ETHERNET - TRAME

1. Présentation du challenge

- **Objectif** : Retrouver des données confidentielles dissimulées dans une trame réseau brute.
- **Donnée fournie** : Une suite d'octets en hexadécimal représentant une trame complète.

2. Analyse Technique (Décomposition de la trame)

L'analyse consiste à découper la trame couche par couche selon le modèle OSI.

Couche 2 : Ethernet

- **Adresse MAC Destination** : `00 05 73 a0 00 00`
- **Adresse MAC Source** : `e0 69 95 d8 5a 13`
- **Type de protocole** : `86 dd` (indique le protocole **IPv6**)

Couche 3 : IPv6

Version : `6`

Payload (Taille des données) : `00 9b`

Next Header : `06` (indique le protocole **TCP**)

IP Source : `2607:5300:0060:2abc:0000:0000:bade:code`

IP Destination : `2001:41d0:0002:4233:0000:0000:0000:0004`

Couche 4 : TCP

- **Port Source** : `96 74`
- **Port Destination** : `00 50` (indique le protocole **HTTP**)

3. Analyse de la charge utile (Payload)

La conversion de l'hexadécimal en texte ASCII révèle une requête HTTP:

```
GET / HTTP/1.1
Authorization: Basic Y29uZmk6ZGVudGlhbA==
User-Agent: insaneBrowser
Host: www.myipv6.org
Accept: */*
```

On identifie une **Authentification Basique** (Basic Auth). Les identifiants sont encodés en **Base64** juste après le mot "Basic".

4. Résolution : Décodage Base64

Pour obtenir les données confidentielles, il faut extraire et décoder la chaîne Base64 identifiée.

Extraction de la valeur Hexa :

`59 32 39 75 5a 6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d`

Conversion Hexa vers ASCII (Base64) :

`Y29uZmk6ZGVudGlhbA==`

Décodage du Base64 :

Chaîne : `Y29uZmk6ZGVudGlhbA==`

Résultat : `confi:dential`

5. Conclusion

- **Donnée confidentielle trouvée** : `confidential`
- **Leçon apprise** : L'authentification HTTP "Basic" est vulnérable car elle se contente d'encoder les identifiants en Base64 sans aucun chiffrement. Toute personne interceptant la trame Ethernet peut lire les accès en clair.

Challenge réalisé sur la plateforme Root-me

Waya CHEMLA

Signature numérique de Waya CHEMLA
Date : 2026.01.07 14:07:29 +01'00'