Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En Vue de l'Obtention du Diplôme de Master en Informatique

Option : Administration et sécurité des reseaux

Thème :

Audit et definition d'une politique de sécurité. Cas d'etude SONATRACH DP.

Réalisé par :

M^{lle} BORDJAH Dahia BOUDJADI Amel

Devant le jury composé de :

Président :	M^{r}	K.KABYL,	Université de Béjaia.
Examinateur :	M^{r}	N.SALHI,	Université de Béjaia.
Examinateur :	M^{R}	A.BAADACHE	Université de Béjaia.
Encadreur :	M^{R}	M.HAMMOUMA,	Université de Béjaia.

Juin 2013

Remerciements

Nous tenons à exprimer nos vifs remerciements et notre profonde gratitude à l'ensemble du personnel de la SONATRACH DP, de l'université de Bejaia, et à tous ceux qui ont contribué à la réalisation de ce travail.

Nos remerciements vont également à nos promoteurs Mr LAMINI Rabeh et Mr HAMMOUMA Moumen pour leurs conseils judicieux, ainsi qu'à l'ensemble du corps enseignant de l'université de Bejaïa.

Un grand merci va à nos familles, pour leur soutien permanent et indéfectible.
Un merci pudique à nos amis, nos collègues en Master 2 et à tous ceux qui ont contribué à la concrétisation de cette œuvre.

Nous rendons grâce à Dieu, le tout puissant et miséricordieux, de nous avoir donné le courage et la patience pour mener à bien et à terme ce modeste travail.

Dédicaces

Je dédie ce modeste travail :

à mes parents, à mes grands parents,
à mes deux frères Fayçal et Fouad ,à ma sœur Assia,
à toute ma famille de prés et de loin , à mes collègues,
à tous mes amis,
à Sabrina, Hamida, Dalal, Asma, Kahita, kahina, Maya, Nassima, Ma binome Amel, Youyou
à ceux que j'ai pas pu citer.
Dahia

Je dédie ce modeste travail :

à mes parents.
Amel

Table des matières

Liste des Abréviations

AFAI	Association Française de l'Audit et du Conseil Informatique.
ARP	Address resolution protocol.
ASP	Active Server Pages.
BASE	Interface Basic Analysis and Security Engine.
COBIT	Control objectives for information and technology.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information.
DHCP	Dynamic Host Control Protocol.
DMZ	Zone démilitarisée.
DNS	Domain Name System.
EAP	Extensible Authentication Protocol.
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité.
FAI	Fournisseur d'Accès Internet.
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité.
ICMP	Internet Control Message Protocol.
IDS	Système de Détection d'Intrusions.
IOS	Internetwork Operating System.
IP	Internet Protocol.
IPS	Système de Prévention d'Intrusions
IPsec	Internet Protocol Security.
ISACA	Information Systems Audit and Control Association.
ITIL	Information Technology Infrastructure Library.
LAN	Local Area Network.
LTS	Long Term Support.
MAC	Media Access Control.
MARION	Méthodologie d'Analyse de Risques Informatiques Orientée par Niveau.
MEHARI	MEthode Harmonisée d'Analyse de Risques.
NAC	Network Admission Control
N-IPS	Network Intrusion Protocol Prevention.
OSI	Open Systems Interconnection.
PHP	Personal Home Page.

Radius Remote Authentication Dial-In User Service.
RPC Remote Procedure call.
RSSI Risques de sécurité des systèmes d'information.
SGBD Système de Gestion de Base de données.
SMSI Système de Management de la Sécurité de l'Information
SQL Structured Query Language.
SSH Secure Shell.
SSI sécurité des systèmes d'information.
SSL Secure Sockets Layer.
TCP Transmission Control Protocol.
TI Test d'Intrusions.
UDP User Datagram Protocol.
URPF Unicast Reverse Forwarding Protocol.
VLAN Virtual Local Area Network.
VPN Virtual Private Network.
WAN Wide Area Network.

