

Rapport de Pentest et Analyse de Conformité RGPD

**Identification et Gestion des Vulnérabilités au sein du Système d'Information**

Eloham Caron

Bts Sio Option SISR

Date de l’intervention : 13/10/2022 et 14/12/2023

Date de Soumission : 10/03/2024

Destiné à : Jean-François Revel Bruno-Drogue, Proviseur Algoud.

Confidentialité : Ce document contient des informations sensibles et confidentielles. Sa diffusion est limitée aux personnes autorisées par Algoud Laffemas

Table des matières

[I. Contexte et objectif 4](#_Toc162884707)

[A. Ressources humaines : 4](#_Toc162884708)

[B. Contexte actuel 4](#_Toc162884709)

[II. Méthodologie PTES et Build 5](#_Toc162884710)

[1. Approche éthique : 5](#_Toc162884711)

[B. Accent sur la communication : 5](#_Toc162884712)

[C. Build : archives de l’ensemble des travaux 5](#_Toc162884713)

[III. Reconnaissance : OSINT 7](#_Toc162884714)

[1. Absence de frontière entre les différentes classes de données 7](#_Toc162884715)

[2. Utilisation de Maltego 7](#_Toc162884716)

[3. Interrogation des sources de données : 8](#_Toc162884717)

[4. Corrélation et visualisation des données : 8](#_Toc162884718)

[5. Analyse des relations : 8](#_Toc162884719)

[A. Schéma simplifié d'analyse Maltego 9](#_Toc162884720)

[B. Schéma des informations liées au domaine pouvant être utilisées pour du phishing 10](#_Toc162884721)

[IV. Enumeration : analyse des menaces 13](#_Toc162884722)

[A. Utilisation de l’outil Nmap : 13](#_Toc162884723)

[B. Outil Searchsploit : 14](#_Toc162884724)

[C. Conclusion : Importance de l'Énumération pour la Sécurité du Réseau 17](#_Toc162884725)

[V. Exploitation : Les failles exploitées : 18](#_Toc162884726)

[A. Exploitation via Command Prompt (cmd) due à une gestion défaillante des droits d'accès : 18](#_Toc162884727)

[1. Exploitation des autorisations de serveur par le biais d'un raccourci : 18](#_Toc162884728)

[2. Exécution privilégiée et contournement des restrictions : 18](#_Toc162884729)

[3. Absence de limitations et implications de sécurité : 18](#_Toc162884730)

[4. Les journaux sont sous forme de fichiers .cmd et sont facilement accessibles avec l'exploit. 18](#_Toc162884731)

[5. Conclusion de la méthodologie : 18](#_Toc162884732)

[6. Recommandations : 19](#_Toc162884733)

[B. Vulnérabilités d'Exploitation du Routeur Cisco Meraki et du Serveur HTTP Lighttpd 19](#_Toc162884734)

[1. Contournement de mots de passe lors de la Deuxième Exploitation du Routeur 19](#_Toc162884735)

[2. Conclusion sur l’exploit : 20](#_Toc162884736)

[C. Exploit Attaque par Injection JavaScript : 21](#_Toc162884737)

[1. Conclusion 22](#_Toc162884738)

[2. Recommandations : 22](#_Toc162884739)

[D. Exploitation d'une Faille de Sécurité dans la Boîte à Outils d'Atos 22](#_Toc162884740)

[1. Conclusion : 25](#_Toc162884741)

[2. Recommandations 25](#_Toc162884742)

[E. Exploit de sécurité : vulnérable à une attaque web 25](#_Toc162884743)

[1. Possibilité de copier tous les fichiers et leurs corrections. 26](#_Toc162884744)

[F. Attaque par canal latéral via une imprimante réseau 26](#_Toc162884745)

[1. Imprimante HP : 28](#_Toc162884746)

[2. Les failles non exploitées 31](#_Toc162884747)

[3. Possible usurpation d’identité 31](#_Toc162884748)

[4. Risque de brute force : 33](#_Toc162884749)

[5. Utilisation de l’outils Hydra : 36](#_Toc162884750)

[VI. Phase de post-exploitation : analyse : 37](#_Toc162884751)

[A. Exploits et Vulnérabilités Identifiées : 37](#_Toc162884752)

[B. Recommandations pour améliorer la Sécurité : 38](#_Toc162884753)

[VII. RGPD 39](#_Toc162884754)

[A. Violation des principes de confidentialité et d'intégrité (Article 5 [1] f du RGPD) 39](#_Toc162884755)

[B. Manquement à l'obligation de sécurité des données (Article 32 du RGPD) 40](#_Toc162884756)

[C. Violation du principe de limitation de l'usage (Article 5 [1] b du RGPD) 40](#_Toc162884757)

[1. Conséquences et risques pour l'établissement : 40](#_Toc162884758)

[D. Notifications obligatoires (Articles 33 et 34 du RGPD) 40](#_Toc162884759)

[E. Sanctions administratives (Article 83 du RGPD) 41](#_Toc162884760)

[F. Répercussions sur la réputation 41](#_Toc162884761)

[G. Actions recommandées : 41](#_Toc162884762)

[VIII. Conclusion du rapport. 41](#_Toc162884763)

[IX. RECOMMANDATION RGPD : 42](#_Toc162884764)

[A. Recommandation concernant le RGPD 42](#_Toc162884765)

[1. Modules de la CNIL sur le RGPD : 42](#_Toc162884766)

[2. MOOC de l'ANSSI sur la sécurité numérique : 42](#_Toc162884767)

[X. Proposition de changement du réseau : 43](#_Toc162884768)

[XI. Outils, sources et bibliographie : 44](#_Toc162884769)

[A. Les outils utilisés comprennent : Hydra : 44](#_Toc162884770)

[B. RGPD : 44](#_Toc162884771)

[C. Vulnérabilité : 44](#_Toc162884772)

[XII. Tables des illustrations 45](#_Toc162884773)

# Contexte et objectif

L'établissement Algoud-Laffemas (cité scolaire Briffaut), basé à Valence dans l’académie de Grenoble, est le plus important de la région Auvergne-Rhône-Alpes. Il propose une large gamme de formations, allant de la Troisième Prépa-Métiers aux classes préparatoires et aux BTS, couvrant divers secteurs tels que les sciences, l'industrie et les services. Il joue un rôle clé dans la formation de professionnels qualifiés, contribuant ainsi au développement économique de la région. De plus, en favorisant l'inclusion sociale et en offrant des opportunités éducatives diversifiées, il contribue également au progrès social de la communauté.[[1]](#footnote-1)

## Ressources humaines :

L'établissement compte entre 250 et 499 salariés, ce qui reflète son importance. Ce campus comprend les bâtiments Algoud et Laffemas, ainsi que le Greta, des formations en alternance ainsi qu’une classe d’ATS.

Dans le dans le cadre de ma formation BTS j’ai entrepris une mission de pentest sous le contrôle et les conseils de mon professeur Monsieur Bruno DROGUE qui m'a permis d'obtenir les autorisations nécessaires de façon à encadrer mon travail dans les limites légales.

## Contexte actuel

Le 21 mars 2024, une cyberattaque a ciblé une cinquantaine de lycées en Île-de-France, associées à des menaces d'attentat revendiquées faussement au nom de « l'État islamique ». Ces attaques ont exploité des vulnérabilités dans les Environnements Numériques de Travail (ENT), entraînant l'envoi massif de courriels menaçants à des élèves, enseignants et parents, et la suspension temporaire de l'accès à ces plateformes éducatives. Ces événements soulignent l'urgence et l'importance de notre mission de renforcement de la cybersécurité dans les infrastructures éducatives, mettant en lumière les risques réels et la nécessité d'une vigilance constante face à la cybermenace.[[2]](#footnote-2)

La structure actuelle des systèmes de messagerie de la région Auvergne-Rhône-Alpes, avec des adresses e-mail facilement identifiables et regroupées sous un même nom de domaine, augmente significativement le risque de subir des attaques de phishing. Des enseignants ont été ciblés par des attaques de phishing et certains se sont fait piéger. Quelques comptes ont été compromis.

L'objectif de cette mission consiste à identifier les failles de sécurité des systèmes informatiques de la cité scolaire Briffaut et de proposer des mesures pour les corriger. De plus, ce projet vise à démontrer les problèmes liés au RGPD que j'ai identifiés en amont.

# Méthodologie PTES[[3]](#footnote-3) et Build

La méthodologie PTES (Penetration Testing Execution Standard) est un ensemble de lignes directrices organisées pour mener à bien des tests d'intrusion de manière méthodique et efficace. Elle est largement reconnue dans l'industrie de la cybersécurité et vise à normaliser les pratiques de tests d'intrusion pour garantir une approche cohérente et rigoureuse. Voici une explication de son fonctionnement et de ses principes fondamentaux :

1. Organisation en phases : La méthodologie PTES est organisée en sept phases distinctes, chacune couvrant un aspect spécifique du processus de test d'intrusion. Ces phases sont conçues pour être exécutées de manière séquentielle, mais elles peuvent également être itératives en fonction des besoins du projet. Les sept phases sont :

* Pré-engagement : Définition des objectifs, du périmètre et de la portée du test.
* Reconnaissance : Collecte d'informations sur la cible, y compris des informations publiques et des analyses de vulnérabilité.
* Énumération : Évaluation des vulnérabilités et des risques pour déterminer les scénarios d'attaque.
* Exploitation : Utilisation des vulnérabilités identifiées pour accéder aux systèmes cibles.
* Post-exploitation : Maintien de l'accès aux systèmes compromis et collecte d'informations supplémentaires.
* Rapports et recommandations : Documentation des résultats du test et des recommandations pour remédier aux vulnérabilités découvertes.
* Archivage : Stockage sécurisé des données collectées pendant le test.

