

Root-Me Write-up: Kerberos Authentication

Kerberos - Authentication

10 Points 

WOOF WOOF WOOF!

Author	Level	Validations
nuts_ · 28 May 2024	① 	2696 Challengers 1%

Statement

You have been asked by Cat Corporation's SOC team to retrieve a user's password linked to a suspicious Kerberos connection.

Flag format: `RW{userPrincipalName:password}`

* The userPrincipalName must be written in lowercase.

sha256sum: 0770efe5374637534fe55fdf51a3b7a1d5c58a1d6027d7143ce0a491ffd66405

[Download the challenge](#)

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: KRB5KDC_ERR_PREAMUTH_REQUIRED
60	0.199721031	192.168.122.1	192.168.122.100	KRB5	327	AS-REQ
61	0.199721039	192.168.122.100	192.168.122.1	KRB5	178	AS-REP
69	0.264321887	192.168.122.1	192.168.122.100	KRB5	1626	TGS-REQ
71	0.265044249	192.168.122.100	192.168.122.1	KRB5	1648	TGS-REP
70	0.268290706	192.168.122.1	192.168.122.100	SMB2	1594	Session Setup Request

```

Frame 51: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)
Ethernet II, Src: 54:54:01:97:49:54 (54:54:01:97:49:54), Dst: 52:54:01 (52:54:01:97:49:54)
Internet Protocol Version 4, Src: 192.168.122.1 (192.168.122.1), Dst: 192.168.122.100 (192.168.122.100)
Transmission Control Protocol, Src Port: 55280, Dst Port: 88, Seq: 1, Ack: 1, Len: 273
Kerberos
    Recv Mark: 269 bytes
    as-req
        pnvno: 5
        msg-type: krb-as-req (10)
        - padata: 2 items
            - PA-DATA pa-ENC-TIMESTAMP (2)
                + padata-type: pa-ENC-TIMESTAMP (2)
                    + padata-value: 00000000000000000000000000000000
                    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    cipher: fc8bbe22b2c967b222ed73dd7610ea71b2ae0c1b0c3688bfff7fecffdebd4054471350cb6e...
            - PA-DATA pa-PAC-REQUEST
        - req-body
    [Response in: 61]

```

[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: KRB5KDC_ERR_PREAMUTH_REQUIRED
60	0.199721031	192.168.122.1	192.168.122.100	KRB5	327	AS-REQ
61	0.199721039	192.168.122.100	192.168.122.1	KRB5	178	AS-REP

```

Frame 60: 327 bytes on wire (2616 bits), 327 bytes captured (2616 bits) on interface virbr0, id 0
Ethernet II, Src: 54:54:01:97:49:54 (54:54:01:97:49:54), Dst: 52:54:00:65:4c:4d (52:54:00:65:4c:4d)
Internet Protocol Version 4, Src: 192.168.122.1 (192.168.122.1), Dst: 192.168.122.100 (192.168.122.100)
Transmission Control Protocol, Src Port: 55282, Dst Port: 88, Seq: 1, Ack: 1, Len: 273
Kerberos
    Recv Mark: 269 bytes
    as-req
        pnvno: 5
        msg-type: krb-as-req (10)
        - padata: 2 items
            - PA-DATA pa-ENC-TIMESTAMP (2)
                + padata-type: pa-ENC-TIMESTAMP (2)
                    + padata-value: 00000000000000000000000000000000
                    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    cipher: fc8bbe22b2c967b222ed73dd7610ea71b2ae0c1b0c3688bfff7fecffdebd4054471350cb6e...
            - PA-DATA pa-PAC-REQUEST
        - req-body
    [Response in: 61]

```

No.	Time	Source	Destination	Protocol	Length	Info
51	0.045193731	192.168.122.1	192.168.122.100	KRB5	247	AS-REQ
52	0.045033481	192.168.122.100	192.168.122.1	KRB5	248	KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
60	0.199721071	192.168.122.1	192.168.122.100	KRB5	327	AS-REQ
61	0.200566492	192.168.122.100	192.168.122.1	KRB5	1741	AS-REP
> Frame 60: 327 bytes on wire (2616 bits), 327 bytes captured (2616 bits) on interface virbr0, id 0						
> Ethernet II, Src: 54:54:01:97:49:54 (54:54:01:97:49:54), Dst: 52:54:00:65:4c:4d (52:54:00:65:4c:4d)						
> Internet Protocol Version 4, Src: 192.168.122.1 (192.168.122.1), Dst: 192.168.122.100 (192.168.122.100)						
> Transmission Control Protocol, Src Port: 55282, Dst Port: 88, Seq: 1, Ack: 1, Len: 273						
> Kerberos						
> Record Mark: 269 bytes						
> as-req						
> pwno: 5						
> msg-type: krb-as-req (10)						
> padata: 2 items						
> req-body						
> Padding: 0						
> kdc-options: 50000000						
> cname						
> name-type: kRB5-NT-PRINCIPAL (1)						
> cname-string: 1 item						
> CNameString: william.dupond						
> realm: CATCORP.LOCAL						
> sname						
> till: Feb 21, 2024 00:00:46 00000000000000000000000000000000 PST						
> rtime: Feb 21, 2024 00:00:48 00000000000000000000000000000000 PST						
> nonce: 498314083						
> More fragments (ip.flags.mf), 1 bit						
Packets: 103 · Displayed: 7 (0.00%)						

Relevant Packet Fields

Encryption Type (etype): AES256-CTS-HMAC-SHA1-96 (18)

Realm: CATCORP.LOCAL

CNameString (username): william.dupond

Ciphertext:

fc8bbe22b2c967b222ed73dd7616ea71b2aeoc1boc3688bfff7fecffdebd4054
471350cb6e36d3b55ba3420be6co210b2d978d3f51d1eb4f

Building the Hashcat Format

Hashcat requires the following AS-REP format:

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

Constructed Hash

```
$krb5pa$18$william.dupond$CATCORP.LOCAL$fc8bbe22b2c967b222ed73dd7616ea71b2aeoc1boc3688bfff7fecffdebd4054
```

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**.

```
loki@SolarisFortress: ~
File Actions Edit View Help
└$ hashcat -m 19900 kerberosAuth.txt /usr/share/wordlists/rockyou.txt.gz
Completing file
dirbuster@ john.lst@ rockyou.txt@ sqlmap.txt@ 
fasttrack.txt@ metasploit@ rockyou.txt.gz@ wifite.txt@ 
fern-wifi@ nmap.lst@ seclists@ 
147 AS-REQ
148 KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
127 AS-REQ
141 AS-REP
```

Hashcat Command

```
hashcat -m 19900 krb_hash.txt rockyou.txt
```

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

The screenshot shows a terminal window titled 'hashcat' with the command 'hashcat -m 1850 -o /tmp/kitty.txt kitty@catcorp.local:password'. The session details pane shows the following information:

```

Session.....A...: hashcat!mused24: False
Status.....: Cracked!muse25: 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....: 78592/16344385 (0.55%)
Rejected....: 0/78592 (0.00%)
Restore.Point.: 78592/16344385 (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% CPU: 100% RAM: 99:00:48.000000000 PST
Hardware.Mon.#2.: Util: 95% CPU: 100% RAM: 99:00:48.000000000 PST
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.