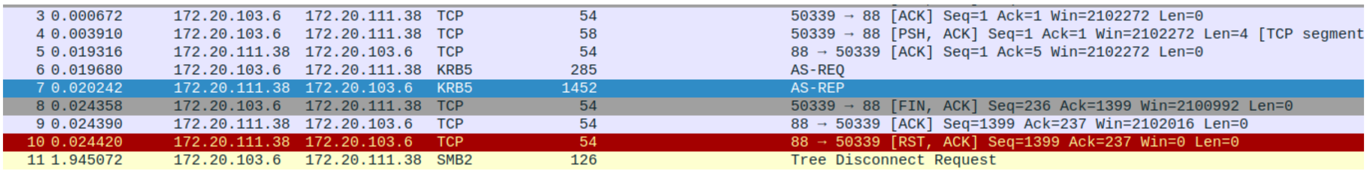
Midnight CTF 2022

Category : Network

Challenge : Le jeton de catwoman

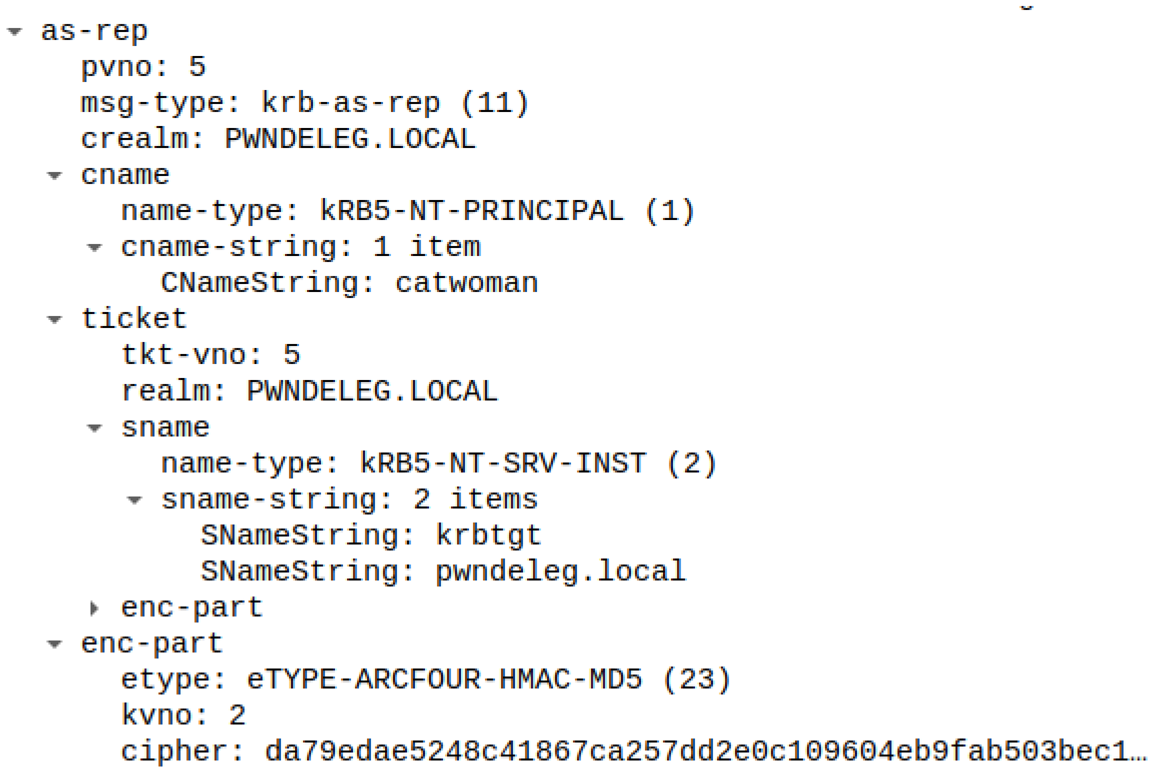
Difficulty : easy

They give us a pcapng file with a kerberos 5 auth and tell us the user's password is the flag :



```
 3 0.000672   172.20.103.6   172.20.111.38  TCP    54   50339 → 88 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
 4 0.003910   172.20.103.6   172.20.111.38  TCP    58   50339 → 88 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=4 [TCP segment
 5 0.019316   172.20.111.38  172.20.103.6   TCP    54   88 → 50339 [ACK] Seq=1 Ack=5 Win=2102272 Len=0
 6 0.019680   172.20.103.6   172.20.111.38  KRB5  285   AS-REQ
 7 0.020242   172.20.111.38  172.20.103.6   KRB5 1452   AS-REP
 8 0.024358   172.20.103.6   172.20.111.38  TCP    54   50339 → 88 [FIN, ACK] Seq=236 Ack=1399 Win=2100992 Len=0
 9 0.024390   172.20.111.38  172.20.103.6   TCP    54   88 → 50339 [ACK] Seq=1399 Ack=237 Win=2102016 Len=0