## Approche éthique :

La méthodologie PTES repose sur l'éthique et la légalité. Avant de commencer un test d'intrusion, une autorisation écrite doit être obtenue de la part du propriétaire des systèmes à tester. Cela garantit que le test est effectué légalement et dans le respect des lois et réglementations en vigueur.

## Accent sur la communication :

La méthodologie PTES met également l'accent sur la communication tout au long du processus. Il est essentiel de maintenir une communication ouverte avec les parties prenantes pour s'assurer que les objectifs du test sont clairement compris et que les résultats sont communiqués de manière efficace.

Voici les six phases de la méthodologie PTES (Penetration Testing Execution Standard) :

En résumé, la méthodologie PTES fournit un cadre structuré pour mener des tests d'intrusion de manière éthique, organisée et efficace. En suivant cette méthodologie, les professionnels de la cybersécurité peuvent identifier et atténuer les vulnérabilités dans les systèmes informatiques, contribuant ainsi à renforcer la sécurité globale des organisations.

## Build : archives de l’ensemble des travaux

L’ensemble des travaux est archivé dans un  « build ». Le build est structuré avec un compte rendu général et six sous-dossiers nommés comme suit, qui contiennent les ressources associées à chaque phase :

1\_Phase\_exploration : Ce dossier inclut les étapes initiales de reconnaissance et de collecte d'informations sur le système ou le réseau.

2\_Phase\_exploration\_approfondie : Ce dossier traite d'une exploration plus détaillée et d'une analyse approfondie du système ou du réseau.

**3\_Phase\_OSINT** : Ce dossier est consacré aux techniques d'Open-Source Intelligence pour recueillir et analyser des données publiquement accessibles.

**5\_Phase\_exploit** : Le nom suggère une erreur dans la séquence des dossiers, passant de la phase 3 directement à la phase 5, qui se concentre sur l'exploitation des vulnérabilités identifiées.

**6\_Phase\_exploit\_final** : Ce dossier contient des informations sur l'exploitation finale, y compris les résultats et l'impact de l'exploitation.

**Documentation** : Ce dossier est destiné à stocker des documents de référence, des guides et des procédures soutenant les phases d'exploitation.

Chaque dossier est marqué pour refléter une étape dans le processus de build, assurant un suivi et une organisation clairs du projet.

# Reconnaissance : OSINT

La phase OSINT (Open Source Intelligence) [[4]](#footnote-4)consiste à recueillir des informations sur la cible à partir de sources publiques telles que les moteurs de recherche, les réseaux sociaux, les forums en ligne, etc. L'objectif est d'obtenir des données utiles pour planifier les attaques et identifier les vulnérabilités.

Pour cette phase de reconnaissance, j'ai principalement utilisé l'outil **Maltego** ainsi que **l'explorateur** **de** **fichiers** de **Google** pour certaines recherches.

Les ressources relatives à cette partie sont disponibles dans le dossier du build 1\_Phase\_exploration

### Absence de frontière entre les différentes classes de données

Nous avons un accès libre au dossier des autres classes avec des droits totaux tels que la suppression, la copie, la lecture, etc. De plus, nous avons accès aux sauvegardes de l'établissement. Nous constatons donc un problème dans la configuration des droits utilisateurs.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, nombre  Description générée automatiquement |  |

Figure 1 : ressources partagées.

Une image contenant texte, Police, ligne, nombre

Description générée automatiquement

Figure 2 : autres ressources partagées.

Les fichiers de sauvegardes sont accessibles par tous les utilisateurs connectés, y compris les élèves.

### Utilisation de Maltego[[5]](#footnote-5)

Maltego est un logiciel de collecte et de visualisation de renseignements, développé par Paterva, utilisé dans le domaine de la sécurité informatique, de la police, de la gendarmerie et du renseignement. Il offre une interface graphique conviviale pour l'analyse et la corrélation des données provenant de différentes sources ouvertes, notamment des bases de données en ligne, des réseaux sociaux, des registres publics, des enregistrements DNS, etc.

Le fonctionnement de Maltego repose sur l'utilisation d'API (Interfaces de Programmation d'Applications) pour interroger et récupérer des données à partir de différentes sources. Actuellement, Maltego offre une intégration avec plus de 72 API, ce qui lui permet d'accéder à une vaste gamme de sources de données. Ces API fournissent des informations variées telles que des profils de réseaux sociaux, des enregistrements DNS, des données géographiques, des informations sur les noms de domaine, etc.

Voici comment fonctionne Maltego avec ces API :

### Interrogation des sources de données :

Maltego interagit avec les API pour interroger les différentes sources de données disponibles en ligne. Il envoie des requêtes aux API et récupère les informations pertinentes.

### Corrélation et visualisation des données :

Une fois les données récupérées, Maltego les organise et les visualise sous forme de graphiques. Il permet de représenter les relations entre les différentes entités (comme les personnes, les entreprises, les sites web, etc.) sous forme de nœuds et de liens.

### Analyse des relations :

Maltego permet aux utilisateurs d'analyser les relations entre les différentes entités pour détecter des schémas, des tendances ou des anomalies. Cela peut aider à identifier des connexions cachées ou des points faibles dans un système.

En raison de sa puissance et de sa polyvalence, Maltego est largement utilisé par les forces de l'ordre, les services de renseignement et les professionnels de la sécurité pour mener des enquêtes, des investigations et des analyses de renseignements. Son interface conviviale et ses capacités d'analyse avancées en font un outil précieux pour la collecte et l'analyse de données dans le domaine de la sécurité et de l'enquête.

## Schéma simplifié d'analyse Maltego

Une image contenant capture d’écran, ligne, diagramme, Parallèle

Description générée automatiquement

Figure 3 Analyse Maltego des DNS associés.

Sur ce schéma simplifié de l'analyse réalisée à l'aide de l'outil Maltego, on retrouve les serveurs DNS, les adresses IP et d'autres informations pertinentes pour l'énumération.

## Schéma des informations liées au domaine pouvant être utilisées pour du phishing

Figure 4 : Mail et contacts liés au nom de domaine ac-grenoble

.

L'avantage de Maltego réside dans sa capacité à fournir un résumé détaillé et plus lisible des informations. Dans cet exemple, nous avons une liste d'adresses IPv4 et les services associés, tels qu’Apache, Tomcat, Java, etc. Nous sommes déjà en phase d'énumération. Le logiciel se positionne entre l'OSINT et l'énumération, ce qui est souvent un défi pour les logiciels automatisés.

Une image contenant texte, nombre, capture d’écran

Description générée automatiquement

Figure 5 Adresse IPv4 publique de l'entreprise.

On trouve également ici les services de domaine associés, ce qui suggère que l'établissement n'héberge pas son site web lui-même, mais le fait héberger par la région Auvergne-Rhône-Alpes, qui est à son tour régie par nfrance.com.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Figure 6 Analyse régionale avec Maltego.

Une image contenant texte, capture d’écran

Description générée automatiquement

Figure 7 Liste des serveurs DNS

La capture que j'ai effectuée présente la liste des serveurs DNS associés, ainsi que des informations FTP utiles. Cette combinaison d'informations est précieuse, car elle fournit une vision holistique de l'infrastructure réseau de l'entreprise. Les serveurs DNS révèlent les adresses IP associées aux noms de domaine, ce qui peut être crucial pour identifier les points d'entrée potentiels dans le réseau. En outre, les détails FTP peuvent indiquer la présence de serveurs FTP accessibles, ce qui peut représenter une vulnérabilité si ces serveurs ne sont pas correctement sécurisés. En somme, cette capture fournit des données essentielles pour évaluer la sécurité et la robustesse du réseau de l'entreprise.

# Enumeration : analyse des menaces

L'objectif d'une phase d'énumération dans le cadre des PTES (Penetration Testing Execution Standard) est de collecter des informations détaillées sur les systèmes et les réseaux ciblés afin d'identifier des vulnérabilités potentielles et de préparer des attaques ciblées.

Dans cette phase, nous utiliserons les outils suivants :

- Nmap

- Searchsploit

- Metasploit

- Exploit DB

- Kali Linux

- Shell

- Batch scripting

## Utilisation de l’outil Nmap [[6]](#footnote-6):

Nmap est un outil de découverte de réseau et de scanner de ports largement utilisé dans le domaine de la cybersécurité. Il permet de découvrir les hôtes et les services sur un réseau informatique en envoyant des paquets IP et en analysant les réponses.

Nmap offre plusieurs fonctionnalités essentielles :

* **Découverte de réseau :** Il peut scanner un réseau pour trouver des hôtes actifs, en utilisant différentes techniques telles que le ping ICMP, le scan ARP, ou même des scans de port pour détecter les systèmes en ligne.
* **Scanner de ports :** Nmap peut scanner les ports d'un hôte pour déterminer quels services sont en cours d'exécution, quels ports sont ouverts et quelles versions de logiciels sont utilisées. Cela peut aider à identifier les vulnérabilités potentielles.
* **Fonctionnalités avancées :** Il offre des fonctionnalités avancées telles que la détection d'OS, la détection de versions de services, la prise en charge de scripts personnalisés (Nmap Scripting Engine) pour l'automatisation des tâches de sécurité, et plus encore.

Nmap est réputé pour sa rapidité et son efficacité, capable de scanner de grands réseaux en peu de temps. Son utilisation flexible le rend compatible avec plusieurs plateformes, y compris Windows, Linux et macOS, et peut être utilisé en ligne de commande ou avec des interfaces graphiques tierces. En résumé, Nmap est un outil puissant et polyvalent largement utilisé dans la cybersécurité pour la découverte et l'audit des réseaux.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Figure 8 Analyse avec Nmap 1

|  |  |
| --- | --- |
| Utilisation de la commande « nmap -sN » pour obtenir des détails plus techniques et intéressants. | Faiblesse repérer |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | On peut obtenir directement le modèle du routeur ainsi que le port sur lequel il est ouvert.  Le service lighthttpd nécessite une mise à jour.  La version de Linux est trop ancienne. |

Figure 9 : Analyse avec Nmap 2.

On constate que la version de Lighttpd n'a pas été mise à jour depuis 2019 et que la dernière mise à jour date de 2018. Les changements apportés en 2019 sont mineurs, et les failles de sécurité actuellement présentes sont nombreuses et répertoriées. De plus, le service n'est pas reconnu comme étant très sécurisé, surtout en l'absence de mises à jour, ce qui expose à de fortes vulnérabilités de 2018 à 2022. Une mise à jour vers des versions plus récentes serait bénéfique.

## Outil Searchsploit :

Searchsploit, intégré à [Kali Linux](https://www.kali.org/), [[7]](#footnote-7)est un outil en ligne de commande permettant de rechercher des exploits dans la base de données [Exploit Database (ExploitDB)[[8]](#footnote-8),](https://www.exploit-db.com/) gérée par Offensive Security. Cette base stocke une large gamme d'exploits, de shellcodes et de documents sur les vulnérabilités. Lorsqu'on lance une recherche avec Searchsploit, celui-ci interroge ExploitDB en fonction de critères tels que le logiciel, la version, etc., afin de trouver des exploits pertinents.

D'autre part, Metasploit[[9]](#footnote-9), un framework d'exploitation open source, utilise également ExploitDB comme source de référence pour tester les vulnérabilités. Metasploit offre une interface unifiée permettant de développer des exploits et de mener des attaques contre des systèmes cibles. Les exploits découverts avec Searchsploit peuvent être intégrés dans Metasploit pour exécuter des attaques ciblées.

En somme, Searchsploit facilite l'accès à ExploitDB, offrant aux chercheurs en sécurité une manière rapide de trouver des exploits adaptés à leurs besoins. Metasploit, quant à lui, fournit une plateforme complète pour exploiter ces vulnérabilités de manière contrôlée, en les intégrant dans des scénarios d'attaques spécifiques.

Une image contenant texte, capture d’écran, menu, Police

Description générée automatiquement

Figure 10 Analyse avec l'outil Searchsploit.

La capture d'écran montre une liste de vulnérabilités associées à différentes versions du noyau Linux. Elles sont caractérisées par des noms descriptifs tels que « Heap Overflow », « Use-After-Free », « Local Privilege Escalation », et d'autres termes techniques spécifiques à la sécurité informatique. Ces termes indiquent des types de failles qui peuvent être exploitées par des attaquants pour obtenir des **privilèges** **non** **autorisés** [[10]](#footnote-10)ou causer un **déni de service** [[11]](#footnote-11)sur un système.

Maintenant, nous allons analyser le routeur Cisco Meraki MX250 [[12]](#footnote-12)que nous avons identifié grâce à une analyse Nmap.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Figure 11 Analyse Cisco Meraki MX250

Cette faille pourrait créer un problème d'accès à l'ensemble du lycée. Par conséquent, il serait nécessaire de mettre en place un VLAN et une redondance pour y remédier.

Un CVE (Common Vulnerabilities and Exposures) est une référence unique attribuée à une vulnérabilité de sécurité spécifique. Cette référence permet aux chercheurs en sécurité, aux administrateurs système et aux entreprises de faire référence à des vulnérabilités de manière standardisée. Chaque CVE est accompagné de détails sur la vulnérabilité, y compris sa description, son impact potentiel, et des solutions possibles pour la corriger. La liste de toutes les failles de sécurité depuis la dernière mise à jour ainsi que la faille que j'ai trouvée sur le JavaScript sont les suivantes :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Figure 12 CVE et faille publique Lighttpd.

Ces pistes seront donc utilisées ultérieurement lors du pentest, mais il est certain que ce protocole HTTP est exploitable pour tout type d'attaque à développer.

## Conclusion : Importance de l'Énumération pour la Sécurité du Réseau

L'énumération a révélé d'importantes vulnérabilités dans le routeur Cisco Meraki MX250, notamment par l'utilisation d'outils comme Nmap et Searchsploit. Nmap a identifié des services, des ports ouverts, et des versions logicielles obsolètes, exposant le système à des failles connues, comme celles affectant le service Lighttpd et le système d'exploitation Linux. Searchsploit a mis en évidence des vulnérabilités critiques telles que des dépassements de tampon et des escalades de privilèges. Ces découvertes accentuent la nécessité de mettre à jour régulièrement les logiciels et d'adopter des mesures de sécurité telles que les VLANs pour protéger contre les accès non autorisés et maintenir la continuité des opérations. Cette phase d'énumération est vitale pour identifier les faiblesses et renforcer la défense des infrastructures réseau contre les cyberattaques.

# Exploitation : Les failles exploitées :

## Exploitation via Command Prompt (cmd) due à une gestion défaillante des droits d'accès :

### Exploitation des autorisations de serveur par le biais d'un raccourci :

Il a été constaté que, bien que l'exécution de commandes (CMD) et de scripts Visual Basic (VBS) soit directement bloquée sur les postes clients et que les droits administrateur soient restreints, l'ouverture d'une console via un raccourci dans un dossier partagé contourne ces restrictions. Cette capacité d'éviter les restrictions locales s'explique par le fait que les utilisateurs n'ont pas le droit de lancer des commandes directement, mais ils obtiennent implicitement les autorisations nécessaires du serveur lorsque l'action est initiée à partir d'un emplacement contrôlé par ce dernier. Ainsi, tout fichier exécuté depuis le serveur agit avec les privilèges du serveur lui-même, y compris la possibilité d'exécuter des commandes comme si elles étaient lancées par un administrateur.

### Exécution privilégiée et contournement des restrictions :

En exploitant cette vulnérabilité, un fichier batch préparé et déposé dans un espace de libre-échange sur le serveur peut être exécuté avec des droits administrateur, même si l'utilisateur local ne possède pas ces droits. Cela signifie que la console de commande (CMD), normalement inaccessible à l'utilisateur standard en raison des politiques de sécurité, est exécutée avec des privilèges élevés côté serveur. Il est important de noter que cette faille n'affecte que les commandes ou programmes normalement interdits ; les applications ou commandes autorisées par défaut ne sont pas concernées par cette méthode d'escalade de privilèges.

### Absence de limitations et implications de sécurité :

La méthode permet non seulement d'accéder à des zones normalement restreintes, mais aussi d'exercer un contrôle quasi total sur le système, y compris la possibilité de révoquer les droits d'autres utilisateurs ou d'en accorder de nouveaux sans aucune restriction. Cela démontre une vulnérabilité majeure dans la gestion des droits d'accès et la séparation des privilèges au sein de l'infrastructure réseau.

### Les journaux sont sous forme de fichiers .cmd et sont facilement accessibles avec l'exploit.

|  |  |
| --- | --- |
| L’utilisation de fichiers de log sous forme de .cmd est une pratique peu sécurisée, car ces fichiers peuvent être facilement modifiés ou supprimés,  Compromettant ainsi l'intégrité des données de journalisation. De plus, le fait qu'ils soient accessibles facilement avec un exploit souligne une faille de sécurité importante dans la configuration du système.  Il est crucial de mettre en place des mesures de sécurité appropriées pour protéger les fichiers de log et limiter l'accès à ceux-ci pour garantir l'intégrité et la confidentialité des données de journalisation. | Une image contenant texte, menu, capture d’écran, document  Description générée automatiquement  Figure 13 Dossier des journaux/logs. |

### Conclusion de la méthodologie :

Cette découverte met en évidence un défaut critique dans la configuration des droits d'accès et l'exécution des commandes sur le réseau de l'établissement. En permettant l'exécution de commandes avec des privilèges élevés par le biais du serveur, un vecteur d'attaque potentiel est créé, offrant aux acteurs mal intentionnés la possibilité d'exploiter cette faille pour obtenir un accès non autorisé à des informations sensibles et effectuer des actions malveillantes sans contrainte.

### Recommandations :

Pour remédier à cette situation, il est impératif de revoir la configuration de l'Active Directory ainsi que les droits des utilisateurs. Il est également recommandé de mettre en place des restrictions sur les fichiers avec les extensions .bat, .cmd, .batch et .vbs. Ces mesures aideront à renforcer la sécurité du système et à limiter les risques d'exploitation via Command Prompt (cmd).

## Vulnérabilités d'Exploitation du Routeur Cisco Meraki et du Serveur HTTP Lighttpd

À la suite de la phase d'OSINT, j'ai récupéré des informations utiles telles que l'adresse MAC et l'adresse IPv4 du routeur central du réseau. De plus, j'ai découvert qu'un serveur HTTP non sécurisé était hébergé sur le port 8090, utilisant une version très ancienne de Lighttpd. Nous utiliserons ces informations pour la phase deux d'exploitation.



Figure 14 Version Lighttpd exploitée.

Nous pouvons accéder facilement au routeur Cisco Meraki.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia  Description générée automatiquement  Figure 15 Interface Cisco Meraki MX250. | J'ai demandé à un camarade de confiance de réaliser un speed test avec moi, pour donner suite à l'analyse des fiches techniques, pour confirmer ma théorie. L'internet a été désactivé pendant environ 3 minutes dans la salle, ce qui confirme que le serveur tombe avec seulement 5 personnes. |

Une attaque par déni de service (DoS) vise à rendre un service inaccessible en surchargeant le système ciblé avec un flux de trafic excessif, épuisant ainsi ses ressources et l'empêchant de répondre aux demandes légitimes. Cela peut se faire en inondant le système de requêtes ou en épuisant ses ressources, ce qui entraîne des perturbations ou des interruptions de service.[[13]](#footnote-13)

### Contournement de mots de passe lors de la Deuxième Exploitation du Routeur

L'attaque consiste à contourner les mots de passe pour accéder au routeur en exploitant des vulnérabilités ou des erreurs de configuration, permettant à l'attaquant d'accéder à la page d'administration sans saisir de mot de passe.

Si l'on se connecte à un autre port du routeur Cisco Meraki grâce à Nmap, on peut accéder à une page d'administration qui est normalement bloquée par défaut en fonction de notre adresse IP. Cependant, si l'on change d'adresse IP pour une autre différente de celle fournie par le DHCP, on peut directement activer le mode administrateur sans avoir à entrer de mot de passe ou à effectuer une injection SQL ou toute autre manipulation supplémentaire.

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Figure 16 Utilisation du changement de port Meraki.

Cette page apparaît effectivement lorsque l'on change d'adresse IP, ce qui nous permet d'accéder au mode administrateur sans difficulté

.Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

Figure 17 Utilisation du changement d'adresse IP.

### Conclusion sur l’exploit :

Il serait important d'ajouter un VLAN pour isoler le routeur et éviter que l'on puisse s'y connecter simplement en tapant son adresse IP, peu importe notre poste. De plus, une liste de contrôle d'accès (ACL) devrait être configurée pour bloquer les trames Nmap et tout test de connexion au serveur provenant des plages d'adresses utilisateur. Il serait également crucial de bloquer les utilisateurs qui tentent d'attribuer une adresse IP si leur adresse MAC n'est pas ajoutée à la liste blanche.

## Exploit Attaque par Injection JavaScript :

Une attaque par injection JavaScript consiste à insérer du code JavaScript malveillant dans une application web afin de compromettre son fonctionnement ou d'exploiter des vulnérabilités. Cette technique peut être utilisée pour voler des données sensibles, prendre le contrôle de sessions utilisateur, ou détourner le navigateur vers des sites frauduleux.[[14]](#footnote-14)

Dans cette nouvelle phase d'exploitation, nous allons utiliser le menu classique du routeur Cisco et tenter d'entrer un mot de passe. Je n'ai pas encore essayé, mais je soupçonne fortement qu'il soit le même que les mots de passe administratifs que j'ai trouvés dans des dossiers juste avant. Pour ce test, nous n'aurons pas besoin de mots de passe, mais simplement de contourner le formulaire ou d'effectuer une injection JavaScript qui n'est pas bloquée.

Lorsque nous saisissons notre mot de passe, cela ouvre une interface JavaScript qui n'est pas du tout sécurisée. Cela ne constitue pas un problème lié à l'administrateur, mais plutôt à la vieille version du routeur.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure 18 Fenêtre de connexion

Pour réaliser une attaque JavaScript de manière discrète sans altérer le site, car les méthodes d'attaque JavaScript que j'utilise habituellement créeraient une vulnérabilité trop importante et affecteraient considérablement le serveur, j'ai opté pour une approche plus « diplomatique ».

Mon objectif n'était pas de compromettre le réseau existant. J'ai examiné la console des événements JavaScript pour voir si quelque chose s'affichait lorsque l'on tentait de se connecter. En général, elle est bloquée, cryptée ou les informations ne sont que rarement affichées en clair, sauf sur les machines virtuelles de test. Dans ce cas précis, le routeur n'ayant pas été mis à jour depuis un certain temps, les données sont affichées en clair, et nous avons directement accès à la méthode de l'API qui envoie des données, ainsi qu'au fichier JavaScript associé.

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Figure 19 Exploration de la commande « get » dans la Console JavaScript

Les méthodes HTTP GET, POST, PUT, DELETE et HEAD sont utilisées pour interagir avec les serveurs web. Voici une brève explication de chacune et comment un pirate peut les exploiter :

* GET: Utilisée pour demander des données à partir d'une ressource spécifiée. Les données sont envoyées dans l'URL sous forme de chaîne de requête. Un pirate peut exploiter cette méthode en modifiant les paramètres dans l'URL pour accéder à des informations sensibles ou pour provoquer des actions non autorisées sur le serveur.
* POST : Utilisée pour envoyer des données au serveur pour traitement. Contrairement à GET, les données ne sont pas visibles dans l'URL. Un pirate peut exploiter cette méthode en envoyant des données malveillantes dans les champs de formulaire pour compromettre le serveur, comme l'injection SQL ou l'injection de code.
* PUT : Utilisée pour mettre à jour une ressource existante sur le serveur. Si mal configurée, cette méthode peut permettre à un pirate de modifier des données sensibles sur le serveur.
* DELETE : Utilisée pour supprimer une ressource spécifiée sur le serveur. Une mauvaise gestion de cette méthode peut permettre à un pirate de supprimer des données importantes ou même de causer des dommages irréparables au serveur.
* HEAD : Similaire à GET, mais ne renvoie que les en-têtes de réponse sans le corps de la réponse. Cette méthode est souvent utilisée pour vérifier l'existence d'une ressource et récupérer des métadonnées. Bien que moins souvent exploitée par les pirates, elle peut être utilisée pour sonder le serveur à la recherche de vulnérabilités.

L'activation de HTTPS est essentielle pour sécuriser les échanges de données entre le navigateur et le serveur. HTTPS chiffre les données transmises, ce qui rend beaucoup plus difficile pour un pirate d'intercepter ou de modifier les informations sensibles. Cela protège également contre les attaques de type « man-in-the-middle » où un attaquant tente d'intercepter ou de modifier les données entre le navigateur et le serveur. En utilisant HTTPS, les sites web peuvent assurer la confidentialité, l'intégrité et l'authenticité des données échangées, réduisant ainsi le risque d'exploitation des méthodes HTTP par les pirates.

### Conclusion

En exploitant une injection JavaScript, nous avons réussi à accéder à une interface non sécurisée du routeur Cisco en contournant le formulaire de connexion. Cela souligne l'importance de maintenir à jour les équipements réseau pour éviter de telles vulnérabilités. Les méthodes HTTP telles que GET, POST, PUT, DELETE et HEAD peuvent être exploitées par les pirates pour accéder à des données sensibles. L'activation de HTTPS est essentielle pour sécuriser les échanges de données et réduire le risque d'exploitation des méthodes HTTP par les pirates.

### Recommandations :

Il serait important d'activer le HTTPS et de mettre à jour les différents services. Plus de détails sont disponibles à la fin du document.

## Exploitation d'une Faille de Sécurité dans la Boîte à Outils d'Atos

Le quatrième exploit est basé sur les notions abordées dans le premier. Nous allons utiliser les documents que nous avons trouvés, notamment une variété de documents essentiels que nous trouverons dans le dossier suivant :



Figure 20 Ressource liée à cette phase d'exploitation :

Ces documents n'ont jamais été conçus pour les élèves ou les enseignants, mais plutôt pour les référents. Ils regroupent toutes les informations sur l'utilisation des outils administratifs, leur configuration, etc. En somme, ces documents doivent être maintenus dans le plus strict secret.

Une image contenant texte, capture d’écran, menu, Police

Description générée automatiquement

Figure 21 Documentation Atos sur les différents outils

Le document qui nous intéresse est celui permettant de réinitialiser n'importe quel mot de passe via la boîte à outils d'Atos.

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement  Figure 22 Boîte à outils Atos 1. | Figure 23 Boîte à outils Atos 2. |

La boîte à outils était censée être accessible uniquement aux personnes les plus qualifiées de cet établissement. En réalité, elle est finalement accessible aux étudiants en utilisant la méthode de l'exploit numéro [indiquer le numéro de l'exploit]. Nous avons alors littéralement tous les accès.

La dernière mise à jour apportée au réseau date de 2017, ce qui explique ce type de faille. Nous ne tiendrons pas compte de l'année 2018, car elle n'apporte rien de pertinent dans ce contexte.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Figure 24 Boîte à outils Atos 3

À la suite de tests, il apparaît que la boîte à outils ne respecte pas le RGPD, car il est possible d'afficher les mots de passe d'autres personnes. Normalement, les mots de passe des utilisateurs ne devraient même pas être visibles par l'administrateur ; celui-ci devrait simplement être en mesure de les réinitialiser.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Figure 25 Simulation d'élèves mal intentionnés.

