« La maîtrise vient avec le temps, l'échec fait partie du chemin. Restez curieux, restez constants. »

Sécurité des Réseaux

Projet de Fin de session

Titre du projet : Conception et sécurisation d'un réseau informatique avec pfSense, portail captif et système IDS

Introduction :

Ce projet de fin de session du cours *Sécurité des Réseaux* vise à amener les étudiants à concevoir et sécuriser un réseau complet à l'aide de pfSense. L'implémentation technique est réalisée individuellement, tandis que le rapport est produit en groupe, favorisant ainsi l'autonomie et le travail collaboratif.

Les étudiants doivent configurer un réseau segmenté, appliquer des règles de filtrage, mettre en place un portail captif, un IDS, et analyser le trafic réseau avec Zenmap et Wireshark. Ce projet permet de consolider les compétences techniques tout en développant l'esprit d'équipe, la rigueur et la capacité à documenter des choix techniques dans un contexte réaliste.

Partie 1 – Présentation générale du projet

Contexte du cours :

- **Cours** : Sécurité des Réseaux
- **Session** : ÉTE 2025 (Groupe Matin)
- **Enseignant responsable** : Bounama GUEYE
- **Poids dans la session** : **40 % de la note finale**
- **Note maximale** : **100 points**

Répartition des responsabilités :

- **Rédaction du rapport** : réalisée en **groupe** (maximum 3 étudiants) ***(30 Points)***
- **Implémentation technique (VirtualBox, pfSense, clients, services)** : réalisée **individuellement** ***(70 points)*** **et présentation individuelle et goupe des travaux en salle.**

Objectifs pédagogiques :

Ce projet vise à :

- Déployer un réseau informatique segmenté et sécurisé dans VirtualBox
- Configurer un pare-feu pfSense avec trois interfaces réseau (WAN, LAN1, LAN2)
- Mettre en œuvre un **portail captif** pour l'authentification des utilisateurs
- Installer un **IDS (Snort)** pour surveiller les flux réseau
- Créer des **règles de filtrage avancées** dans pfSense
- Utiliser **Nmap** pour le scan réseau et **Wireshark** pour analyser le trafic

Résultat attendu :

Chaque étudiant devra :

- Réaliser l'**implémentation complète du réseau** sur sa propre machine
- Générer des captures d'écran de toutes les configurations requises
- Participer à la **rédaction commune** du rapport technique de groupe

Partie 2 – Architecture réseau et préparation des machines

Objectif :

Mettre en place une architecture réseau virtuelle avec **pfSense comme pare-feu**, trois interfaces réseau, deux segments LAN, un accès WAN, et des machines clientes. Une machine **Metasploitable** est ajoutée au LAN1 pour simuler un hôte vulnérable destiné aux tests de sécurité.

Description de l'architecture :

1. PfSense (pare-feu) – VM principale :

- 3 interfaces réseau :
  - **WAN** : accès Internet (mode pont)
  - **LAN1** : 192.168.2.0/24 – passerelle : 192.168.2.254
  - **LAN2** : 172.16.2.0/24 – passerelle : 172.16.2.254
- Rôle :
  - Distribution d'adresses via DHCP
  - Application des règles de sécurité
  - Fourniture des services (portail captif, IDS Snort, etc.)

2. LAN1 – 192.168.2.0/24 :

- **Machine cliente 1 (Client1)** – OS au choix (Windows/Linux)
- **Machine cliente 2 (Client2)** – OS au choix (Windows/Linux)
- **Machine Metasploitable 2** – **Adresse IP fixe : 192.168.2.5**
  - Rôle : cible vulnérable pour les tests Nmap, Snort, etc.
- **PfSense LAN1 Gateway** : 192.168.2.254

3. LAN2 – 172.16.2.0/24 :

- **Machine cliente 3 (Client3)** – OS au choix (Windows/Linux)
- **Machine cliente 4 (Client4)** – OS au choix (Windows/Linux)
- **PfSense LAN2 Gateway** : 172.16.2.254

4. WAN :

- Connecté en **mode pont (bridge)** sur l'interface physique hôte pour donner accès à Internet

Configuration recommandée :

- **VirtualBox** avec réseau en mode :
  - WAN : **Accès par pont**
  - LAN1 & LAN2 : **Réseau interne** (noms séparés pour chaque LAN)
- Chaque interface de pfSense associée à la bonne zone
- Adresse statique configurée manuellement sur Metasploitable

Partie 3 – Configuration DHCP sur pfSense

Objectif :

Mettre en place un service DHCP dans pfSense pour distribuer automatiquement les adresses IP aux machines des deux réseaux LAN.

