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...

How to use Kerberoasting - T1208 for Privilege Escalation

Posted by Josh Abraham

Next entry:

Signed Scripts Proxy Execution - T1216

Previous entry:

Summary of April MITRE ATT&CK RELEASE

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 organ

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...

Public so
years. On
command
domain w
common t

The requi
Ability to
already o
Admin ac

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

Download the file and save it locally for now.

Load Invoke-Kerberoast and execute it while saving the output to `kerb.txt`

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

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...

Try o

Test yo