### Conclusion :

Le quatrième exploit révèle la gravité de la situation : l'accès non autorisé à la boîte à outils Atos, utilisée à des fins administratives, est désormais possible pour les étudiants. Cette faille, résultant d'une négligence de mise à jour depuis 2017, compromet sérieusement la sécurité du système. De plus, la violation du RGPD, avec la possibilité d'afficher les mots de passe des utilisateurs, accentue la gravité de la situation.

### Recommandations

Il serait judicieux de mettre en place un mot de passe pour la boîte à outils, car les élèves parviendront toujours à trouver un moyen de l'ouvrir. Cependant, un mot de passe à l'entrée serait une mesure intéressante à envisager.

## Exploit de sécurité : vulnérable à une attaque web

La prépa du lycée Algoud est un environnement très sensible, car les étudiants travaillent intensément pendant une certaine période pour accéder à de grandes écoles ou participer à d'importants concours. Ils ont de grands projets, et le simple fait de ne pas pouvoir accéder à des ressources, ne serait-ce que pour un jour, serait critique, car ils devraient alors rattraper un retard déjà intense pour eux.

Actuellement, la prépa fonctionne entièrement sur le cloud, en utilisant le cloud de l'éducation nationale. La seule sécurité réside dans le fait que le lien n'est pas répertorié, il n'y a aucun mot de passe en place. Les étudiants et les professeurs ont tous des droits administrateur, leur permettant de faire à peu près ce qu'ils veulent. Pour une petite prépa, cela peut être acceptable, mais si une personne externe trouve le lien, comme dans le cas présent, cela pourrait être une catastrophe.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure 26 Site de la prépa pour l'exportation de documents.

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

Figure 27 Lien vers les documents.

Avec le lien ci-dessous, il est possible de téléverser n'importe quel fichier et le faire passer pour un travail pratique (TP) contenant un virus intégré ou autre. On peut même insérer un fichier reverseshell.php, permettant ainsi un accès total en SSH ou autre, ce qui permettrait de compromettre entièrement le site sans aucune limitation.

Un reverse shell est un type de shell qui s'exécute sur un système distant et permet à un attaquant d'obtenir un accès en ligne de commande à ce système

### Possibilité de copier tous les fichiers et leurs corrections.

Le lien donne également accès à tous les mots de passe et à toutes les corrections disponibles. Les données des étudiants contenues dans leurs dossiers, leurs travaux pratiques, et autres sont accessibles, ainsi que des données internes à la classe, ce qui ne respecte pas le RGPD (Règlement Général sur la Protection des Données).

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Figure 28 Explorateur de la prépa.

Il sera donc nécessaire d'implémenter des mots de passe pour les différents liens, de mettre en place un système de gestion des comptes et de bloquer l'envoi de fichiers PHP, qui sont automatiquement interprétés et peuvent ainsi facilement conduire à une attaque dévastatrice.

## Attaque par canal latéral via une imprimante réseau

Sur le réseau affiché, toutes les imprimantes et les serveurs d'impression sont visibles par tous les utilisateurs, ce qui pourrait ne pas être souhaitable dans un environnement où les utilisateurs devraient uniquement avoir accès aux imprimantes spécifiques de leur salle ou zone. Cela pose des problèmes de sécurité et de gestion, notamment parce que l'accès aux panneaux web d'administration des imprimantes ne nécessite aucun mot de passe, offrant des droits complets à quiconque double-clique sur ces icônes.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure 29 Liste des imprimantes et serveurs d'impression en mode promiscuité.

On accède directement au contrôle des imprimantes, et j'ai voulu vérifier que nous ne disposions pas uniquement des droits de visualisation, ce qui aurait déjà été suffisant pour une attaque.

Cependant, comme le démontre la suite, je possède des droits d'administrateur complets.

|  |  |
| --- | --- |
| 172.22.247.203 | 172.22.247.238 |
| Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia  Description générée automatiquement  Figure 30 Interface web de l'imprimante Epson 1. | Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur  Description générée automatiquement  Figure 31 Interface web de l'imprimante Epson 2. |

Dans les captures suivantes, j'ai tenté de modifier bien plus que les paramètres d'impression généraux de l'imprimante. J'ai également exploré les options de langue, le temps de mise à jour technique, et pour terminer, j'ai effectué des ajustements concernant le réseau, tels que l'adresse IP, le masque, et autres. Cette série de modifications est accessible à tout utilisateur.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur  Description générée automatiquement  Figure 32 Interface web de l'imprimante Epson 3. | Une image contenant texte, capture d’écran, nombre  Description générée automatiquement  Figure 33 Interface web de l'imprimante Epson 4. |

En fait, le masque pour les imprimantes permet 2046 postes, ce qui est bien plus que nécessaire pour un réseau dédié aux imprimantes, étant donné que nous avons au maximum 100 imprimantes. Je suis d'avis qu'un changement de masque de sous-réseaux serait fortement envisageable.

Une image contenant texte, logiciel, nombre, ligne

Description générée automatiquement

Figure 34 Interface web de l'imprimante Epson Réseaux 5.

Et le résultat pour chaque manipulation reste constant :

Une image contenant texte, logiciel, Icône d’ordinateur, Logiciel multimédia

Description générée automatiquement

Figure 35 Interface web de l'imprimante Epson 6.

### Imprimante HP :

Pour démontrer que cela ne concerne pas uniquement les imprimantes Epson, mais tous les périphériques de ce réseau, je vais effectuer une dernière démonstration sur les appareils HP. Mais cela n'est qu'un exemple ; toutes les marques de périphériques de ce réseau sont concernées.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Figure 36 Interface web de l'imprimante HP 1.

J'ai ajouté mon contact pour vérifier si cela fonctionne sans soucis, et j'ai également vérifié les adresses IP et le masque, mais je n'ai rencontré aucun blocage.

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Description générée automatiquement

Figure 37 Interface web de l'imprimante HP 2.

Cette démonstration est gentille et innocente, mais imaginer les conséquences pour le réseau si un véritable hacker s’y était intéressé.

À préciser, j'ai remis toutes les imprimantes à l'identique une fois mes tests effectués.

Un hacker peut facilement, même sans expertise informatique, effectuer une attaque de l'homme du milieu en redirigeant chaque imprimante vers lui en utilisant la passerelle par défaut. De plus, il pourrait même utiliser les imprimantes pour attaquer le reste du réseau.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Figure 38 : Interface web de l'imprimante HP 3

Le Telnet est activé, ce qui est déjà une catastrophe en termes de sécurité, surtout pour une attaque de l'homme du milieu, étant donné le masque de sous-réseaux actuel et ce qu'il permet encore plus. De plus, j'ai remarqué un service FTP avec le mot de passe par défaut « admin admin », ce qui ouvre la possibilité d'envoyer n'importe quoi sur le serveur d'impression.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Figure 39 Interface web du serveur d'impression

Les failles disponibles sur ces appareils sont nombreuses et permettent une attaque de l'homme du milieu sans aucune frontière.

Le DHCP pour les versions IPv4 et IPv6 est activé sur les imprimantes, ce qui me semble inutile puisqu'elles sont supposées utiliser des adresses IP fixes. Cela représente une vulnérabilité supplémentaire qui pourrait être corrigée.

La communication en HTTPS est désactivée alors qu'elle est disponible en local.

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement

Figure 40 Interface web de l'imprimante HP 4.

### Les failles non exploitées

Dans cette section du document, nous nous concentrons exclusivement sur l'identification des vulnérabilités observées. Il est important de souligner que notre approche exclut l'exploitation de ces failles. Cette décision est le résultat d'une réflexion approfondie visant à prévenir la destruction d'accès à des services essentiels et à éviter de provoquer des perturbations majeures, tout en minimisant les désagréments pour le personnel. Nous sommes conscients que certaines vulnérabilités, si exploitées, pourraient entraîner des conséquences significatives, y compris des interruptions de service pour l'établissement. C'est pourquoi nous avons choisi une démarche responsable, centrée sur la détection et la documentation des failles sans engager d'actions susceptibles de nuire à l'infrastructure ou à la continuité des opérations.

### Possible usurpation d’identité

La capture d'écran ci-dessous n'est qu'un exemple, mais une personne mal intentionnée qui n'aurait pas pour seul objectif de démontrer une mauvaise sécurisation et de vous communiquer les failles aurait pu exploiter les mots de passe disponibles, comme ceux de la web radio.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure 41 Document interne sur la web radio.

Les adresses de récupération et autres, nous avons le mot de passe du CDI, mais nous avons également d'autres mots de passe et autres informations.

Le potentiel pour un hacker en termes d'usurpation d'identité est immense, car nous avons des documents internes d'achat et d'échange.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Figure 42 Facture interne

Les listes envoyées au professeur et à l'administration concernent les professeurs principaux. Les données datent de l'époque du test, mais je peux vous garantir qu'elles sont actualisées chaque année après vérification. De plus, nous disposons des comptes des élèves, comprenant leurs prénom, classe et mot de passe (pour la plupart). Même lorsque le mot de passe est caché par des étoiles, nous avons soit la taille du mot de passe, soit d'autres informations personnelles de l'élève qui en permettent la découverte par attaque par « brute force ». Dans d'autres documents, il suffit simplement d'effacer la mise en forme du texte et le mot de passe apparaît. De plus, nous avons la dernière date de connexion/de partage de fichier, ce qui nous permet de créer des e-mails très crédibles pour le phishing. Le hacker n'aurait même pas besoin de fournir beaucoup d'efforts.

