Extracting Service Account Passwords with Kerberoasting

blog.netwrix.com/2022/08/31/extracting-service-account-passwords-with-kerberoasting

Jeff Warren

In our LDAP reconnaissance post, we explored how an attacker can perform reconnaissance to discover service accounts to target in a Windows Active Directory (AD) domain. Now let's explore one way an attacker can use to compromise those accounts and exploit their privileges: Kerberoasting. This technique is especially scary because it requires no administrator privileges in the domain, is very easy to perform and is virtually undetectable.

Handpicked related content:

[On-demand Webinar] 4 Service Account Attacks and How to Protect Against Them

Kerberoasting: Overview

Kerberoasting is an attack that abuses a feature of the Kerberos protocol to harvest password hashes for Active Directory user accounts: Any authenticated domain user can request service tickets for an account by specifying its Service Principal Name (SPN), and the ticket granting service (TGS) on the domain controller will return a ticket that is encrypted using the NTLM hash of the account's password.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

Therefore, once an adversary has discovered service account SPNs using a tactic like LDAP reconnaissance, they can collect tickets for all those accounts. By taking that data offline, they can perform a brute force attack to crack each service account's plaintext password — with zero risk of detection or account lockouts.

It takes just minutes for an attacker to gain access to a domain, collect tickets and begin the cracking process. From there, it's just a waiting game until they have compromised one or more service accounts, which they can use to steal or encrypt sensitive data or do other damage.

Adversaries focus on service accounts for several reasons. First, these accounts often have far more extensive privileges than other AD user accounts, so compromising them grants the attacker more access. In addition, service account passwords rarely change, so the adversary is likely to retain access for a long time. To understand the types of access that can be garnered using Kerberoasting, look at the list of Active Directory SPNs maintained by Sean Metcalf.

Kerberoasting: How it works

Step 1. Obtain the SPNs of service accounts.

. There are many ways to get these SPNs, including:

- PowerShell queries and LDAP reconnaissance
- Active Directory Module for PowerShell
- GetUserSPNs script in the Kerberoast toolkit
- Get-NetUser command of PowerSploit

Step 2. Request service tickets for service account SPNs.

Simply execute a couple of lines of PowerShell, and a service ticket will be returned and stored in memory to your system.

```
Add-Type –AssemblyName System.IdentityModel
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken –ArgumentList ‘MSSQLSvc/jefflab-
sql02.jefflab.local:1433’
```

