

SPN Discovery

Services that support Kerberos authentication require to have a Service Principal Name (SPN) associated to point users to the appropriate resource for connection. Discovery of SPNs inside an internal network is performed via LDAP queries and can assist red teams to identify hosts that are running important services such as Terminal, Exchange, Microsoft SQL etc. and being stealthy at the same time. Furthermore identification of SPNs is the first step to the kerberoasting attack.

[Tim Medin](#) explained SPN really well in his talk [Attacking Kerberos: Kicking the Guard Dog of Hades](#) with practical examples. [Sean Metcalf](#) also provided some good resources regarding SPN including an extensive list of [Active Directory Service Principal Names](#) which can be found at the end of the article.

SetSPN

[SetSPN](#) is a native windows binary which can be used to retrieve the mapping between user accounts and services. This utility can add, delete or view SPN registrations.

```
1 setspn -T pentestlab -Q */*
```

```
meterpreter > powershell_shell
PS > setspn -T pentestlab -Q */*
Checking domain DC=pentestlab,DC=local
CN=WIN-PTELU2U07KG,OU=Domain Controllers,DC=pentestlab,DC=local
TERMSRV/WIN-PTELU2U07KG
TERMSRV/WIN-PTELU2U07KG.pentestlab.local
GC/WIN-PTELU2U07KG.pentestlab.local/pentestlab.local
MSSQLSvc/WIN-PTELU2U07KG.pentestlab.local:1433
MSSQLSvc/WIN-PTELU2U07KG.pentestlab.local
MSSQLSvc/WIN-PTELU2U07KG.pentestlab.local:16140
MSSQLSvc/WIN-PTELU2U07KG.pentestlab.local:SQLEXPRESS
IMAP/WIN-PTELU2U07KG
IMAP/WIN-PTELU2U07KG.pentestlab.local
IMAP4/WIN-PTELU2U07KG
IMAP4/WIN-PTELU2U07KG.pentestlab.local
POP/WIN-PTELU2U07KG
POP/WIN-PTELU2U07KG.pentestlab.local
POP3/WIN-PTELU2U07KG
POP3/WIN-PTELU2U07KG.pentestlab.local
exchangeRFR/WIN-PTELU2U07KG
exchangeRFR/WIN-PTELU2U07KG.pentestlab.local
exchangeMDB/WIN-PTELU2U07KG
exchangeMDB/WIN-PTELU2U07KG.pentestlab.local
```

setspn – Service Discovery

Services that are bind to a domain user account and not a computer account are more likely configured with a weak password since the user has selected the password. Therefore services which they have their **Canonical-Name** to **Users** should be targeted for Kerberoasting. From the list of SPNs below the service **PENTESTLAB_001** is associated with a user account.

```
CN=WIN-2NE38K15TGH,CN=Computers,DC=pentestlab,DC=local
  WSMAN/WIN-2NE38K15TGH
  WSMAN/WIN-2NE38K15TGH.pentestlab.local
  E3514235-4B06-11D1-AB04-00C04FC2DCD2/9b22dfb4-d71f-4a53-b856-563c3fc978b
5/pentestlab.local
  E3514235-4B06-11D1-AB04-00C04FC2DCD2/8056fa52-ce80-4826-bcb8-af7576bd447
5/pentestlab.local
  E3514235-4B06-11D1-AB04-00C04FC2DCD2/a25a50ca-02b7-4be8-bc6b-e7590895fc7
0/pentestlab.local
  E3514235-4B06-11D1-AB04-00C04FC2DCD2/2224aa3a-63d1-493d-a57a-e8d84d0ebe5
7/pentestlab.local
  TERMSRV/WIN-2NE38K15TGH
  TERMSRV/WIN-2NE38K15TGH.pentestlab.local
  RestrictedKrbHost/WIN-2NE38K15TGH
  HOST/WIN-2NE38K15TGH
  RestrictedKrbHost/WIN-2NE38K15TGH.pentestlab.local
  HOST/WIN-2NE38K15TGH.pentestlab.local
CN=PENTESTLAB Admin 001,CN=Users,DC=pentestlab,DC=local
  PENTESTLAB_001/WIN-PTELU2U07KG.PENTESTLAB.LOCAL:80

Existing SPN found!
```