LAN1 – Configuration du DHCP via console (terminal)

Informations :

- Interface : **LAN1**
- Réseau : 192.168.2.0/24
- Passerelle (pfSense) : 192.168.2.254
- Plage DHCP : 192.168.2.10 à 192.168.2.100

Étapes (dans la console pfSense) :

1. Démarrer la VM pfSense
2. Dans le menu texte de configuration, taper : 2 pour configurer les interfaces
3. Choisir **LAN** puis attribuer l'adresse IP statique :
   192.168.2.254 avec masque /24
4. Lorsque pfSense demande **Activer le serveur DHCP sur le LAN ?**
   Répondre : y
5. Indiquer la plage d'adresses :
   - Début : 192.168.2.10
   - Fin : 192.168.2.100
6. Laisser les autres champs (passerelle, DNS, etc.) vides ou par défaut

À inclure dans le rapport :

- Capture de l'écran console montrant la configuration DHCP activée
- Capture du test avec une machine cliente ayant reçu une IP dans la plage

LAN2 – Configuration du DHCP via interface Web

Informations :

- Interface : **LAN2**
- Réseau : 172.16.2.0/24
- Passerelle (pfSense) : 172.16.2.254
- Plage DHCP : 172.16.2.10 à 172.16.2.100

Étapes (dans l'interface Web pfSense) :

1. Accéder à l'interface Web depuis une machine LAN1 :
   https://192.168.2.254
   (login : admin, mot de passe : pfsense)
2. Aller dans : Services > DHCP Server > LAN2
3. Cocher **Enable DHCP Server on LAN2 interface**
4. Définir la plage :
   - From : 172.16.2.10
   - To : 172.16.2.100
5. Laisser les options DNS, Gateway par défaut ou manuellement
6. Cliquer sur **Save** puis **Apply Changes**

À inclure dans le rapport :

- Capture de l'interface Web avec la configuration active du serveur DHCP sur LAN2
- Capture d'un client LAN2 ayant reçu une adresse dans la plage

Partie 4 – Mise en place d'un Portail Captif sur LAN1

Objectifs :

- Contrôler l'accès des utilisateurs du réseau LAN1 à Internet
- Mettre en œuvre un portail captif pour forcer l'authentification via navigateur web
- Gérer des utilisateurs locaux et valider leur connexion
- Documenter chaque étape avec des captures dans le rapport collectif

Principe du portail captif :

Quand un utilisateur se connecte au LAN1 et tente d'accéder à un site web, il est automatiquement redirigé vers une page d'authentification hébergée sur pfSense. Une fois connecté, il peut accéder à Internet.

Étapes de mise en place dans pfSense :

Étape 1 : Créer une zone de portail captif

1. Aller dans le menu Services > Captive Portal
2. Cliquer sur **+ Add**
3. Donner un nom à la zone (ex. : LAN1-portal)
4. Sélectionner l'**interface LAN1**
5. Cocher **Enable Captive Portal**
6. Sauvegarder et appliquer les changements

Capture à insérer dans le rapport : création de la zone et interface associée

Étape 2 : Définir la méthode d'authentification

1. Toujours dans l'onglet de la zone créée, aller dans Authentication
2. Choisir : **Local User Manager**
3. Sauvegarder

Capture à insérer : sélection du mode d'authentification

Étape 3 : Créer les utilisateurs

1. Aller dans System > User Manager
2. Cliquer sur **+ Add**
3. Créer **trois utilisateurs distincts** (ex : user1, user2, user3)
    - Remplir : username, mot de passe
4. Sauvegarder à chaque fois

Captures à insérer : création de chaque utilisateur avec identifiant et mot de passe (masqués)

Étape 4 : Personnaliser le portail (optionnel)

1. Retourner dans Services > Captive Portal > Zone
2. Onglet **File Manager** : ajouter un logo ou modifier la page HTML
3. Peut inclure :
    - Message de bienvenue
    - Logo de l'établissement
    - Politique d'utilisation