10 0.024420   172.20.111.38  172.20.103.6   TCP    54   88 → 50339 [RST, ACK] Seq=1399 Ack=237 Win=0 Len=0
11 1.945072   172.20.103.6   172.20.111.38  SMB2  126   Tree Disconnect Request
```

In the AS-REP you can see the user, the domain and the HASH in etype 23:

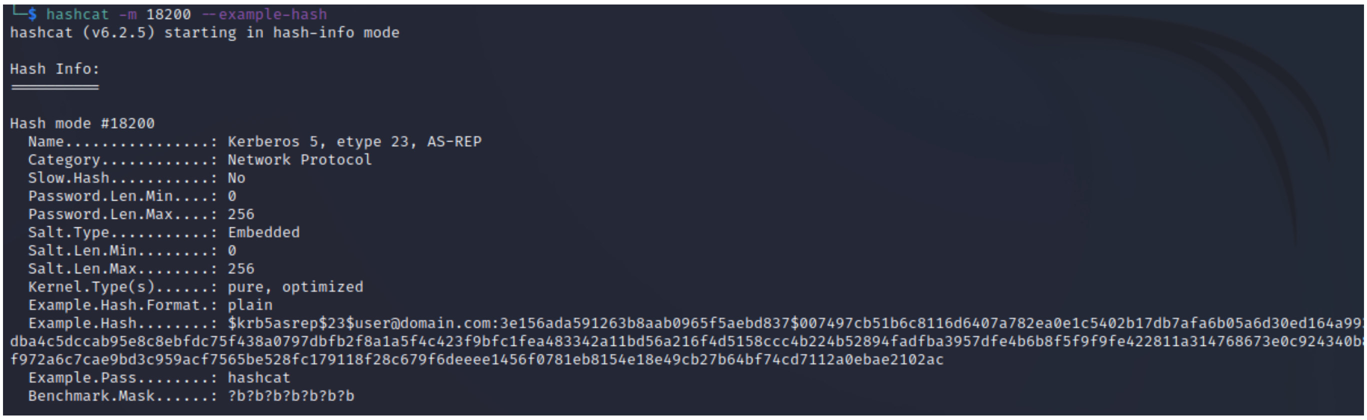


```
▾ as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    crealm: PWNDELEG.LOCAL
  ▾ cname
      name-type: kRB5-NT-PRINCIPAL (1)
    ▾ cname-string: 1 item
        CNameString: catwoman
  ▾ ticket
      tkt-vno: 5
      realm: PWNDELEG.LOCAL
    ▾ sname
        name-type: kRB5-NT-SRV-INST (2)
      ▾ sname-string: 2 items
          SNameString: krbtgt
          SNameString: pwndeleg.local
    ▸ enc-part
  ▾ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      kvno: 2
      cipher: da79edae5248c41867ca257dd2e0c109604eb9fab503bec1…
```

You can find here some information about kerberos protocol and ticket distribution : https://adsecurity.org/?p=2293

