the necessary permissions to request service tickets from the Kerberos authentication service. This can be done by compromising a legitimate user's account with the appropriate permissions.
2. The attacker uses the compromised account to request a large number of service tickets from the Kerberos authentication service.
3. The Kerberos authentication service issues the requested service tickets to the attacker.

with the service tickets.

5. Once the passwords have been cracked, the attacker gains access to the accounts associated with the service tickets.
6. The attacker can now use the compromised accounts to gain unauthorized access to sensitive information or to carry out other malicious activities.
7. The attacker continues to repeat this process, obtaining additional service tickets and cracking the passwords associated with them to gain access to more accounts.
8. The attacker can use the compromised accounts to gain further network access and carry out more advanced attacks, such as moving laterally within the network or deploying malware.

## Kerberoasting Attack Example

1. During Operation Wocao, threat actors used PowerSploit's Invoke-Kerberoast module to request encrypted service tickets and brute-force the passwords of Windows Service Accounts offline. These service tickets can then be used to authenticate as the associated service accounts on other systems within the network. The threat actors then used a brute-force attack to try and guess the passwords of these service accounts, which are often weak or shared among multiple accounts. By cracking the password of a service account, the threat actors could gain access to sensitive systems and data within the network.

Ticket Granting Service (TGS) tickets for Active Directory Service Principal Names (SPNs) to crack offline.

The Solorigate backdoor incident was a cyber attack that targeted various organizations, including government agencies and technology companies. The attackers, believed to be the APT29 group, used a sophisticated backdoor called “Solorigate” to access the victims’ networks. One of the tactics used by the attackers was Kerberoasting. By cracking the password of a service account, the attackers can gain access to sensitive systems and data within the network.

3. In another incident, the FIN7 threat group used Kerberoasting for credential access and performed lateral movement through the network.

## Kerberoasting Attack Detection & Prevention Strategies

### Identity Security

Identity Security is a new capability that detects attacks targeting identity infrastructure such as Active Directory. These solutions can detect identity settings within Active Directory that leave it vulnerable to attack, and can detect potential Kerberoasting attacks in near-real-time.

Another way to prevent a Kerberoasting attack is to use strong and unique passwords for all accounts. This makes it more difficult for attackers to crack the passwords associated with the service tickets they obtain.

which requires users to provide an additional verification form when logging into their accounts. This can help to prevent attackers from accessing accounts even if they manage to obtain the service tickets and crack the passwords.

Additionally, organizations can use tools and technologies to detect and prevent Kerberoasting attacks. For example, they can use network monitoring tools to detect unusual activity related to the Kerberos authentication protocol and use intrusion detection systems to alert them to potential attacks.

Overall, a combination of strong passwords, two-factor authentication, and security technologies can help to prevent a Kerberoasting attack and protect against unauthorized access to sensitive information.

## Threat Hunting

In the context of a Kerberoasting attack, threat hunting can be used to identify and prevent the initial compromise of a user account used to request service tickets from the Kerberos authentication service. This can help to prevent the attacker from obtaining the service tickets and launching the attack.

Additionally, threat hunting can detect unusual activity related to the Kerberos authentication protocol, such as a large number of requested service tickets or attempts to crack the passwords associated with those tickets. This can help to identify a Kerberoasting attack in progress and take appropriate action to defend against it.

Singularity™ Identity Security Posture Management solution and report assessments of potential vulnerabilities in the enterprise. The Singularity Identity Security solution detects attackers attempting Kerberos ticket enumeration and triggers events on potential Kerberoasting attacks.

## Deception Technology

Deception technology can potentially be used to help defend against Kerberoasting attacks. Deception technology, which includes decoys, lures, and bait, is designed to lure attackers and to detect and defend against attempted attacks.

In the context of a Kerberoasting attack, deception technology can be used to create fake accounts that can be used to request service tickets from the Kerberos authentication service. It can then monitor the activity associated with these fake accounts and detect any attempts to crack the passwords associated with the service tickets.