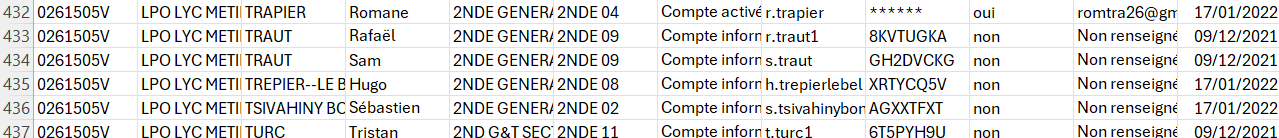


Figure 43 Compte rendu Moodle.

Et pour attaquer le lycée, on pourrait se faire passer pour l'une des écoles d'Erasmus avec lesquelles vous avez communiqué par le passé. Étant donné que nous possédons tous les fichiers, y compris les diplômes des professeurs et autres informations, cela serait facile à réaliser.

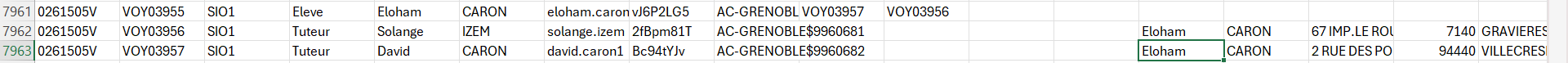
Une image contenant texte, capture d’écran, Police, logo

Description générée automatiquement

Figure 44 Document interne relatif à Erasmus.

### Risque de brute force :

Et si nous parlons d'une attaque directe contre les élèves ou les professeurs par brute force, je vais prendre l'exemple avec mes propres données personnelles pour respecter le RGPD, mais j'aurais pu utiliser n'importe quel autre élève. En utilisant le logiciel Crisis et les informations disponibles dans mon fichier Excel, je peux directement créer une liste de mots de passe en fonction de mes informations personnelles dans ces documents.



Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure 45 Génération de mots de passe crisis.

En utilisant cet outil, nous sommes en mesure de définir directement les paramètres souhaités et de générer une quantité de mots de passe titanesque, puis de les essayer en quelques secondes. Malgré les mesures de sécurité anti-brute force mises en place, l'outil est capable de générer des tokens d'identification basés sur les mots de passe.

Les tokens d'identification sont des jetons numériques qui représentent l'authentification de l'utilisateur. Ils sont utilisés pour accéder à des ressources informatiques ou des services en ligne. Ces tokens peuvent être basés sur des mots de passe, des clés cryptographiques ou d'autres méthodes d'authentification. Dans ce cas précis, les tokens sont générés à partir de mots de passe.

Lorsqu'un utilisateur utilise un token d'identification pour se connecter à un système, le système vérifie l'authenticité du token. Si le token est valide, l'utilisateur est autorisé à accéder aux ressources ou aux droits associés au token.

Bien que ces tokens soient réinitialisés après chaque connexion, ils confèrent néanmoins des droits administrateur complets. Cela signifie que même s'ils sont réinitialisés, lorsqu'ils sont utilisés, ils accordent à l'utilisateur les plus hauts niveaux d'accès et de contrôle sur le système ou les données auxquels ils sont associés.

De plus, ces tokens ne sont pas particulièrement difficiles à décrypter grâce à des techniques de brute force. La brute force est une méthode d'attaque où l'attaquant essaie de deviner les mots de passe en les essayant un par un jusqu'à ce qu'il trouve le bon. Dans ce cas, l'outil est capable de générer et d'essayer rapidement une grande quantité de mots de passe, ce qui rend la tâche de deviner le mot de passe associé au token plus facile pour un

Attaquant.

L'exemple ci-dessous utilise des mots de passe classiques, mais j'aurais également pu utiliser ces fameux tokens à la place. Les tokens d'identification auraient permis une authentification similaire, mais avec une sécurité potentiellement plus élevée et des droits d'accès plus précis.

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Figure 46 Génération de mots de passe crisis 2.

Les mots de passe pouvant être générés en seulement 4 secondes d'exécution sont extrêmement nombreuses.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure 47 Liste de mots de passe.

Très vite Crisis permet de générer des mots de passe à partir des informations publiques des utilisateurs : le nom, le prénom, l’adresse, la date de naissance, etc. Autant d’information qu’il a été possible de collecter soit parce que publiques sur le site web du lycée et autre ENT, soit parce que piratées sur le serveur de fichier du lycée. La copie d’écran ci-dessous montre quelques mots de passe générés.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Figure 48 Liste de mots de passe 2.

Les mots de passe générés peuvent être ensuite utilisés pour une attaque en brute force d’autant plus facilement qu’il n’y a pas de dispositifs activés pour interdire ce type d’attaque.

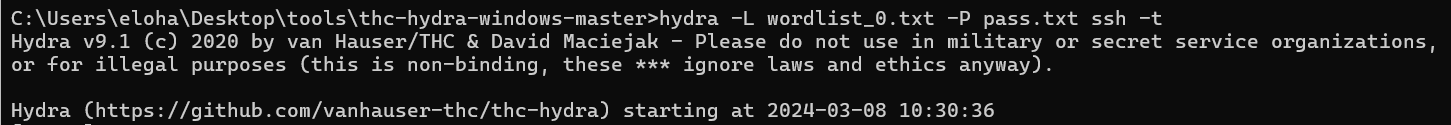
### Utilisation de l’outils Hydra :

Hydra est un outil de test de pénétration largement utilisé dans le domaine de la sécurité informatique. Il fonctionne en essayant différentes combinaisons de noms d'utilisateur et de mots de passe pour accéder à des systèmes, des services ou des applications. Son utilisation principale est de tester la robustesse des mécanismes d'authentification, tels que les pares-feux, les serveurs web, etc.

Cependant, Hydra peut être utilisé à des fins malveillantes, car il peut compromettre la sécurité d'un système en obtenant un accès non autorisé. Il est couramment inclus dans les distributions Linux dédiées à la sécurité, comme Kali Linux, ce qui le rend facilement accessible à des individus mal intentionnés.

La liste des protocoles supportée est impressionnante, je cite : Astérisque, AFP, Cisco AAA, authentification Cisco, activation Cisco, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM -GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, proxy HTTP, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, auditeur Oracle, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, SAP / R3, SIP, SMB, SMTP, Enum SMTP, SNMP v1 + v2 + v3, SOCKS5, SSH (v1 et v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC et XMPP.

Les options pertinentes dans Hydra pour la brute force de tokens (bien que non utilisées dans ce cas) pourraient inclure :



Il est important de noter que l'utilisation de ces options pour brute-forcer des tokens sans autorisation peut être contraire aux lois sur la sécurité informatique et aux politiques de sécurité. Ces actions peuvent entraîner des conséquences juridiques graves.

Cependant, il est aujourd'hui facile pour quiconque de mener une attaque directe contre les utilisateurs, étant donné la disponibilité généralisée d'informations personnelles telles que la taille des mots de passe, les anciens mots de passe et même les mots de passe actuels, comme démontré précédemment. Il est donc crucial d'imposer et de mettre en place des mesures drastiques de sécurité pour contrer cette menace.

# Phase de post-exploitation : analyse :

## Exploits et Vulnérabilités Identifiées :

La phase de Pentest a mis en évidence plusieurs failles et exploits significatifs au sein du système d'information, démontrant l'urgence de mesures correctives pour sécuriser l'infrastructure réseau. Voici un résumé détaillé des vulnérabilités exploitées et des recommandations pour chaque exploit identifié.

#### Exploitation des Autorisations de Serveur :

* Description : Une gestion défaillante des droits d'accès permet l'exécution de commandes via un raccourci, contournant les restrictions locales grâce aux privilèges implicites obtenus du serveur.
* Impact Potentiel : Accès non autorisé à des zones normalement restreintes et possibilité de contrôler le système avec des privilèges élevés.
* Recommandation : Révision de la configuration de l'Active Directory et des droits utilisateurs, avec des restrictions sur les fichiers exécutables susceptibles de lancer des commandes.

#### Vulnérabilités du Routeur Cisco Meraki et du Serveur HTTP Lighttpd :

* Description : L'utilisation d'une version obsolète de Lighttpd sur un serveur HTTP non sécurisé et l'exploitation des vulnérabilités du routeur Cisco Meraki pour accéder à l'administration sans mot de passe.
* Impact Potentiel : Accès administratif non autorisé et possibilité de distribuer des configurations réseau malveillantes.
* Recommandation : Mise à jour vers les versions les plus récentes de Lighttpd, configuration d'un VLAN pour isoler le routeur, et mise en place de listes de contrôle d'accès.

#### Attaque par Injection JavaScript :

* Description : Injection de code JavaScript malveillant dans une interface web non sécurisée pour compromettre son fonctionnement ou exploiter des vulnérabilités.
* Impact Potentiel : Vol de données sensibles, prise de contrôle de sessions utilisateur, et redirection vers des sites malveillants.
* Recommandation : Activation de HTTPS pour sécuriser les échanges de données et mise à jour des équipements réseau pour corriger les vulnérabilités.

#### Exploitation de la Boîte à Outils d'Atos :

* Description : Accès non autorisé à une boîte à outils administrative, permettant la réinitialisation de mots de passe sans contraintes.
* Impact Potentiel : Compromission de l'intégrité du système et violation de la confidentialité des données utilisateur.
* Recommandation : Imposition d'un mot de passe robuste pour la boîte à outils et mise à jour du réseau pour corriger les failles de sécurité.

