# Pratiques de l'Investigation Numérique

*« Like a conscientious and methodical craftsman, every day, refine your practice. Only in this way will you be and remain an expert in your art. »*

**Département de Génie Informatique**

Cybersécurité et Investigation Numérique

**4ème année**

**LABS d'Investigation Numérique**

**Thierry MINKA**, Sr-Eng, Sr-Lead Auditor, GRC Expert, Legal Expert in Cybercrime

# Table des matières

# 1. Introduction Générale

## 1.1 Contexte et Objectifs

L'investigation numérique et la cybersécurité sont des domaines critiques dans l'informatique moderne. Avec l'augmentation des cyberattaques, il est impératif pour les étudiants en informatique d'acquérir des compétences pratiques leur permettant de comprendre, analyser et répondre aux menaces actuelles. Les **Labs d'Investigation Numérique** proposés ici permettent aux étudiants de simuler des scénarios réalistes d'attaques, de compromission et d'investigation dans des environnements contrôlés. Ces Labs sont une contribution pour renforcer les capacités des étudiants et les préparer à évoluer dans des environnements de production.

L'objectif principal de ces Labs est de permettre aux étudiants de se familiariser avec des environnements sécurisés, de comprendre les mécanismes d'attaques et de compromission, et d'apprendre à analyser les systèmes après une attaque pour proposer des solutions de renforcement de la sécurité.

Ces Labs contribuent à développer des compétences clés telles que :

- ☑La configuration de réseaux sécurisés, incluant des zones démilitarisées (DMZ).
- ☑La création de malwares et la simulation d'attaques pour comprendre les techniques des attaquants.
- ☑L'analyse post-compromission d'un système pour identifier les traces laissées par une attaque.
- ☑La proposition de contre-mesures efficaces pour sécuriser des environnements de production.

En somme, ces travaux pratiques ont pour vocation d'aider à préparer les étudiants à des environnements réels, tout en respectant l'éthique et les règles de sécurité.

## 1.2 Importance des Labs en Informatique

Dans un contexte où les entreprises et institutions doivent faire face à des menaces croissantes en matière de cybersécurité, il est essentiel que les étudiants en informatique maîtrisent non seulement les concepts théoriques mais

aussi les outils et techniques pratiques pour protéger les systèmes. Les Labs d'Investigation Numérique offrent aux étudiants la possibilité de se confronter à des situations réelles tout en étant dans un environnement sécurisé et contrôlé. Ils leur permettent de :

- ☑Identifier et exploiter des vulnérabilités dans des environnements isolés.
- ☑Conduire des analyses post-compromission pour comprendre l'impact des attaques.
- ☑Proposer des recommandations concrètes pour améliorer la sécurité des systèmes informatiques.

## 2. Notes et Remarques

### 2.1 Éthique et Légalité

Les Labs d'Investigation Numérique présentés dans ce document sont exclusivement à des fins pédagogiques. Il est essentiel que les étudiants comprennent que toute tentative d'utiliser les techniques présentées dans un contexte non autorisé est strictement interdite et illégale. Toute simulation d'attaque ou d'analyse numérique doit être réalisée dans un environnement contrôlé et ne doit jamais être exécutée sur des systèmes ou réseaux réels sans une autorisation explicite.

Toute infraction à ces règles peut entraîner des poursuites judiciaires. **Il est essentiel que chaque étudiant comprenne ses responsabilités** en tant que professionnel de la sécurité et agisse conformément aux normes éthiques et légales du secteur.

### 2.2 Sécurité de l'environnement

Les environnements utilisés dans ces Labs doivent être entièrement isolés du réseau de production. L'utilisation de machines virtuelles dans un réseau local ou des simulateurs de réseau comme GNS3 garantit que les simulations d'attaques ne peuvent pas affecter des systèmes réels. Il est impératif de toujours travailler dans un environnement sécurisé et de s'assurer que ces environnements ne sont accessibles que par des utilisateurs autorisés.

### 2.3 Bon à savoir

☑ Chaque étudiant exécutera SEUL, l'ensemble des tâches décrites dans ces Labs.
☑ En cas de similarité, la note du devoir sera divisée par le nombre d'étudiants concernés.
☑ La réalisation de ces Labs, SEUL, vous aidera au-delà de la note que vous pensez obtenir en vous faisant aider ou en copiant le travail de quelqu'un d'autre.
☑ Toute ressemblance avec une situation ou des faits survenus dans la réalité n'est que pure coïncidence.
☑ Chaque Lab donne lieu à la production d'un **rapport d'exécution** détaillé contenant les différentes captures d'écran illustrant les tâches réalisées.

## 3. Outils Utilisés dans les Labs

### 3.1 Outils d'Investigation et d'Attaque

Les outils utilisés dans ces Labs sont des logiciels libres ou professionnels couramment employés par les professionnels de la sécurité pour les tests d'intrusion, l'analyse forensique et la simulation d'attaques.

☑**Kali Linux** : Système d'exploitation complet dédié à la sécurité informatique, intégrant une large gamme d'outils d'analyse, de test d'intrusion et d'investigation. Il est utilisé tout au long des Labs pour préparer et exécuter des attaques, ainsi que pour analyser les environnements compromis.

☑**GNS3** : Simulateur de réseaux, utilisé pour créer et configurer des environnements réseaux complexes incluant des machines virtuelles, des routeurs, des switches, des firewalls, et des serveurs. Il permet de simuler des environnements de production dans un réseau isolé.

☑**OWASP ZAP et Burp Suite** : Outils de proxy web utilisés pour intercepter et modifier le trafic HTTP. Ils permettent d'analyser les requêtes envoyées aux applications web et d'identifier les failles de sécurité comme les injections SQL ou les failles XSS.

☑**SQLMap** : Outil d'injection SQL automatisé permettant de tester et d'exploiter des bases de données vulnérables en envoyant des requêtes malveillantes pour manipuler les données.

☑**Nikto** : Scanner de vulnérabilités web. Il détecte les configurations dangereuses, les fichiers non sécurisés et les versions de logiciels vulnérables sur les serveurs web.

☑**Hydra** : Outil de force brute utilisé pour tester la robustesse des systèmes d'authentification en essayant des combinaisons multiples de mots de passe.

☑**Wireshark** : Outil d'analyse de trafic réseau. Il capture et inspecte les paquets réseau pour identifier les activités suspectes et analyser les communications réseau entre les machines.

☑**Metasploit** : Framework d'exploitation de vulnérabilités. Il permet de lancer des attaques complexes sur des systèmes vulnérables et d'exécuter du code malveillant pour tester la sécurité des systèmes.

☑**Autopsy** : Outil d'analyse forensique permettant de récupérer des artefacts numériques (fichiers, logs) à partir d'une image disque, souvent utilisée dans les enquêtes post-compromission.

