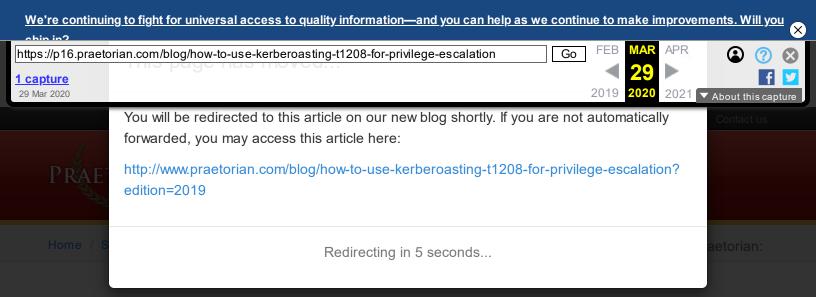
https://web.archive.org/web/20200329173843/https://p16.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation





#### . .

Signed Scripts
Proxy Execution -

#### Previous entry:

Summary of April MITRE ATT&CK RELEASE

# 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

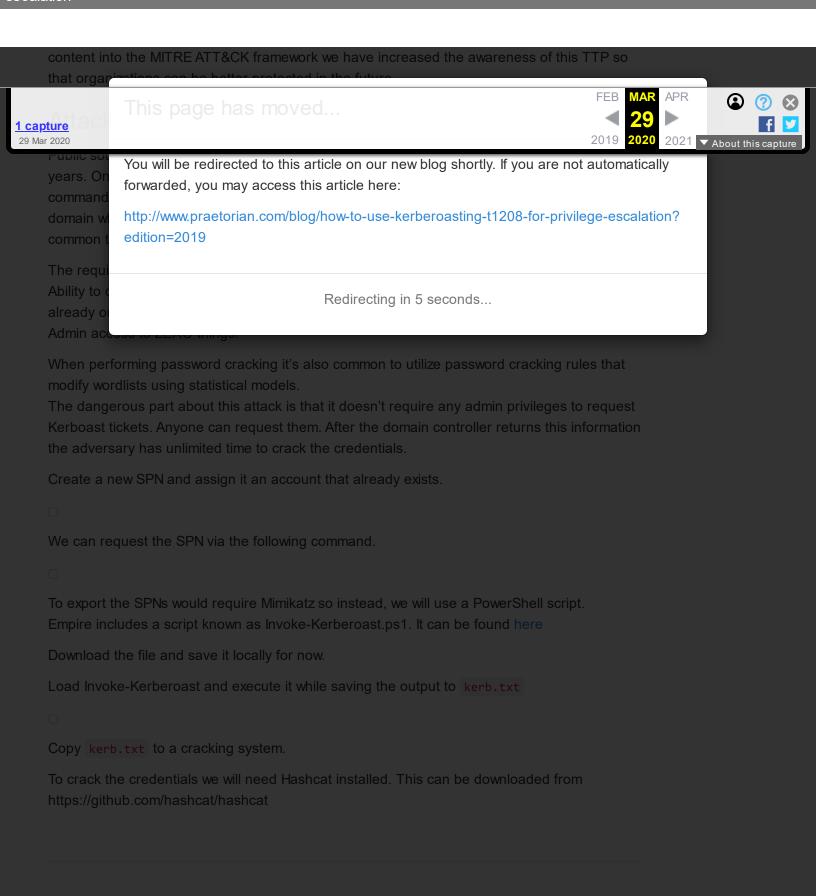
Kerberoasting is a very useful attack for escalation of privileges. What is a service principal name? A service principal name is a Microsoft method to tie a domain account (user or computer) to a network service. This occurs often when installing new services such as MSSQL. During installation, the 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

### How to use Kerberoasting - T1208 for Privilege Escalation - 31/10/2024 19:17

https://web.archive.org/web/20200329173843/https://p16.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation



#### How to use Kerberoasting - T1208 for Privilege Escalation - 31/10/2024 19:17

https://web.archive.org/web/20200329173843/https://p16.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilegeescalation

