***REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE***



**MINISTERE DE LA FORMATION ET DE L’ENSEIGNEMENT PROFESSIONNELS**

**INSTITUT NATIONAL SPECIALISE DE LA FORMATION PROFESSIONNELLE EL HAMRI ORAN**

###### Mémoire de fin d’étude pour l’obtention du diplôme de Brevet de technicien Supérieur en administration et sécurité de les réseaux informatiques

**THÉME**

Protéction et sécurisation de l’infrastructure du réseau informatique de l’IHFR avec Linux

**Réalisé par** : Bessadat Ahmed Oussama

**Encadré par** : M. Addou Ahmed

ANNÉE DE FORMATION 2025-2026

**REMERCIEMENTS**

En tout premier lieu, nous remercions DIEU, le Tout Puissant, qui nous a éclairé le bon chemin et nous a aidé à réaliser ce modeste travail.

Nous tenons à remercier mon encadreur, monsieur Addou Ahmed pour nous avoir donné l’opportunité de travailler sur ce projet, pour son soutien scientifique qu’il nous a apporté tout au long de la réalisation de ce mémoire.

Nous adressons également nos remerciements à tous nos enseignants, qui nous ont donné les bases de la science.

Enfin nous remercions toutes personnes qui ont contribué de près ou de loin à l’achèvement de ce travail.

**DÉDICACES**

Mon soutien moral et source de joie et de bonheur, celui qui s’est toujours sacrifié pour me voir réussir, Mon dieu que je te donne tout le louange et que je te demande de me rapprocher chez vous toujours.

A mes parents et ma grands mère Fatima : Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études. Aucune dédicace ne pourrait exprimer mon respect, ma considération et mes profonds sentiments envers eux. Je prie le bon Dieu de les bénir, de veiller sur eux, en espérant qu’ils seront toujours fiers de moi.

A mes amies que mon dieu de les gardent. Et à toute ma famille et à tous ceux que j’aime.

Bessadat Ahmed Oussama

Table des matières

[Liste des abréviations 7](#_Toc206584941)

[Listes des figures 11](#_Toc206584942)

[1. Introduction 12](#_Toc206584943)

[2. Présentation du réseau IHFR 12](#_Toc206584944)

[3. Objectifs et problématique 13](#_Toc206584945)

[4. Méthodologie adoptée 14](#_Toc206584946)

[a. Analyse initiale du réseau IHFR 14](#_Toc206584947)

[b. Conception de la stratégie de sécurisation 14](#_Toc206584948)

[c. Mise en œuvre des mesures de protection 14](#_Toc206584949)

[d. Tests et évaluation 14](#_Toc206584950)

[e. Documentation et recommandations 14](#_Toc206584951)

[Chapitre I fondement de la cybersécurité 15](#_Toc206584951)

[1. Introduction 16](#_Toc206584952)

[2. Les concepts de la cybersécurité 16](#_Toc206584953)

[3. Les types de menaces et vulnérabilités 19](#_Toc206584954)

[4. Présentation des outils utilisés 21](#_Toc206584955)

[a. Ubuntu server 21](#_Toc206584956)

[b. Kali linux 22](#_Toc206584957)

[c. VirtualBox 23](#_Toc206584958)

[d. Cisco Packet Tracer 24](#_Toc206584959)

[5. Les bonnes pratique de sécurité réseau 25](#_Toc206584960)

[1. Systéme de détection d’intrusion 25](#_Toc206584961)

[2. La connaissance du paysage des menaces 26](#_Toc206584962)

[3. La gestion des incidents 26](#_Toc206584963)

[6. Conclusion 27](#_Toc206584964)

[**Chapitre** **II** **environment** **et** **préparation** 28](#_Toc206584964)

[1. Description de l’architecture réseau IHFR 29](#_Toc206584965)

[2. Matériels et logiciels utilisés 38](#_Toc206584966)

[3. Installation et configuration initiale des machines 38](#_Toc206584967)

[a. Objectif 39](#_Toc206584968)

[b. Installation des machines dans Packet Tracer 39](#_Toc206584969)

[c. Installation et Configuration Initiale de Kali Linux 40](#_Toc206584970)

[4. Plan d’adressage IP 40](#_Toc206584971)

[**Chapitre III diagnostic initial 43**](#_Toc206584971)

[1. Scan réseau avec Nmap 44](#_Toc206584972)

[2. Analyse de vulnérabilités avec NIKTO 45](#_Toc206584973)

[3. Analyse du trafic avec WIRESHARK 46](#_Toc206584974)

[4. Analyse et detection avec emun4linux 47](#_Toc206584975)

[5. Identification des failles de sécurité 47](#_Toc206584976)

[1. Sécurisation réseau dans packet tracer 49](#_Toc206584977)

[a. VLANs et segmentation 49](#_Toc206584978)

[b. Port Security 52](#_Toc206584979)

[2. Sécurisation serveur Ubuntu 54](#_Toc206584980)

[a. Permission fichiers 54](#_Toc206584981)

[b. suppression / blocage d’accés non autorisés 54](#_Toc206584982)

[c. Configuration firewall UFW 55](#_Toc206584983)

[3. Protection contre le sniffing 55](#_Toc206584984)

[a. ICMP blocking 56](#_Toc206584985)

[b. Filtrage des ports sensibles 56](#_Toc206584986)

[4. Durcissement hardware 57](#_Toc206584987)

[a. Mot de passe sur les équipements réseau 57](#_Toc206584988)

[b. Désactivation services inutiles 57](#_Toc206584989)

[**Chapitre V résultat et analyse 58**](#_Toc206584989)

[1. Introduction 59](#_Toc206584990)

[2. Les résultats des nouveaux scans 59](#_Toc206584991)

[3. Comparaison avant/ aprés la sécurisation 62](#_Toc206584992)

[4. Conclusion 63](#_Toc206584993)

[5. L’évolution de la protection et sécurité du réseau de IHFR 64](#_Toc206584994)

[6. Grosse au mode des résultats 64](#_Toc206584995)

[**• Conclusion et recommadations 65**](#_Toc206584996)

[1. Bilan du projet 65](#_Toc206584997)

[2. Limites rencontrées 65](#_Toc206584998)

[3. Perspectives d’amélioration 66](#_Toc206584999)

[REFERENCES BIBLIOGRAPHIQUES 67](#_Toc206585000)

# Liste des abréviations

* **IHFR** : Institut Hydrométéorologique de Formation et de Recherches
* **LAN** : Local Area Network (Réseau local)
* **VLAN** : Virtual Local Area Network (Réseau local virtuel)
* **IP** : Internet Protocol
* **DHCP** : Dynamic Host Configuration Protocol
* **DNS** : Domain Name System
* **HTTP** : HyperText Transfer Protocol
* **HTTPS** : HyperText Transfer Protocol Secure
* **FTP** : File Transfer Protocol
* **SSH** : Secure Shell
* **IDS** : Intrusion Detection System (Système de Détection d’Intrusion)
* **IPS** : Intrusion Prevention System (Système de Prévention d’Intrusion)
* **UFW** : Uncomplicated Firewall
* **ACL** : Access Control List (Liste de contrôle d’accès)
* **NAT** : Network Address Translation
* **PAT** : Port Address Translation
* **MITM** : Man In The Middle (Attaque de l’homme du milieu)
* **AP** : Access Point (Point d’accès)
* **NIC** : Network Interface Card (Carte réseau)
* **OS** : Operating System (Système d’exploitation)
* **VM** : Virtual Machine (Machine virtuelle)
* **Nmap** : Network Mapper (outil de scan réseau)
* **Nikto** : Web Vulnerability Scanner (scanner de vulnérabilités web)
* **Wireshark** : Network Protocol Analyzer (analyseur de trafic réseau)
* ​
* **Enum4linux** : Outil d’énumération d’informations sur les systèmes Windows/Linux via SMB
* **SMB** : Server Message Block (Protocole de partage de fichiers et imprimantes)
* **DoS** : Denial of Service (Déni de service)
* **DDoS** : Distributed Denial of Service (Déni de service distribué)
* **XSS** : Cross-Site Scripting
* **CIA** : Confidentiality, Integrity, Availability (Confidentialité, Intégrité, Disponibilité)
* **APT** : Advanced Persistent Threat (Menace persistante avancée)
* **IP** : Internet Protocol
* **ping** : Packet Internet Groper (Commande de test de connectivité réseau)
* **ifconfig** : Interface Config (Affichage configuration réseau – remplacé par ip)
* **ip** : Internet Protocol (Commande moderne pour gestion IP et routes)
* **netstat** : Network Statistics (Statistiques réseau et connexions actives)
* **traceroute** : Trace Route (Tracer le chemin réseau d’un paquet)
* **arp** : Address Resolution Protocol (Table ARP)
* **nslookup** : Name Server Lookup (Résolution DNS)
* **dig** : Domain Information Groper (Interrogation DNS avancée)
* **ufw** : Uncomplicated Firewall (Pare-feu simplifié Ubuntu)
* **iptables** : IP Tables (Filtrage de paquets Linux)
* **ssh** : Secure Shell (Connexion sécurisée à distance)
* **openssl** : Open Secure Sockets Layer (Outil de cryptographie et certificats)
* **nmap** : Network Mapper (Scan réseau et ports)
* **nikto** : Web Vulnerability Scanner (Scanner de vulnérabilités web)
* **wireshark** : Network Protocol Analyzer (Analyse de trafic réseau)
* **tcpdump** : TCP Dump (Capture et analyse en ligne de commande)
* ​
* **enum4linux** : Enumeration for Linux (Énumération SMB sur serveurs Windows/Linux)
* **lynis** : Linux Audit System (Audit de sécurité sur Linux)
* **apt** : Advanced Package Tool (Gestionnaire de paquets Ubuntu/Debian)
* **systemctl** : System Control (Gestion des services sous systemd)
* **service** : Commande de gestion de services (ancien système init)
* **ps** : Process Status (Affichage des processus actifs)
* **top** : Table Of Processes (Affichage dynamique des processus)
* **htop** : Interactive Process Viewer (Version interactive améliorée de top)
* **chmod** : Change Mode (Modification des permissions de fichiers)
* **chown** : Change Owner (Modification propriétaire/groupe d’un fichier)
* **ls** : List (Lister les fichiers et dossiers)
* **cd** : Change Directory (Changer de répertoire)
* **pwd** : Print Working Directory (Afficher le chemin du répertoire courant)
* **mkdir** : Make Directory (Créer un dossier)
* **rm** : Remove (Supprimer un fichier ou dossier)
* **cp** : Copy (Copier un fichier ou dossier)
* **mv** : Move (Déplacer ou renommer un fichier/dossier)
* **Packet Tracer (CLI)** : Console d’administration Cisco

# 

# Listes des figures

[‎1 Architecture réseau globale de l’IHFR 13](#_Toc206607145)

[‎2 Les organisations réglementaire du cybersécurité 19](#_Toc206607146)

[‎3 Logo de UBUNTU SERVER 22](#_Toc206607147)

[‎4: Logo de KALI LINUX 23](#_Toc206607148)

[‎5 Logo de VIRTUALBOX 24](#_Toc206607149)

[‎6 Logo de cisco packet tracer 24](file:///C:\Users\OUSSAMA\Desktop\STUDY\MEMOIRE\MEMOIRE%20DOCUMENT.docx#_Toc206607150)

[‎7: Schéma de le principe de circulation des données en utilisant détection d’intrusion 25](file:///C:\Users\OUSSAMA\Desktop\STUDY\MEMOIRE\MEMOIRE%20DOCUMENT.docx#_Toc206607151)

[‎8 Schéma de la La gestion des incidents 27](#_Toc206607152)

[‎9 Architecture réseau globale de l’IHFR 29](#_Toc206607153)

[**‎10** Schéma du la salle serveur 30](file:///C:\Users\OUSSAMA\Desktop\STUDY\MEMOIRE\MEMOIRE%20DOCUMENT.docx#_Toc206607154)

[‎11 la salle serveur du l’institut 30](file:///C:\Users\OUSSAMA\Desktop\STUDY\MEMOIRE\MEMOIRE%20DOCUMENT.docx#_Toc206607155)

## Introduction

Dans un environnement numérique où les échanges de données sont constants et stratégiques, la sécurité réseau constitue un enjeu majeur pour toute organisation. L’IHFR, en tant qu’infrastructure critique, doit garantir la disponibilité, l’intégrité et la confidentialité des informations circulant sur son réseau. Les menaces telles que les intrusions, le phishing, les malwares ou encore les interceptions de données peuvent compromettre non seulement le fonctionnement interne, mais également la réputation et la confiance des partenaires. Dans ce contexte, la mise en place de mesures de protection robustes, adaptées aux besoins spécifiques de l’institution, est indispensable. La cybersécurité réseau ne se limite pas à un simple ensemble d’outils techniques : elle repose également sur une organisation proactive, une surveillance continue et une formation des utilisateurs afin de prévenir, détecter et réagir efficacement aux incidents.

## Présentation du réseau IHFR

L’Institut Hydrométéorologique de Formation et de Recherches (I.H.F.R.) a été créé en 1970 par l’ordonnance 70-52 du 20/07/70 pour former les personnels météorologiques de différents niveaux et assurer la spécialisation et la qualification en météorologie.

En 1974, l’I.H.F.R. a été agréé comme Centre Régional de Formation Professionnelle en Météorologie par l’Organisation Météorologique Mondiale (O.M.M.) et à ce titre, il a la charge de former les météorologues des pays africains.

En 1988, il a été érigé en Institut National de Formation Supérieure, sous tutelle administrative du Ministère des Transports et sous tutelle pédagogique du Ministère de l’Enseignement Supérieur par Décret 88-207 du 18-10-88.

**Siège :** Hail Ibn Rochd HLM Gambetta – Oran, BP 7019 EsSeddikia 31025 Oran

**Tel:**041421221/041422801

**Fax :** 041 421 312 / 041 422 801

l’infrasrtucture de ’Institut Hydrométéorologique de Formation et de Recherche (IHFR) est composé de :

7 département : la direction, la tour, imprimerie, pédagogie, bilbiothéque, salle standard et salle serveur.

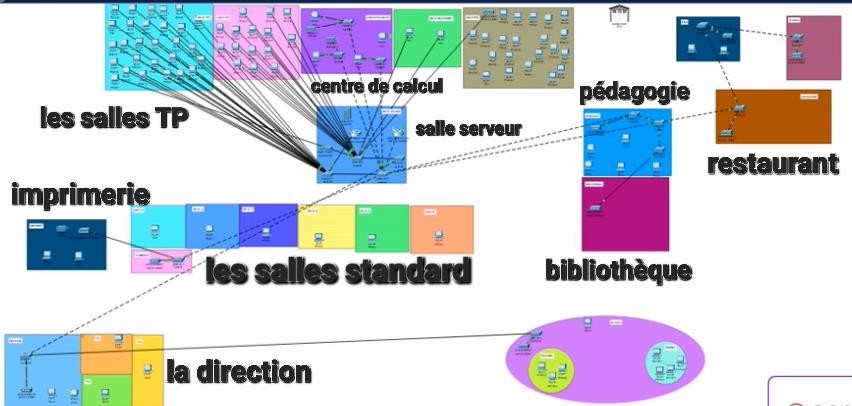
113 PC répartis sur 32 salles

1 serveur principal

2 routeurs principaux

17 switches

10 points d’accès Wi-Fi



‎0‑1 Architecture réseau globale de l’IHFR

Ce schéma présente la structure de les équipements installer sur les département de l’infrasrtructure, il contient :

Deux routeurs interconnectés

Un cœur de réseau avec un serveur

Plusieurs switches connectés au département Accès Wi-Fi pour zones spécifiques

Liaison Ethernet entre les bâtiments

## Objectifs et problématique

L’objectif principal de ce projet est de concevoir et mettre en œuvre une architecture réseau sécurisée pour l’IHFR, capable de résister aux menaces internes et externes tout en garantissant la continuité des services. Plus spécifiquement, il s’agit de :

Identifier et analyser les vulnérabilités présentes dans le réseau existant.

Mettre en place des mesures de protection adaptées, incluant des solutions matérielles et logicielles. Renforcer la résilience du système face aux attaques courantes telles que les scans, intrusions, sniffing ou exploitation de failles web.

Évaluer l’efficacité des mesures déployées à travers des tests avant et après sécurisation.

La problématique à laquelle nous répondons est la suivante :

###### Comment assurer la sécurité et la fiabilité du réseau IHFR face à l’augmentation constante des cybermenaces, tout en maintenant un fonctionnement optimal et accessible aux utilisateurs autorisés ?

