

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://p16.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation

1 capture
29 Mar 2020

FEB

MAR

APR

29

2020

2019

2021

⌂

?

✕

f

t

About this capture

Resources | Careers | Contact us

Return to praetorian.com



Home / Security Blog / How to use Kerberoasting - T1208 for Privilege Escalation

Redirecting in 5 seconds...

You will be redirected to this article on our new blog shortly. If you are not automatically forwarded, you may access this article here:

<http://www.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation?edition=2019>

How to use Kerberoasting - T1208 for Privilege Escalation

Posted by Josh Abraham

What is MITRE ATT&CK?

For anyone that isn’t familiar with MITRE ATTACK Framework - feel free to review [this summary](#).

Introduction

Kerberoasting is a very useful attack for escalation of privileges. What is a service principal name? A service principal name is a Microsoft method to tie a domain account (user or computer) to a network service. This occurs often when installing new services such as MSSQL. During installation, the SPNs is created based on the account used. All SPNs contain a host, service and account-name. These can be also be created manually using tools like PowerShell or SetSPNs.exe which is included in the latest versions of Windows by default.

The technique requires an adversary has already gained remote access to a victim system that is connected to a domain. The attacker can retrieve Kerberos tickets from the domain controller for service accounts that are set up as service principal names. Unfortunately, for defenders, this is functionality that is by design and there isn’t a way to disable this capability.

In our experience, Kerberoasting is an attack that is similar to others in that defenders need to fully under it to be able to properly migrate the risks. It’s our goal that through pushing this content into the MITRE ATT&CK framework we have increased the awareness of this TTP so that organizations can be better protected in the future.

Attack Demonstration

Public source-code for conducting a Kerberoasting attack has been available for several years. One example is included in the Empire framework as a PowerShell module. The command Invoke-Kerberoast can be used to generate the hashes from the SPNs within the domain which can be cracked offline using a tool such as John the Ripper or Hashcat. It’s common that attackers will leverage GPUs locally or in the cloud to increase cracking speeds.

The requirements for the attack:

- Ability to query the domain controller as a normal user. This can be a system on the domain already or a non-domain joined access that can communicate with the DC.
- Admin access to ZERO things!

When performing password cracking it’s also common to utilize password cracking rules that modify wordlists using statistical models.

The dangerous part about this attack is that it doesn’t require any admin privileges to request Kerboast tickets. Anyone can request them. After the domain controller returns this information the adversary has unlimited time to crack the credentials.

Create a new SPN and assign it an account that already exists.

○

We can request the SPN via the following command.

○

To export the SPNs would require Mimikatz so instead, we will use a PowerShell script. Empire includes a script known as Invoke-Kerberoast.ps1. It can be found [here](#)

Solve problems.
Get noticed.
Get hired.



Try our Puzzles

Test your problem solving skills. Do you have what it takes?

Try puzzles »



Connect with us on LinkedIn



Follow us on Facebook

Download the file and save it locally for now.

Lead levels: Kerberoasting

[1 capture](#)
29 Mar 2020

1/2

To crack the credentials we
[https://github.com/hashcat](https://github.com/hashcat/hashcat)

This page has moved...

You will be redirected to this article on our new blog shortly. If you are not automatically forwarded, you may access this article here:

<http://www.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation?edition=2019>

Redirecting in 5 seconds...

FEB2019

MAR292020

APR2021

👤

?

✕

f

t

About this capture