☑**Volatility** : Framework d'analyse de la mémoire, permettant d'extraire et d'analyser les informations contenues en mémoire vive (RAM) après une attaque.

### 3.2 Systèmes d'exploitation Utilisés

Les systèmes d'exploitation utilisés dans ces Labs sont sélectionnés pour refléter les environnements que les étudiants rencontreront en milieu professionnel :

☑**Kali Linux** : Utilisé comme système de base pour les étudiants jouant le rôle de l'attaquant ou de l'analyste de sécurité. Kali Linux est choisi pour sa richesse en outils d'investigation et de test d'intrusion.

☑**Windows 10** : Utilisé comme machine cible dans plusieurs Labs, en particulier dans les simulations d'attaques et d'analyses post-compromission. Windows est largement utilisé dans les environnements de production, ce qui en fait une cible idéale pour les scénarios réalistes.

☑**Linux (serveur web)** : Utilisé dans la DMZ pour héberger une application web. Les serveurs Linux sont couramment utilisés dans les environnements professionnels pour leur fiabilité et leur sécurité, mais ils restent des cibles potentielles d'attaques.

## 4. Présentation des Labs

### 4.1 Lab 1 : Configuration d'un Environnement Réseau Fonctionnel et Sécurisé

#### 4.1.1 Objectif

L'objectif de ce Lab est de permettre aux étudiants de créer un environnement réseau complexe dans GNS3. Ils doivent configurer un réseau sécurisé incluant une machine Windows, une DMZ (zone démilitarisée) avec un serveur web sous Linux, un firewall, et un routeur. Ce Lab met en pratique les concepts de segmentation réseau et d'isolation des services critiques.

#### 4.1.2 Résumé des Étapes

☑Création d'un projet dans GNS3 pour configurer un environnement complet incluant des machines virtuelles et des équipements réseau.

☑Configuration d'une DMZ avec un serveur Linux hébergeant une application web, isolé du reste du réseau via un firewall.

☑Mise en place d'un firewall pour contrôler le trafic réseau entre la DMZ, le réseau interne et l'extérieur.

☑Test de connectivité pour s'assurer que seuls les services autorisés peuvent traverser les différentes zones du réseau.

### 4.2 Lab 2 : Création et Test d'un Ransomware Simulé

#### 4.2.1 Objectif

Ce Lab permet aux étudiants de comprendre le fonctionnement d'un ransomware du point de vue de l'attaquant. Ils créent un ransomware simulé sous Kali Linux, le testent sur une machine virtuelle Windows, et envoient l'attaque dans l'environnement de Lab 1. Cela leur permet de mieux appréhender les mécanismes d'attaques et la propagation des malwares.

#### 4.2.2 Résumé des Étapes

☑Création d'un ransomware simulé : Les étudiants développent un script malveillant en Python ou PowerShell qui renomme les fichiers de l'utilisateur, simulant un chiffrement.

☑Transformation du script en exécutable : Utilisation de PyInstaller pour transformer le script en un fichier exécutable.

☑Test sur une machine virtuelle Windows pour observer les effets du ransomware.

☑Envoi du ransomware par e-mail dans l'environnement de Lab 1 pour infecter la machine cible.

## 4.3 Lab 3 : Audit de Sécurité de l'Environnement de Lab 1

### 4.3.1 Objectif

Ce Lab se concentre sur la réalisation d'un audit de sécurité complet de l'environnement de **Lab1**. Les étudiants doivent identifier les failles et vulnérabilités présentes dans l'infrastructure, y compris celles de l'application web située dans la DMZ. Ils doivent également formuler des recommandations pour corriger ces vulnérabilités et empêcher une nouvelle compromission.

### 4.3.2 Résumé des Étapes

☑Scan réseau avec Nmap : Identification des ports ouverts et des services en cours d'exécution dans l'environnement.

☑Utilisation de Nikto et OpenVAS (ou Nessus) pour détecter les vulnérabilités des services web et des équipements réseau.

☑Audit de l'application web avec OWASP ZAP pour détecter les failles dans les pages web (comme les injections SQL, XSS, ou CSRF).

☑Exploitation potentielle des vulnérabilités pour vérifier leur impact, notamment en utilisant Metasploit pour tester des exploits.

☑Rédaction du rapport d'audit avec une analyse détaillée des vulnérabilités et des recommandations pour améliorer la sécurité.

## 4.3 Lab 4 : Simulation d'Attaque sur l'Application Web dans la DMZ

### 4.3.1 Objectif

L'objectif de ce Lab est de permettre aux étudiants de simuler des attaques ciblées sur l'application web hébergée dans la DMZ de **Lab 1**. Les étudiants utiliseront l'environnement d'attaque de **Lab 2** pour préparer et déployer des malwares et exploiter des vulnérabilités spécifiques à l'application web. Ce Lab leur permet d'acquérir une compréhension des

techniques utilisées pour attaquer les applications web, même lorsqu'elles sont protégées dans une DMZ.

### 4.3.2 Résumé des Étapes

☑Identification des vulnérabilités avec Nikto et OWASP ZAP pour détecter les failles dans l'application web.

☑Attaques par injection SQL avec SQLMap : Exploitation des vulnérabilités SQL pour accéder aux bases de données et manipuler les données.

☑Attaques par force brute avec Hydra : Test des pages de login et d'authentification pour vérifier leur robustesse face aux attaques par force brute.

☑Exploitation des vulnérabilités avec Metasploit : Lancement d'exploits spécifiques pour obtenir un accès non autorisé ou exécuter du code malveillant sur le serveur web.

☑Manipulation du trafic HTTP avec OWASP ZAP ou Burp Suite pour tester des attaques comme le Cross-Site Scripting (XSS) et le Cross-Site Request Forgery (CSRF).

☑Rédaction d'un rapport complet sur les attaques réalisées et les failles exploitées, avec des recommandations pour sécuriser l'application web.

## 4.3 Lab 5 : Analyse Post-Compromission

### 4.3.1 Objectif

Dans ce Lab, les étudiants conduisent une analyse forensique après l'attaque de ransomware simulée dans **Lab2**. L'objectif est d'apprendre à examiner les traces laissées par l'attaque sur la machine compromise et de récupérer des preuves à l'aide d'outils d'investigation numérique. Ils utiliseront notamment des outils comme **Autopsy**, **Volatility**, et **Wireshark** pour explorer les artefacts numériques, les journaux système, et les captures réseau.

### 4.3.2 Résumé des Étapes

☑Sauvegarde de l'image disque de la machine compromise en utilisant l'outil dd pour ne pas altérer les preuves.

☑Analyse de l'image disque avec Autopsy : Les étudiants examinent les fichiers, les journaux système, et les programmes récemment exécutés pour identifier les signes de compromission.

☑Analyse mémoire avec Volatility : Les étudiants récupèrent l'image mémoire de la machine compromise pour analyser les processus en cours d'exécution, les connexions réseau, et les données stockées en mémoire vive.

☑Analyse réseau avec Wireshark : Les étudiants capturent et analysent le trafic réseau pour identifier les communications suspectes, telles que les connexions à des serveurs de commande et de contrôle (C&C).

☑Rédaction d'un rapport post-compromission basé sur les preuves récupérées.

# 5. Détail des Labs

## 5.1 Lab1 : Configuration d'un Environnement Réseau Fonctionnel et Sécurisé

### 5.1.1 Objectif

Le présent LAB vise à donner aux étudiants l'occasion de configurer une infrastructure réseau constituée d'un équipement de frontière, d'un réseau local et d'une DMZ. Les étudiants réviseront ainsi la configuration et le paramétrage d'équipements actifs, l'adressage réseau et le partage de ressources. Ce LAB s'inscrit dans un ensemble plus grand visant à réaliser l'investigation numérique dans une société après qu'elle a été victime d'un ransomware.

### 5.1.2 Enoncé

L'étudiant configurera une infrastructure réseau complètement FONCTIONNELLE sur GNS3, constituée comme suit:

1- un équipement de frontière ;
2- une DMZ contenant un poste de travail (serveur Linux, distribution Red-Hat, Debian, Ubuntu) qui contient une application web accessible depuis l'extérieur du réseau d'entreprise comme de l'intérieur;
3- un poste de travail ( muni d'un SE Windows 10 ou supérieur, contenant un antivirus) sur le réseau local qui possède 2 Go de données, de toutes sortes (fichier, exe, Word, PDF, Excel,...);

### 5.1.3 Details des étapes

**1. Création des postes de travail**

1.1. Machines virtuelles

☑Installer un logiciel de virtualisation comme VMWare ou VirtualBox ;

1.2. Machine Virtuelle Windows 10 :

☑Créer une machine virtuelle avec les caractéristiques minimales suivantes :

- DD : 10 Go ;
- RAM : 2 Go.

☑Y installer Windows 10 ou supérieur ;

☑Copier et coller de 2 Go de données sur le Bureau et dans le répertoire « Mes documents » ;

1.3. Machine Virtuelle Linux (serveur web) :

☑Créer une machine virtuelle avec les caractéristiques minimales suivantes :

- DD : 10 Go ;
- RAM : 2 Go.

☑Y installer Linux, de préférence la distribution Red-Hat, Debian ou Ubuntu.

☑Créer une application web. Pour des besoins de célérité liés au délai du LAB, l'étudiant pourrait utiliser un CMS. Les interfaces utilisateur et administrateur doivent être actives et fonctionnelles.

☑Rendre l'application Web fonctionnelle sur la machine virtuelle Linux.

**2. Création de l'infrastructure**

2.1. Installer GNS3;

2.2. Créer un projet intitulé LAB1

2.3. Configuration des équipements actifs de l'infrastructure

2.3.1. Equipement de frontière

☑Ajouter un routeur dans votre projet Lab1 ;

☑Configurer une interface R-Eth0 comme adresse publique du réseau ;

☑Configurer une interface R-Eth1 comme adresse privée, c'est à dire adresse de votre réseau local.

2.3.2. Division du réseau en sous-réseaux

☑Ajouter un switch manageable ;

☑Configurer une interface S-Eth0 pour qu'elle communique avec l'interface privée du routeur R-Eth1 ;

☑Configurer une interface S-Eth1 pour qu'elle communique seulement avec l'interface F-Eth0 du Firewall de la DMZ;

☑Configurer une adresse S-Eth2 pour qu'elle communique avec le sous-réseau local, donc le Poste de Travail sous Windows.

☑Ajouter un Firewall.

☑Configurer une interface F-Eth0 pour qu'elle communique avec l'interface S-Eth1
2.3.2.6. Configurer une interface F-Eth1 pour qu'elle communique avec le Poste de Travail sous Linux (Serveur Web).

**3. Fonctionnement de l'infrastructure**

3.1. Ajout des machines virtuelles

☑Ajouter la machine virtuelle Windows dans le projet Lab1 ;

☑Ajouter la machine virtuelle Linux dans le projet LAB1.

3.2. Configuration des communications

☑Connecter la machine virtuelle Windows sur l'interface S-Eth2 ;

☑Connecter la machine virtuelle Linux sur l'interface F-Eth1.

☑Vérifier que depuis la machine virtuelle Windows vous pussiez surfer (accéder) sur l'application web déployée sur la machine virtuelle Linux.

**Note :** Le Lab1 sera présentée jeudi le 17 octobre 2024, assorti du rapport de conception et de déploiement.

## 5.2 Lab2 : Création et Test d'un Ransomware Simulé depuis Kali Linux

### 5.2.1 Objectif

Ce lab a pour objectif de permettre aux étudiants de simuler une attaque en créant un ransomware sur une machine virtuelle Kali Linux. Le ransomware sera testé dans une machine virtuelle Windows dédiée avant d'être envoyé dans l'environnement réseau configuré dans **Lab 1**. Ce lab se concentre exclusivement sur l'attaque, avec deux scénarios : (1) un fichier attaché auto-exécutable, et (2) un lien dans l'e-mail menant à un téléchargement malveillant.

### 5.2.2 Enoncé

Chaque étudiant va mettre en place un environnement d'attaquant pour concevoir et tester un ransomware avant de l'envoyer par mail pour compromettre la machine Windows du Lab1.

### 5.2.3 Prérequis :

☑**Nouvel environnement réseau** à configurer dans GNS3, appelé **"Environnement d'attaque"**, distinct de celui de **Lab 1**.

☑**Nouvelle machine virtuelle Kali Linux** pour l'attaquant.

☑**Nouvelle machine virtuelle Windows** pour tester le ransomware avant son envoi.

☑L'environnement de **Lab 1** pour simuler la propagation et la compromission dans un réseau cible.

### 5.2.4 Details des étapes

**1. Création de l'environnement d'attaque**

1. 2 Création des postes de travail

☑Lancer Virtual Box

☑ Créer une machine virtuelle Kali Linux (Attaquant) :

- **Nom** : Kali-Linux-Attaquant
- **Disque dur** : 10 Go
- **RAM** : 2 Go
- **OS** : Kali Linux (dernière version)
- **Logiciels nécessaires** : Python, PowerShell, outils de compression (zip), client mail (optionnel), Apache pour hébergement web (si nécessaire)
- **Connectivité réseau** : Doit avoir un accès à internet pour l'envoi d'e-mails et l'hébergement de fichiers si un lien est utilisé.

☑Créer une machine virtuelle Windows (Test du ransomware) :

- **Nom** : Windows-Test
- **Disque dur** : 10 Go
- **RAM** : 2 Go
- **OS** : Windows 10 ou supérieur
- **Logiciels nécessaires** : Python pour exécuter le script, client mail (optionnel)
- **Connectivité réseau** : Doit être capable de recevoir des fichiers transférés de Kali (via clé USB virtuelle ou partage réseau).

1.2 Création de l'environnement GNS3

1.2.1 Création d'un projet GNS3 :

☑Lancez GNS3 ;

☑Créez un nouveau projet intitulé **"Environnement d'attaque"**. Ce projet représentera le réseau de l'attaquant qui sera utilisé pour mener l'attaque.

☑Ajout les 2 machines virtuelles dans votre projet GNS3.

**2. Etapes**

**Étape 1 : Programmation du ransomware simulé sous Kali Linux**

1. **Création du script ransomware** :

☑Sur la machine **Kali-Linux-Attaquant**, ouvrez un éditeur de texte et créez un script Python qui simule le chiffrement de fichiers. Ce script renomme les fichiers en ajoutant l'extension .locked pour simuler une attaque.

☑ Créer un fichier qui liste les fichiers dans le répertoire cible.

☑ Créer un fichier qui contient le message de demande de rançon .

☑Enregistrez ce script sous le nom **ransomware_simule.py**.

2. **Transformation du script en fichier exécutable (EXE)** :

☑Utilisez **PyInstaller** pour transformer votre script Python en un fichier exécutable.

☑ Enregistrez le fichier exécutable sous le nom **ransomware_simule.exe**.

3. **Création d'une archive ZIP contenant l'exécutable** :

☑Compressez l'exécutable dans une archive ZIP sous le nom **Documents_Importants.zip**.

**Étape 2 : Test du ransomware sur la machine virtuelle Windows (Windows-Test)**

1. **Transfert du ransomware** :

☑Transférez l'archive **Documents_Importants.zip** de Kali Linux vers la machine virtuelle **Windows-Test** via un partage réseau ou une clé USB virtuelle.

2. **Test de l'exécution du ransomware** :

☑Sur la machine **Windows-Test**, extrayez l'archive ZIP sur le bureau et exécutez l'exécutable **ransomware_simule.exe** pour simuler l'attaque.

☑Observez que les fichiers du répertoire ciblé (par exemple C:\Users\Etudiant\Desktop\test) sont renommés avec l'extension .locked, et que le message de rançon apparaît.

**Étape 3 : Propagation dans l'environnement cible (Lab 1)**

**Scénario 1 : E-mail avec pièce jointe auto-exécutable**

1. **Envoi d'un e-mail avec la pièce jointe** :

☑Depuis la machine **Kali-Linux-Attaquant**, préparez un e-mail contenant l'archive ZIP **Documents_Importants.zip** avec l'exécutable malveillant en pièce jointe.

☑Utilisez un client de messagerie ou un outil comme **msmtp** pour envoyer cet e-mail.

2. **Compromission de la machine cible dans l'environnement de Lab 1** :

☑Sur la machine virtuelle Windows de **Lab 1**, ouvrez le client de messagerie et téléchargez la pièce jointe.

☑Exécutez le fichier pour lancer le ransomware simulé.

**Scénario 2 : E-mail avec lien pour téléchargement malveillant**

1. **Hébergement du fichier malveillant** :

☑Utilisez **Apache** sur Kali Linux pour héberger l'exécutable malveillant.

☑Le fichier sera accessible via l'URL http://your_kali_ip/ransomware_simule.exe.

2. **Envoi d'un e-mail avec un lien** :

☑Préparez un e-mail contenant un lien vers le fichier hébergé sur le serveur Kali Linux.

3. **Compromission de la machine cible dans l'environnement de Lab 1** :

☑Sur la machine virtuelle Windows de **Lab 1**, ouvrez le client de messagerie et cliquez sur le lien.

☑Téléchargez le fichier et exécutez-le pour lancer le ransomware simulé.

**Étape 4 : Capture des résultats**

1. **Captures d'écran** :

☑Prenez des captures d'écran à chaque étape : création du script sur Kali Linux, test du ransomware sur la machine virtuelle **Windows-Test**, envoi de l'e-mail malveillant, et exécution finale du ransomware sur la machine cible de **Lab 1**.

2. **Rapport d'exécution** :

☑Documentez toutes les étapes du processus dans un rapport. Ce rapport doit inclure les captures d'écran, une explication de chaque étape, et une analyse des résultats.

**Note :** Le Lab2 sera présentée 7 jours après le Lab1, assorti du rapport d'exécution.

## 5.3 Lab3: Simulation d'Attaques sur l'Application Web dans la DMZ

### 5.3.1 Objectifs

Ce lab a pour objectif de simuler différentes attaques contre l'application web présente dans la DMZ de l'environnement de **Lab 1**. Les étudiants utiliseront l'environnement d'attaque de **Lab 2** pour concevoir des malwares et des attaques ciblées sur l'application. L'objectif est de comprendre les techniques d'attaque des applications web, même protégées dans une DMZ.

### 5.3.2 Prérequis

- ☑ **Environnement de Lab 1** (incluant l'application web dans la DMZ).
- ☑ **Environnement d'attaque de Lab 2** (machine Kali Linux utilisée pour préparer les attaques).
- ☑ Outils d'attaque web disponibles sur Kali Linux (machine virtuelle Kali-Linux-Attaque du Lab2) :
  - **OWASP ZAP** ou **Burp Suite** : Proxy pour analyse et manipulation du trafic HTTP.
  - **SQLMap** : Pour les attaques d'injection SQL.
  - **Hydra** : Pour les attaques par force brute sur les authentifications.
  - **Metasploit** : Pour l'exploitation de vulnérabilités.
  - **Nikto** : Scanner de vulnérabilités web.

### 5.3.3 Details des étapes

**Étape 1 : Identification des Vulnérabilités de l'Application Web avec Nikto**

1. **Lancer un scan Nikto** :

   Utilisez **Nikto** pour scanner l'application web dans la DMZ et découvrir des vulnérabilités connues telles que des versions obsolètes, des scripts vulnérables, ou des configurations dangereuses.

2. **Analyser les résultats** :

   Notez les vulnérabilités identifiées, y compris celles liées à des pages d'administration exposées, des fichiers sensibles non protégés ou des versions vulnérables de logiciels web.

**Étape 2 : Attaques par Injection SQL avec SQLMap**

1. **Test d'injection SQL** :

Utilisez **SQLMap** pour tester l'application web pour des vulnérabilités d'injection SQL. Cette technique permet aux attaquants d'exécuter des requêtes SQL non autorisées pour accéder ou modifier des données dans la base de données.

2. **Analyse des résultats** :

   Si SQLMap trouve une vulnérabilité, documentez les bases de données accessibles, les tables et les colonnes. Tentez de récupérer des informations sensibles comme des utilisateurs ou des mots de passe stockés.

3. **Exploitation de la vulnérabilité SQL** :

   Essayez d'exploiter davantage cette faille en utilisant SQLMap pour obtenir un shell sur le serveur web ou en manipulant les données directement dans la base.

**Étape 3 : Attaques par Force Brute sur les Pages d'Authentification avec Hydra**

1. **Identification des pages d'authentification** :

   Utilisez les résultats du scan Nikto ou OWASP ZAP pour identifier les **pages d'authentification** sur l'application web (par exemple, les pages de login ou d'administration).

2. **Attaque par force brute avec Hydra** :

   Utilisez **Hydra** pour tenter une attaque par force brute sur ces pages d'authentification, en essayant plusieurs combinaisons d'identifiants et de mots de passe.

3. **Résultats de l'attaque** :

   Si l'attaque réussit, documentez les identifiants compromis et analysez ce que cela permet d'accomplir dans l'application (par exemple, accès à l'interface d'administration).

**Étape 4 : Manipulation du Trafic et Exploitation des Vulnérabilités avec OWASP ZAP ou Burp Suite**

1. **Configuration de OWASP ZAP ou Burp Suite comme proxy**

☑ **Lancer OWASP ZAP ou Burp Suite** :

- Lancez **OWASP ZAP** ou **Burp Suite** sur la machine **Kali-Linux-Attaque**.
- Configurez le proxy HTTP pour intercepter le trafic entre votre navigateur et l'application web située dans la DMZ. Cela permet d'examiner, modifier et rejouer les requêtes HTTP.

☑ **Configuration du navigateur pour utiliser le proxy** :

- Ouvrez un navigateur web sur la machine **Kali-Linux-Attaque** et configurez-le pour passer par le proxy de **ZAP** ou **Burp Suite**

2. **Analyse des requêtes et réponses**

☑ **Intercepter une requête HTTP**

- Accédez à l'application web dans la DMZ via le navigateur configuré. OWASP ZAP ou Burp Suite interceptera chaque requête HTTP envoyée au serveur.
- Examinez la requête : cherchez les paramètres envoyés avec la requête, les types de données soumises, et le contenu des cookies.

☑ **Manipulation des requêtes** :

- Modifiez les paramètres dans la requête HTTP interceptée pour tester les **failles de validation des entrées**. Par exemple, injectez des caractères spéciaux dans des champs de saisie pour tenter d'exploiter des failles d'injection SQL ou **Cross-Site Scripting (XSS)**.
- Envoyez la requête modifiée au serveur et observez la réponse pour voir si la manipulation a réussi.

3. **Exploitation des vulnérabilités**

☑ **Exploitation des failles XSS (Cross-Site Scripting)** :

- Si l'application ne valide pas correctement les entrées utilisateur, injectez un **script JavaScript** malveillant dans un champ de saisie.
- Si la faille existe, le script sera exécuté dans le navigateur de l'utilisateur, montrant une alerte.

☑ **Exploitation des failles CSRF (Cross-Site Request Forgery)**

- Créez un **formulaire HTML malveillant** qui force un utilisateur connecté à exécuter une action sans son consentement, comme changer un mot de passe. Utilisez OWASP ZAP ou Burp Suite pour injecter ce formulaire dans une page vulnérable.

4. **Attaques supplémentaires**

☑ **Manipulation des sessions**

- Interceptez les **cookies de session** dans les requêtes HTTP et essayez de les utiliser pour voler ou usurper une session active (session hijacking).
- Modifiez les valeurs de cookies pour voir si l'application accepte des valeurs non valides ou permet des actions non autorisées.

**Étape 5 : Exploitation des Vulnérabilités avec Metasploit**

1. **Recherche d'exploits dans Metasploit**

☑ **Lancer Metasploit** :

- Ouvrez Metasploit sur la machine **Kali-Linux-Attaque**

☑ **Recherche des vulnérabilités spécifiques** :

- Utilisez les informations recueillies avec **Nikto**, **SQLMap**, ou **OWASP ZAP** pour rechercher des **exploits** dans Metasploit correspondant aux vulnérabilités détectées.
- Par exemple, si Nikto a identifié une version vulnérable d'un **CMS** ou d'un serveur.

2. **Exploitation d'une vulnérabilité**

☑ **Sélection d'un exploit** :

- Après avoir trouvé un exploit correspondant à la vulnérabilité, sélectionnez-le dans Metasploit

☑ **Configuration de l'exploit** :

- Configurez les paramètres de l'exploit, comme l'URL cible, les options de payload (code à exécuter), et le port du serveur cible.

☑ **Lancer l'exploit :**

- Une fois les paramètres configurés, lancez l'exploit pour tenter de compromettre l'application .

☑ **Obtenir un accès shell sur le serveur web :**

- Si l'exploit est réussi, vous pourrez obtenir un shell interactif sur le serveur web. Cela vous permet de contrôler directement le système de l'application web.

☑ **Exploration des fichiers et ressources sensibles :**

- Une fois connecté au shell, explorez les fichiers sensibles du serveur, récupérez les fichiers de configuration, les bases de données, ou tout autre fichier utile pour l'attaque.
- Par exemple, vous pouvez rechercher des fichiers de configuration contenant des identifiants de base de données ou d'autres services.

**Étape 6 : Capture des Résultats et Analyse**

1. **Documentation des attaques réussies**

☑ Captures d'écran à chaque étape des attaques réussies, y compris :

- Les résultats des scans de vulnérabilités (Nikto, SQLMap, etc.).
- Les manipulations du trafic via OWASP ZAP ou Burp Suite.
- Les attaques de force brute réussies via Hydra.
- Les exploits réussis dans Metasploit (y compris l'obtention d'un shell).

☑ **Résumé des failles exploitées, décrivez les points suivants :**

- Description de la faille : La nature de la vulnérabilité (injection SQL, XSS, session hijacking, etc.).
- Méthode d'exploitation : Les outils utilisés et les étapes suivies pour exploiter la faille.
- Impact : L'impact potentiel de la faille exploitée dans un environnement réel (accès à des informations sensibles, compromission du serveur, etc.).

2. **Résumé global des résultats**

☑ État des vulnérabilités : Indiquez combien de vulnérabilités ont été identifiées et combien ont été exploitées avec succès.