Ce questionnement implique de trouver un équilibre entre performance, accessibilité et robustesse sécuritaire, en tenant compte des contraintes matérielles, logicielles et organisationnelles de l’IHFR.

## Méthodologie adoptée

Pour atteindre les objectifs fixés, nous avons suivi une approche méthodique en plusieurs étapes, combinant analyse, mise en œuvre et évaluation :

### **Analyse initiale du réseau IHFR**

Recensement des équipements matériels et logiciels existants. Observation de la topologie réseau.

Réalisation de scans et d’analyses préliminaires (Nmap, Nikto, Wireshark) afin de mettre en évidence les vulnérabilités.

### **Conception de la stratégie de sécurisation**

Définition des priorités en fonction du niveau de criticité des failles détectées.

Choix des outils de protection adaptés (pare-feu UFW, IDS/IPS avec Snort et Suricata, segmentation VLAN, contrôle d’accès, etc.).

Élaboration d’un plan d’adressage IP structuré pour optimiser la gestion et la sécurité des flux.

### **Mise en œuvre des mesures de protection**

Configuration et durcissement des serveurs sous **Ubuntu Server**.

Segmentation du réseau avec **VLANs** et implémentation de la **Port Security** dans Packet Tracer. Mise en place des règles de pare-feu et blocage des services inutiles.

Application de politiques d’accès strictes et sécurisation physique du matériel.

### **Tests et évaluation**

Réalisation de nouveaux scans et analyses après sécurisation.

Comparaison des résultats avant/après pour mesurer l’efficacité des actions. Ajustement des configurations en fonction des résultats obtenus.

### **Documentation et recommandations**

Rédaction du rapport technique détaillant les mesures appliquées et leurs impacts. Proposition d’axes d’amélioration pour renforcer encore la sécurité.

Cette méthodologie a permis de structurer le projet, de limiter les risques d’oubli et d’assurer que chaque action entreprise réponde à une menace ou un besoin clairement identifié.

**Chapitre I fondement de la cybersécurité**

## Introduction

Une **cyberattaque** est une action malveillante menée par un individu ou un groupe, souvent externe à l’organisation, visant à exploiter les vulnérabilités d’un système informatique ou d’un utilisateur. Elle peut prendre différentes formes, comme le fait de contacter une personne au hasard en lui proposant de fausses offres, promotions ou messages d’alerte, dans le but de tromper sa vigilance.

L’attaquant cherche ainsi à manipuler la victime pour qu’elle communique des informations sensibles, comme ses identifiants, mots de passe ou données bancaires. Une fois ces données obtenues, elles peuvent être utilisées pour accéder illicitement à des systèmes, détourner des fonds, usurper une identité ou nuire à la réputation de la victime ou de son organisation. Ce type d’attaque s’appuie souvent sur l’ingénierie sociale, la fraude en ligne et d’autres techniques de manipulation psychologique, exploitant la confiance ou l’inattention de l’utilisateur.

La **cybersécurité** est l’ensemble des pratiques, techniques et mesures mises en place pour protéger et sécuriser les données, les réseaux et les systèmes informatiques contre toute forme de menace ou d’accès non autorisé. Elle repose sur trois principes fondamentaux : **l’intégrité**, qui garantit que les données ne sont pas altérées ou modifiées de manière non autorisée ; **la confidentialité**, qui assure que seules les personnes autorisées peuvent accéder aux informations sensibles ; et **la disponibilité**, qui veille à ce que les systèmes et les données soient accessibles en permanence aux utilisateurs légitimes. La cybersécurité englobe aussi bien la protection contre les attaques externes (piratage, malwares, phishing) que contre les menaces internes, et implique l’utilisation de pare-feu, de systèmes de détection d’intrusion, de politiques de sécurité strictes et de sensibilisation des utilisateurs. Elle joue un rôle essentiel dans la préservation de la confiance et la continuité des activités dans un environnement numérique de plus en plus exposé aux risques.

La **sécurité réseau** est l’ensemble des pratiques et des mesures mises en œuvre pour protéger l’infrastructure informatique d’une organisation contre tout accès non autorisé, toute utilisation abusive ou toute tentative d’intrusion. Elle englobe la protection des équipements physiques (routeurs, serveurs, commutateurs) ainsi que des communications et des flux de données circulant sur le réseau. Pour garantir cette sécurité, on utilise divers mécanismes tels que les pare-feu, les systèmes de détection et de prévention d’intrusion (IDS/IPS), le chiffrement des communications, l’authentification forte et la segmentation du réseau. L’objectif principal est de préserver la confidentialité, l’intégrité et la disponibilité des informations tout en assurant le bon fonctionnement des services.

## Les concepts de la cybersécurité

La cybersécurité regroupe l’ensemble des méthodes, outils et politiques visant à protéger les systèmes informatiques, les réseaux et les données contre toute forme d’accès non autorisé, de compromission ou de perturbation. Dans le cadre de la protection des infrastructures organisationnelles, plusieurs pratiques sont considérées comme essentielles.

Tout d’abord, **la configuration optimale des pare-feu** constitue une mesure primordiale pour filtrer le trafic réseau, empêcher les intrusions et limiter les communications aux seules connexions autorisées. Ensuite, **l’installation et la mise à jour régulière de logiciels de protection** — tels que les antivirus, les systèmes anti-malware ou encore les systèmes de détection et de prévention d’intrusion (IDS/IPS) — permettent de réduire significativement les risques liés aux cyberattaques. De plus, **la mise en place de renforts matériels** (appliances de sécurité réseau, dispositifs de segmentation physique, systèmes de contrôle d’accès) offre une couche supplémentaire de

protection. Par ailleurs, **l’utilisation de systèmes de leurre** comme les honeypots permet de détecter et d’analyser les tentatives d’intrusion en temps réel, tout en collectant des informations précieuses sur les techniques utilisées par les attaquants. Ces pratiques s’articulent autour de plusieurs concepts structurants :

1. **La conformité réglementaire (compliance)** consiste à respecter les normes, lois et directives imposées par les autorités nationales ou internationales, afin d’assurer un niveau de sécurité conforme et d’éviter d’éventuelles sanctions légales ou financières.
2. **Contrôles spécifiques, cadres et conformité**  
   Le National Institute of Standards and Technology (NIST) est une agence américaine qui développe plusieurs cadres de conformité volontaires, que les organisations du monde entier peuvent utiliser afin de mieux gérer les risques. Plus une organisation est alignée sur ces cadres de conformité, plus son niveau de risque diminue.
3. Parmi les exemples de cadres proposés figurent le **NIST Cybersecurity Framework (CSF)** et le **NIST Risk Management Framework (RMF)**.
4. **La Federal Energy Regulatory Commission – North American Electric Reliability Corporation (FERC-NERC)**  
   La FERC-NERC est une réglementation qui s’applique aux organisations travaillant dans le domaine de l’électricité ou impliquées dans le réseau électrique des États-Unis et d’Amérique du Nord. Ces organisations ont l’obligation de se préparer, d’atténuer et de signaler tout incident de sécurité susceptible d’affecter négativement le réseau électrique. Elles sont également tenues, d’un point de vue légal, de respecter les Critical Infrastructure Protection (CIP) Reliability Standards définis par la FERC.
5. **Le Federal Risk and Authorization Management Program (FedRAMP®)**  
   FedRAMP est un programme du gouvernement fédéral des États-Unis qui standardise l’évaluation de la sécurité, l’autorisation, la surveillance et la gestion des services et solutions en nuage (cloud). Son objectif est d’assurer une cohérence à l’échelle du secteur public américain ainsi qu’avec les fournisseurs de services infonuagiques tiers.
6. **Le Center for Internet Security (CIS®)**  
   Le CIS est une organisation à but non lucratif intervenant dans plusieurs domaines. Elle fournit un ensemble de contrôles destinés à protéger les systèmes et réseaux contre les attaques. Son objectif est d’aider les organisations à établir un plan de défense renforcé. Le CIS propose également des contrôles opérationnels que les professionnels de la sécurité peuvent appliquer en cas d’incident de sécurité.
7. **Le Règlement général sur la protection des données (RGPD / GDPR)**  
   Le RGPD est une réglementation générale de l’Union européenne (UE) visant à protéger le traitement des données des résidents de l’UE ainsi que leur droit à la vie privée, à l’intérieur comme à l’extérieur du territoire de l’UE. Par exemple, si une organisation ne fait pas preuve de transparence quant aux données qu’elle détient sur un citoyen de l’UE et aux raisons de cette conservation, elle commet une infraction susceptible d’entraîner une amende. De plus, en cas de violation et de compromission des données d’un citoyen européen, celui-ci doit être informé. L’organisation concernée dispose de **72 heures** pour notifier le citoyen de l’UE de cette violation.
8. **Payment Card Industry Data Security Standard (PCI DSS)**  
   Le **PCI DSS** est une norme internationale de sécurité conçue pour garantir que les organisations qui stockent, acceptent, traitent ou transmettent des informations liées aux cartes de paiement le fassent dans un environnement sécurisé. L’objectif principal de cette norme de conformité est de réduire la fraude liée aux cartes bancaires.
9. **Health Insurance Portability and Accountability Act (HIPAA)**  
   La loi fédérale américaine **HIPAA**, adoptée en 1996, vise à protéger les informations médicales des patients. Elle interdit le partage de ces informations sans le consentement des personnes concernées. HIPAA est régie par trois règles fondamentales :

**Confidentialité (Privacy Rule)**

**Sécurité (Security Rule)**

**Notification en cas de violation (Breach Notification Rule)**

Les organisations qui stockent des données médicales ont l’obligation légale d’informer les patients en cas de violation de données, car si les **informations de santé protégées (Protected Health Information – PHI)** sont compromises, cela peut entraîner un vol d’identité ou des fraudes à l’assurance. Les PHI englobent les informations relatives à l’état de santé physique ou mental passé, présent ou futur d’un individu, qu’il s’agisse d’un plan de soins ou de paiements liés à ces soins.

En complément de la compréhension de la loi HIPAA, les professionnels de la sécurité doivent également être familiers avec le **Health Information Trust Alliance (HITRUST®)**, qui constitue un cadre de sécurité et un programme d’assurance aidant les institutions à se conformer aux exigences de l’HIPAA.

1. **International Organization for Standardization (ISO)**  
   L’**ISO** a été créée afin d’établir des normes internationales dans les domaines de la technologie, de la fabrication et de la gestion, au-delà des frontières nationales. Elle aide les organisations à améliorer leurs processus et procédures, notamment en matière de gestion des ressources humaines, de planification, de réduction des gaspillages et de qualité des services.
2. **System and Organization Controls (SOC type 1, SOC type 2)**  
   Les standards **SOC 1** et **SOC 2** ont été élaborés par l’**American Institute of Certified Public Accountants (AICPA)** à travers son *Auditing Standards Board*.  
   Ils consistent en une série de rapports qui évaluent les politiques de gestion des accès aux données d’une organisation, à différents niveaux hiérarchiques, tels que :

* Associé
* Superviseur
* Responsable / Manager
* Cadre exécutif
* Fournisseur
* Autres parties prenantes

Ces rapports servent à mesurer la conformité financière et le niveau de gestion des risques d’une organisation. Ils couvrent également la confidentialité, la vie privée, l’intégrité, la disponibilité, la sécurité et la protection globale des données. Tout échec de contrôle dans ces domaines peut conduire à des fraudes.

1. **Les cadres de sécurité (security frameworks)** offrent une méthodologie structurée et des bonnes pratiques permettant de planifier les tâches de prévention, de détection, de réponse et de récupération, assurant ainsi une protection complète et cohérente.
2. **Les contrôles de sécurité (security controls)** englobent l’ensemble des mesures techniques, physiques, managériales et opérationnelles permettant de mettre en application les politiques de sécurité établies. Ces contrôles visent à identifier les vulnérabilités et à mettre en place les solutions adaptées pour chaque scénario de menace.
3. **La posture de sécurité (security posture)** correspond à l’état global de la sécurité d’une organisation, reflétant sa capacité à anticiper, prévenir, détecter et contrer efficacement les menaces. Elle constitue un indicateur clé de la maturité et de la résilience en matière de cybersécurité. En somme, la mise en œuvre cohérente et coordonnée de ces pratiques et concepts permet de construire une architecture de sécurité robuste, capable de faire face aux menaces toujours plus complexes dans un environnement numérique en constante évolution.

****

‎0‑2 Les organisations réglementaire du cybersécurité

## Les types de menaces et vulnérabilités

Les systèmes informatiques et les réseaux sont exposés à une diversité de menaces et de vulnérabilités, chacune présentant des modes d’attaque spécifiques et des impacts potentiellement graves. Parmi celles-ci, **les attaques par logiciels malveillants (malware)** constituent une catégorie majeure : elles reposent sur l’installation, volontaire ou non, d’un programme conçu pour causer des dommages, altérer le fonctionnement du système ou compromettre l’intégrité et la confidentialité des données. Ces logiciels peuvent inclure des virus, des chevaux de Troie, des ransomwares ou encore des spywares.

Une autre menace fréquente est **l’attaque par hameçonnage (phishing)**, qui consiste en une action frauduleuse visant à tromper l’utilisateur en imitant des communications légitimes, dans le but de l’inciter à divulguer des informations sensibles, telles que des identifiants de connexion ou des coordonnées bancaires.

Un autre type, Le **baiting** est une technique d’ingénierie sociale qui exploite la curiosité ou la cupidité des individus afin de compromettre leur sécurité. Cette méthode consiste à attirer la victime avec un « appât » physique ou numérique, souvent présenté comme quelque chose d’utile, d’intéressant ou de gratuit, mais qui cache en réalité une menace. Un exemple courant est le **USB baiting**, où un attaquant dépose intentionnellement une clé USB infectée dans un lieu public ou au sein d’une entreprise, en espérant que quelqu’un la trouve et, par curiosité ou par nécessité, la branche à son ordinateur. Une fois connectée, le périphérique exécute un logiciel malveillant capable de voler des données, d’installer un accès à distance ou de chiffrer les fichiers de la victime. Le baiting ne se limite pas aux supports physiques : il peut également prendre la forme de téléchargements gratuits en ligne, de fausses mises à jour logicielles ou d’offres promotionnelles frauduleuses. Cette technique est particulièrement dangereuse, car elle contourne souvent les mesures de sécurité technique en exploitant le facteur humain, soulignant ainsi l’importance de la sensibilisation et de la formation des utilisateurs à la cybersécurité

On a aussi, Le **watering hole** qui signifi une technique d’attaque ciblée dans laquelle un acteur

malveillant compromet un site web régulièrement fréquenté par un groupe spécifique d’utilisateurs, dans le but d’infecter leurs systèmes ou de voler des informations. Le principe repose sur l’observation des habitudes de navigation de la cible : au lieu d’attaquer directement les victimes, l’attaquant infiltre un site de confiance qu’elles consultent fréquemment. Ce site, devenu piégé, héberge alors des scripts malveillants ou des fichiers infectés, qui exploitent les vulnérabilités des navigateurs ou des systèmes des visiteurs. Un exemple marquant est l’**attaque Holy Water** de 2020, au cours de laquelle plusieurs sites religieux, caritatifs et de bénévolat ont été compromis pour diffuser des malwares aux visiteurs ciblés. Cette méthode est particulièrement redoutable car elle repose sur la confiance préexistante envers le site compromis, rendant la détection plus difficile. Pour s’en prémunir, il est essentiel de maintenir les navigateurs et extensions à jour, d’utiliser des solutions de détection avancée et de sensibiliser les utilisateurs à ne pas accorder une confiance aveugle, même aux sites réputés fiables.

Enfin, **l’attaque de l’homme du milieu (Man-in-the-Middle, MITM)** se produit lorsqu’un attaquant intercepte et manipule les communications entre un utilisateur et un serveur. En s’interposant dans l’échange, il peut accéder aux données transmises, voler des adresses IP, ou se faire passer pour l’expéditeur ou le destinataire légitime, compromettant ainsi la confidentialité et l’intégrité de la communication.

