Invoke-Kerberoast - PowerSploit

Archived: 2026-04-05 18:11:19 UTC

SYNOPSIS

Requests service tickets for kerberoast-able accounts and returns extracted ticket hashes.

Author: Will Schroeder (@harmj0y), @machosec

Required Dependencies: Invoke-UserImpersonation, Invoke-RevertToSelf, Get-DomainUser, Get-DomainSPNTicket

SYNTAX

```
Invoke-Kerberoast [[-Identity] <String[]>] [-Domain <String>] [-LDAPFilter <String>] [-SearchBase <String>]
[-Server <String>] [-SearchScope <String>] [-ResultPageSize <Int32>] [-ServerTimeLimit <Int32>] [-Tombstone]
[-OutputFormat <String>] [-Credential <PSCredential>]
```

DESCRIPTION

Uses Get-DomainUser to query for user accounts with non-null service principle names (SPNs) and uses Get-SPNTicket to request/extract the crackable ticket information. The ticket format can be specified with -OutputFormat \<John/Hashcat>.

EXAMPLES

---------- EXAMPLE 1 ----------

```
Invoke-Kerberoast | fl
```

---------- EXAMPLE 2 ----------

```
Invoke-Kerberoast -Domain dev.testlab.local | fl
```

---------- EXAMPLE 3 ----------

```
$SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -orce
```

$Cred = New-Object System.Management.Automation.PSCredential('TESTLB\dfm.a', $SecPassword) Invoke-Kerberoast -Credential $Cred -Verbose | fl

PARAMETERS

-Identity

A SamAccountName (e.g. harmj0y), DistinguishedName (e.g. CN=harmj0y,CN=Users,DC=testlab,DC=local), SID (e.g. S-1-5-21-890171859-3433809279-3366196753-1108), or GUID (e.g. 4c435dd7-dc58-4b14-9a5e-1fdb0e80d201). Wildcards accepted.

```
 Type: String[]
Parameter Sets: (All)
Aliases: DistinguishedName, SamAccountName, Name, MemberDistinguishedName, MemberName

Required: False
Position: 1
Default value: None
Accept pipeline input: True (ByPropertyName, ByValue)
Accept wildcard characters: False
```

-Domain

Specifies the domain to use for the query, defaults to the current domain.

```
 Type: String
Parameter Sets: (All)
Aliases:

Required: False
Position: Named
Default value: None
Accept pipeline input: False
Accept wildcard characters: False
```

-LDAPFilter

Specifies an LDAP query string that is used to filter Active Directory objects.

```
 Type: String
Parameter Sets: (All)
Aliases: Filter

Required: False
Position: Named
```

```
Default value: None
Accept pipeline input: False
Accept wildcard characters: False
```

-SearchBase

The LDAP source to search through, e.g. "LDAP://OU=secret,DC=testlab,DC=local" Useful for OU queries.

```
 Type: String
Parameter Sets: (All)
Aliases: ADSPath

Required: False
Position: Named
Default value: None
Accept pipeline input: False
Accept wildcard characters: False
```

-Server

Specifies an Active Directory server (domain controller) to bind to.

```
 Type: String
Parameter Sets: (All)
Aliases: DomainController

Required: False
Position: Named
Default value: None
Accept pipeline input: False
Accept wildcard characters: False
```

-SearchScope

Specifies the scope to search under, Base/OneLevel/Subtree (default of Subtree).

```
 Type: String
Parameter Sets: (All)
Aliases:

Required: False
Position: Named
Default value: Subtree
```

```
Accept pipeline input: False
Accept wildcard characters: False
```

-ResultPageSize

Specifies the PageSize to set for the LDAP searcher object.

```
 Type: Int32
Parameter Sets: (All)
Aliases:

Required: False
Position: Named
Default value: 200
Accept pipeline input: False
Accept wildcard characters: False
```

-ServerTimeLimit

Specifies the maximum amount of time the server spends searching. Default of 120 seconds.

```
 Type: Int32
Parameter Sets: (All)
Aliases:

Required: False
Position: Named
Default value: 0
Accept pipeline input: False
Accept wildcard characters: False
```

-Tombstone

Switch. Specifies that the searcher should also return deleted/tombstoned objects.

```
 Type: SwitchParameter
Parameter Sets: (All)
Aliases:

Required: False
Position: Named
Default value: False
Accept pipeline input: False
Accept wildcard characters: False
```

-OutputFormat

Either 'John' for John the Ripper style hash formatting, or 'Hashcat' for Hashcat format. Defaults to 'John'.

```
 Type: String
Parameter Sets: (All)
Aliases: Format

Required: False
Position: Named
Default value: John
Accept pipeline input: False
Accept wildcard characters: False
```

-Credential

A [Management.Automation.PSCredential] object of alternate credentials for connection to the target domain.

```
 Type: PSCredential
Parameter Sets: (All)
Aliases:

Required: False
Position: Named
Default value: [Management.Automation.PSCredential]::Empty
Accept pipeline input: False
Accept wildcard characters: False
```

INPUTS

OUTPUTS

PowerView.SPNTicket

Outputs a custom object containing the SamAccountName, ServicePrincipalName, and encrypted ticket section.

NOTES