#### Vulnérabilité à une Attaque web sur le Cloud de l'Éducation Nationale

* Description \* Absence de mesures de sécurité sur le cloud, permettant le téléversement de fichiers malveillants.
* Impact Potentiel : Compromission totale du site et accès non autorisé à des données sensibles.
* Recommandation : Implémentation de mots de passe, système de gestion des comptes, et blocage de l'envoi de fichiers exécutables.

#### Attaque par Canal Latéral via une Imprimante Réseau

* Description : Toutes les imprimantes et serveurs d'impression sont visibles et accessibles sans restriction, exposant le réseau à des manipulations malveillantes.
* Impact Potentiel : Manipulation des configurations réseau, saturation du réseau avec des requêtes excessives, et possibilité d'attaques par déni de service.
* Recommandation : Segmentation du réseau, mise en place d'authentification forte pour l'accès aux panneaux d'administration des imprimantes, et réduction de la plage d'adresses IP.

Chacune de ces vulnérabilités représente un risque sérieux pour la sécurité du réseau et la confidentialité des données. Il est impératif d'adopter une approche proactive pour les corriger, en mettant en œuvre les recommandations fournies afin de renforcer la sécurité de l'infrastructure informatique.

## Recommandations pour améliorer la Sécurité :

* Segmentation du réseau : Créer des sous-réseaux ou VLANs distincts pour les différents espaces, limitant ainsi l'accès aux imprimantes et aux serveurs d'impression uniquement aux utilisateurs concernés.
* Contrôle d'accès basé sur les rôles : Établir des permissions spécifiques pour que seuls les utilisateurs autorisés puissent accéder aux imprimantes et aux serveurs.
* Authentification forte : Activer l'authentification par mot de passe pour accéder aux panneaux d'administration des imprimantes et serveurs d'impression, en utilisant des mots de passe forts et uniques.
* Réduction de la plage d'adresses IP : Ajuster le masque de sous-réseau pour limiter le nombre d'adresses IP disponibles, aligné sur le nombre réel d'appareils.
* Désactivation des services non sécurisés : Remplacer les services anciens et vulnérables par des alternatives sécurisées telles que SSH et SFTP pour le chiffrement des données transmises.
* Sécurisation du DHCP : Implémenter des mesures de sécurisation pour le DHCP, telles que le DHCP snooping sur les commutateurs, afin de prévenir les attaques de type MitM.

# RGPD

Dans le contexte décrit, où il a été possible d'accéder aux données du serveur, y compris aux données de Pronote, de l'ENT du campus, et d'obtenir des mots de passe, identifiants, adresses postales, adresses e-mail, et autres informations personnelles des étudiants, plusieurs violations du RGPD (Règlement Général sur la Protection des Données) et de la législation française sur la protection des données personnelles sont identifiables. Ces violations sont notamment liées aux principes fondamentaux du RGPD concernant la protection et la sécurité des données personnelles.

Comme illustré ci-dessous, ceci n'est qu'un exemple. Il existe également une version mise à jour incluant les données de plus de 8 000 élèves ainsi que celles de leurs familles :

Une image contenant texte, capture d’écran, nombre

Description générée automatiquement

Figure 49 : liste des comptes Moodle

## Violation des principes de confidentialité et d'intégrité (Article 5 [1] f du RGPD)

Le RGPD exige que les données personnelles soient traitées de manière à garantir une sécurité appropriée, incluant la protection contre le traitement non autorisé ou illicite. L'accès non autorisé aux données personnelles des étudiants constitue une violation directe de ce principe.

Leurs comptes EduConnect comprennent des informations telles que les mots de passe, les prénoms, les noms, les dernières connexions, les classes, les adresses e-mail, et d'autres données.

Une image contenant texte, capture d’écran, menu, nombre

Description générée automatiquement

## Manquement à l'obligation de sécurité des données (Article 32 du RGPD)

L'article 32 impose aux responsables du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque. Cela inclut la protection des données contre l'accès non autorisé ou illégal. Le fait que des données aussi sensibles puissent être accessibles sans autorisations adéquates révèle un manquement grave à cette obligation.

## Violation du principe de limitation de l'usage (Article 5 [1] b du RGPD)

Les données personnelles doivent être collectées pour des finalités spécifiques, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. L'accès non autorisé et l'usage potentiel de ces données à d'autres fins que celles pour lesquelles elles ont été collectées constituent une violation de ce principe.

### Conséquences et risques pour l'établissement :

## Notifications obligatoires (Articles 33 et 34 du RGPD)

En cas de violation de données personnelles, le responsable du traitement est tenu de notifier la violation à l'autorité compétente (CNIL en France) sans retard injustifié, au plus tard 72 heures après en avoir pris connaissance. Si la violation présente un risque élevé pour les droits et libertés des personnes physiques, les individus concernés doivent également être informés sans délai.

## Sanctions administratives (Article 83 du RGPD)

Les violations du RGPD peuvent entraîner des sanctions financières significatives pour l'établissement responsable. Les amendes peuvent aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, selon le montant le plus élevé.

## Répercussions sur la réputation

Au-delà des sanctions financières, les violations de données peuvent gravement nuire à la réputation de l'établissement, affectant sa confiance auprès des étudiants, des parents, et du personnel.

## Actions recommandées :

Notification immédiate à la CNIL et aux personnes concernées, si applicable.

Audit de sécurité pour identifier et corriger les failles.

Renforcement des mesures de sécurité pour prévenir de futures violations.

Révision des politiques de traitement des données pour assurer leur conformité avec le RGPD.

En résumé, l'accès non autorisé aux données personnelles des étudiants représente une violation sérieuse du RGPD et de la législation française, exposant l'établissement à des risques juridiques, financiers, et réputationnels significatifs. Il est impératif de prendre des mesures immédiates pour répondre à cette situation et prévenir de futures occurrences.

# Conclusion du rapport.

En conclusion, ce rapport de pentest et d'analyse de conformité RGPD met en lumière des vulnérabilités critiques au sein du système d'information, exposant l'établissement à des risques significatifs en matière de sécurité des données et de conformité réglementaire. Les techniques d'exploitation démontrées, notamment le contournement des restrictions d'accès et l'exécution privilégiée, soulignent l'urgence de revoir et de renforcer les politiques de sécurité informatique. De plus, les violations du RGPD identifiées, concernant notamment la protection et la sécurité des données personnelles, exigent une attention immédiate pour éviter des conséquences juridiques et financières lourdes, sans parler des répercussions sur la réputation de l'établissement.

Les recommandations proposées, telles que l'audit de sécurité, la notification à la CNIL, et le renforcement des mesures de sécurité, sont des étapes essentielles pour remédier aux failles identifiées et pour s'aligner avec les exigences du RGPD. Il est impératif que l'établissement prenne des mesures concrètes et immédiates pour protéger les informations sensibles et pour garantir un environnement numérique sécurisé pour tous les utilisateurs.

Ce rapport souligne également l'importance d'une sensibilisation et d'une formation continues en matière de cybersécurité pour tous les membres de l'établissement, afin de prévenir de futures violations et d'instaurer une culture de la sécurité informatique robuste. En prenant les actions recommandées et en s'engageant dans une démarche proactive de protection des données, l'établissement peut non seulement répondre aux exigences réglementaires, mais aussi renforcer la confiance des étudiants, des parents, et du personnel dans sa capacité à sécuriser les informations critiques.

# RECOMMANDATION RGPD :

Dans le cadre des recommandations pour donner suite au rapport de Pentest et d'analyse de conformité RGPD, il est vivement conseillé à tous les membres de l'établissement de suivre des formations spécialisées pour renforcer leurs connaissances et compétences en matière de protection des données et de sécurité informatique. À cette fin, deux ressources pédagogiques gratuites et officielles de l'État français sont particulièrement recommandées :

## Recommandation concernant le RGPD

### Modules de la CNIL sur le RGPD :

* MODULE 1 : LE RGPD ET SES NOTIONS CLÉS
* MODULE 2 : LES PRINCIPES DE LA PROTECTION DES DONNÉES

Ces modules sont disponibles sur le site de la CNIL à l'adresse suivante : [Atelier RGPD de la CNIL] (<https://atelier-rgpd.cnil.fr/>).

Ces formations en ligne visent à familiariser les utilisateurs avec le Règlement Général sur la Protection des Données (RGPD) et à leur apprendre à gérer correctement les informations personnelles conformément à la réglementation en vigueur. Ces modules sont conçus pour être accessibles à tous, offrant une compréhension claire et approfondie des exigences légales, des droits des individus, et des obligations des organisations en matière de protection des données personnelles.

### MOOC de l'ANSSI sur la sécurité numérique :

Pour approfondir les connaissances en matière de sécurité informatique et adopter les bonnes pratiques, le MOOC de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), intitulé **SecNumacadémie**, est également recommandé.

Accessible à l'adresse : (<https://secnumacademie.gouv.fr/>), ce cours en ligne gratuit offre une formation de base sur divers aspects de la cybersécurité, y compris la sécurisation des appareils personnels et professionnels, la protection contre les logiciels malveillants, et la sensibilisation aux différentes méthodes d'attaque informatique.