## Présentation des outils utilisés

Dans le cadre de la mise en place et de l’évaluation des mesures de cybersécurité du réseau IHFR, plusieurs outils logiciels et environnements ont été mobilisés. **Ubuntu Server** a servi de système d’exploitation principal pour l’hébergement des services et la configuration des solutions de sécurité, tandis que **Kali Linux** a été utilisé comme plateforme spécialisée pour les tests d’intrusion et les audits de sécurité. L’environnement de virtualisation **VirtualBox** a permis de déployer et d’isoler les machines virtuelles nécessaires aux simulations. Pour la simulation et la modélisation de l’infrastructure réseau physique, l’outil **Cisco Packet Tracer** a été exploité. Sur le plan de la protection, le pare-feu **UFW** a été configuré pour filtrer le trafic réseau, tandis que les systèmes de détection et de prévention d’intrusions **Snort** et **Suricata** ont permis d’identifier les activités malveillantes. L’accès sécurisé aux serveurs a été assuré via **SSH**, et le service **Apache2** a été utilisé pour l’hébergement web. Le serveur DNS a été implémenté à l’aide de **Bind9**, et la configuration réseau a été gérée avec **Netplan**. Pour l’audit de sécurité approfondi, l’outil **Lynis** a fourni une analyse détaillée de la configuration du système. Enfin, **Wireshark** et **Nmap** ont été employés respectivement pour l’analyse approfondie du trafic réseau et pour l’exploration ainsi que la cartographie des hôtes et services disponibles sur le réseau.

## Ubuntu server

**Ubuntu Server** est une déclinaison du système d’exploitation Ubuntu spécifiquement conçue et développée pour constituer l’ossature des infrastructures informatiques et servir de pilier au fonctionnement d’Internet. Il s’appuie sur la robustesse, la sécurité et la flexibilité d’Ubuntu afin de répondre aux besoins variés des entreprises, des institutions et des fournisseurs de services.

Grâce à son architecture optimisée, **Ubuntu Server** offre une évolutivité à la fois économique et technique, adaptée aussi bien aux centres de données publics qu’aux environnements privés. Il permet de déployer efficacement des infrastructures complexes, telles qu’un cloud OpenStack, un cluster Kubernetes ou encore une ferme de rendu pouvant atteindre 50 000 nœuds, tout en assurant une gestion optimisée des ressources

Reconnu pour sa stabilité, sa compatibilité matérielle étendue et sa vaste communauté de support, **Ubuntu Server** se distingue par sa capacité à offrir un rapport qualité-prix exceptionnel, en garantissant des performances de type *scale-out* idéales pour les environnements à forte charge et pour les besoins de calcul distribué à grande échelle.



‎0‑3 Logo de UBUNTU SERVER

## Kali linux

**Kali Linux** (anciennement connu sous le nom de **BackTrack Linux**) est une distribution Linux open source, basée sur Debian, permettant d’effectuer des tests de pénétration avancés et des audits de sécurité. Elle fonctionne sur de multiples plateformes et est librement accessible, aussi bien aux professionnels de la sécurité informatique qu’aux passionnés.

Cette distribution intègre plusieurs centaines d’outils, de configurations et de scripts, incluant des modifications spécifiques au secteur, afin de permettre aux utilisateurs de se concentrer sur des tâches spécialisées telles que la criminalistique informatique (*computer forensics*), l’ingénierie inverse et la détection de vulnérabilités, sans être distraits par des activités sans rapport.

Spécialement conçue pour répondre aux besoins des testeurs d’intrusion expérimentés, cette distribution suppose que l’utilisateur possède déjà une connaissance approfondie et une familiarité avec le système d’exploitation Linux en général.

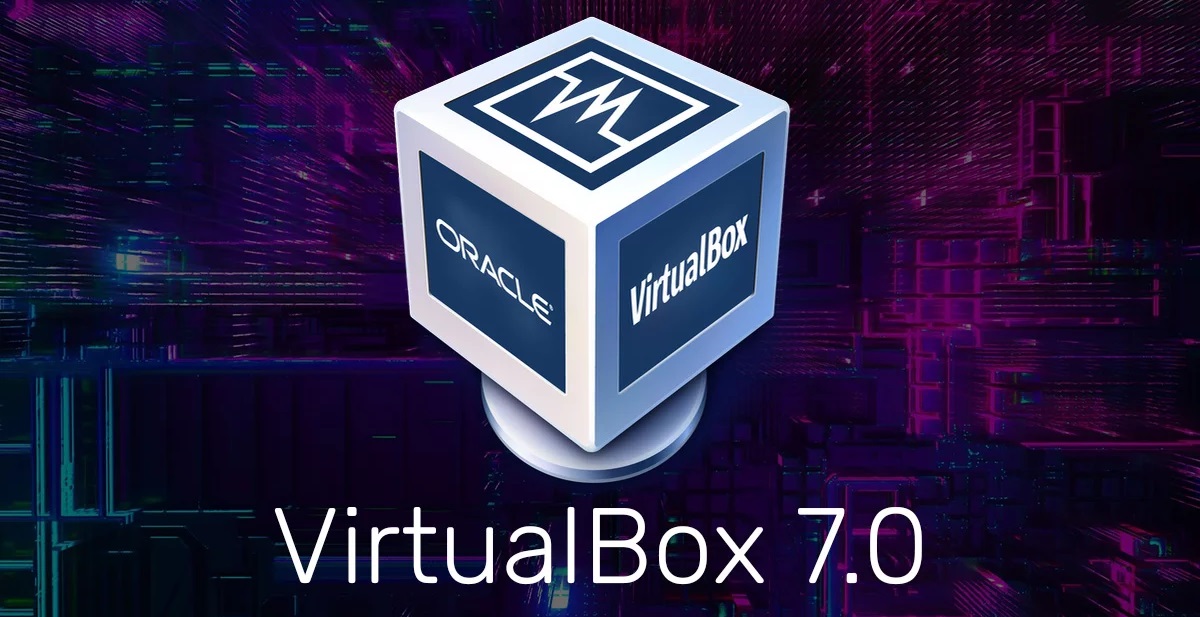


‎0‑4: Logo de KALI LINUX

### **VirtualBox**

**Oracle VM VirtualBox** est une application de virtualisation multiplateforme. Que signifie cela ? D’une part, elle peut être installée sur vos ordinateurs existants équipés de processeurs Intel ou AMD, qu’ils fonctionnent sous Windows, macOS, Linux ou Oracle Solaris. D’autre part, elle étend les capacités de votre ordinateur en lui permettant d’exécuter simultanément plusieurs systèmes d’exploitation au sein de machines virtuelles distinctes.

Par exemple, il est possible d’exécuter Windows et Linux sur un Mac, d’exécuter Windows Server sur un serveur Linux, ou encore de faire tourner Linux sur un PC Windows, et ce, tout en continuant à utiliser vos applications existantes. Vous pouvez installer et exécuter autant de machines virtuelles que vous le souhaitez, les seules limites pratiques étant l’espace disque disponible et la mémoire vive.



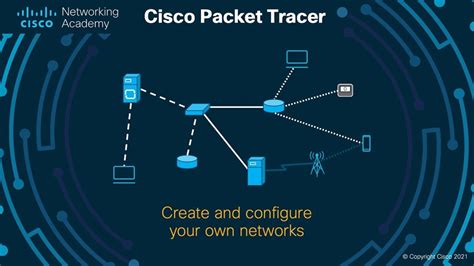
‎0‑5 Logo de VIRTUALBOX

### **Cisco Packet Tracer**

Cisco Packet Tracer est un logiciel de simulation réseau complet, destiné à l’enseignement et à l’apprentissage de la création de topologies réseau et de la reproduction de réseaux informatiques modernes. Cet outil offre une combinaison unique d’expériences réalistes de simulation et de visualisation, de fonctionnalités d’évaluation et de création d’activités, ainsi que des possibilités de collaboration et de compétition entre utilisateurs.

Grâce à ses fonctionnalités innovantes, il aide les étudiants et les enseignants à collaborer, à résoudre des problèmes et à assimiler les concepts réseaux dans un

environnement social stimulant et dynamique.



‎0‑6 Logo de cisco packet tracer

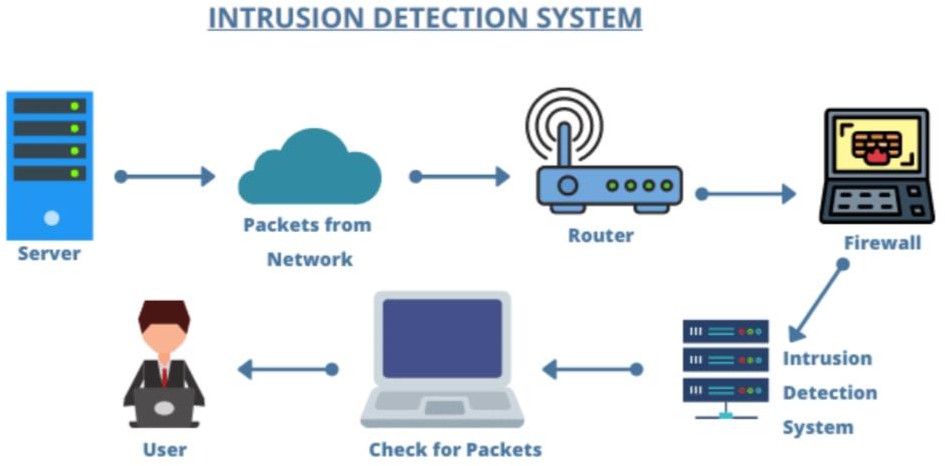
## Les bonnes pratique de sécurité réseau

La sécurité réseau repose sur l’application de bonnes pratiques visant à réduire les risques de compromission et à assurer la confidentialité, l’intégrité et la disponibilité des données. Parmi les mesures fondamentales, on retrouve la mise en place d’une segmentation réseau afin de limiter la propagation d’attaques et de mieux contrôler les flux de données. L’utilisation de pare-feux correctement configurés et de systèmes de détection/prévention d’intrusions permet de filtrer et surveiller le trafic en temps réel. Le recours à des protocoles sécurisés, tels que SSH pour l’administration à distance et HTTPS pour les échanges web, garantit la protection des communications contre les interceptions. Il est également essentiel de maintenir à jour l’ensemble des systèmes et applications pour corriger rapidement les vulnérabilités connues. L’authentification forte, combinée à une gestion stricte des droits

d’accès, renforce la protection des ressources sensibles. Enfin, la mise en place de solutions de sauvegarde régulière et de plans de reprise après sinistre assure la continuité des activités en cas d’incident majeur.

### **Systéme de détection d’intrusion**

Un système de détection d’intrusion (*Intrusion Detection System – IDS*) est un dispositif ou un logiciel spécialisé dont la fonction principale est de surveiller, analyser et détecter en temps réel toute activité suspecte ou malveillante au sein d’un réseau informatique ou d’un système d’information. Il permet d’identifier des tentatives d’accès non autorisé, des comportements anormaux ou des attaques connues et inconnues pouvant compromettre l’intégrité, la confidentialité ou la disponibilité des données et des ressources. L’IDS joue un rôle crucial dans la protection des actifs informationnels et des infrastructures critiques, en fournissant aux administrateurs réseau des alertes précises pour réagir rapidement face aux menaces. En complément de cette capacité de détection, certains systèmes IDS peuvent être couplés à des mécanismes de prévention (IPS – *Intrusion Prevention System*) afin de bloquer automatiquement les activités hostiles avant qu’elles n’atteignent leurs cibles. Ce type de technologie s’inscrit dans une approche proactive de la cybersécurité, visant à renforcer la résilience des systèmes face à l’évolution constante des menaces informatiques.



‎0‑7: Schéma de le principe de circulation des données en utilisant détection d’intrusion

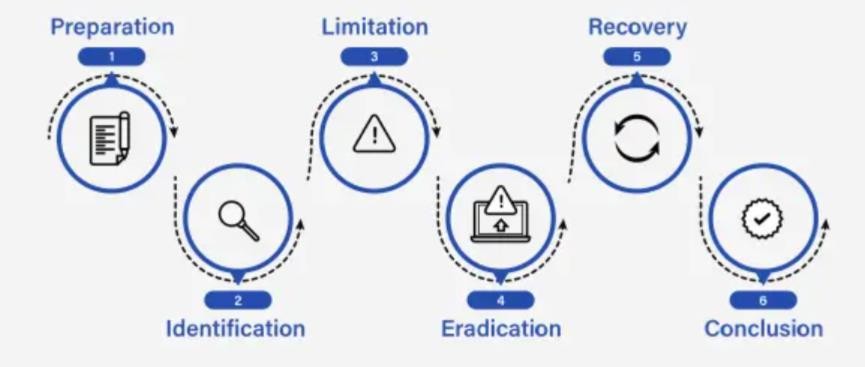
Ce schéma illustre le principe de circulation des données en utilisant notre système de détection d’intrusion (IDS). Le processus commence par l’envoi de requêtes par l’utilisateur (*user*). Avant que le serveur ne réponde directement, les paquets transitent par le réseau Internet, où le routeur les intercepte pour les filtrer à l’aide du pare-feu (*firewall*). Ainsi, les données ne sont pas uniquement filtrées par le pare-feu : le système IDS analyse et surveille également toutes les activités suspectes. Si tous les paquets de données sont jugés légitimes, l’utilisateur reçoit les informations de manière sécurisée, prêtes à être utilisées.

### **La connaissance du paysage des menaces**

La connaissance du paysage des menaces (« threat landscape knowledge ») constitue un élément fondamental de la cybersécurité moderne. Elle consiste à suivre de manière régulière et systématique l’actualité, les rapports spécialisés et les mises à jour concernant les menaces informatiques, notamment les attaques de rançongiciels (ransomware) et les activités des acteurs malveillants. Cette veille proactive permet d’identifier les tendances émergentes, les nouvelles vulnérabilités, ainsi que les techniques, tactiques et procédures utilisées par les cybercriminels. En s’appuyant sur ces informations, les organisations peuvent adapter leurs mesures de protection, renforcer leurs politiques de sécurité, et mettre en place des plans de défense adaptés afin de prévenir les pertes de données et de limiter l’impact des cyberattaques. Une telle démarche implique la mobilisation de sources fiables, la collaboration avec des communautés de sécurité, et l’intégration de ces connaissances dans la stratégie globale de gestion des risques.

### **La gestion des incidents**

En réponse aux incidents de sécurité informatique, la gestion des incidents (Incident Response) consiste à mettre en place un ensemble structuré de politiques, de procédures et de mécanismes opérationnels visant à détecter, analyser, contenir, éradiquer et remédier aux menaces susceptibles de compromettre la sécurité du système d’information. Cette approche proactive et organisée permet non seulement de limiter l’impact des attaques, mais aussi de rétablir rapidement la continuité des opérations. Parmi les incidents les plus fréquents figurent les campagnes de phishing (hameçonnage) par courriel, qui visent à tromper les utilisateurs afin d’obtenir frauduleusement des informations sensibles ou d’introduire des logiciels malveillants dans le réseau. La méthodologie adoptée dans un plan de réponse aux incidents repose généralement sur plusieurs étapes clés : la préparation (mise en place des outils et formation des équipes), la détection et l’analyse (identification rapide de l’incident et évaluation de son ampleur), la containment (isolation des systèmes compromis), l’éradication (suppression de la menace), la récupération (restauration des systèmes) et enfin le retour d’expérience (analyse post- incident pour améliorer les mesures préventives). Une telle organisation assure non seulement une défense réactive, mais aussi un renforcement continu de la posture de cybersécurité.



‎0‑8 Schéma de la La gestion des incidents

## Conclusion

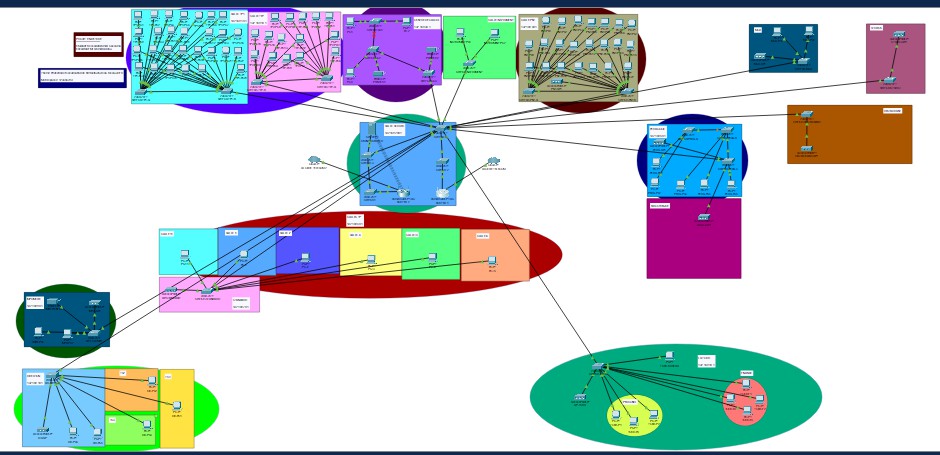
Nous avons abordé plusieurs notions sur les fondements de la cybersécurité en passant par les différents concepts de sécurité pour pouvoir comprendre tout ce qu’il concerne le danger et la protection.