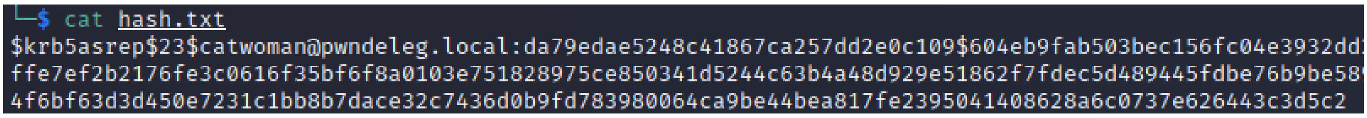
> The encryption type of the requested Kerberos service ticket is RC4_HMAC_MD5 which means the service account’s NTLM password hash is used to encrypt the service ticket. This means that Kerberoast can attempt to open the Kerberos ticket by trying different NTLM hashes and when the ticket is successfully opened, the correct service account password is discovered.

I used hashcat to find the password :



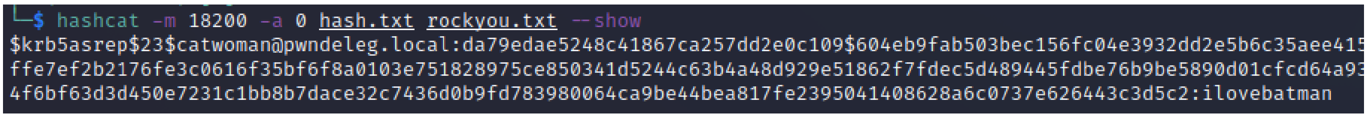
```
└─$ hashcat -m 18200 --example-hash
hashcat (v6.2.5) starting in hash-info mode

Hash Info:
=========

Hash mode #18200
  Name................: Kerberos 5, etype 23, AS-REP
  Category............: Network Protocol
  Slow.Hash...........: No
  Password.Len.Min....: 0
  Password.Len.Max....: 256
  Salt.Type...........: Embedded
  Salt.Len.Min........: 0
  Salt.Len.Max........: 256
  Kernel.Type(s)......: pure, optimized
  Example.Hash.Format.: plain
  Example.Hash........: $krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6b05a6d30ed164a99
dba4c5dccab95e8c8ebfdc75f438a0797dbfb2f8a1a5f4c423f9bfc1fea483342a11bd56a216f4d5158ccc4b224b52894fadfba3957dfe4b6b8f5f9f9fe422811a314768673e0c924340b
f972a6c7cae9bd3c959acf7565be528fc179118f28c679f6deeee1456f0781eb8154e18e49cb27b64bf74cd7112a0ebae2102ac
  Example.Pass........: hashcat
  Benchmark.Mask......: ?b?b?b?b?b?b?b
```

Now that we have an example, we can write our hash.txt that contain our cipher data with the correct format :



```
└─$ cat hash.txt
$krb5asrep$23$catwoman@pwndeleg.local:da79edae5248c41867ca257dd2e0c109$604eb9fab503bec156fc04e3932dd
ffe7ef2b2176fe3c0616f35bf6f8a0103e751828975ce850341d5244c63b4a48d929e51862f7fdec5d489445fdbe76b9be58
4f6bf63d3d450e7231c1bb8b7dace32c7436d0b9fd783980064ca9be44bea817fe2395041408628a6c0737e626443c3d5c2
```

Let's use rocky word list to attack it !



```
└─$ hashcat -m 18200 -a 0 hash.txt rockyou.txt --show
$krb5asrep$23$catwoman@pwndeleg.local:da79edae5248c41867ca257dd2e0c109$604eb9fab503bec156fc04e3932dd2e5b6c35aee415
ffe7ef2b2176fe3c0616f35bf6f8a0103e751828975ce850341d5244c63b4a48d929e51862f7fdec5d489445fdbe76b9be5890d01cfcd64a93
4f6bf63d3d450e7231c1bb8b7dace32c7436d0b9fd783980064ca9be44bea817fe2395041408628a6c0737e626443c3d5c2:ilovebatman
```

We found the password --> **ilovebatman**

flag : MCTF{ilovebatman}