

## **WRITE-UP log2.1**

**Partie 2** : log2.1 – Attack Identification & Timeline  
Objectif Identifier :

Le type exact de l'attaque réussie

La date précise de l'attaque

**Format du flag :**

CSCC{type\_attaque\_date\_attaque}

### **Fichiers Utilisés**

```
log2.1/
└── ids/snort.log
└── firewall/iptables.log
└── system/auth.log
```

### **Étape 1** – Analyse des alertes IDS

La première étape consiste à analyser les alertes générées par le système de détection d'intrusion.

#### **Commande utilisée**

```
grep "success" snort.log
```

#### **Résultat clé**

```
[**] sql_injection success [**] {TCP} 185.199.109.153 -> 10.0.0.5
```

La présence du mot success indique une attaque ayant réellement abouti.

### **Étape 2** – Corrélation avec l'IP identifiée en log2.0

Pour éliminer les faux positifs, on corrèle avec l'IP de l'attaquant trouvée précédemment.

#### **Commande**

```
grep "185.199.109.153" snort.log
```

#### **Résultat**

```
sql_injection detected
sql_injection success
```

L'attaque SQL Injection est la seule associée à cette IP avec un succès confirmé.

### **Étape 3** – Vérification côté Firewall

Les logs firewall permettent de confirmer une activité anormale au même instant.

#### **Commande**

```
grep "185.199.109.153" iptables.log
```

**Résultat**

```
DROP TCP 185.199.109.153:443 -> 10.0.0.5:80
```

Preuve d'un trafic suspect bloqué après exploitation.

**Étape 4** – Confirmation par les logs système

Les logs système montrent une conséquence directe de l'attaque.

**Commande**

```
grep "Accepted password" auth.log
```

**Résultat**

```
Accepted password for anonymos from 185.199.109.153
```

Cela confirme que l'attaque a permis une authentification valide.

**Reconstruction de la Timeline**

Heure Événement

02:14:30	SQL Injection détectée
02:14:31	SQL Injection réussie
02:14:33	Blocage Firewall
02:14:34	Authentification système

**Analyse Forensics**

Plusieurs types d'attaques apparaissent dans les logs IDS.

Une seule :

Associée à l'IP identifiée en log2.0

Marquée comme success

Entraîne des actions post-exploitation

**L'attaque valide est donc SQL Injection.**

**Conclusion Partie 2 – log2.1**

Type d'attaque : SQL Injection

Date de l'attaque : 2004-02-04

▶ FLAG FINAL – log2.1  
CSCC{sql\_injection\_2004-02-04}

☒ Remarque Finale

La partie log2.1 demande :

Analyse avancée IDS / Firewall

Corrélation inter-parties (log2.0 → log2.1)

Reconstruction d'une timeline réaliste