**Chapitre II : environnement et préparation**

## Description de l’architecture réseau IHFR

L’architecture réseau de l’IHFR a été conçue pour assurer à la fois performance, sécurité et évolutivité, tout en répondant aux besoins spécifiques de l’infrastructure informatique de l’organisation. Le réseau est structuré selon une topologie hiérarchique combinant un cœur de réseau centralisé, chargé de la gestion des flux de données, et des segments périphériques destinés aux différents départements et services. Un pare-feu central est placé à la frontière entre le réseau interne et l’accès Internet, garantissant un filtrage strict du trafic entrant et sortant. Les serveurs essentiels, tels que le serveur web (Apache2), le serveur DNS (Bind9) et les systèmes de supervision et de détection d’intrusion (Snort, Suricata), sont hébergés sur des machines virtuelles isolées, déployées sous **Ubuntu Server** au sein d’un environnement **VirtualBox** pour faciliter la gestion et la maintenance.

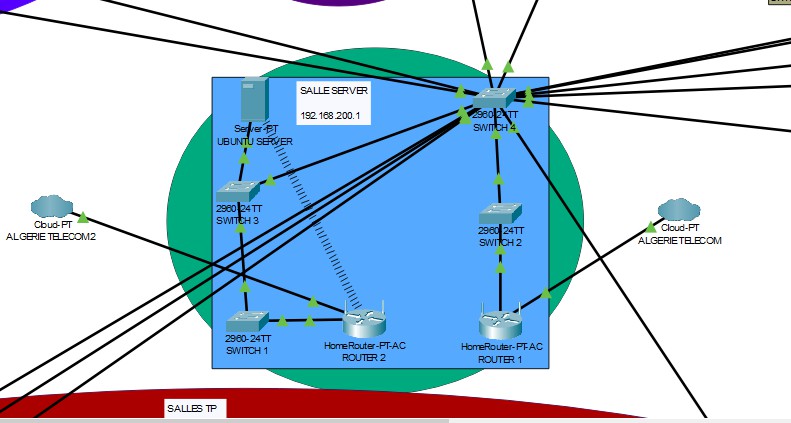
La connectivité interne est assurée via un schéma d’adressage IP statique configuré avec **Netplan**, tandis que les postes administratifs et techniques sont répartis sur des VLAN distincts, ce qui permet de segmenter les flux et de limiter les risques de propagation d’attaques. Des outils tels que **UFW** pour la gestion des règles de pare-feu, **SSH** pour l’administration sécurisée et **Wireshark** pour l’analyse du trafic complètent le dispositif technique. Enfin, des stations de test fonctionnant sous **Kali Linux** sont utilisées pour simuler des scénarios d’attaque et évaluer l’efficacité des mesures de protection mises en place. Cette architecture modulaire et sécurisée offre à l’IHFR un environnement réseau robuste, capable de résister aux menaces tout en assurant un fonctionnement fluide et fiable.



‎0‑9 Architecture réseau globale de l’IHFR

L’architecture réseau de l’Institut Hydrométéorologique de Formation et de Recherches (IHFR) est organisée autour de sept départements interconnectés : la Direction, la Tour, l’Imprimerie, la Pédagogie, la Bibliothèque, la Salle Standard et la Salle Serveur. Chaque département est équipé d’infrastructures informatiques adaptées à ses besoins opérationnels spécifiques, tout en étant relié au réseau central pour assurer la cohérence et la continuité des services. La **Direction** dispose de postes de travail fixes et de connexions sécurisées, permettant la gestion administrative et stratégique de l’institut. La **Tour**, en tant que centre de supervision et de coordination, intègre plusieurs postes de travail répartis par fonction (bureau, finance, personnel) et bénéficie d’un point d’accès sans fil pour les communications

internes. L’**Imprimerie** est équipée de postes informatiques, d’imprimantes réseau et d’un point d’accès, optimisant ainsi la production et la diffusion de documents. Le département **Pédagogie** constitue un pôle central pour les enseignants et les formateurs, tandis que la **Bibliothèque**, connectée à ce dernier, offre aux utilisateurs un accès aux ressources numériques via un réseau filaire et Wi-Fi sécurisé. La **Salle Standard** joue un rôle de nœud intermédiaire en reliant plusieurs salles spécialisées et périphériques au réseau principal. Enfin, la **Salle Serveur**, cœur de l’infrastructure, héberge les serveurs Ubuntu assurant des services essentiels tels que le DHCP, le DNS et le HTTP, ainsi que les dispositifs de routage, de commutation et de sécurité. L’ensemble de ces départements est interconnecté par une dorsale réseau fiable et sécurisée, garantissant un haut niveau de performance, de disponibilité et de protection des données.

****

**‎0‑10** Schéma du la salle serveur

‎0‑11 la salle serveur du l’institut

La **salle serveur** constitue le cœur névralgique de l’infrastructure réseau, assurant la centralisation et

la gestion optimale des services informatiques de l’établissement. Elle est configurée avec une **adresse IP statique**, facilitant l’identification et l’accès permanent aux ressources hébergées. Intégrée au **VLAN 200**, elle joue un rôle pivot dans la segmentation logique du réseau afin d’optimiser la sécurité et la performance des communications internes. L’architecture de cette salle repose sur **un cœur de réseau hébergeant le serveur principal**, chargé de fournir les services essentiels (tels que DHCP, DNS, HTTP, ou encore les outils de supervision). L’interconnexion interne est assurée par **quatre switchs reliés entre eux**, permettant une redondance et une meilleure répartition du trafic, ainsi qu’**un switch central** qui assure la liaison avec l’ensemble du réseau institutionnel. Pour garantir un **débit Internet optimal** et éviter toute saturation, l’accès **Wi-Fi est réservé exclusivement au serveur**, tandis que les autres équipements sont reliés par **des liaisons Ethernet filaires**, assurant à la fois stabilité, sécurité et hautes performances. Cette conception vise à offrir une infrastructure fiable, évolutive et résiliente, adaptée aux besoins stratégiques de l’établissement.

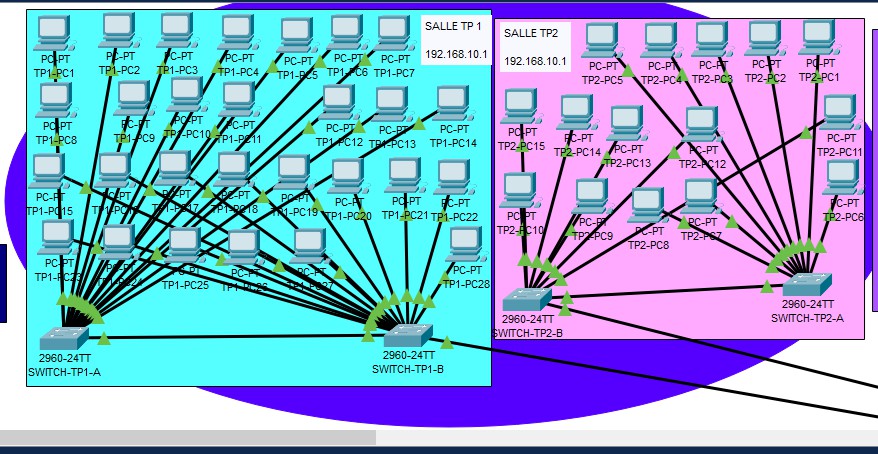


**Figure 13 :** salle tp 1 du réseau IHFR

**Figure 12 :** les routeurs du réseau IHFR

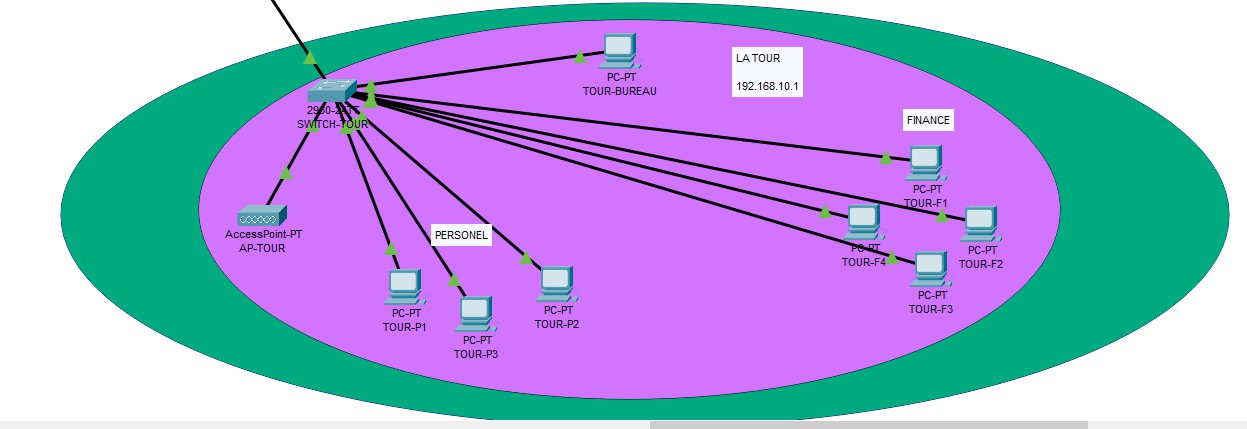


**Figure 14 : salle tp 2 du réseau IHFR**

****les salles TP1 et TP2 sont configurées pour partager une plage d’adresses IP unique, ce qui permet une gestion centralisée et homogène des ressources réseau. Ces deux salles sont intégrées dans le **VLAN 10**, assurant ainsi la segmentation logique du trafic et renforçant la sécurité en isolant ce segment du reste du réseau. Chacune des deux salles dispose de son propre switch, et ces deux switches sont reliés directement au switch 4, qui joue le rôle d’agrégateur intermédiaire.L’architecture globale repose sur quatre switches interconnectés, convergeant vers un switch central assurant la distribution et la coordination de l’ensemble du réseau.

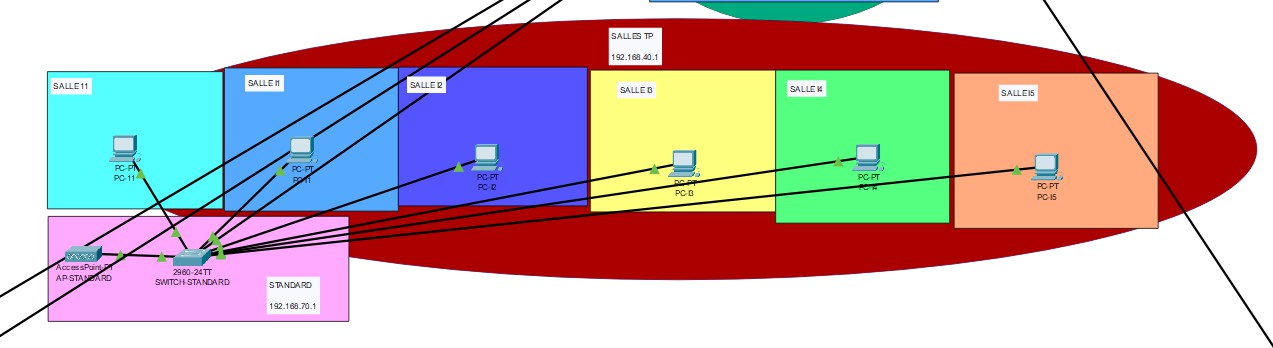
**Figure 15 :** Schéma de la salle TP1 et TP2 avec VLAN attribués

Les connexions entre les équipements sont réalisées via des liaisons Ethernet haut débit, garantissant une transmission fiable et rapide des données. Dans cette configuration, six postes de travail sont directement connectés à l’un des switches, chacun étant affecté à un port distinct pour optimiser la gestion du trafic et faciliter le diagnostic en cas de dysfonctionnement.



**Figure 16 :** Schéma de la tour avec VLAN attribués

La **Tour** est intégrée au réseau IHFR avec une **adresse IP unique** lui permettant une identification claire dans l’infrastructure. Elle appartient au **VLAN 20**, garantissant la segmentation et la sécurisation de ses échanges avec les autres zones du réseau. L’équipement réseau principal de cette zone comprend **un switch** et **un point d’accès** assurant la connectivité filaire et sans fil. Les **huit postes de travail** qui y sont installés reçoivent **automatiquement leurs adresses IP et leurs paramètres réseau** grâce au serveur **Ubuntu**, via le **switch 4** auquel la Tour est reliée. Les différents équipements sont interconnectés par une **liaison Ethernet** assurant un transfert de données fiable et rapide.



**Figure 17 :** Schéma de standard

La **salle Standard** est configurée avec une **adresse IP unique** correspondant à son réseau local dédié, identifié par le **VLAN 70**. Elle est équipée d’un **switch** et d’un **point d’accès sans fil**, permettant de connecter à la fois des postes fixes et des périphériques mobiles.

L’ensemble des **sept postes de travail** présents dans cette salle obtiennent automatiquement leurs paramètres réseau (**adresse IP, passerelle, DNS**) grâce au **serveur Ubuntu**, via le **switch 4** qui joue un rôle central dans la distribution.

La communication entre les équipements de la salle est assurée par une **liaison Ethernet** fiable.

###### 

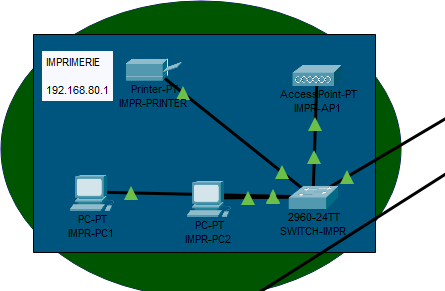
**Figure** 18 : Schéma de la salle PNT avec VLAN attribués

La **salle PNT** est intégrée au réseau de l’IHFR et identifiée par une **adresse IP unique** dans le plan d’adressage. Elle appartient au **VLAN 60**, ce qui permet de segmenter logiquement le trafic réseau et de renforcer la gestion ainsi que la sécurité. L’infrastructure de cette salle repose sur **deux switchs** interconnectés, ainsi qu’**un point d’accès sans fil** permettant la connexion des périphériques mobiles. Un total de **sept postes de travail** y sont installés ; chacun obtient automatiquement sa configuration réseau (**adresse IP, passerelle et DNS**) de manière dynamique grâce au **serveur Ubuntu**, via le **switch 4**. Tous les équipements de cette salle sont reliés par des **liaisons Ethernet** assurant un débit stable et une faible latence pour les communications internes et externes.

###### 

**Figure 19** :Schéma de la salle pédagogie avec VLAN attribués

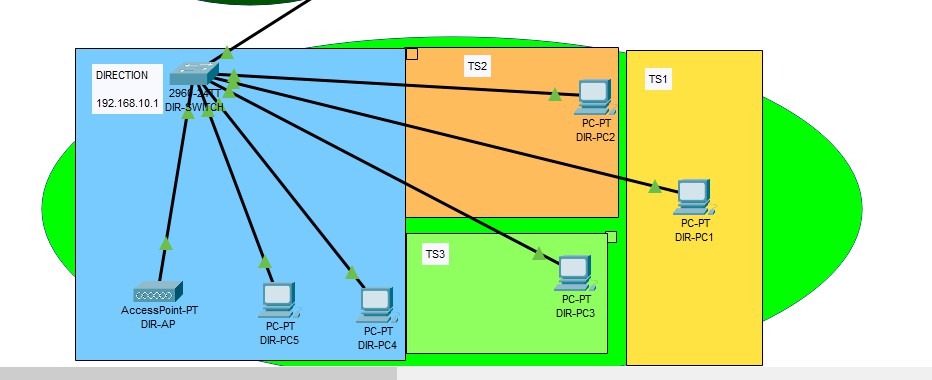
La **salle pédagogie** dispose d’une **adresse IP unique** attribuée conformément au **VLAN 50**. Elle est équipée de **trois switchs** et d’**un point d’accès** assurant la connectivité filaire et sans fil. Les **cinq postes de travail** de la salle reçoivent leurs paramètres réseau **dynamiquement** via le **serveur Ubuntu**, en passant par le **switch 4**. L’interconnexion entre tous les équipements est assurée par une **liaison Ethernet** fiable, garantissant un échange de données rapide et sécurisé.