SetSPN – SPN Records

GetUserSPNs

Tim Medin developed a PowerShell script which is part of kerberoast toolkit and can query the active directory to discover only services that are associated with a user account as a more focused approach compared to SetSPN.

```
1 powershell_import /root/Desktop/GetUserSPNs.ps1
```

```
meterpreter > powershell_import /root/Desktop/GetUserSPNs.ps1
[+] File successfully imported. Result:

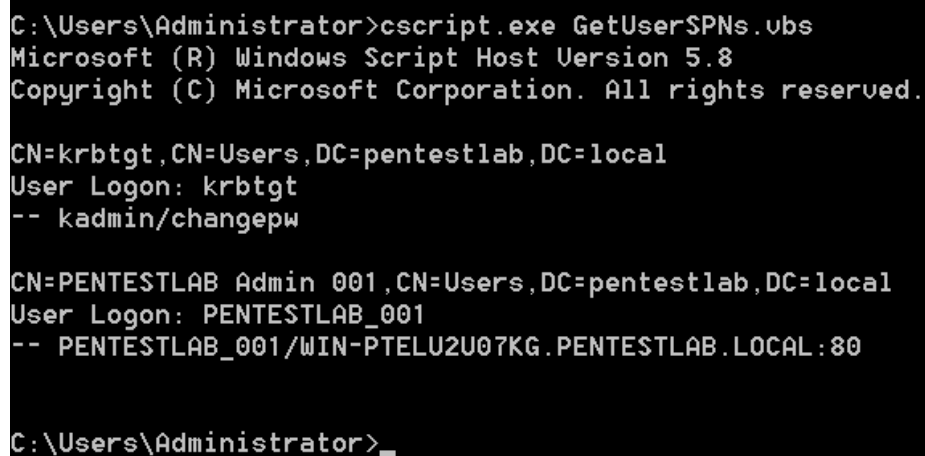
ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=pen
testlab,DC=local
PasswordLastSet      : 3/18/2018 12:53:47 AM

ServicePrincipalName : PENTESTLAB_001/WIN-PTELU2U07KG.PENTESTLAB.LOCAL:80
Name                 : PENTESTLAB Admin 001
SAMAccountName       : PENTESTLAB_001
MemberOf             :
PasswordLastSet      : 5/26/2018 12:44:35 PM
```

GetUserSPNs – PowerShell Script

There is also a VBS script which is part of the same toolkit and can provide the same information. The script can be executed from the windows command prompt by using the native Windows binary **cscript**.

```
1 cscript.exe GetUserSPNs.vbs
```



```
C:\Users\Administrator>cscript.exe GetUserSPNs.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

CN=krbtgt,CN=Users,DC=pentestlab,DC=local
User Logon: krbtgt
-- kadmin/changepw

CN=PENTESTLAB Admin 001,CN=Users,DC=pentestlab,DC=local
User Logon: PENTESTLAB_001
-- PENTESTLAB_001/WIN-PTELU2U07KG.PENTESTLAB.LOCAL:80

C:\Users\Administrator>_
```

GetUserSPNs – VBS Script

PowerShell AD Recon

Similarly to what [Tim Medin](#) developed [Sean Metcalf](#) wrote various PowerShell scripts to perform recon against Kerberos. These scripts are part of [PowerShell AD Recon](#) repository and can query the Active Directory for interesting services such as Exchange, Microsoft SQL, Terminal etc. Sean bind each script to a specific service depending on what SPN the red teamer would like to discover. The following script will identify all the Microsoft SQL instances on the network.

```
1 powershell_import /root/Discover-PSMSSQLServers.ps1
2 powershell_execute Discover-PSMSSQLServers
```

```

meterpreter > powershell_import /root/Discover-PSMSSQLServers.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute Discover-PSMSSQLServers
[+] Command execution completed:
Processing 1 (user and computer) accounts with MS SQL SPNs discovered in AD Forest DC=pentestlab,DC=local

Domain          : pentestlab.local
ServerName      : WIN-PTELU2U07KG.pentestlab.local
Port           : 1433
Instance       :
ServiceAccountDN :
OperatingSystem : {Windows Server 2012 R2 Standard Evaluation}
OSServicePack   :
LastBootup     : 5/25/2018 12:43:03 PM
OSVersion      : {6.3 (9600)}
Description     :

```

PowerShell AD Recon – MSSQL Servers Discovery

Microsoft Exchange servers can be also discovered with the **PSMSEExchangeServers** script.

