

# SAE 3 Cyber.04 – Découvrir le pentesting

## Devis pour Audit de Sécurité Informatique-SAE 3.04

**Auteur :** Labeste Bastien

**Encadrant :** Laborde Ludovic



---

*Client : Connect3s SAS*

*Prestataire : Bastien Labeste, Consultant en Cybersécurité*

*Date : 15/12/2024*

---

## 1. Objectif du Projet

Réalisation d'un test d'intrusion approfondi sur les systèmes informatiques de l'entreprise afin d'identifier les vulnérabilités critiques, d'évaluer leur impact et de fournir des recommandations détaillées pour renforcer la sécurité.

---

## 2. Étendue du Projet

- **Systèmes concernés** : Serveur Samba (172.18.0.4) et serveur Web (172.19.0.2) hébergeant DVWA.
  - **Approche** : Méthode de boîte grise, incluant reconnaissance, exploitation, persistance, et pivot SSH.
  - **Durée estimée** : 4 semaines.
- 

## 3. Prestations Incluses

### 1. Analyse de sécurité initiale :

- Scans réseau avec Nmap pour identifier les services exposés.
- Analyse des configurations système et identification des vulnérabilités.

### 2. Exploitation des vulnérabilités :

- Exploitation des failles identifiées (CVE-2017-7494, vulnérabilités d'upload, etc.).
- Tests d'injection SQL et commande.

### 3. Tests avancés :

- Mise en place de techniques de pivot SSH pour explorer le réseau interne.
- Installation et configuration de solutions de persistance (Cron, VNC).

### 4. Recommandations et rapport final :

- Rédaction d'un rapport détaillé avec hiérarchisation des vulnérabilités (CVSS).
- Proposition de solutions concrètes pour sécuriser les systèmes.

---

#### 4. Tarifs et Estimation des Coûts

- **Frais journaliers** : 700 € / jour.
- **Durée totale estimée** : 20 jours.
- **Total estimé** : 14 000 € HT.

---

#### 5. Conditions Générales

- Les tests seront effectués dans un environnement contrôlé, avec les autorisations nécessaires.
- Toute donnée sensible sera traitée avec confidentialité.
- Le devis est valable 30 jours à compter de sa date d'émission.

---

Si cette proposition convient, je reste à votre disposition pour toute clarification ou ajustement.

#### **Signature**

Bastien Labeste

Consultant en Cybersécurité