Suppose an attacker attempts to carry out a Kerberoasting attack against a decoy. In that case, it can alert the security team and provide them with information about the attack, such as the IP address of the attacker and the tools and techniques they are using. This can help the security team to defend against the attack and to prevent it from causing damage.

While deception technology can be effective in some cases, they are not a complete solution to the problem of Kerberoasting attacks. Organizations must use a combination of security measures to protect against these attacks.

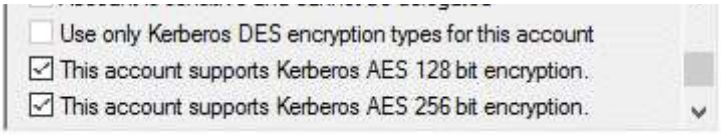
your security is robust with Singularity XDR to detect such risks early.



## How to Protect and Mitigate Kerberoasting Attacks

Organizations can implement the following best practices to prevent the entire domain from getting compromised as a mitigation strategy.

- Ensure all service accounts have long, complex passwords (greater than 25).
- Change service account passwords regularly (at least once a year).
- Use group managed service accounts (gMSAs) that provide password management and eliminate the need for an administrator to manually manage each service account's credentials.
- MITRE ATT&CK also recommends enabling AES Kerberos encryption (or another stronger encryption algorithm) rather than RC4, making it difficult for attackers to crack hashes offline. Enable the AES 128/256-bit encryption type using the checkboxes in the Account tab.




## Kerberos Security Policy Settings and Recommendations

Organizations should pay close attention to the Kerberos policy settings to reduce the risk of attackers stealing credentials. These policy settings are under *Computer ConfigurationWindows SettingsSecurity SettingsAccount PoliciesKerberos Policy*.

An attacker can explore vulnerable policy settings to exploit them. The following are Kerberos security policy settings and recommended options.

1. Enforce user logon restrictions – If this policy setting is disabled, users might get session tickets for services they do not have the right to use. The recommendation is to set this policy to “Enabled”.
2. Maximum lifetime for service ticket – This policy determines the maximum number of minutes to use a granted session ticket to access a particular service.

The recommendation is to set this policy to 600 minutes. Configuring too high a value for the “Maximum lifetime for service ticket” might allow users to access network resources outside their logon hours. Also, disabled user accounts might continue to access network services with valid service tickets issued before their accounts were disabled.

- Maximum lifetime for user ticket – This policy determines the maximum user’s ticket-granting ticket expires, the system must request a new one

hours. Configuring too high of a value might allow users to access network resources outside their logon hours. Also, disabled user accounts might continue to have access to network services with valid user tickets issued before their accounts were disabled. Configuring too low a value might affect the Key Distribution Center (KDC) performance in requesting tickets and result in a DoS attack.

- Maximum lifetime for user ticket renewal – This policy setting determines the period (in days) to renew a user's ticket-granting ticket. The recommendation is to set this policy to 7 days. Configuring too high a value might allow users to renew very old user tickets.
- Maximum tolerance for computer clock synchronization – This policy setting determines the maximum time difference (in minutes) that Kerberos V5 tolerates between the time on the client clock and the time on the domain controller that provides Kerberos authentication. The recommendation is to set this policy to a value of 5 minutes.

## How SentinelOne Singularity Identity Protects from Kerberoasting Attacks

SentinelOne Singularity Identity continuously monitors Active Directory for attacks such as Kerberoasting. The Ranger AD solution detects Kerberos ticket enumeration and triggers events on potential Kerberoasting attacks. Singularity Identity also deploys deceptive credentials, including hashes, authentication tokens, and Kerberos tickets. This allows detecting attackers using deceptive tickets and redirects them to decoys systems

# More About Kerberoasting

## Kerberoasting and Mimikatz

Mimikatz is a tool that can be used to carry out a Kerberoasting attack. Mimikatz is a utility designed to extract sensitive information from a computer system, including passwords and other authentication credentials.