- 1 `powershell_import /root/Discover-PSMSEExchangeServers.ps1`
- 2 `powershell_execute Discover-PSMSEExchangeServers`

```

meterpreter > powershell_import /root/Discover-PSMSEExchangeServers.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute Discover-PSMSEExchangeServers
[+] Command execution completed:
Processing 1 (user and computer) accounts with MS Exchange SPNs discovered in AD Forest DC=pentestlab,DC=local

Domain          : pentestlab.local
ServerName      : WIN-PTELU2U07KG.pentestlab.local
OperatingSystem : {Windows Server 2012 R2 Standard Evaluation}
OSServicePack   :
LastBootup     : 5/25/2018 12:43:03 PM
OSVersion      : {6.3 (9600)}
Description     :

```

PowerShell AD Recon – Exchange Servers Discovery

Enumeration of service accounts is important as these accounts might be configured with a weak password. The attributes **PasswordLastSet** and **LastLogon** can provide an indication of services which have a higher possibility to have a weak password set.

- 1 `powershell_import /root/Find-PSServiceAccounts.ps1`
- 2 `powershell_execute Find-PSServiceAccounts`

```

meterpreter > powershell_import /root/Find-PSServiceAccounts.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute Find-PSServiceAccounts
[+] Command execution completed:
Discovering service account SPNs in the AD Domain pentestlab.local

Domain          : pentestlab.local
UserID          : krbtgt
PasswordLastSet : 03/18/2018 07:53:47
LastLogon       : 01/01/1601 00:00:00
Description     : Key Distribution Center Service Account
SPNServers      :
SPNTypes        : {kadmin}
ServicePrincipalNames : {kadmin/changepw}

Domain          : pentestlab.local
UserID          : PENTESTLAB_001
PasswordLastSet : 05/26/2018 19:44:35
LastLogon       : 01/01/1601 00:00:00
Description     :

```

PowerShell AD Recon – Service Accounts

Empire

PowerShell Empire has also a module which can display Service Principal Names (SPN) for domain accounts. This module is part of the Situational Awareness category and it should be used as stealth network recon in a red team engagement.

```
1 usemodule situational_awareness/network/get_spn
```

```

(Empire: 52AFV4KC) > usemodule situational_awareness/network/get_spn
(Empire: powershell/situational_awareness/network/get_spn) > info

      Name: Get-SPN
      Module: powershell/situational_awareness/network/get_spn
NeedsAdmin: False
OpsecSafe: True
      Language: powershell
MinLanguageVersion: 2
      Background: True
      OutputExtension: None

Authors:
  @_nullbind

Description:
  Displays Service Principal Names (SPN) for domain accounts
  based on SPN service name, domain account, or domain group
  via LDAP queries.

Comments:
  https://raw.githubusercontent.com/nullbind/Powershellery/master/Stable-ish/Get-SPN/Get-SPN.psml

```

Empire – SPN Module

The services will be presenting in the following format.

Account	Server	Service
-----	-----	-----
WIN-PTELU2U07KG\$	44405317-cf7c-4ac7-aacb-fc 2badffc9d8	E3514235-4B06-11D1-AB04-00 C04FC2DCD2
WIN-PTELU2U07KG\$	44405317-cf7c-4ac7-aacb-fc 2badffc9d8._msdcs.pentestlab.local	ldap
WIN-PTELU2U07KG\$	44405317-cf7c-4ac7-aacb-fc 2badffc9d8._msdcs.pentestlab.local	RPC
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	exchangeAB
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	exchangeMDB
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	exchangeRFR
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	HOST
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	IMAP
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	IMAP4
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	ldap
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	POP
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	POP3
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	RestrictedKrbHost
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	SMTP
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	SmtpSvc
WIN-PTELU2U07KG\$	WIN-PTELU2U07KG	TERMSRV

