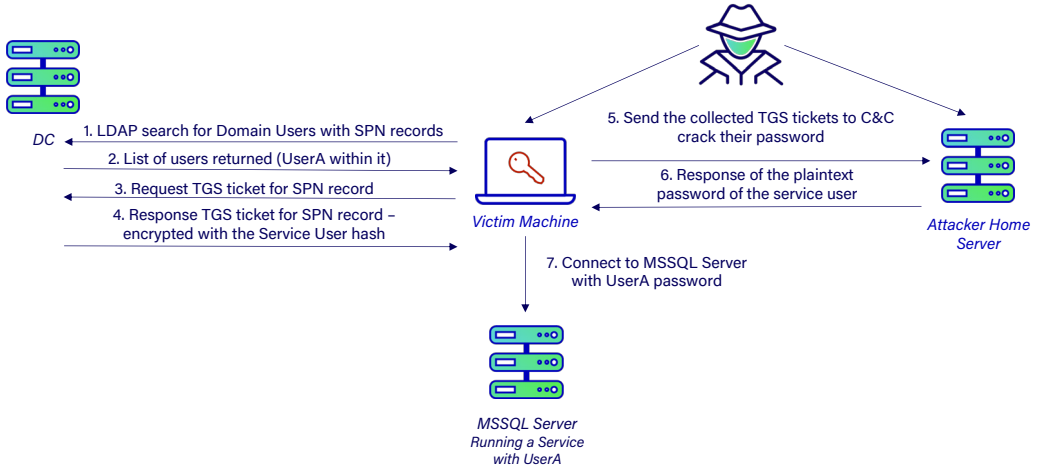
illusive

Technical Brief on Kerberoasting Attacks and How to Protect Yourself

How the Attack Works

Kerberoasting is an attack technique where an attacker requests a Kerberos service ticket for any service, captures the ticket granting service (TGS) ticket from memory, and then attempts to crack the service credential offline using a password-cracking tool such as John the Ripper, Hashcat, etc. When successfully executed, the attacker now has the password for the targeted service account. What makes this technique effective is that the passwords for service accounts are set by humans, which typically means that they are 10-14 characters long and often weak. This means that they can be cracked in a short amount of time. Additionally, passwords for service accounts often are not changed very often, which provides plenty of time for the password cracking to succeed, even with a longer, more complex password.

Kerberoasting Attacks Step by Step



How Organizations Can Protect Themselves from Kerberoasting Attacks

Because Kerberoasting utilizes standard Windows functionality to obtain the TGS ticket and then cracks the service credential offline, it is difficult to detect. Additionally, many service accounts have elevated privileges and, in some cases, are members of the Domain Admin and other highly privileged groups.

We recommend the following actions to detect Kerberoasting attempts, reduce their chances of success and minimize the impact of damaging attacks:

1. Create a list of users with a Service Principle Name (SPN) that are potential targets of Kerberoasting. There are various tools and methods available to query all SPNs in your network:
   - GetUserSPNs.ps1
   - Microsoft's Built-In DC Utility

2. Monitor the relevant Windows Event ID in your SIEM. The request for a Kerberos TGS ticket is an essential element of Kerberoasting. Domain Controllers can log TGS requests by configuring "Audit Kerberos Service Ticket Operations" under Account Logon to log successful Kerberos TGS ticket requests. Enabling this audit category will result in two interesting event IDs being logged:
   - 4769: A Kerberos service ticket (TGS) was requested
   - 4770: A Kerberos service ticket was renewed

These event IDs can generate a lot of events in an environment, which is why logging of them is typically disabled. To reduce the number of events being logged, employ event filtering to reduce the number of events being logged:

- Filter on Audit Success
- Look for TGS tickets with RC4 / DES encryption
  - Ticket Encryption: 0x17 (Ticket Encryption Type - RC4).
  - Ticket Encryption: 0x1 OR 0x2 OR 0x3 (Ticket Encryption Type - DES).
- Filter out 4769 events:
  - From service accounts - Optional.
  - For service names with a "$" which are typically for computer accounts (or trusts or Managed Service Accounts, all accounts where Windows automatically generates a long, complex password).

Once the data is accessible in the SIEM, there are several activities which indicate possible Kerberoasting activity:

- A single user requesting RC4 / DES encrypted TGS tickets for several services.
- Multiple RC4/DES encrypted TGS requests over time for multiple service principal names.

3. Ensure that service accounts have long, complex passwords and configure them to expire frequently. Successful Kerberoasting attacks rely on the attacker being able to crack the service account password before it changes. Long (25 or more characters), complex passwords take much longer to crack. If the password changes before the attacker can crack the password, then the attack will be unsuccessful.

4. Create "decoy" service accounts with fake SPNs. Since attackers are searching the Domain Controller for accounts with SPNs, this can be effective in detecting Kerberoasting attempts. As these service accounts are not associated with a real service, there is no legitimate reason for a TGS to be requested for any of these decoy service accounts. Configure your SIEM to alert on a TGS request for any of the decoy service accounts.

Combined with Illusive's deception-based Attack Detection System, Illusive is the most effective and efficient platform for quickly detecting and stopping malicious lateral movement before attackers reach business-critical assets.