Capture suggérée : aperçu de la page ou gestion des fichiers HTML

Étape 5 : Tester le portail captif

1. Depuis une machine sur **LAN1**, accéder à un site web (ex. www.google.com)
2. La redirection doit apparaître automatiquement vers la **page de login**
3. Saisir un des identifiants créés (user1, user2, etc.)
4. Une fois authentifié, accéder à Internet

Captures attendues :

- Redirection vers la page d'authentification
- Connexion réussie
- Accès Internet confirmé

Éléments à vérifier et insérer dans le rapport :

Élement Capture attendue	
Création de la zone Captive Portal	✓
Sélection de l'interface LAN1	✓
Choix de l'authentification locale	✓
Création de 3 utilisateurs	✓
Redirection vers la page de login	✓
Connexion réussie et accès à Internet	✓

Partie 5 – Règles de filtrage dans pfSense

Objectif :

Mettre en œuvre des règles de filtrage dans pfSense afin de :

- Contrôler les communications entre les LAN
- Sécuriser l'accès à Internet
- Restreindre l'accès à des machines sensibles (comme Metasploitable)
- Implémenter des règles horaires pour restreindre certains usages

Liste complète des règles à configurer

Règle 1 – Autoriser l'accès Internet depuis LAN2

- **Interface** : LAN2
- **Action** : Pass
- **Source** : LAN2 net

- **Destination** : any
- **Protocole** : any
- **Description** : Autoriser Internet depuis LAN2

À capturer : Écran des règles de LAN2 montrant cette règle.

Règle 2 – Autoriser la communication LAN2 → LAN1

- **Interface** : LAN2
- **Action** : Pass
- **Source** : LAN2 net
- **Destination** : 192.168.2.0/24
- **Protocole** : any
- **Description** : Autoriser accès LAN2 vers LAN1

Règle 3 – Bloquer la communication LAN1 → LAN2

- **Interface** : LAN1
- **Action** : Block
- **Source** : LAN1 net
- **Destination** : 172.16.2.0/24
- **Protocole** : any
- **Description** : Bloquer accès LAN1 vers LAN2
- Cocher l'option **Log packets** pour vérification dans les journaux

Règle 4 – Autoriser uniquement le http vers Metasploitable depuis une IP spécifique

- **Interface** : LAN2
- **Action** : Pass
- **Source** : 172.16.2.10 (ex. client autorisé)
- **Destination** : 192.168.2.5 (Metasploitable)
- **Protocole** : TCP
- **Port destination** : 80
- **Description** : Autoriser http de client LAN2 vers Metasploitable

Règle 5 – Bloquer tout autre accès vers Metasploitable

- **Interface** : LAN2
- **Action** : Block
- **Source** : LAN2 net
- **Destination** : 192.168.2.5
- **Protocole** : any
- **Description** : Bloquer accès vers Metasploitable sauf http

Cette règle doit être **placée après** la règle 4 dans la liste.

Règle 6 – Autoriser uniquement le ping entre les deux LAN

- **Sur LAN1** :
  - Action : Pass
  - Protocole : ICMP
  - Source : LAN1 net
  - Destination : 172.16.2.0/24
  - Description : Autoriser ping LAN1 → LAN2
- **Sur LAN2** :

- Action : Pass
- Protocole : ICMP
- Source : LAN2 net
- Destination : 192.168.2.0/24
- Description : Autoriser ping LAN2 → LAN1

Règle 7 – Bloquer Internet pour LAN2 selon une plage horaire

- **Étape 1 : Créer un planning**
  - Menu : Firewall > Schedules > Add
  - Nom : BlocageNuit
  - Jours : Tous
  - Heures : de 20h00 à 08h00
- **Étape 2 : Appliquer la règle**
  - Interface : LAN2
  - Action : Block
  - Source : LAN2 net
  - Destination : any
  - Schedule : BlocageNuit
  - Description : Bloquer Internet de nuit depuis LAN2