☑ Évaluation de la sécurité de l'application : Donnez une évaluation globale de la sécurité de l'application web, basée sur les résultats des attaques et sur la facilité ou la difficulté à exploiter les vulnérabilités.

**Étape 7 : Rapport détaillé**

1. Un rapport décrivant toutes les attaques menées sur l'application web, incluant les captures d'écran et les résultats des outils utilisés (Nikto, SQLMap, Hydra, Metasploit, etc.).
2. Résumé des vulnérabilités identifiées et exploitées, avec une analyse des impacts potentiels.
3. Proposez des recommandations précises et pratiques pour corriger les vulnérabilités identifiées.
4. Priorisez les actions à mettre en œuvre pour améliorer la sécurité de l'application et du serveur web.

**Note :** Le Lab3 sera présenté 7 jours après le Lab2, assorti du rapport d'execution

## 5.4 Lab4: Simulation Audit de Sécurité de l'Environnement du Lab1

### 5.4.1 Objectifs

L'objectif de ce lab est de conduire un audit de sécurité complet de l'environnement réseau configuré dans **Lab 1**. Les étudiants doivent identifier les failles et vulnérabilités dans l'infrastructure, y compris celles liées à l'application web située dans la DMZ, et formuler des recommandations pour éviter qu'une attaque similaire à celle simulée dans **Lab 2** ne se reproduise.

### 5.4.2 Prérequis

- ☑ **Environnement réseau** de **Lab 1** (machine virtuelle Windows, DMZ avec serveur web Linux, routeur, firewall).
- ☑ **Outils d'audit de sécurité disponibles sur Kali Linux** :
  - **Nmap :** Analyse des ports et des services ouverts.
  - **OpenVAS ou Nessus :** Scanner de vulnérabilités pour détecter les failles sur les systèmes.
  - **Nikto :** Scanner de vulnérabilités pour les serveurs web.
  - **Wireshark :** Analyse réseau.
  - **Metasploit (optionnel)** : Exploitation des vulnérabilités.
- ☑ **Caractéristiques minimales des machines virtuelles :**
- ☑ **Machine virtuelle Kali Linux (Audit de sécurité)** :
  - **Nom :** Kali-Linux-Audit
  - **Disque dur :** 10 Go
  - **RAM :** 2 Go
  - **OS :** Kali Linux (dernière version)
  - **Logiciels nécessaires :** Nmap, OpenVAS, Nikto, Metasploit, Wireshark

### 5.4.3 Details des étapes

**Étape 1 : Audit du Réseau avec Nmap**

1. **Scan de l'infrastructure réseau** :

☑ Utilisez **Nmap** pour scanner l'infrastructure réseau complète. Ce scan doit inclure tous les équipements présents dans l'environnement de **Lab 1** : routeur, switch, firewall, machines dans le réseau local et dans la DMZ.

2. **Découverte des ports ouverts et services actifs** :

☑ Identifiez les ports ouverts sur chaque machine et les services associés.

☑ Documentez tous les ports ouverts, en particulier sur la machine **Windows-Victim** et le serveur Linux dans la DMZ.

3. **Identification des services vulnérables** :

☑ Notez les services qui peuvent être potentiellement vulnérables (services non sécurisés, versions obsolètes, etc.).

**Étape 2 : Scanner de Vulnérabilités avec OpenVAS ou Nessus**

1. **Configuration et exécution d'un scan de vulnérabilités** :

☑ Lancez **OpenVAS** ou **Nessus** sur la machine **Kali-Linux-Audit** et configurez un scan complet de l'infrastructure.
☑ Exécutez un scan de vulnérabilités sur :
- La machine Windows compromise (de **Lab 1**).
- Le serveur Linux dans la DMZ.
- Les équipements de réseau (routeur, firewall).

2. **Analyse des résultats** :

☑ Examinez les vulnérabilités détectées, en particulier celles de **haute** et **critique** sévérité.

☑ Documentez les vulnérabilités trouvées et associez-les aux composants de l'infrastructure.

3. **Exploration des failles critiques** :

☑ Pour chaque faille critique identifiée, expliquez en quoi elle pourrait être exploitée par un attaquant.

**Étape 3 : Audit de Sécurité de l'Application Web avec Nikto**

1. **Scan de l'application web** :

☑ Utilisez **Nikto** pour scanner l'application web située sur le serveur dans la DMZ. Ce scan permettra d'identifier les vulnérabilités spécifiques aux applications web (failles dans les scripts, configurations inadéquates, versions de CMS vulnérables, etc.).

2. **Analyse des vulnérabilités web** :

☑ Notez les vulnérabilités détectées, telles que les mauvaises configurations, les scripts vulnérables, ou les pages d'administration non sécurisées.

☑ **CMS** : Si l'application utilise un **CMS** (WordPress, Joomla, etc.), vérifiez les vulnérabilités spécifiques à la version du CMS.

3. **Recherche de vulnérabilités supplémentaires** :

☑ En complément de Nikto, utilisez un outil comme **OWASP ZAP** ou **Burp Suite** pour tester la sécurité de l'application web, notamment pour détecter les failles comme l'injection SQL ou le Cross-Site Scripting (XSS).

**Étape 4 : Surveillance et Analyse du Réseau avec Wireshark**

1. **Capture du trafic réseau** :

☑ Utilisez **Wireshark** pour capturer et analyser le trafic réseau entre les machines de l'infrastructure.

☑ Portez une attention particulière au trafic entre l'application web dans la DMZ et les machines extérieures au réseau.

2. **Analyse des connexions suspectes** :

☑ Recherchez des connexions non sécurisées, des paquets chiffrés ou tout autre trafic suspect qui pourrait indiquer une tentative d'attaque ou de fuite d'informations.

**Étape 5 : Exploitation des Vulnérabilités avec Metasploit (Optionnel)**

1. **Exploitation des vulnérabilités critiques** :

☑ Si des vulnérabilités critiques ont été identifiées (par exemple, une version obsolète d'un service), vous pouvez utiliser **Metasploit** pour simuler une attaque et vérifier leur exploitabilité.

2. **Simulation d'attaque** :

☑ Utilisez Metasploit pour tenter une exploitation sur les services vulnérables détectés lors de l'audit. Cette étape permet de valider si les vulnérabilités identifiées sont exploitables dans l'environnement de production.

**Étape 6 : Rapport détaillé**

☑ Résumez toutes les failles identifiées dans l'environnement de **Lab 1** et dans l'application web.

☑ Présentez les vulnérabilités classées par niveau de criticité (faible, moyen, élevé, critique).

☑ Pour chaque faille identifiée, proposez une recommandation concrète pour corriger la vulnérabilité.

☑ Incluez un **plan d'action priorisé** pour guider les actions correctives à mener en premier.

