WRITE-UP log2.0:

Partie 1 : log2.0 – Initial Access Identification

Objectif Identifier :

L'alias de l'attaquant

L'adresse IP externe utilisée lors de l'accès initial

Format du flag :

CSCC{nom_attaquant_ip_attaquant}

📁 Fichiers Utilisés

```
log2.0/
├── web/nginx_access.log
└── application/app.log
```

Étape 1 – Analyse du trafic HTTP

On commence par analyser les requêtes sensibles :

Requêtes POST

Pages /login

Accès administrateur

Commande utilisée

```
grep "POST /login.php" nginx_access.log
```

Résultat pertinent

```
185.199.109.153 - anonymos [04/Feb/2004:02:14:30 +0000]
"POST /login.php HTTP/1.1" 302
```

Code HTTP 302 indique une redirection après une authentification réussie.

Étape 2 – Vérification d'un accès administrateur

Un accès administrateur valide doit être confirmé par une ressource protégée.

Commande

```
grep "/admin" nginx_access.log
```

Résultat

```
GET /admin/dashboard.php HTTP/1.1" 200
```

👉 HTTP 200 confirme l'accès autorisé

👉 Même IP et même alias

Étape 3 – Corrélation avec les logs applicatifs

Les logs applicatifs confirment les actions à privilèges élevés.

Commande
```
grep "privileged_access" app.log
```

Résultat
```
[2004-02-04 02:14:32] WARN privileged_access
user=anonymos ip=185.199.109.153
```

Confirmation côté application, ce qui élimine tout faux positif.

Analyse Forensics

Élément	Valeur
Alias attaquant	anonymos
IP source	185.199.109.153
Méthode	Authentification Web
Résultat	Accès administrateur valide

Les autres IP et utilisateurs présents dans les logs :

Échouent (401, 403)

N'accèdent jamais aux ressources /admin

Ne déclenchent aucune action critique

✅ Conclusion Partie 1 – log2.0

L'unique séquence montrant :

Authentification réussie

Accès à une ressource protégée

Confirmation applicative

correspond à l'attaquant suivant :

🚩 FLAG FINAL – log2.0
```
CSCC{anonymos_185.199.109.153}
```

🏁 Remarque Finale

La partie log2.0 exige :

Analyse de volumes importants de logs

Compréhension des codes HTTP

Corrélation multi-sources

Ce qui correspond exactement au niveau HARD attendu en CSCC.