À inclure dans le rapport : Les captures des règles et les résultats des tests

Tests à effectuer

Test	Attendu
Accès Internet depuis LAN2	✓ Fonctionne (Règle 1)
Ping LAN2 → LAN1	✓ Fonctionne (Règle 2)
Ping LAN1 → LAN2	✗ Bloqué (Règle 3)
Accéder au site de Metasploitable avec 192.168.2.5 sur un navigateur client du LAN 2	✓ Fonctionne (Règle 4)
Autre trafic LAN2 → Metasploitable	✗ Bloqué (Règle 5)
Ping inter-LAN uniquement	✓ ICMP autorisé, autres services bloqués (Règle 6)
Navigation Internet depuis LAN2 la nuit	✗Bloquée (Règle 7)

Partie 6 – Installation et configuration de Snort (IDS) sur pfSense

Objectifs :

- Mettre en place un **système de détection d'intrusions (IDS)** avec **Snort** sur pfSense
- Surveiller en temps réel le trafic réseau sur une ou plusieurs interfaces
- Détecter les comportements suspects ou attaques (ex : scan Nmap, ping ICMP, vulnérabilités connues)
- Documenter toutes les étapes de configuration et les alertes générées

Présentation rapide :

- **Snort** est un IDS open source capable de détecter des attaques par signatures (ex : port scanning, buffer overflow, exploit réseau, etc.)
- Sur pfSense, il s'installe en tant que **paquet additionnel**, configurable via l'interface web

Étapes d'installation et de configuration :

Étape 1 : Installation de Snort

1. Accéder à pfSense via l'interface web (https://192.168.2.254)
2. Aller dans : System > Package Manager > Available Packages
3. Rechercher **Snort**
4. Cliquer sur **Install**
5. Confirmer et attendre la fin de l'installation

Capture attendue : installation de Snort dans le Package Manager

Étape 2 : Configuration de base

1. Aller dans : Services > Snort
2. Onglet **Global Settings** :
    - Activer la **téléchargement des règles** (Snort VRT ou Emerging Threats)
    - Cocher **Enable OpenAppID detectors** (optionnel)
    - Enregistrer

Capture : écran des Global Settings avec les options activées

Étape 3 : Ajouter une interface à surveiller

1. Aller dans l'onglet **Interfaces**
2. Cliquer sur **+ Add**
3. Sélectionner l'interface à surveiller :
    - Recommandé : **LAN1** ou **LAN2**
4. Donner un nom descriptif (ex : Snort-LAN1)
5. Sauvegarder

Capture attendue : interface Snort activée sur LAN1 ou LAN2

Étape 4 : Activer la détection et les règles

1. Une fois l'interface ajoutée, cliquer sur son nom
2. Aller dans l'onglet **Categories** :
    - Sélectionner les règles à appliquer (ex. : scan, malware, policy, etc.)
3. Dans **Interface Settings** :
    - Cocher **Enable Snort**
    - Cocher **Block offenders** (si IPS souhaité, optionnel)
4. Sauvegarder et **Apply Changes**

Capture : interface Snort activée avec règles sélectionnées

Étape 5 : Test de détection

1. Depuis une machine sur LAN2, effectuer un **scan Nmap** ou un **ping** vers LAN1 (Metasploitable)
2. Aller dans : Services > Snort > Alerts
3. Vérifier si des **alertes sont déclenchées**

Captures attendues :

- Écran des alertes avec horodatage, type, adresse IP source/destination

- Exemple d'alerte : port scan détecté, attaque brute force, etc.

Éléments à vérifier et insérer dans le rapport :

Élément	Capture attendue
Installation réussie de Snort	✓
Paramètres globaux (règles, AppID)	✓
Ajout d'une interface Snort (LAN1/LAN2)	✓
Activation des catégories de règles	✓
Exemple d'alerte Snort déclenchée	✓

Partie 7 – Analyse complémentaire avec Zenmap

Objectifs :

- Utiliser **Zenmap** pour effectuer un scan visuel du réseau
- Identifier les ports ouverts et services actifs sur la machine **Metasploitable**
- Générer automatiquement une **topologie réseau** à partir des résultats du scan
- Documenter les résultats dans le rapport collectif

Étapes d'utilisation de Zenmap

1. Lancer Zenmap

- Depuis une machine cliente (Windows avec Zenmap installé)
- Interface graphique de **Nmap**

2. Définir la cible et le type de scan

Cible : 192.168.2.0/24

Commande de scan (à saisir dans la barre "Command" ou choisir un profil prédéfini) :

nmap -sS -sV -O 192.168.2.0/24

Option	Description
-sS	Scan SYN furtif
-sV	Détection des versions des services
-O	Détection du système d'exploitation