Empire – SPN Discovery

PowerShellery

[Scott Sutherland](#) before implementing the **Get-SPN** module to Empire had created several Powershell scripts as part of [PowerShellery](#) which can gather SPNs for various services. Some of these require PowerShell v2.0 and some other PowerShell v3.0.

```
1 Get-SPN -type service -search "*"
```

```
PS C:\Users\Administrator> Import-Module .\Get-SPN.psm1
PS C:\Users\Administrator> Get-SPN -type service -search "*"

Name           : WIN-PTELU2U07KG
SAMAccountName : WIN-PTELU2U07KG$
Description    :
UserPrincipalName :
DN             : CN=WIN-PTELU2U07KG,OU=Domain
                Controllers,DC=pentestlab,DC=local
Created        : 3/18/2018 7:53:47 AM
LastModified   : 5/29/2018 3:25:34 PM
PasswordLastSet : 5/21/2018 1:26:20 AM
AccountExpires : <Never>
LastLogon      : 5/30/2018 2:12:59 PM
GroupMembership : CN=Exchange Install Domain Servers,CN=Microsoft Exchange
                System Objects,DC=pentestlab,DC=local CN=Managed
                Availability Servers,OU=Microsoft Exchange Security
                Groups,DC=pentestlab,DC=local CN=Exchange Trusted
                Subsystem,OU=Microsoft Exchange Security
                Groups,DC=pentestlab,DC=local CN=Exchange
                Servers,OU=Microsoft Exchange Security
                Groups,DC=pentestlab,DC=local
```

Powershellery – GetSPN

Results can be also formatted as a table for easier mapping of accounts and services.

```
1 Get-SPN -type service -search "*" -List yes | Format-Table
```

```
PS C:\Users\Administrator> Get-SPN -type service -search "*" -List yes | Format-Table
```

Account	Server	Service
krbtgt	changePW	kadmin
PENTESTLAB_001	WIN-PTELU2U07KG.PENTEST...	PENTESTLAB_001
WIN-2NE38K15TGH\$	2224aa3a-63d1-493d-a57a...	E3514235-4B06-11D1-AB0...
WIN-2NE38K15TGH\$	8056fa52-ce80-4826-bcb8...	E3514235-4B06-11D1-AB0...
WIN-2NE38K15TGH\$	9b22dfb4-d71f-4a53-b856...	E3514235-4B06-11D1-AB0...
WIN-2NE38K15TGH\$	a25a50ca-02b7-4be8-bc6b...	E3514235-4B06-11D1-AB0...
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH	HOST
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH	RestrictedKrbHost
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH	TERMSRU
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH	WSMAN
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH.pentest...	HOST
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH.pentest...	RestrictedKrbHost
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH.pentest...	TERMSRU
WIN-2NE38K15TGH\$	WIN-2NE38K15TGH.pentest...	WSMAN

PowerShellery – GetSPN Table

There is also an additional script which can obtain the UserSID, the service and the actual User.

```
1 Import-Module .\Get-DomainSpn.psm1
2 Get-DomainSpn
```

```
PS C:\Users\Administrator> Import-Module .\Get-DomainSpn.psm1
PS C:\Users\Administrator> Get-DomainSpn
```

UserSid	: 150000052100024275195222151449612059234221143233300
User	: WIN-PTELU2U07KG\$
UserCn	: WIN-PTELU2U07KG
Service	: TERMSRU
ComputerName	: WIN-PTELU2U07KG
Spn	: TERMSRU/WIN-PTELU2U07KG
LastLogon	: 5/30/2018 2:12 PM
Description	:
UserSid	: 150000052100024275195222151449612059234221143124400
User	: WIN-2NE38K15TGH\$
UserCn	: WIN-2NE38K15TGH
Service	: WSMAN
ComputerName	: WIN-2NE38K15TGH
Spn	: WSMAN/WIN-2NE38K15TGH
LastLogon	: 5/25/2018 1:44 PM
Description	:

PowerShellery – Get-DomainSpn

Impacket

Service Principal Names can be also discovered from non-joined domain systems with the python version of **GetUserSPNs** which is part of impacket. However valid domain credentials are required for communication with the Active Directory as token based authentication cannot be used.

```
1 ./GetUserSPNs.py -dc-ip 10.0.0.1 pentestlab.local/test
```

```
root@kali:/usr/share/doc/python-impacket/examples# ./GetUserSPNs.py -dc-ip 10.0.0.1 pentestlab.local/test
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

Password:
ServicePrincipalName                                     Name                MemberOf    Pa
sswordLastSet      LastLogon
-----
PENTESTLAB_001/WIN-PTELU2U07KG.PENTESTLAB.LOCAL:80      PENTESTLAB_001      20
18-05-26 15:44:35 <never>
```

Impacket – Get User SPN

Resources

- <https://adsecurity.org/?p=230>
- <https://adsecurity.org/?p=1508>
- http://adsecurity.org/?page_id=183
- <https://github.com/nullbind/Powershellery>
- <https://github.com/PyroTek3/PowerShell-AD-Recon>