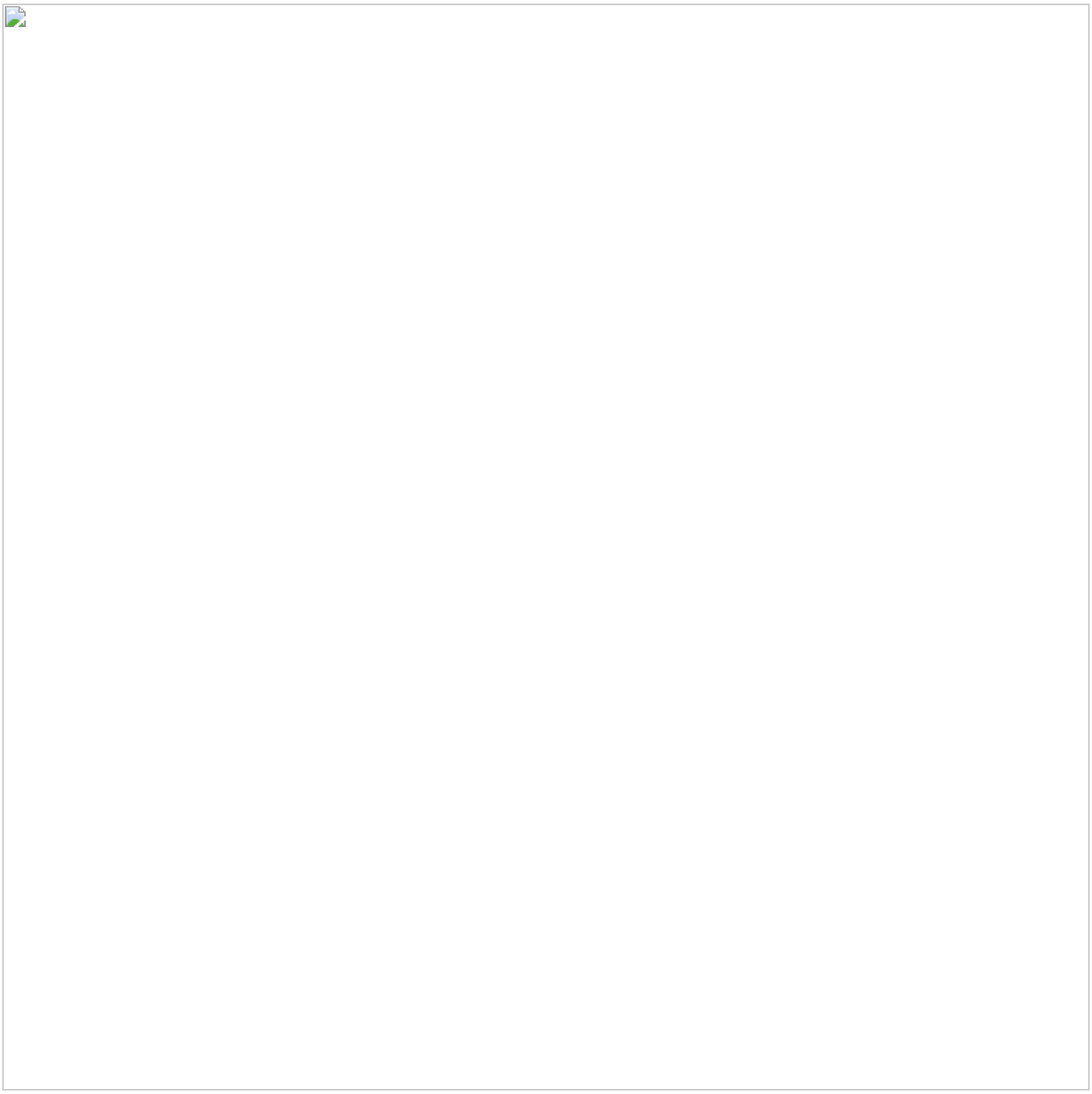
Step 3. Extract service tickets using Mimikatz.

Mimikatz will extract local tickets and save them to disk for offline cracking. Simply install Mimikatz and issue a single command:

Service Accounts_extra ticket

Step 4. Crack the tickets.

Kerberos tickets are encrypted with the password of the service account associated with the SPN specified in the ticket request. The Kerberoasting tools provide a Python script to crack tickets and provide their cleartext passwords by running a dictionary of password hashes against them. It can take some configuration to make sure you have the required environment to run the script, but this blog covers those details.



Alternatively, you can gather Kerberos tickets using the GetUserSPNs script and crack them with the Hashcat password recovery tool.

Protecting against Kerberoasting attacks

The primary mitigation for Kerberoasting attacks is to ensure that all service accounts use long, complex passwords that are harder to crack, and rotate them regularly to minimize the time the account could be used by an adversary who manages to crack a password. Using group managed service accounts is a best practice for assigning random, complex passwords that can be rotated automatically.

Since adversaries crack the tickets offline, the process does not result in any network traffic, making that part of the attack undetectable. But you can spot the earlier steps by monitoring Active Directory with a solid security solution. In particular, service accounts are normally used from the same systems in the same ways, so watch for detect anomalous authentication requests. In addition, monitor for spikes in service ticket requests.

Finally, security specialists also recommend disabling RC4-based encryption. Otherwise, even if a user account supports AES encryption, an attacker can request an RC4-encrypted ticket, which is easier to crack than one created using AES encryption.

Jeff Warren