**Figure 20 :**l’imprimerie avec VLAN attribués

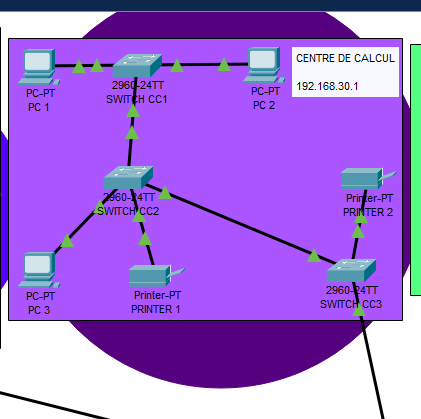
L’imprimerie de l’IHFR est intégrée au réseau via une **adresse IP unique**, conformément à la politique d’adressage définie. Elle est associée au **VLAN 80**, qui isole logiquement le trafic afin d’améliorer la sécurité et la gestion des flux. L’infrastructure locale de cette salle repose sur **trois switchs** interconnectés et **un point d’accès Wi-Fi** pour assurer la couverture réseau sans fil.

Un total de **cinq postes de travail** y sont déployés ; ils reçoivent automatiquement leurs configurations réseau (adresse IP, passerelle, DNS) de manière dynamique grâce au **serveur Ubuntu**, via le **switch 4** qui centralise la liaison vers le cœur du réseau. Les interconnexions entre les équipements se font au moyen de **liaisons Ethernet** fiables, garantissant une communication rapide et stable entre tous les périphériques.



**Figure 21 :** Schéma de la direction avec VLAN attribués

La **direction** dispose d’une adresse IP unique attribuée conformément à son plan d’adressage. Elle est intégrée au **VLAN 90**, dédié à ce service, garantissant ainsi l’isolement et la sécurité de son trafic réseau. L’infrastructure locale comprend **un switch** et **un point d’accès** permettant la connexion à la fois filaire et sans fil. Les **cinq postes de travail** de la direction reçoivent leurs adresses IP et paramètres réseau **dynamiquement** via le **serveur Ubuntu**, par l’intermédiaire du **switch 4** auquel cette salle est reliée. Tous les équipements sont connectés entre eux par **liaisons Ethernet**, assurant une communication fiable et performante.



**Figure 22 :** Schéma de le centre de calcul avec VLAN attribués

Le centre de calcul est attribué à un réseau disposant d’une adresse IP unique et est configuré au sein du VLAN 30, garantissant ainsi une segmentation logique et sécurisée du trafic. L’infrastructure interne de cette salle est constituée de trois commutateurs interconnectés, assurant la distribution du réseau, ainsi que de deux imprimantes réseau accessibles à l’ensemble des utilisateurs autorisés.

Trois postes de travail sont installés et reçoivent automatiquement leurs configurations réseau (adresses IP, passerelle, DNS) de manière dynamique via le serveur Ubuntu, par l’intermédiaire du commutateur 4, ce qui optimise la gestion et la centralisation des ressources. L’ensemble des équipements est relié par des connexions Ethernet filaires, offrant une stabilité, un débit élevé et une fiabilité accrue pour les traitements de données intensifs caractéristiques des activités du centre de calcul.

## Matériels et logiciels utilisés

Pour la mise en place et la sécurisation du réseau IHFR, L’outil **VirtualBox** a été utilisé pour héberger des machines virtuelles dédiées, permettant de déployer différents systèmes et services de manière isolée. Du côté logiciel, **Ubuntu Server** a servi de base pour l’hébergement des services critiques, tandis que **Kali Linux** a été employé pour les tests d’intrusion et l’audit de sécurité. Des outils réseau tels que **Packet Tracer** ont permis de modéliser et de simuler l’architecture avant sa mise en production. Pour la sécurisation, des solutions comme **UFW** pour la gestion des pare-feux, **Snort** et **Suricata** pour la détection et la prévention des intrusions, **SSH** pour l’administration à distance, et **Apache2** pour la gestion des services web ont été intégrées. Le service DNS a été géré via **Bind9**, tandis que la configuration réseau a été assurée avec **Netplan**. Des outils de surveillance et d’audit comme **Lynis**, d’analyse de trafic comme **Wireshark**, et de scan de ports comme **Nmap** complètent l’arsenal technique utilisé, assurant une approche globale et robuste en matière de cybersécurité.

## Installation et configuration initiale des machines

L’installation et la configuration initiale des machines ont constitué une étape essentielle dans la mise en place de l’infrastructure réseau IHFR. Cette phase a débuté par le déploiement des systèmes d’exploitation sur les différentes machines virtuelles crées via **VirtualBox**. Les serveurs principaux ont été installés avec **Ubuntu Server** afin d’assurer un environnement stable et sécurisé pour l’hébergement des services critiques, tandis que **Kali Linux** a été configuré destinées aux tests de pénétration et à l’audit de sécurité.

Parallèlement, les outils nécessaires à la sécurité et à l’administration ont été installés : **SSH** pour l’accès distant sécurisé, **UFW** pour la gestion du pare-feu, **Apache2** pour l’hébergement des services web, et **Bind9** pour la gestion des résolutions DNS internes. Les solutions de détection et prévention des intrusions, **Snort** et **Suricata**, ont été déployées afin de renforcer la surveillance du trafic réseau. Des utilitaires comme **Lynis**, **Wireshark** et **Nmap** ont

également été mis en place dès cette phase pour permettre un suivi constant et un diagnostic précis de l’état du réseau.

Dans le cadre de la mise en place de l’infrastructure réseau de l’Institut, l’installation et la configuration initiale d’Ubuntu Server ont constitué la première étape technique majeure. Le processus a été réalisé dans un environnement virtualisé (VirtualBox/VMware) afin de faciliter les tests, la maintenance et les futures évolutions.

L’installation a débuté par le téléchargement de l’image ISO officielle d’Ubuntu Server depuis le site officiel, garantissant ainsi l’utilisation d’une version stable et sécurisée. Après avoir monté cette image sur la machine virtuelle, le processus d’installation a été lancé. Les paramètres de langue, de disposition du clavier et de fuseau horaire ont été configurés pour correspondre au contexte local (français et fuseau horaire UTC+1).

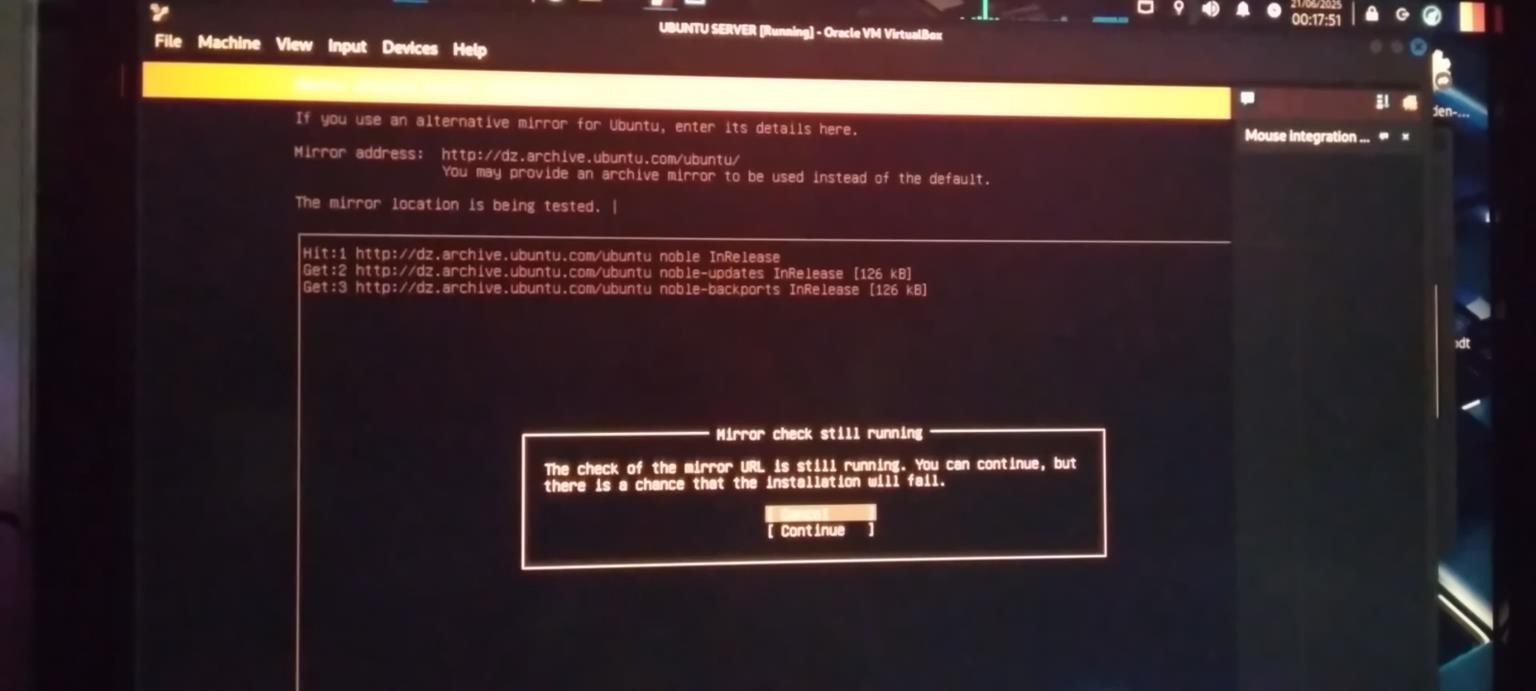
Concernant le stockage, une configuration en partitionnement manuel a été retenue : une partition **EFI** pour le démarrage, une partition **root** pour le système d’exploitation et les services, ainsi qu’une partition **swap** dimensionnée en fonction de la mémoire vive disponible. Cette organisation favorise une meilleure gestion des ressources et une maintenance simplifiée.

Lors de la configuration réseau, l’interface principale a été associée à une adresse IP statique afin de garantir la stabilité des communications avec l’ensemble du réseau interne. Le serveur a ensuite été nommé conformément à la nomenclature prévue pour l’infrastructure, permettant ainsi une identification rapide dans le plan d’adressage.

Après l’installation du noyau et des composants de base, un compte administrateur avec des privilèges **sudo** a été créé. Les mises à jour de sécurité ont été appliquées immédiatement via la commande :

sudo apt update && sudo apt upgrade -y

Les services essentiels (SSH, HTTP, DNS, DHCP) ont été installés progressivement, en privilégiant une configuration minimale sécurisée avant tout déploiement fonctionnel. La connexion SSH a été activée pour permettre l’administration à distance, avec un renforcement de la sécurité via la désactivation de l’authentification par mot de passe et l’usage exclusif de clés cryptographiques.



**Figure 23 :** fenétre d’installation d’ubuntu server

### **Objectif**

Cette étape vise à préparer l’ensemble des machines et équipements réseau simulés dans Cisco Packet Tracer afin de reproduire fidèlement l’infrastructure informatique de l’Institut Hydrométéorologique de Formation et de Recherches (IHFR). L’objectif est de mettre en place un environnement fonctionnel où chaque poste et équipement pourra communiquer avec le serveur principal Ubuntu, recevoir automatiquement une configuration réseau, et accéder aux services mis en place.

La maquette réseau a été conçue en respectant la topologie réelle de l’IHFR, comprenant :

**PC fixes** répartis dans les différentes salles (TP, Direction, Bibliothèque, etc.).

###### Serveur central Ubuntu Server.

**Switchs d’interconnexion** et **points d’accès Wi-Fi**. **Routeurs** pour le routage inter-VLAN.

**Imprimantes réseau** pour certaines salles spécifiques.

Configuration des **VLAN** selon le plan défini (VLAN200-SRV, TP1, TP2, etc.).

### **Installation des machines dans Packet Tracer**

###### Ajout des serveurs :

###### Un serveur a été placé dans la salle serveur et nommé SRV-Ubuntu. Le serveur est connecté au switch principal du VLAN SRV. Paramétrage des PC :

**IP statique ou DHCP** :

Les PC ont été configurés pour obtenir automatiquement leur adresse IP via le serveur DHCP simulé (hébergé sur le serveur Ubuntu dans la simulation).

**Passerelle par défaut** : définie selon le VLAN d’appartenance. **DNS** : adressé vers le serveur Ubuntu (192.168.x.x selon VLAN). **Configuration du serveur Ubuntu (simulation)**

Adresse IP statique définie dans le VLAN200-SRV.

Activation des services DHCP, DNS et HTTP dans la simulation. Test de ping depuis plusieurs PC pour vérifier la connectivité.

## Installation et Configuration Initiale de Kali Linux

###### Lancement de l’installation

Montage de l’image ISO de Kali Linux.

Démarrage de la machine et sélection de l’option **Graphical Install**. Paramétrage linguistique et régional

**Langue** : Français

**Pays** : Algérie

**Clavier** : Français (AZERTY)

###### Configuration réseau

Attribution automatique d’une adresse IP via DHCP lors de l’installation. Domaine laissé vide pour la configuration locale.

**Création des comptes utilisateurs** Définition du mot de passe **root** sécurisé Partitionnement du disque

Mode **Assisté – utiliser tout le disque**. Système de fichiers en ext4.

Création d’une seule partition racine / et d’une partition swap.

###### Installation du système

Sélection du dépôt officiel Kali pour la mise à jour des paquets. installation des outils de base préconfigurés.

Installation du chargeur d’amorçage GRUB sur le disque principal.

###### Configuration initiale post-installation

Mise à jour du système

sudo apt update && sudo apt upgrade -y

Installation d’outils supplémentaires

Afin de préparer l’environnement pour les tests de sécurité, les paquets suivants ont été installés :

sudo apt update && sudo apt install -y apache2 isc-dhcp-server bind9net-tools nmap wireshark

###### Configuration réseau manuelle

sudo nano /etc/network/interfaces

###### Sécurisation initiale

sudo ufw enable

sudo ufw allow 22/tcp

## Plan d’adressage IP

Le plan d’adressage IP du réseau IHFR a été élaboré de manière à assurer une organisation logique, une gestion simplifiée et une évolutivité future de l’infrastructure. Chaque sous-réseau a été conçu selon les besoins fonctionnels et sécuritaires des différents segments du réseau. L’adressage repose sur une plage IP privée conforme à la norme **RFC 1918**, garantissant que les adresses ne sont pas routables sur Internet et limitant ainsi l’exposition directe aux menaces externes.

L’ensemble du réseau est structuré comme suit :

VLAN 200 – SERVEURS (SRV)

Sous-réseau : 192.168.200.0/24 Passerelle : 192.168.200.1

DNS interne : 192.168.200.10 (Ubuntu Server)

Statique : 192.168.200.10-29 (serveurs: DHCP, DNS, HTTP, IDS, etc.)

DHCP : (souvent pas de DHCP ici, mais possible .50-.99 pour VMs de test)

VLAN 10 – TP-SALLES (TP1 & TP2)

Sous-réseau : 192.168.10.0/24 Passerelle : 192.168.10.1

Statique : 192.168.10.1-29

DHCP : 192.168.10.120-199

VLAN 20 – TOUR

Sous-réseau : 192.168.20.0/24 Passerelle : 192.168.20.1

Statique : 192.168.20.1-29

DHCP : 192.168.20.1-199

VLAN 70 – SALLE STANDARD

Sous-réseau : 192.168.70.0/24 Passerelle : 192.168.70.1

DHCP : 192.168.70.1-199

VLAN 60 – PNT

Sous-réseau : 192.168.60.0/24 Passerelle : 192.168.60.1

DHCP : 192.168.60.50-199

VLAN 50 – PÉDAGOGIE + BIBLIOTHÈQUE

Sous-réseau : 192.168.50.0/24 Passerelle : 192.168.50.1

Statique : 192.168.50.20-29

DHCP : 192.168.50.50-199

VLAN 80 – IMPRIMERIE

Sous-réseau : 192.168.80.0/24 Passerelle : 192.168.80.1

Statique : 192.168.80.10-19

DHCP : 192.168.80.50-199

VLAN 90 – DIRECTION

Sous-réseau : 192.168.90.0/24 Passerelle : 192.168.90.1

Statique : 192.168.90.20-29

DHCP : 192.168.90.50-199

VLAN 30 – CENTRE DE CALCUL

Sous-réseau : 192.168.30.0/24 Passerelle : 192.168.30.1

Statique : 192.168.30.10-19

DHCP : 192.168.30.50-199

Le **plan IP** est accompagné d’une politique stricte de réservation d’adresses statiques pour les serveurs et d’attribution dynamique via **DHCP** pour les clients. Cela permet de simplifier la gestion tout en conservant la stabilité des services critiques. L’utilisation de sous-réseaux distincts, associée à des règles de pare-feu UFW, permet de segmenter le trafic et de limiter la propagation des menaces potentielles. Cette approche garantit un adressage IP structuré, cohérent et aligné avec les objectifs de performance et de sécurité du réseau IHFR.