**Note :** Le Lab4 sera présenté 7 jours après le Lab3, assorti du rapport d'exécution.

## 5.5 Lab5: Analyse Post-Compromission après une Attaque par Ransomware : Ma première investigation numérique

### 5.5.1 Objectifs

Ce lab a pour objectif de conduire une analyse post-compromission suite à une attaque par ransomware dans l'environnement de **Lab 1**. Les étudiants utiliseront des outils d'investigation numérique pour examiner les traces laissées par l'attaque, identifier les signes de compromission, et tenter de remonter aux responsables de l'attaque en analysant les e-mails et en utilisant des outils d'investigation OSINT (Open-Source Intelligence).

### 5.5.2 Prérequis

- ☑ **Environnement réseau** de **Lab 1** dans lequel l'attaque simulée a eu lieu (machine virtuelle Windows compromise).
- ☑ **Nouvelle machine virtuelle Kali Linux** pour l'analyse post-compromission (distincte de la machine attaquante de Lab 2).
- ☑ Outils d'investigation numérique disponibles sur **Kali Linux** :
  - **Autopsy** (analyse de disque)
  - **Wireshark** (analyse réseau)
  - **Volatility** (analyse mémoire)
  - **Foremost** (récupération de fichiers supprimés)
  - **Maltego** (outil OSINT pour la recherche de responsables)
  - Analyse des entêtes d'e-mails

1. **Création de l'environnement d'analyse**

☑ **Création d'une nouvelle machine virtuelle Kali Linux (Kali-Linux-Analyse)** :

☑ Dans GNS3, créez une nouvelle machine virtuelle **Kali Linux** dédiée à l'analyse post-compromission.

☑ Installez tous les outils nécessaires à l'investigation numérique (Autopsy, Wireshark, Volatility, Maltego, etc.).

2. **Caractéristiques minimales des machines virtuelles :**

☑ **Machine virtuelle Kali Linux (Analyse post-compromission)** :

- **Nom** : Kali-Linux-Analyse
- **Disque dur** : 10 Go
- **RAM** : 2 Go

- **OS** : Kali Linux
- **Logiciels nécessaires** : Autopsy, Wireshark, Volatility, Foremost, Maltego
- **Connectivité réseau** : Accès au réseau pour analyser les fichiers extraits de la machine compromise.

☑ **Machine virtuelle Windows compromise** (Lab 1) :

- **Nom** : Windows-Victim
- **Disque dur** : 10 Go (ou plus si des données volumineuses sont présentes)
- **RAM** : 2 Go
- **OS** : Windows 10 ou supérieur
- **Rôle** : Cette machine a été victime de l'attaque simulée dans le Lab 2.

### 5.5.3 Details des étapes

**Étape 1 : Sauvegarde de l'image du disque**

1. **Création d'une image disque** :

☑ Utilisez un outil comme **dd** pour créer une image complète du disque de la machine compromise, afin d'éviter toute altération des preuves : **windows_victim.img**

2. **Validation de la sauvegarde** :

☑ Assurez-vous que l'image a été correctement créée et est prête à être analysée dans Autopsy.

**Étape 2 : Analyse avec Autopsy**

1. **Lancement d'Autopsy** :

☑ Lancez Autopsy sur votre machine Kali Linux

2. **Création d'un nouveau cas et importation de l'image disque** :

☑ Créez un nouveau cas dans Autopsy et importez l'image **windows_victim.img**.

3. **Analyse des artefacts Windows** :

☑ **Recherche des fichiers récemment modifiés** : Identifiez les fichiers chiffrés par le ransomware (ex. .locked).

☑ **Examen des logs du système** : Analysez les journaux système pour rechercher des connexions suspectes ou des modifications de fichiers critiques.

☑ **Analyse des programmes exécutés** : Listez les programmes récemment exécutés pour trouver des indices sur les activités malveillantes.

**Étape 3 : Analyse réseau avec Wireshark**

1. **Capture et analyse du trafic réseau** :

☑ Exécutez Wireshark sur la machine compromise pour capturer les communications réseau actuelles ou utilisez une capture précédente si elle existe.

☑ **Recherche de connexions suspectes** : Analysez le trafic réseau pour identifier les connexions externes suspectes ou des paquets chiffrés liés à l'activité du ransomware.

**Étape 4 : Analyse mémoire avec Volatility**

1. **Capture de l'image mémoire** :

☑ Utilisez un outil comme **DumpIt** pour capturer l'image mémoire de la machine compromise et l'importer dans Volatility.

2. **Utilisation de Volatility** :

☑ Analysez l'image mémoire pour rechercher des processus suspects et des connexions réseau actives au moment de l'attaque.

**Étape 5 : Analyse des logs système et récupération de fichiers**

1. **Analyse des logs** :

☑ Utilisez des outils comme **Sleuthkit** ou **Autopsy** pour examiner les logs Windows et repérer des événements suspects.

2. **Récupération de fichiers supprimés avec Foremost** :

☑ Utilisez **Foremost** pour récupérer des fichiers supprimés par le ransomware :

**Étape 6 : Recherche des responsables de l'attaque**

1. **Analyse des e-mails et des entêtes**

☑ **Extraction des e-mails suspectés** :

- Utilisez **Autopsy** pour extraire les e-mails reçus sur la machine compromise. Recherchez les communications demandant une rançon.

☑ **Analyse des entêtes d'e-mails** :

- Examinez les entêtes des e-mails suspects pour obtenir des informations sur l'expéditeur (adresse e-mail, adresse IP des serveurs).

2. **Recherche OSINT avec Maltego**

☑ **Lancement de Maltego** :

- Lancez Maltego sur Kali Linux pour rechercher des informations sur l'adresse e-mail identifiée.

☑ **Analyse de l'adresse e-mail** :

- Utilisez Maltego pour rechercher des informations associées à l'adresse e-mail, telles que des comptes de réseaux sociaux ou des forums où cette adresse est active.

3. **Recherche dans les bases de données de ransomwares**

☑ **Consultation des bases de données publiques** :

- Utilisez des ressources comme **ID Ransomware** ou **Ransomware Tracker** pour rechercher l'adresse e-mail ou l'empreinte du ransomware.

☑ **Résultats des bases de données** :

- Documentez si l'adresse e-mail ou le ransomware sont associés à des groupes d'attaquants connus.

**Étape 7 : Rapport d'analyse**

☑ Documentez vos découvertes avec des captures d'écran de chaque étape clé : analyse des disques, analyse réseau, analyse mémoire, et recherches OSINT.

☑ Fournissez un rapport complet détaillant toutes les étapes suivies, les résultats obtenus, et les recommandations pour prévenir ce type d'attaque.