Capture attendue : interface Zenmap avec cible saisie et scan lancé

3. Analyser les résultats

- Onglet **Nmap Output** : affiche les ports ouverts, services, OS estimé
- Onglet **Ports / Hosts** : vue structurée par protocole
- Onglet **Topology** : **visualise la topologie réseau**
  - Clic sur les nœuds pour explorer les détails
- Onglet **Host Details** : résumé des informations système
- Onglet **Scans** : historique des scans effectués

Captures attendues :

- Résultats dans **Nmap Output**
- Vue **Topology** générée automatiquement

- Détails du host (Metasploitable)

Éléments à inclure dans le rapport :

Élément Capture attendue	
Interface de Zenmap avec commande et cible	✓
Résultats du scan (Nmap Output ou Host Details)	✓
Carte Topologique générée automatiquement	✓
Identification des ports ouverts et services actifs	✓

Barème du projet de fin de session – 100 points (40 % de la note finale)

Implémentation individuelle (70 points)
Rapport rédigé en groupe (collectif) (30 points)

Partie	Points	Détails
1. Présentation générale et structure de projet	5 pts	Page de garde, objectifs du projet, contexte bien présenté
2. Architecture réseau (VirtualBox + topologie)	5 pts	Création de pfSense avec WAN, LAN1, LAN2, Metasploitable, schéma clair
3. DHCP LAN1 (console)	5 pts	Configuration via console + test DHCP + capture
4. DHCP LAN2 (interface Web)	5 pts	Configuration via interface Web + test DHCP + capture
5. Règles de filtrage (de base et avancées)	15 pts	Internet, filtrage inter-LAN, accès SSH restreint, ICMP, planning horaire, logs
6. Portail Captif sur LAN1	15 pts	Activation, page de login, création de 3 utilisateurs, test de connexion
7. Snort (IDS) sur pfSense	15 pts	Installation, configuration, règles de détection activées, captures, analyse
8. Tests de connectivité + interfaces pfSense	5 pts	Ping vers passerelles, attribution IP, interfaces visibles
9. Analyse complémentaire (Wireshark & Nmap)	5 pts	Scan Nmap vers Metasploitable, captures ICMP/DNS/HTTP, export .pcapng
10. Rapport final collectif (forme + fond)	30 pts	Rédaction claire, rigueur technique, qualité des explications et captures, cohérence globale
Total	100 points	

Ce que vous devez faire

Présentation en salle (le Mardi 10 juin et Mercredi 11 juin 2025)

- Chaque groupe présente son projet en classe
- Chaque membre doit présenter son travail
- Durée : 10 à 12 minutes

Rapport collectif (à rendre le samedi 14 juin)

- Un seul rapport PDF par groupe
- Avec captures, explications et toutes les étapes du projet
- À remettre nommé : Projet_Reseaux_Eté2024_NomGroupe

Bonne Chance

« Ce n'est pas en réussissant du premier coup qu'on apprend, mais en persévérant après chaque erreur »

Documentation complémentaire

pfSense – Documentation officielle

- https://docs.netgate.com/pfsense/en/latest/
- https://www.dir-tech.com/comment-configurer-un-lab-pfsense-avec-virtualbox/
- https://forum.netgate.com/

Portail Captif pfSense

- https://www.youtube.com/watch?v=JmCadrWt1ag
- https://docs.netgate.com/pfsense/en/latest/services/captiveportal/index.html

Snort IDS sur pfSense

- https://docs.netgate.com/pfsense/en/latest/packages/snort/index.html
- https://leblogdolivyeahh.wordpress.com/2020/08/27/pfsense-snort-detection-dintrusion/
- https://www.youtube.com/watch?v=1wAOjVob49w

Zenmap / Nmap

- https://nmap.org/zenmap/
- https://nmap.org/book/man-briefoptions.html
- https://nmap.org/book/toc.html
- https://www.youtube.com/watch?v=20hEGSv2hr8

Wireshark – Analyse réseau

https://www.wireshark.org/docs/
https://zestedesavoir.com/tutoriels/677/wireshark-pour-les-nuls/
https://www.youtube.com/watch?v=uEa1HLQRsfQ
https://www.youtube.com/watch?v=aQZV9H_wUFM