**Chapitre III – diagnostic initial**

## Scan réseau avec Nmap

Pour analyser la topologie et identifier les machines actives ainsi que les services en écoute sur le réseau IHFR, nous avons utilisé **Nmap** (Network Mapper), un outil open source puissant permettant de réaliser des scans complets ou ciblés.

La première étape a consisté à effectuer un **scan Ping** avec la commande :

sudo nmap -sn 192.168.1.40

Ce scan a permis de détecter l’ensemble des hôtes actifs dans le réseau, en retournant leurs adresses IP, leurs adresses MAC et, lorsque possible, le nom de leur fabricant. Cette étape a permis de confirmer la présence et l’accessibilité des serveurs, postes clients et périphériques réseau.

Ensuite, un **scan de ports** a été réalisé sur des machines spécifiques afin d’identifier les services disponibles et d’évaluer les points d’entrée potentiels :

sudo nmap -sV 192.168.1.40

Ce scan a révélé les ports ouverts ainsi que les versions exactes des services exécutés (Apache, SSH, DNS, etc.). Ces informations sont essentielles pour effectuer un audit de sécurité et repérer d’éventuelles vulnérabilités liées à des services obsolètes ou mal configurés.

Dans le cadre de la protection du réseau IHFR, les résultats obtenus via Nmap ont été exploités pour

:

* Cartographier l’ensemble de l’infrastructure active.
* Identifier les hôtes et services à surveiller.
* Définir des règles de pare-feu UFW pour limiter l’accès aux ports critiques.

Cette méthodologie permet d’intégrer la **détection préventive** au processus global de cybersécurité, garantissant une visibilité permanente sur l’état du réseau et renforçant sa résilience face aux attaques.



**Figure 24 :** fenétre de test avec les commandes du logiciel nmap

## Analyse de vulnérabilités avec NIKTO

Dans le cadre de l’audit de sécurité du réseau IHFR, nous avons utilisé **Nikto**, un outil open source spécialisé dans l’analyse des serveurs web afin de détecter d’éventuelles vulnérabilités. Nikto effectue un balayage complet du serveur en testant des milliers de fichiers, répertoires et configurations susceptibles de poser un risque.

L’analyse a été effectuée sur le serveur web principal hébergé à l’adresse IP **192.168.1.40**, à l’aide de la commande :

sudo nikto -h [http://192.168.1.40](http://192.168.1.40/)

Les premiers résultats ont révélé la présence de fichiers et en-têtes HTTP non sécurisés, notamment

:

L’absence de l’en-tête **X-Content-Type-Options**, pouvant permettre l’exécution de contenus dans un format différent de celui attendu.

La détection de fichiers sensibles tels que des listes ou mots de passe potentiels (.passwd, .lst).

Ces vulnérabilités pouvaient être exploitées par un attaquant pour obtenir des informations sensibles ou contourner les protections mises en place.

Afin de corriger ces failles, plusieurs actions ont été menées :

Suppression des fichiers inutiles ou sensibles dans le répertoire /var/www/html/.

Configuration d’Apache pour forcer l’ajout de l’en-tête HTTP **X-Content-Type-Options: nosniff**. Renforcement des permissions d’accès aux répertoires et fichiers du serveur web

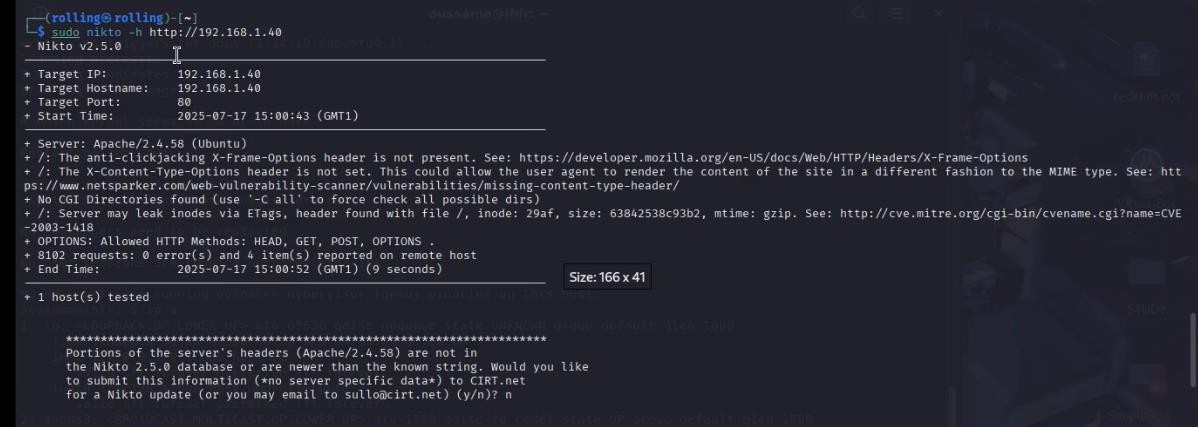
Après application de ces mesures, un nouveau scan Nikto a été lancé :

sudo nikto -h [http://192.168.1.40](http://192.168.1.40/)

Cette fois-ci, le rapport n’a détecté aucune vulnérabilité critique, ce qui confirme l’efficacité des mesures correctives appliquées.

L’utilisation de Nikto a ainsi permis :

* D’identifier rapidement les failles web potentielles.
* De mettre en œuvre des actions correctives ciblées.
* De valider l’amélioration du niveau de sécurité du serveur web IHFR.



**Figure 25 :** fenétre de test avec les commandes du logiciel nikto

## Analyse du trafic avec WIRESHARK

Dans le cadre de la sécurisation du réseau IHFR, nous avons utilisé **Wireshark**, un analyseur de paquets réseau, afin d’observer et d’interpréter les échanges de données circulant sur l’infrastructure. Cet outil permet de capturer le trafic en temps réel et d’identifier d’éventuelles anomalies ou comportements suspects pouvant révéler des attaques ou des fuites d’informations. L’analyse a été réalisée depuis une machine de supervision connectée au réseau, avec un filtrage ciblé sur les protocoles critiques (HTTP, HTTPS, DNS, SSH et ICMP). Les étapes principales ont été :

**Démarrage de la capture** sur l’interface réseau connectée au segment cible.

**Application de filtres Wireshark** afin de se concentrer sur des types spécifiques de paquets (exemple : http, icmp, dns).

**Observation des flux** pour détecter des requêtes ou réponses inhabituelles, comme un trafic HTTP non chiffré contenant des informations sensibles.

**Vérification des adresses IP et MAC** pour repérer d’éventuelles connexions non autorisées. **Détection d’anomalies** telles que des requêtes DNS vers des domaines inconnus ou un nombre anormal de paquets ICMP pouvant indiquer un début d’attaque par déni de service (DoS).

Les captures ont révélé :

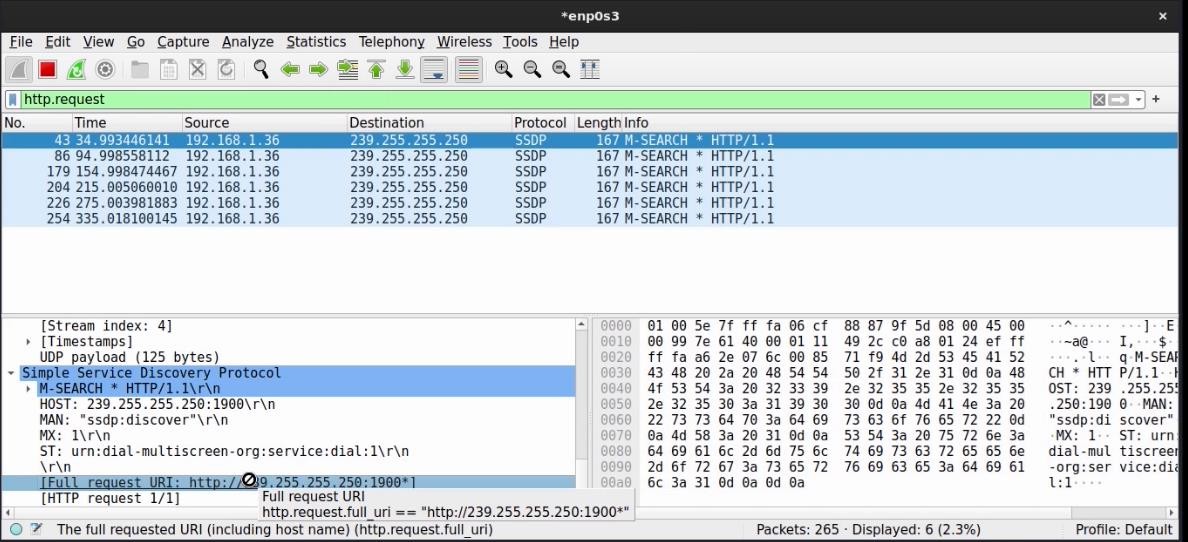
La présence de communications HTTP en clair, exposant le contenu échangé à une interception. Quelques tentatives de ping (ICMP) provenant d’adresses externes non reconnues.

Suite à ces observations, les mesures suivantes ont été mises en place :

**Forcer l’utilisation du protocole HTTPS** sur le serveur web afin de chiffrer les échanges.

**Bloquer les requêtes ICMP non nécessaires** via le pare-feu UFW.

**Mettre en place une surveillance continue** afin de détecter rapidement toute tentative d’intrusion. Grâce à Wireshark, nous avons pu confirmer que le trafic réseau, après les corrections appliquées, ne présentait plus de transmissions critiques en clair et que les flux entrants/sortants correspondaient aux usages légitimes du réseau IHFR.

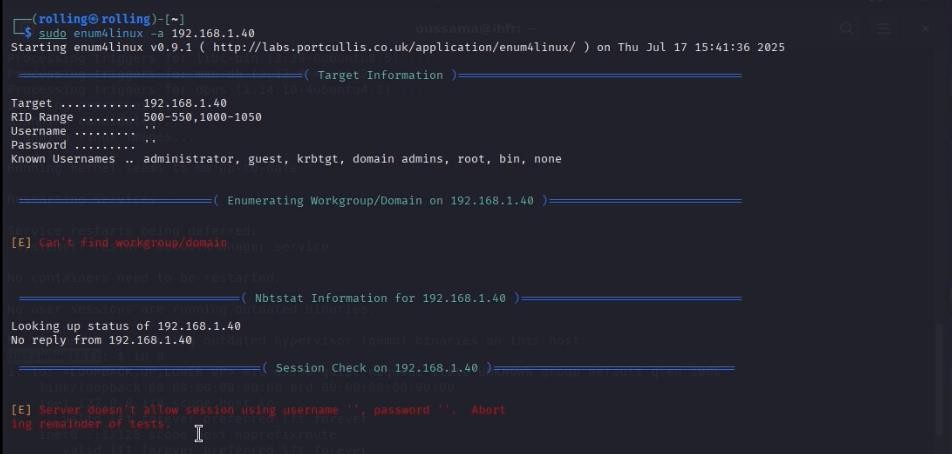


**Figure 26 :** fenétre de test avec le logiciel wireshark

## Analyse et detection avec emun4linux

Pour approfondir le diagnostic initial, l’outil **enum4linux** a été utilisé afin de collecter des informations détaillées sur les comptes utilisateurs, et la configuration NetBIOS du système cible. Cet utilitaire permet de réaliser une énumération poussée sans nécessiter d’authentification préalable. L’exécution de la commande :

enum4linux -a 192.168.1.40



**Figure 27 :** fenétre de test avec le logiciel enum4linux

## Identification des failles de sécurité

L’identification des failles de sécurité constitue une étape essentielle dans la protection du réseau IHFR. Elle permet de repérer les points faibles susceptibles d’être exploités par des attaquants afin d’anticiper et de neutraliser les risques. Cette phase a été menée à l’aide de plusieurs outils complémentaires, notamment **Nmap** pour le scan des ports, **Nikto** pour l’analyse des vulnérabilités web, ainsi que **Lynis** et **Snort** pour l’audit système et la détection

d’intrusions.

Les analyses réalisées ont permis de détecter :

**Ports ouverts non sécurisés** accessibles depuis l’extérieur, augmentant la surface d’attaque. **Absence de certains en-têtes de sécurité HTTP** sur le serveur web, pouvant faciliter des attaques de type injection ou cross-site scripting.

**Présence de services non nécessaires** actifs sur certaines machines, augmentant les risques d’exploitation.

**Trafic non chiffré** détecté lors de la capture avec Wireshark, exposant des données sensibles.

Chaque vulnérabilité a été classée et documentée pour proposer des contre-mesures adaptées. Cette approche structurée a permis de prioriser les actions correctives, en commençant par les menaces les plus graves, tout en assurant une amélioration progressive de la posture de sécurité du réseau.

**Chapitre IV – Mise en place des protections**

## Sécurisation réseau dans packet tracer

## VLANs et segmentation

La mise en place de **VLANs (Virtual Local Area Networks)** dans le réseau IHFR a permis d’assurer une meilleure organisation du trafic et de renforcer la sécurité globale. Le principe repose sur la segmentation logique du réseau physique en plusieurs sous-réseaux indépendants, chacun dédié à un usage spécifique. Ainsi, des VLANs distincts ont été créés pour séparer les départements tels que l’administration, les utilisateurs standards, les serveurs, ainsi que les zones dédiées aux invités.

Par ailleurs, la segmentation par VLAN facilite également la mise en œuvre de politiques de sécurité personnalisées pour chaque segment du réseau, comme la limitation des ports, l’application de filtrage spécifique ou encore la surveillance ciblée du trafic. Dans le cadre de ce projet, cette approche a permis de cloisonner efficacement les ressources critiques et de minimiser les risques d’intrusion interne ou externe.

###### Création de le VLAN 10

dans **CLI (ligne de commande)** :

Switch> enable

Switch# configure terminal Switch(config)# vlan 10 Switch(config-vlan)# name Direction Switch(config-vlan)# exit

**assignement les ports au VLAN 10** Switch(config)# interface range fa0/1 - 5 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 10 Switch(config-if-range)# exit

###### Création de le VLAN 20

sur **SWITCH-TOUR**

dans l’onglet **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 20 Switch(config-vlan)# name TOUR Switch(config-vlan)# exit

**assignement les ports au VLAN 20** Switch(config)# interface range fa0/1 - 8 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 20 Switch(config-if-range)# exit

###### Création de le VLAN 70 sur le switch de la salle Standard

sur le **switch de la salle Standard**

dans l’onglet **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 70 Switch(config-vlan)# name **Standard** Switch(config-vlan)# exit

###### assignement les ports au VLAN 70

Switch(config)# interface range fa0/1 - 6 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 70 Switch(config-if-range)# exit

###### Création de le VLAN 60

sur **le switch de la salle PNT** (PNT-SW) dans **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 60 Switch(config-vlan)# name PNT Switch(config-vlan)# exit

###### assignement les ports des 22 PC au VLAN 60

Switch(config)# interface range fa0/1 - 22 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 60 Switch(config-if-range)# exit

###### Création de le VLAN 30 sur chaque switch de la salle

sur le **switch principal** de la salle de calcul dans l’onglet **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 30 Switch(config-vlan)# name CALCUL Switch(config-vlan)# exit

###### assignement les ports des PC et imprimantes au VLAN 30

Switch(config)# interface range fa0/1 - 5 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 30 Switch(config-if-range)# exit

###### Création de le VLAN 40 sur chaque switch (TP1 et TP2)

Sur **SW-TP1**

Switch> enable

Switch# configure terminal Switch(config)# vlan 40

Switch(config-vlan)# name TP-SALLES Switch(config-vlan)# exit

###### assignement les ports des PC au VLAN 40

TP1 → 28 PC (ports Fa0/1 à Fa0/28) Switch(config)# interface range fa0/1 - 28 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 40 Switch(config-if-range)# exit

TP2 → 15 PC (ports Fa0/1 à Fa0/15) Switch(config)# interface range fa0/1 - 15 switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 40 Switch(config-if-range)# exit

###### Création de le VLAN 50 sur les switchs de la salle pédagogie

sur **le switch principal de la salle pédagogie**

dans l’onglet **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 50

Switch(config-vlan)# name PEDAGO-BIBLIO Switch(config-vlan)# exit

###### assignement les ports des 5 PC et des 3 AP au VLAN 50

Switch(config)# interface range fa0/1 - 7 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 50

Switch(config-if-range)# exit Switch(config)# interface fa0/8 Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 50 Switch(config-if)# exit

###### Création de le VLAN 80

sur le **switch de la salle Imprimerie**

dans l’onglet **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 80

Switch(config-vlan)# name IMPRIMERIE Switch(config-vlan)# exit

###### assignement les ports des équipements au VLAN 80

Switch(config)# interface range fa0/1 - 4 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 80 Switch(config-if-range)# exit

###### Création de le VLAN de la salle serveur

sur le **switch où est connecté le serveur**

dans l’onglet **CLI**

Switch> enable

Switch# configure terminal Switch(config)# vlan 200

Switch(config-vlan)# name SERVEUR\_IHFR Switch(config-vlan)# exit

###### assignement le port du serveur au VLAN 200

Switch(config)# interface fa0/1 Switch(config-if)# switchport mode access Switch(config-if)# switchport access vlan 200 Switch(config-if)# exit

## Port Security

La fonctionnalité **Port Security** a été implémentée sur les switchs du réseau IHFR afin de limiter les risques d’accès non autorisé et de renforcer le contrôle physique sur les points de connexion. Ce mécanisme permet d’associer un nombre restreint d’adresses MAC à chaque port du switch,

empêchant ainsi la connexion de périphériques non autorisés.