**Note :** Le Lab5 sera présenté 7 jours après le Lab4, assorti du rapport d' exécution.

## 6. Modèle de Rapport

### I. Introduction

☑ **Nom de l'étudiant** :

☑ **Date** : date la soumission du rapport

☑ **Environnement analysé** : (ex. Windows 10 – Machine victime dans Lab 1, donner une description plus fournie)

☑ **Objectif du rapport** :

Ce rapport documente l'analyse post-compromission réalisée à la suite de l'attaque par ransomware simulée dans l'environnement de **Lab 1**. L'objectif est d'identifier les traces laissées par l'attaque, de comprendre le comportement du ransomware, de rechercher l'origine des e-mails utilisés et de tenter d'identifier les responsables de l'attaque.

### II. Méthodologie

Décrivez ici les étapes générales de votre analyse, les outils utilisés, et la méthodologie suivie pour l'investigation.

### III. Outils utilisés :

☑ **Autopsy** : Analyse de l'image du disque
☑ **Wireshark** : Capture et analyse du trafic réseau
☑ **Volatility** : Analyse de l'image mémoire
☑ **Foremost** : Récupération de fichiers supprimés
☑ **Maltego** : Recherche d'informations OSINT sur les e-mails suspects
☑ **Analyse des entêtes d'e-mails**

### IV. Étapes d'investigation :

1. Sauvegarde de l'image du disque de la machine compromise.
2. Analyse du disque avec Autopsy pour rechercher les artefacts du ransomware.
3. Analyse du trafic réseau avec Wireshark.
4. Analyse de l'image mémoire avec Volatility.
5. Extraction et analyse des logs systèmes et récupération des fichiers supprimés.
6. Recherche des responsables de l'attaque en analysant les e-mails et en utilisant des outils OSINT.

### A. Sauvegarde de l'image du disque

Décrivez ici comment vous avez effectué la sauvegarde de l'image du disque de la machine compromise. Incluez la commande utilisée pour créer l'image disque, et précisez la taille de celle-ci.

### B. Analyse avec Autopsy

Décrivez ici comment vous avez configuré Autopsy pour analyser l'image disque et les artefacts que vous avez trouvés.

Précisez les découvertes importantes (fichiers modifiés, exécution suspectes, artefacts systèmes, fichiers récupérés)

### C. Analyse réseau avec Wireshark

Décrivez ici comment vous avez configuré Wireshark pour capturer et analyser le trafic réseau. Notamment la durée de la capture, les différents filtres utilisés, les connexions suspectes, les paquets chiffrés ou non autorisés.

### D. Analyse mémoire avec Volatility

Décrivez ici comment vous avez capturé l'image mémoire de la machine compromise et comment vous l'avez analysée. Précisez les processus suspects, les connexions réseau découvertes.

### E. Analyse des logs système

Décrivez ici les logs du système que vous avez extraits et analysés (par exemple, les logs des événements Windows). Mentionnez toute anomalie repérée dans ces logs.

### F. Récupération de fichiers avec Foremost

Si vous avez utilisé **Foremost** pour récupérer des fichiers supprimés, mentionnez ici les fichiers récupérés et leurs extensions.

### G. Recherche des responsables de l'attaque

Décrivez ici comment vous avez analysé les e-mails envoyés par l'attaquant, et ce que vous avez découvert dans les entêtes d'e-mails (adresse IP, adresses e-mails des expéditeurs, etc.).

Mentionnez les e-mails que vous avez identifiés comme suspects (liés à l'attaque).

Expliquez ici comment vous avez utilisé **Maltego** pour rechercher des informations sur l'adresse e-mail identifiée.

Résumez les informations trouvées, telles que des comptes de réseaux sociaux, des forums, ou toute autre information liée à l'adresse e-mail de l'attaquant.

Mentionnez ici si vous avez trouvé des informations sur l'e-mail ou le ransomware dans des bases de données publiques comme **ID Ransomware** ou **Ransomware Tracker**.

## V. 10. Conclusion

Fournissez ici un résumé des conclusions tirées de l'analyse.

☑ **Comportement du ransomware** :
Décrivez ce que vous avez découvert sur le comportement du ransomware (comment il chiffre les fichiers, comment il communique avec des serveurs externes, etc.).

☑ **Identité ou traces de l'attaquant** :
Mentionnez toute information pertinente obtenue sur l'identité ou la localisation potentielle des attaquants. Indiquez également si l'adresse e-mail a été utilisée dans d'autres attaques connues.

☑ **Recommandations** :
Mentionnez les recommandations générales pour éviter ce type de compromission à l'avenir (utilisation d'antivirus, surveillance réseau, etc.).

## VI. 11. Annexes

Ajoutez ici toutes les captures d'écran pertinentes et les fichiers logs obtenus pendant l'analyse. Vous pouvez également inclure des fichiers récupérés comme annexes.

**Note :** Le Rapport d' Expertise sera présenté 7 jours après le Lab5, et défendu publiquement.

## 7. Conclusion Générale

Les Labs d'Investigation Numérique que nous avons explorés à travers ce document permettent aux étudiants de s'immerger dans des scénarios réalistes de cybersécurité, les amenant à comprendre et maîtriser à la fois les techniques d'attaque et de défense. Ces travaux pratiques offrent une opportunité unique de mettre en œuvre les connaissances théoriques acquises en cours, tout en les confrontant aux défis pratiques des environnements professionnels.

Les étudiants ont été amenés à construire des environnements réseau sécurisés, à créer et tester des malwares, à analyser des systèmes compromis et à auditer des infrastructures réseau pour détecter des failles et proposer des recommandations de sécurité. Chaque étape leur a permis de développer des compétences essentielles en sécurité informatique, incluant la configuration de systèmes sécurisés, l'investigation numérique, et la simulation d'attaques, le tout dans un cadre éthique et légal strict.

Ces labs contribuent non seulement à renforcer la capacité des étudiants à détecter et réagir aux cyberattaques, mais aussi à leur inculquer une méthodologie rigoureuse pour la prévention, l'analyse et la résolution d'incidents. L'objectif ultime de ces exercices est de former des professionnels capables de protéger efficacement les systèmes d'information dans des environnements de production.

En fin de compte, les Labs d'Investigation Numérique représentent une approche complète pour renforcer les compétences pratiques des étudiants, les préparant ainsi à affronter les défis croissants de la sécurité des systèmes d'information. Grâce à ces travaux pratiques, les futurs experts en sécurité sont mieux armés pour protéger les organisations contre les menaces numériques et pour répondre de manière proactive aux incidents de sécurité.

*« Like a conscientious and methodical craftsman, every day, refine your practice. Only in this way will you be and remain an Expert. »*

***Thierry MINKA***