In the context of a Kerberoasting attack, Mimikatz can obtain service tickets from the Kerberos authentication service and then crack the associated passwords. This allows an attacker to gain unauthorized access to the accounts associated with the service tickets.

Mimikatz is a powerful tool that can be used for both legitimate and malicious purposes. While it can be useful for security professionals to test the security of their systems, it can also be used by attackers to carry out cyber attacks. As a result, organizations must protect against its use in a Kerberoasting attack.

## Kerberoasting and Golden Tickets

Kerberoasting and Golden Tickets are both techniques that can be used to

Kerberos authentication service and then using specialized tools to crack the passwords associated with those tickets. This allows an attacker to gain unauthorized access to the accounts associated with the service tickets.

A Golden Ticket, on the other hand, is a forged Kerberos ticket that can be used to authenticate as any user on a network. This allows an attacker who has obtained a Golden Ticket to gain unauthorized access to the network and to carry out other malicious activities.

While both techniques can be used to attack the Kerberos authentication protocol, they have different mechanisms and can be used for different purposes. It is important for organizations to understand the differences between these techniques and to protect against them to maintain the security of their systems.

The golden ticket attack is similar to a Kerberoasting attack, in which an attacker extracts and decrypts existing tickets in order to gain access to network resources. However, in a golden ticket attack, the attacker creates a completely new and forged ticket, which allows them to bypass any access controls or authentication protocols that are in place.

## Kerberoasting and Silver Tickets

A Silver Ticket is a forged Kerberos ticket that allows an attacker to impersonate a legitimate service on a network. This allows the attacker to access network resources and perform other malicious activities.

While both techniques can be used to attack the Kerberos authentication



purposes. It is important for organizations to understand the differences

security of their systems.

Many organizations provision service accounts with too many permissions, often with weak passwords, making an easy way for an attacker to go from domain user to domain admin. Implementing continuous assessment and validating Kerberos configurations can avoid being vulnerable to privilege escalations and lateral movement.

## Kerberoasting Attack FAQs

**What Is a Kerberoasting Attack?**

**What Types Of Accounts Are Typically Targeted In Kerberoasting?**

**How Can Organizations Defend Against Kerberoasting Attacks?**

**What Tools Are Used To Perform Kerberoasting?**

**Can Multi-Factor Authentication (MFA) Prevent Kerberoasting?**

# Discover More About Threat Intelligence

Threat Intelligence

## How to Prevent Ransomware Attacks?

Do you want to know how to prevent ransomware attacks? Read our guide on ransomware attack prevention as we cover tips, techniques, and even how to identify and mitigate these...

Read More →

Threat Intelligence

## What Is Predictive Threat Intelligence? How AI Helps Anticipate Cyber Threats

Predictive threat intelligence can help you stay ahead of emerging threats by forecasting what's yet to come. Learn how to expect attacks before they happen.

Read More →

Threat Intelligence

## Cyber Threat Intelligence Lifecycle

Learn about the cyber threat intelligence lifecycle. Explore its different stages, how it works, and know how to implement it. See how SentinelOne can help.

Threat Intelligence

## What Is Behavioral Threat Detection & How Has AI Improved It?

Behavioral threat detection uses AI to monitor user and system patterns, flagging deviations that signature-based tools miss.

Federal Government
Finance
Healthcare
Higher Education
K-12 Education
Manufacturing
Retail
State and Local Government
Cybersecurity for SMB

Labs
Case Studies
Videos
Product Tours
Events
Cybersecurity 101
eBooks
Webinars
Whitepapers
Press
News
Ransomware Anthology

**Company**

About Us
Our Customers
Careers
Partners
Legal & Compliance
Security & Compliance
Investor Relations
S Foundation
S Ventures