Cette mesure contribue à **réduire les risques d’attaques internes** telles que le spoofing d’adresses MAC ou l’ajout non autorisé de machines sur le réseau. Elle renforce également la traçabilité et le suivi des équipements, facilitant les audits de sécurité.

###### Activation le filtrage ICMP sur toutes les machines sensible

Empêche la détection par ping :

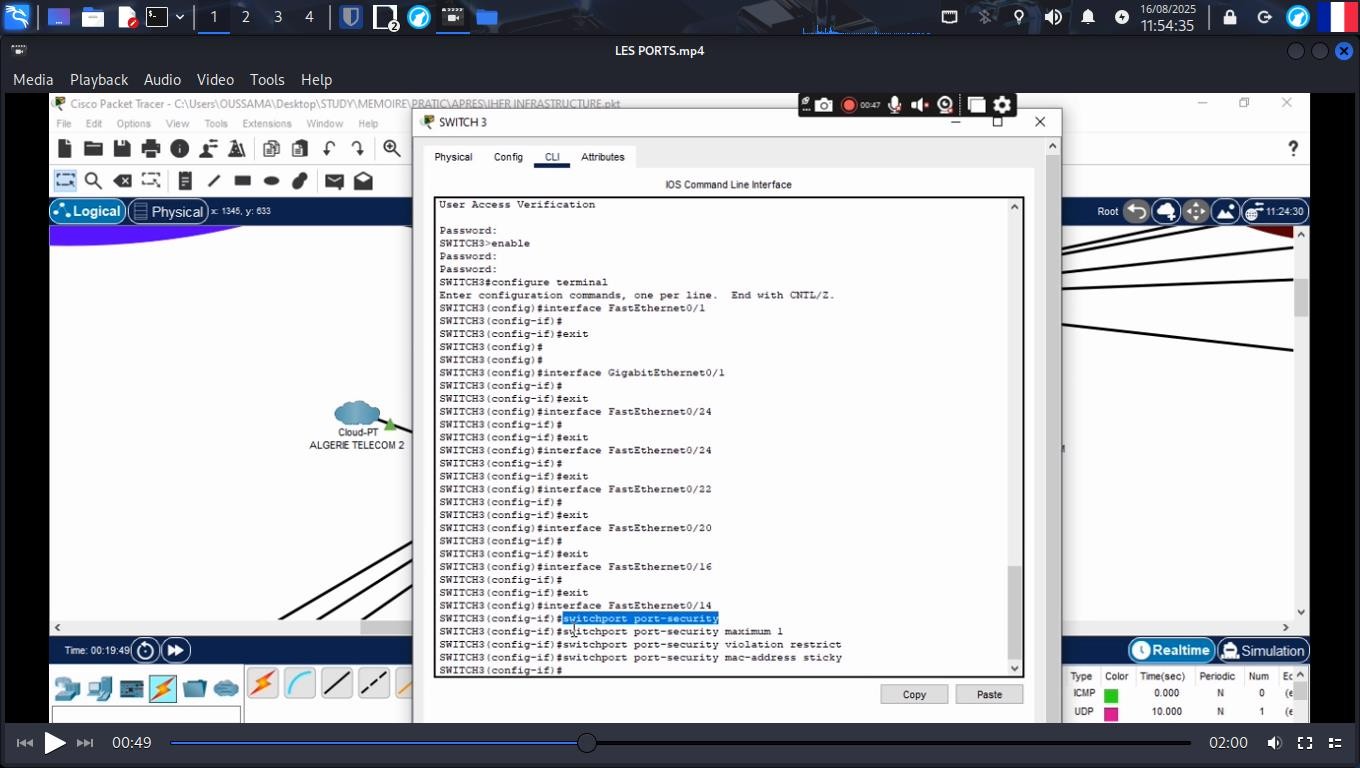
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP.

###### Cache de les adresses MAC visibles

Activeation **Port Security** sur les switches :

Switch(config-if)# switchport port-security Switch(config-if)# switchport port-security maximum 1

Switch(config-if)# switchport port-security violation restrict Switch(config-if)# switchport port-security mac-address sticky Cela empêche la connexion de machines non autorisées.



**Figure 28 :** fenétre de console de switch 3

## Sécurisation serveur Ubuntu

La sécurisation du serveur Ubuntu du réseau IHFR a constitué une étape essentielle afin de garantir la protection des services hébergés et des données sensibles. La démarche a commencé par la mise à jour complète du système et des paquets via apt update et apt upgrade, afin de corriger toutes les failles connues.

Un **pare-feu UFW (Uncomplicated Firewall)** a été configuré pour restreindre les flux réseau aux seuls ports nécessaires, notamment SSH, HTTP/HTTPS et les services internes.

En parallèle, des outils de détection et de prévention d’intrusion tels que **Snort** et **Suricata** ont été installés et configurés pour surveiller en temps réel le trafic réseau et bloquer les tentatives suspectes.

Pour renforcer la sécurité applicative, le serveur **Apache2** a été durci par la désactivation des modules inutiles, la mise en place d’en-têtes de sécurité HTTP et la restriction des droits d’accès aux répertoires.

Cette combinaison de mesures préventives et réactives assure un haut niveau de résilience du serveur Ubuntu face aux menaces internes et externes, tout en garantissant la disponibilité et l’intégrité des services offerts sur le réseau IHFR.

## Permission fichiers

###### Mettre à jour le système

sudo apt update && sudo apt upgrade -y

###### Sécurité Réseau de base (Firewall + Accès)

sudo apt install ufw -y

sudo ufw default deny incoming sudo ufw default allow outgoing sudo ufw allow ssh

sudo ufw allow 53 # DNS sudo ufw allow 80 # HTTP sudo ufw allow 67 # DHCP sudo ufw enable

### **suppression / blocage d’accés non autorisés**

**Sécurité du les accès SSH** sudo nano /etc/ssh/sshd\_config Désactiver le login root : PermitRootLogin no

Changer le port SSH :

Port 2222

Sécurité des services (DNS, DHCP, Web) **Sécuriser le serveur DNS (Bind9)** Refuser les requêtes externes :

sudo nano /etc/bind/named.conf.options

Ajoute dans options :

allow-query { localhost; 192.168.0.0/16; }; recursion yes;

###### Sécuriser Apache2 (serveur HTTP)

Installer :

sudo apt install apache2 -y

###### installer un certificat SSL (HTTPS) :

sudo apt install openssl sudo a2enmod ssl

sudo systemctl restart apache2

###### activation SSL dans Apache :

sudo nano /etc/apache2/sites-available/default-ssl.conf

Changement :

SSLCertificateFile /etc/ssl/certs/apache.crt SSLCertificateKeyFile /etc/ssl/private/apache.key Puis :

sudo a2ensite default-ssl

sudo systemctl reload apache2

## Configuration firewall UFW

Pour renforcer la sécurité du réseau IHFR, le pare-feu **UFW** (*Uncomplicated Firewall*) a été mis en place sur le serveur Ubuntu. L’objectif principal était de limiter les communications réseau aux seuls services indispensables, tout en bloquant l’ensemble des autres ports pour réduire la surface d’attaque.

La configuration a débuté par la définition d’une politique par défaut stricte : **refuser toutes les connexions entrantes** (*deny incoming*) et **autoriser uniquement les connexions sortantes** (*allow outgoing*). Ensuite, des règles spécifiques ont été établies afin de permettre l’accès aux services essentiels :

**SSH (port 22)**, limité à certaines adresses IP autorisées pour l’administration à distance ; **HTTP (port 80)** et **HTTPS (port 443)** pour le fonctionnement du serveur web Apache ; Autres ports nécessaires pour les services internes (DNS, etc.), ouverts uniquement selon les besoins.

Chaque modification a été appliquée et testée à l’aide de commandes de diagnostic pour garantir que les services autorisés restaient accessibles tout en bloquant efficacement les autres tentatives de connexion.

## Protection contre le sniffing

Le sniffing consiste à intercepter et analyser le trafic réseau, souvent à l’aide d’outils comme **Wireshark**, afin de capturer des informations sensibles telles que des identifiants, mots de passe ou données confidentielles. Pour protéger le réseau IHFR contre ce type de menace, plusieurs mesures ont été mises en place.

Tout d’abord, le chiffrement des communications a été généralisé à travers l’utilisation de protocoles sécurisés comme **HTTPS** (SSL/TLS) pour les échanges web, **SSH** pour l’administration

à distance. Ces solutions garantissent que les données circulant sur le réseau ne sont pas lisibles en clair, rendant leur exploitation quasi impossible même en cas d’interception.

Ensuite, une **segmentation réseau** via des VLANs a été implémentée dans Packet Tracer, limitant le trafic sensible à des sous-réseaux isolés afin de réduire les risques de capture par des utilisateurs non autorisés. Des règles strictes au niveau du pare-feu (**UFW**) complètent cette approche, empêchant tout accès inutile aux segments critiques.

Enfin, des outils de détection d’intrusion comme **Snort** et **Suricata** ont été déployés pour surveiller en temps réel le trafic et alerter en cas de comportement suspect pouvant indiquer une tentative de sniffing. Cette combinaison de mesures proactives et réactives assure une protection robuste contre les interceptions de données sur le réseau IHFR.

## ICMP blocking

Sans Le protocole **ICMP** (Internet Control Message Protocol) est principalement utilisé pour tester la connectivité réseau, par exemple via la commande *ping*. Cependant, il peut également être exploité par des attaquants pour réaliser des activités de reconnaissance, comme la cartographie du réseau, l’identification des machines actives ou encore des attaques par déni de service (**ICMP Flood**).

Afin de réduire la surface d’attaque, le réseau IHFR a été configuré pour **bloquer le trafic ICMP entrant non nécessaire**. Cette mesure a été appliquée au niveau du pare-feu **UFW** sur le serveur Ubuntu, en filtrant les paquets ICMP tout en maintenant les fonctionnalités essentielles internes. Par exemple, les commandes de diagnostic peuvent être autorisées uniquement depuis des adresses IP spécifiques de l’administrateur réseau.

Cette restriction empêche un utilisateur externe de détecter facilement les hôtes actifs du réseau ou de saturer les ressources avec un trafic ICMP massif. Combinée aux autres mécanismes de filtrage et de segmentation déjà mis en place, cette politique renforce significativement la résilience du réseau IHFR face aux tentatives de reconnaissance et d’attaque.

## Filtrage des ports sensibles

Dans un réseau sécurisé, il est essentiel de limiter l’exposition des ports utilisés par des services critiques. Les **ports sensibles** comme **22 (SSH)**, **53 (DNS)**, **80 (HTTP)**, **443 (HTTPS)** ou encore certains ports utilisés pour la gestion à distance et les bases de données, constituent des cibles privilégiées pour les attaquants. Leur ouverture sans contrôle augmente considérablement le risque d’intrusion, d’exploitation de failles ou de compromission de données.

Pour le réseau IHFR, un filtrage strict a été appliqué au niveau du pare-feu **UFW** et des équipements réseau. Les ports non utilisés ont été fermés par défaut, tandis que les ports indispensables sont **ouverts uniquement pour des adresses IP autorisées**. Par exemple, l’accès au port **22** pour l’administration SSH est restreint aux machines de l’équipe technique via une liste blanche, empêchant ainsi toute tentative d’attaque par force brute depuis l’extérieur.

Ce principe de **moindre privilège** garantit que chaque service n’est accessible que par les utilisateurs et machines légitimement autorisés, réduisant fortement la surface d’attaque et améliorant la posture globale de cybersécurité du réseau IHFR.

## Durcissement hardware

Le **durcissement matériel** (hardware hardening) consiste à mettre en place des mesures physiques et techniques pour protéger les équipements réseau et serveurs contre toute manipulation, vol ou dégradation non autorisée. Du point de vue de la configuration, les **ports inutilisés sur les switches sont désactivés** pour éviter tout branchement non autorisé, et les **mots de passe BIOS/UEFI** sont activés afin d’empêcher toute modification de configuration matérielle ou amorçage sur un périphérique externe. Enfin, un inventaire complet du matériel est maintenu à jour pour permettre un suivi précis et une réaction rapide en cas de perte ou de vol.

Ces mesures de durcissement garantissent que la sécurité du réseau IHFR ne repose pas uniquement sur la protection logicielle, mais également sur une **défense physique robuste** contre les menaces externes et internes.

## Mot de passe sur les équipements réseau

La mise en place de **mots de passe sécurisés** sur les équipements réseau constitue une étape essentielle pour prévenir tout accès non autorisé à la configuration et à l’administration des infrastructures. Dans le réseau IHFR, chaque périphérique critique — tels que les routeurs, switches et pare-feu — est protégé par des identifiants uniques et robustes, conformes aux bonnes pratiques de cybersécurité.

Trois niveaux de protection ont été appliqués :

**Mot de passe d’accès console** : empêche toute connexion physique directe sans authentification préalable.

**Mot de passe en mode privilégié** : protège la configuration interne de l’équipement, évitant toute modification non souhaitée.

Ces mots de passe sont choisis selon des critères stricts : longueur minimale de 12 caractères, combinaison de lettres majuscules, minuscules, chiffres et caractères spéciaux, et renouvellement périodique afin de limiter le risque de compromission. De plus, l’option **service password- encryption** est activée sur les équipements Cisco pour empêcher l’affichage en clair des mots de passe dans les fichiers de configuration. L’application systématique de cette politique renforce la

**sécurité d’accès administratif** et réduit significativement la surface d’attaque liée à l’exploitation directe des équipements

## Désactivation services inutiles

La désactivation des services inutiles sur les équipements réseau et les serveurs est une mesure essentielle pour réduire la surface d’attaque et limiter les risques de compromission. Chaque service actif constitue un point d’entrée potentiel qu’un attaquant peut exploiter ; il est donc important de ne conserver que ceux strictement nécessaires au fonctionnement du réseau IHFR.

Sur les **équipements Cisco** configurés dans Packet Tracer, les services non requis ont été désactivés afin d’empêcher la divulgation d’informations sensibles et d’éviter des attaques de type reconnaissance.

Cette politique de **minimalisme fonctionnel** a pour objectif de réduire les vecteurs d’attaque, de limiter les ressources consommées inutilement et d’améliorer la stabilité générale de l’infrastructure réseau.

**Chapitre V – Résultats et analyse**

## Introduction

Cette section présente les résultats obtenus suite à la mise en place des mesures de sécurité et de protection sur l’infrastructure réseau de l’IHFR, ainsi que l’analyse de leur efficacité. Elle permet d’évaluer concrètement l’impact des configurations réalisées, tant sur le plan de la sécurité que sur celui des performances et de la stabilité du réseau. Les tests effectués, les outils utilisés (comme Kali Linux pour les audits de vulnérabilité), ainsi que les incidents simulés, permettent de valider la robustesse des dispositifs mis en place. Une attention particulière est portée à l’identification des points forts et des éventuelles failles résiduelles afin d’envisager des améliorations futures.

## Les résultats des nouveaux scans

Après la mise en œuvre des différentes mesures de sécurité sur l’infrastructure du réseau IHFR, de nouveaux scans ont été réalisés afin d’évaluer leur efficacité. Les outils utilisés — **Nmap** pour l’analyse des ports ouverts et des services actifs, **Nikto** pour l’audit des vulnérabilités sur les serveurs webet **Wireshark** pour surveiller le trafic réseau — ont permis d'obtenir une vue complète de l’état de la sécurité après durcissement du système. Les résultats obtenus révèlent une nette amélioration : les ports sensibles sont désormais filtrés ou fermés, les services critiques sont correctement protégés, les communications sont mieux chiffrées et les fuites d’information via le réseau sont considérablement réduites. Cette analyse confirme l’efficacité des configurations appliquées et met en lumière les progrès réalisés en matière de cybersécurité.