Le suivi de ces formations est essentiel pour s'assurer que tous les acteurs de l'établissement sont équipés pour identifier, prévenir, et répondre efficacement aux risques liés à la sécurité des données et des systèmes d'information. L'investissement dans la formation continue en matière de protection des données et de cybersécurité est crucial pour maintenir un haut niveau de sécurité et de conformité réglementaire, et pour protéger l'intégrité, la confidentialité, et la disponibilité des informations sensibles au sein de l'organisation.

# Proposition de changement du réseau :

Comme nous l'avons vu précédemment, l'un des problèmes principaux du réseau est l'absence de séparation entre les différents réseaux et les différents bâtiments. Il faudrait mettre en place une séparation, et le meilleur moyen serait d'utiliser un VLAN par Active Directory. Par exemple, il est nécessaire que les SN puissent accéder à leur réseau depuis le CDI. Cependant, le problème actuel est que tout le monde a accès au réseau SN et tout le monde a accès au CDI. De plus, lorsque l'on passe par le CDI, le réseau SN est entièrement accessible et les droits sont mal gérés. Cette méthode serait parfaite, car elle garantirait une sécurité maximale, mais elle nécessiterait une équipe conséquente et du temps pour être mise en place. Une alternative serait de créer un script automatisé pour gérer cela, mais cette solution est la meilleure, mais aussi la plus difficile à installer.

Une autre solution pourrait être de créer un VLAN par salle. Par exemple, nous pourrions avoir un VLAN 179 avec l'adresse IP 172.22.179.1 et un masque de 255.255.255.0. Nous utilisons un masque qui permet jusqu'à 30 appareils par salle, car généralement il n'y en a pas plus. Nous nommons les VLAN en fonction des noms des salles, ce qui facilite grandement la gestion. Si nous devons désactiver internet pour un examen afin de prévenir la triche, cela se fait simplement. Cette approche nous offre une vision claire de la gestion du réseau.

Cette solution est beaucoup plus simple à mettre en place, très pratique pour les examens et pour avoir une vision claire du réseau. Cependant, si deux classes veulent travailler ensemble dans des salles différentes, nous sommes obligés d'avoir une zone partagée sur le serveur qui est configurée par Active Directory, donc nous retombons sur le même problème. En ce qui concerne les élèves de SN, soit nous les fusionnons avec le CDI, ce qui ne corrige aucun problème, soit nous les isolons, mais cela serait gênant pour eux, car ils ne pourraient plus travailler en dehors de leur atelier.

Pour le service des imprimantes, il serait nécessaire de les connecter soit à leur salle respective, soit de les intégrer à un réseau avec un masque de sous-réseaux approprié. Il faudrait leur attribuer un mot de passe robuste, désactiver le DHCP v4 et V6, désactiver Telnet et mettre en place SSH, modifier les mots de passe FTP et utiliser un autre protocole plus sécurisé que le FTP.

# Outils, sources et bibliographie :

## Les outils utilisés comprennent : Hydra :

<https://www.kali-linux.fr/hacking/tutohydrabruteforce>

Brute force : L'outil n'est plus disponible sur le site officiel, ayant été interdit par le gouvernement. Seule la documentation reste accessible.

<https://www.kali-linux.fr/hacking/crisis-wordlist-generator>

Il est disponible ici, bien que de manière incomplète pour éviter son bannissement :

<https://sourceforge.net/projects/crisis-wordlist-generator/files/latest/download>

kits batch :

<https://github.com/kushfj/pentesting>

## RGPD :

CHAPITRE VIII - Voies de recours, responsabilité et sanctions :

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre8>

Pour la formation des employés :

<https://atelier-rgpd.cnil.fr/>

<https://secnumacademie.gouv.fr/>

## Vulnérabilité :

https://www.cert.ssi.gouv.fr/avis/CERTA-2012-AVI-674/

<https://www.cvedetails.com/vulnerability-list/vendor_id-2713/Lighttpd.html>

# Tables des illustrations

[Figure 1 : ressources partagées. 7](#_Toc162884774)

[Figure 2 : autres ressources partagées. 7](#_Toc162884775)

[Figure 3 Analyse Maltego des DNS associés. 9](#_Toc162884776)

Figure 4 : Mail et contacts liés au nom de domaine ac-grenoble

[Figure 5 Adresse IPv4 publique de l'entreprise. 11](#_Toc162884778)

[Figure 6 Analyse régionale avec Maltego. 11](#_Toc162884779)

[Figure 7 Liste des serveurs DNS 12](#_Toc162884780)

[Figure 8 Analyse avec Nmap 1 13](#_Toc162884781)

[Figure 9 : Analyse avec Nmap 2. 14](#_Toc162884782)

[Figure 10 Analyse avec l'outil Searchsploit. 15](#_Toc162884783)

[Figure 11 Analyse Cisco Meraki MX250 16](#_Toc162884784)

[Figure 12 CVE et faille publique Lighttpd. 17](#_Toc162884785)

[Figure 13 Dossier des journaux/logs. 18](#_Toc162884786)

[Figure 14 Version Lighttpd exploitée. 19](#_Toc162884787)

[Figure 15 Interface Cisco Meraki MX250. 19](#_Toc162884788)

[Figure 16 Utilisation du changement de port Meraki. 20](#_Toc162884789)

[Figure 17 Utilisation du changement d'adresse IP. 20](#_Toc162884790)

[Figure 18 Fenêtre de connexion 21](#_Toc162884791)

[Figure 19 Exploration de la commande « get » dans la Console JavaScript 21](#_Toc162884792)

[Figure 20 Ressource liée à cette phase d'exploitation : 22](#_Toc162884793)

[Figure 21 Documentation Atos sur les différents outils 23](#_Toc162884794)

[Figure 22 Boîte à outils Atos 1. 23](#_Toc162884795)

[Figure 23 Boîte à outils Atos 2. 23](#_Toc162884796)

[Figure 24 Boîte à outils Atos 3 24](#_Toc162884797)

[Figure 25 Simulation d'élèves mal intentionnés. 24](#_Toc162884798)

[Figure 26 Site de la prépa pour l'exportation de documents. 25](#_Toc162884799)

[Figure 27 Lien vers les documents. 25](#_Toc162884800)

[Figure 28 Explorateur de la prépa. 26](#_Toc162884801)

[Figure 29 Liste des imprimantes et serveurs d'impression en mode promiscuité. 27](#_Toc162884802)

[Figure 30 Interface web de l'imprimante Epson 1. 27](#_Toc162884803)

[Figure 31 Interface web de l'imprimante Epson 2. 27](#_Toc162884804)

[Figure 32 Interface web de l'imprimante Epson 3. 28](#_Toc162884805)

[Figure 33 Interface web de l'imprimante Epson 4. 28](#_Toc162884806)

[Figure 34 Interface web de l'imprimante Epson Réseaux 5. 28](#_Toc162884807)

[Figure 35 Interface web de l'imprimante Epson 6. 28](#_Toc162884808)

[Figure 36 Interface web de l'imprimante HP 1. 29](#_Toc162884809)

[Figure 37 Interface web de l'imprimante HP 2. 29](#_Toc162884810)

[Figure 38 : Interface web de l'imprimante HP 3 29](#_Toc162884811)

[Figure 39 Interface web du serveur d'impression 30](#_Toc162884812)

[Figure 40 Interface web de l'imprimante HP 4. 31](#_Toc162884813)

[Figure 41 Document interne sur la web radio. 32](#_Toc162884814)

[Figure 42 Facture interne 32](#_Toc162884815)

[Figure 43 Compte rendu Moodle. 33](#_Toc162884816)

[Figure 44 Document interne relatif à Erasmus. 33](#_Toc162884817)

[Figure 45 Génération de mots de passe crisis. 34](#_Toc162884818)

[Figure 46 Génération de mots de passe crisis 2. 35](#_Toc162884819)

[Figure 47 Liste de mots de passe. 35](#_Toc162884820)

[Figure 48 Liste de mots de passe 2. 36](#_Toc162884821)

[Figure 49 : liste des comptes Moodle 39](#_Toc162884822)

1. <https://algoud-laffemas.ent.auvergnerhonealpes.fr/> [↑](#footnote-ref-1)
2. <https://www.francetvinfo.fr/faits-divers/ce-que-l-on-sait-de-la-cyberattaque-et-des-menaces-d-attentat-qui-ont-vise-une-cinquantaine-de-lycees-d-ile-de-france_6438022.html> [↑](#footnote-ref-2)
3. http://www.pentest-standard.org/index.php/Main\_Page [↑](#footnote-ref-3)
4. https://osintframework.com/ [↑](#footnote-ref-4)
5. https://www.maltego.com/ [↑](#footnote-ref-5)
6. https://nmap.org/ [↑](#footnote-ref-6)
7. https://www.kali.org/ [↑](#footnote-ref-7)
8. https://www.exploit-db.com/ [↑](#footnote-ref-8)
9. https://www.metasploit.com/ [↑](#footnote-ref-9)
10. https://www.cyberark.com/fr/products/privileged-access-manager/ [↑](#footnote-ref-10)
11. https://fr.wikipedia.org/wiki/Attaque\_par\_d%C3%A9ni\_de\_service [↑](#footnote-ref-11)
12. https://www.wifi-france.com/cisco-meraki/mx250 [↑](#footnote-ref-12)
13. <https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service> [↑](#footnote-ref-13)
14. https://www.softwaretestinghelp.com/javascript-injection-tutorial/ [↑](#footnote-ref-14)