Write-Up : Root-Me Kerberos Authentication

1. Comprendre le Challenge

Objectif : Nous disposons d'une capture réseau (`.pcap`) contenant du trafic Kerberos. Notre mission est d'intercepter une demande d'authentification et de cracker le mot de passe de l'utilisateur.

Format du flag : `RM{userPrincipalName:password}`

- **Important :** L'userPrincipalName (UPN) doit être écrit entièrement en **minuscules !!!!**.

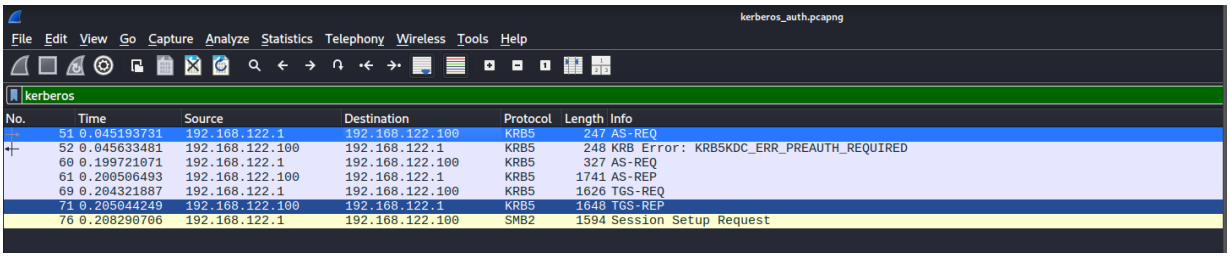
---

2. Analyse avec Wireshark

Ouvrez le fichier `.pcap` et filtrez le trafic pour ne voir que le protocole Kerberos.

- **Filtre Wireshark :** `kerberos`

Nous recherchons un paquet de type **AS-REQ** (Authentication Service Request). C'est le tout premier paquet envoyé par un utilisateur pour dire "Bonjour, je suis X, je veux me connecter".



---

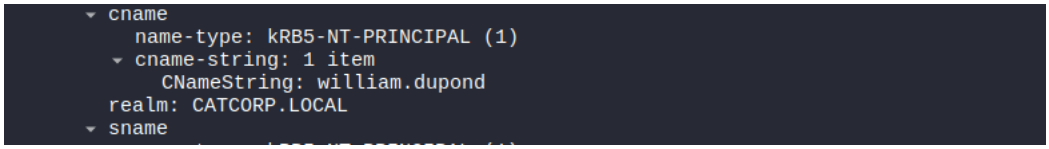
3. Extraction des données critiques

Dans le paquet **AS-REQ**, regardez dans le panneau de détails (en bas) et déroulez l'arborescence : `Kerberos` > `req-body`

Nous devons noter 3 informations et récupérer 1 longue chaîne hexadécimale :

1. **Username (cname) :** `william.dupond`
2. **Realm (Domaine) :** `CATCORP.LOCAL`
3. **Etype (Encryption Type) :** `18`

Cipher (Le hash) : C'est la longue chaîne chiffrée située dans `padata` > `PA-ENC-TIMESTAMP` > `enc-part` > `cipher`.



---

4. Construction du Hash

Pour que l'outil de crack (Hashcat) comprenne ce qu'on lui donne, il faut formater ces données ainsi : `$krb5pa$etype$username$realm$cipher`

Ce qui donne dans notre cas :

Plaintext
```
$krb5pa$18$william.dupond$CATCORP.LOCAL$0770efe537...[reste du cipher]
```

Sauvegardez cette ligne dans un fichier nommé `hash.txt`.

---

5. Cracking du mot de passe

Nous allons utiliser **Hashcat** avec le mode **19900** (spécifique au Kerberos 5 AS-REQ Pre-Auth etype 18).

Commande :

Bash
```
hashcat -m 19900 hash.txt /usr/share/wordlists/rockyou.txt
```

Après quelques secondes/minutes, Hashcat trouve la correspondance. **Résultat :** `kittycat12`

---

6. Reconstruction du Flag (Attention au pièges !)

Il faut assembler l'UPN et le mot de passe.

- L'UPN est `username` + `@` + `domaine`.
- Le challenge exige des **minuscules**.

Erreur classique : `william.dupond@CATCORP.LOCAL` (Domaine en majuscules)

Erreur classique : `william.dupond@catcorp.com` (Mauvaise extension, c'est du local)

Format correct : `william.dupond@catcorp.local`

Flag Final :

Plaintext
```
RM{william.dupond@catcorp.local:kittycat12}
```