##### **Les résultats de Nmap**

sudo nmap -p 137,138,139,445 192.168.1.40

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 17:49 CET Nmap scan report for 192.168.1.40

Host is up (0.00021s latency).

PORT STATE SERVICE

137/tcp closed netbios-ns 138/tcp closed netbios-dgm 139/tcp closed netbios-ssn 445/tcp closed microsoft-ds

MAC Address: 08:00:27:63:00:33 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

##### **Les résultats de l’énumerisation des service**

sudo enum4linux -a 192.168.1.40

[sudo] password for rolling:

Starting enum4linux v0.9.1 ( <http://labs.portcullis.co.uk/application/enum4linux/> ) on Mon Aug 4 17:39:12 2025

=========================================( Target Information

)=========================================

Target 192.168.1.40

RID Range ........ 500-550,1000-1050

Username ''

Password ''

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

============================( Enumerating Workgroup/Domain on 192.168.1.40

)============================

[E] Can't find workgroup/domain

================================( Nbtstat Information for 192.168.1.40

)================================

Looking up status of 192.168.1.40 No reply from 192.168.1.40

===================================( Session Check on 192.168.1.40

)===================================

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

#### Les résultats de l’énumerisation du WEB

sudo nikto -h [http://192.168.1.40](http://192.168.1.40/)

- Nikto v2.5.0

+ Target IP: 192.168.1.40

+ Target Hostname: 192.168.1.40

+ Target Port: 80

+ Start Time: 2025-08-04 17:50:56 (GMT1)

+ Server: Apache/2.4.58 (Ubuntu)

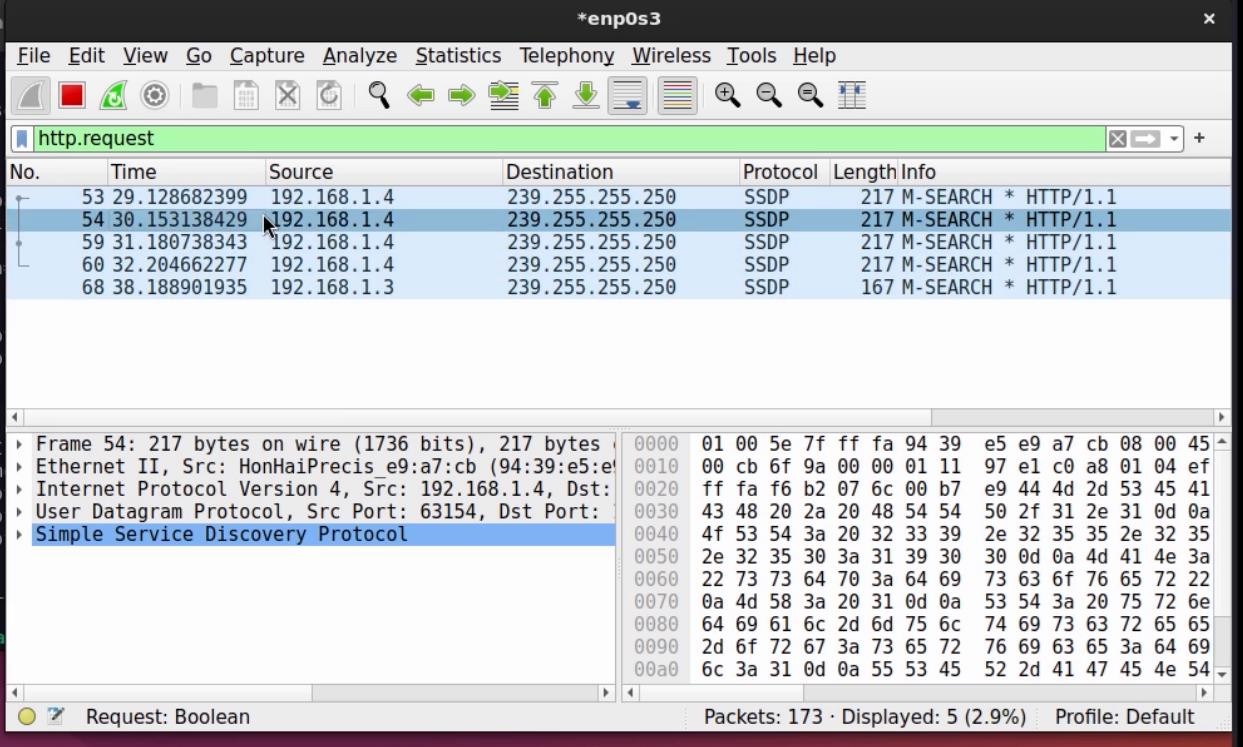
+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ 8102 requests: 0 error(s) and 0 item(s) reported on remote host

+ End Time: 2025-08-04 17:51:05 (GMT1) (9 seconds)

+ 1 host(s) tested

#### Les résultats de scan du les packet sur le réseau IHFR avec WIRESHARK

****

**Figure 29 :** fenétre de scan de wireshark

## Comparaison avant/ aprés la sécurisation

Afin de mesurer l’impact réel des mesures de sécurité mises en place dans le cadre de ce projet, une comparaison détaillée entre l’état initial du réseau (avant sécurisation) et l’état final (après durcissement) a été réalisée. Cette comparaison repose sur les résultats obtenus via plusieurs outils d’analyse tels que **Nmap, Nikto, Wireshark et des tests web**. Elle permet d’illustrer concrètement les failles détectées dans la configuration d’origine (comme l’exposition de ports sensibles, la présence de services obsolètes ou encore le trafic réseau non chiffré) et les améliorations apportées après l’implémentation des bonnes pratiques de sécurisation.

##### Risques identifiés (avant protection)

Des tests réalisés avec Kali Linux ont permis de détecter plusieurs vulnérabilités :

* Accès non autorisé entre VLANs
* Services HTTP exposés sans headers de sécurité
* Fichiers sensibles accessibles via Nikto
* Services Samba répondant anonymement (Enum4linux)
* Hôtes réseaux facilement détectables via Nmap

##### Mesures de sécurité mises en place

###### Réseau :

Configuration de VLANs sur tous les switchs

###### Switchs :

Activation de Port-Security (limitation d'adresses MAC) Désactivation des ports inutilisés

###### Pare-feu :

Filtrage du trafic WAN vers LAN

###### Serveur Ubuntu :

* Installation des services DNS (Bind9), DHCP, Apache2
* Configuration d'UFW (pare-feu logiciel)
* Configuration des headers HTTP (X-Frame-Options, X-Content-Type-Options)
* Suppression des fichiers sensibles détectés

###### Tests de résultats :

* Réduction du nombre de ports ouverts visibles via Nmap
* Disparition des fichiers sensibles via Nikto
* Session Samba bloquée via Enum4linux

##### Limites et recommandations

* Le réseau simulé dans Packet Tracer est limité aux fonctionnalités de Cisco ASA
* Il est recommandé d’ajouter un IDS/IPS comme Snort ou Suricata
* Intégration d’une solution de supervision centralisée (SIEM)

### **Conclusion**

Le réseau IHFR a été sécurisé à plusieurs niveaux : logique (VLANs), système (pare-feu, UFW, ), et physique (Port-Security, segmentation). Les tests de sécurité réalisés avec Kali Linux montrent une nette amélioration de la posture de sécurité. L'infrastructure est maintenant mieux protégée contre les intrusions, l'espionnage, et les erreurs de configuration.

## L’évolution de la protection et sécurité du réseau de IHFR

Au début du projet, l’infrastructure réseau de l’IHFR présentait plusieurs faiblesses en matière de sécurité, notamment l’absence de segmentation, la présence de services non sécurisés, et un manque de mécanismes de détection et de prévention des intrusions. Grâce à une analyse approfondie et à l’implémentation progressive de mesures correctives, l’environnement réseau a connu une évolution significative en termes de protection et de résilience. Cette évolution s’est traduite par l’activation de politiques de sécurité sur les équipements réseau (pare-feu, port-security, VLANs), le renforcement des configurations système (durcissement des serveurs, filtrage de ports, mots de passe forts), ainsi que l’installation d’outils de surveillance et d’analyse du trafic. L’ensemble de ces actions a permis d’ériger une couche de sécurité proactive et adaptée aux besoins spécifiques de l’infrastructure de l’IHFR.

## Grosse au mode des résultats

L’ajout de Les résultats obtenus à la suite des différents scans de sécurité démontrent clairement l’impact positif des mesures de sécurisation mises en œuvre dans le réseau de l’IHFR. Avant l’application des stratégies de durcissement et de segmentation, les scans révélaient plusieurs vulnérabilités : des ports critiques laissés ouverts , des services non sécurisés accessibles publiquement, et des transmissions non chiffrées détectées dans le trafic réseau. Nikto avait également détecté plusieurs failles dans les configurations web, notamment la divulgation d'informations sensibles et l’absence d’en-têtes de sécurité.

Après l'application des mesures correctives (filtrage des ports, activation de VLANs, désactivation de services inutiles, renforcement des mots de passe, mise à jour des logiciels, durcissement du système, etc.), une nette amélioration a été observée. Les nouveaux scans Nmap n'ont plus révélé de ports non essentiels exposés. Nikto n’a détecté aucune vulnérabilité critique sur le serveur web protégé, et les captures Wireshark ont montré une réduction significative du trafic en clair, grâce au blocage des protocoles obsolètes. De plus, les journaux système et les outils de monitoring mis en place ont permis de confirmer la stabilité et la sécurité accrue de l’infrastructure.

Ces résultats prouvent l’efficacité des stratégies de défense implémentées, tout en soulignant l’importance d’une politique de sécurité continue et adaptée aux besoins évolutifs du réseau. Il est toutefois recommandé de maintenir une veille active et d’effectuer régulièrement des audits pour anticiper de nouvelles menaces et garantir la pérennité des protections mises en place.

## Conclusion et recommadations

## Bilan du projet

Le projet de sécurisation et de protection du réseau informatique de l’Institut Hydrométéorologique de Formation et de Recherches (IHFR) a permis de mettre en évidence l’importance d’une approche méthodologique et structurée dans la mise en place d’une infrastructure réseau fiable et résiliente. À travers une démarche progressive, allant du diagnostic initial à la mise en œuvre des mesures correctives, il a été possible d’identifier les failles existantes, de les analyser, puis de proposer des solutions adaptées à l’environnement de l’institut.

Dans un premier temps, l’audit initial réalisé à l’aide d’outils comme **Nmap, Wireshark, Nikto et Enum4linux** a révélé plusieurs vulnérabilités critiques, notamment la présence de services exposés, un trafic non chiffré, des ports ouverts non nécessaires ainsi que des partages réseau insuffisamment protégés. Ces résultats ont confirmé la nécessité de renforcer la sécurité de l’infrastructure.

Ensuite, la mise en place des mécanismes de sécurisation a permis d’apporter des améliorations significatives. L’utilisation des **VLANs** pour segmenter le réseau a favorisé une meilleure isolation des départements et réduit les risques de propagation des attaques. Le **Port Security** a limité l’accès physique aux équipements réseau, tandis que la configuration de **UFW** sur le serveur Ubuntu a permis de filtrer efficacement le trafic et de réduire la surface d’attaque. Le durcissement du serveur, incluant la gestion des permissions, la désactivation des services inutiles et la mise en place de mots de passe robustes, a également renforcé la protection des données et des applications critiques.

Par ailleurs, la partie pratique réalisée avec **Packet Tracer, Ubuntu Server, Kali Linux et divers outils de cybersécurité** a permis de simuler, tester et valider les configurations adoptées dans un environnement contrôlé. Ces simulations se sont révélées essentielles pour anticiper les comportements du réseau et vérifier l’efficacité des mesures de sécurité.

Enfin, l’évaluation finale, réalisée par de nouveaux scans de vulnérabilité, a montré une nette amélioration de la posture de sécurité du réseau IHFR. Plusieurs failles initialement détectées ont été corrigées, le trafic réseau est désormais mieux surveillé, et la structure globale est plus résiliente face aux cybermenaces.

En somme, ce projet a permis de **renforcer la sécurité de l’infrastructure réseau IHFR**, de sensibiliser à l’importance des bonnes pratiques en cybersécurité, et d’établir une base solide pour de futures évolutions. Bien que certaines limites persistent, notamment en termes de ressources matérielles et humaines, le travail accompli constitue une étape déterminante vers la mise en place d’un réseau moderne, sécurisé et durable.

## Limites rencontrées

Malgré les résultats satisfaisants obtenus au cours de ce projet de sécurisation, certaines limites ont été rencontrées, tant sur le plan technique que logistique :

##### **Environnement simulé vs réalité**

La majorité des configurations réseau ont été testées dans Cisco Packet Tracer, un outil puissant mais limité. les fonctionnalités avancées de sécurité, notamment les tests de charge, les attaques complexes ou les configurations firewall détaillées, ne peuvent pas y être entièrement reproduites.

##### **Ressources matérielles limitées**

L’infrastructure de l’IHFR ne dispose pas encore de tous les équipements nécessaires à la mise en œuvre complète (comme des routeurs de nouvelle génération, des pare-feux physiques dédiés, ou des sondes de détection d'intrusion), ce qui a

limité l'application réelle de certaines solutions prévues dans la simulation.

##### **Temps de déploiement restreint**

Le calendrier du projet a été contraint par des impératifs académiques et organisationnels. Certaines phases, comme les tests d’intrusion avancés ou la mise en place d’une supervision en temps réel, n'ont pas pu être poussées aussi loin que souhaité.

##### **Manque de sensibilisation des utilisateurs**

Bien que le système ait été sécurisé techniquement, la sensibilisation des utilisateurs (agents, stagiaires, chercheurs) aux bonnes pratiques de cybersécurité reste une faiblesse persistante qui pourrait compromettre les efforts mis en place.

La sécurité d’un réseau n’est jamais figée. Le serveur Ubuntu et les systèmes réseau nécessitent des mises à jour régulières et une surveillance continue, ce qui nécessite des ressources humaines compétentes que l’IHFR ne possède pas encore de façon permanente.

## Perspectives d’amélioration

Malgré les résultats positifs obtenus, plusieurs pistes peuvent être explorées pour renforcer davantage la sécurité et la résilience du réseau de l’IHFR :

**Mise en place d’un système de détection d’intrusion (IDS)** : Intégrer des outils comme **Snort**, **Suricata** permettrait une surveillance proactive des menaces internes et externes en temps réel. **Sauvegardes automatisées et plan de reprise** : Déployer un **système de sauvegarde automatique** des configurations et des données critiques, ainsi qu’un **plan de reprise après sinistre (PRA)** pour assurer la continuité de service en cas de panne ou d’attaque.

**Authentification renforcée** : Ajouter l’**authentification multifactorielle (MFA)** pour les connexions aux services sensibles (SSH, interfaces d’administration web, accès à distance). **Supervision centralisée du réseau** : Mettre en place une **solution de supervision** comme **Nagios**, **Zabbix** ou **Grafana + Prometheus** pour surveiller en temps réel l’état des équipements, services, et détecter les anomalies.

**Audit de sécurité régulier** : Réaliser des **audits périodiques** (tests d’intrusion internes/externes) pour maintenir un haut niveau de sécurité face à l’évolution des menaces.

**Sensibilisation des utilisateurs** : Organiser des **formations régulières** pour le personnel sur les bonnes pratiques de cybersécurité (phishing, gestion des mots de passe, navigation sécurisée, etc.). **Virtualisation des services critiques** : Migrer certains services vers des **environnements virtualisés ou conteneurisés** (comme Docker) pour améliorer leur isolation et leur facilité de déploiement/reprise.

**Mise à jour continue** : Automatiser la **veille sur les vulnérabilités** et les **mises à jour de sécurité**

sur tous les équipements (serveur, routeurs, switches, etc.).

Ces perspectives visent à faire évoluer l’infrastructure de l’IHFR vers un modèle plus résilient, proactif et conforme aux standards actuels de cybersécurité.

# REFERENCES BIBLIOGRAPHIQUES

* site ubuntu: https://documentation.ubuntu.com/server/
* site kali: <https://www.kali.org/docs/introduction/what-is-kali-linux/>
* site vitualbox: <https://www.virtualbox.org/manual/ch01.html>
* site cisco academy: <https://www.netacad.com/cisco-packet-tracer>
* les cours de Google Cybersecurity Certificate
* site de hackthebox: <https://www.hackthebox.com/>
* site de tryhackme : <https://tryhackme.com/>