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

L'INFORMATIQUE est devenue un outil incontournable de gestion, d'organisation, de production et de communication. Le réseau informatique de l'entreprise met en oeuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises ou personnes ou les importe à partir d'autres sites. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Il est donc impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données ses caractères électroniques et confidentiels. Les données sensibles du système d'information de l'entreprise sont donc exposées à des actes de malveillance dont la nature et la méthode d'intrusion sont indéterminablement changeantes. Les prédateurs et voleurs s'attaquent aux ordinateurs essentiellemnt par le biais d'accès aux réseaux reliant l'entreprise à l'extérieur.

Le développement des réseaux, la croissance exponentielle des terminaux à protéger, la prolifération de nouvelles menaces sur Internet démontrent que la mise en place d'un audit de sécurité informatique demeure un enjeu stratégique majeur, d'où la nécessité de définir une politique de sécurité claire et fiable.

Un audit de sécurité informatique consiste à s'adosser sur le savoir-faire d'un expert talentieux dans le but d'analyser et de s'assurer que toutes les règle de la politique de sécurité soient judicieusement appliquées pour enfin valider les moyens de protection et les dispositions sécuritaires mis en oeuvre.

La politique de sécurité d'une entreprise se fonde avant tout sur une gestion des risques décrivant les ressources critiques de l'entreprise, ses objectifs de sécurité, ses vulnérabilités, les probabilités d'occurence de menaces sur ces ressources vitales, ainsi que leurs concéquences sur l'entreprise.

En outre, la détection d'intrusions reste une nécessité pour assurer la complétude d'une politique de sécurité. Ce qui fait des systèmes de détection d'intrusions un élément crucial pour une sécurité optimale d'un réseau. Ils permettent de détecter les tentatives d'intrusions tout en prenant en compte une base de signature des différentes attaques connues.

Afin de cerner convenablement le sujet, le canevas suivant est adopté :
Le premier chapitre est réservé à la présentation de l'organisme d'accueil. Son but est de se familiariser avec l'entreprise SONATRACH "Division Production" et de se fixer ainsi les idées sur la démarche à suivre pour répondre aux exigences voilées derrière le thème énoncé plus haut dans ce document.

Quelques rappels théoriques des différentes attaques les plus connues, la politique de sécurité informatique et ses différents objectifs, ainsi que la présentation des différentes parades faisant face aux diverses attaques sont traités dans le second chapitre.

Le troisième chapitre est consacré à l'audit de sécurité informatique, lequel est scindé en deux parties primordiales : La première comporte une étude théorique qui définit le thème d'audit de la sécurité informatique et ses différentes normes avec ses diverses méthodes. Quant à la seconde partie, elle est axée sur le choix d'une démarche judicieuse pour l'application de la méthode EBIOS afin de mettre en place un processus d'audit de sécurité.

Le quatrième chapitre, quant à lui, présente les systèmes de détection d'intrusions ainsi que l'environnement de travail. Nous détaillerons dans un premier temps les systèmes de détection d'intrusions en se basant principalement sur l'IDS Snort. Enfin, pour la mise en place et le test de ce dernier, nous spécifions l'environnement de notre travail et tous les outils y afférents.

La définition d'une politique de sécurité ainsi que la mise en place de l'IDS Snort pour une amélioration future de la sécurité du réseau de la SONATRACH DP est l'objet du cinquième chapitre.

CHAPITRE 1

PRÉSENTATION DE L'ORAGANISME D'ACCUEIL

1.1 Introduction

Afin de nous familiariser avec l'environnement de l'entreprise, nous avons d'emblée cherché à définir l'activité principale de la SONATRACH "Division Production", ses différentes divisions qui la constituent ainsi que les taches associées à chaque division. nous nous sommes intéressées par la suite à la Division Informatique afin de comprendre l'architecture réseau de l'entreprise, pour enfin illustrer les différents équipements qui la constitue.

Ce chapitre est ainsi, une introduction au réseau et à l'environnement de l'entreprise SONATRACH "Division Production".

1.2 Présentation de la SONATRACH

SONATRACH "Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures" est une entreprise publique algérienne et un acteur majeur de l'industrie pétrolière.

SONATRACH est une compagnie nationale d'envergure internationale, c'est la clé de voûte de l'économie algérienne.

Le groupe pétrolier et gazier SONATRACH intervient dans l'exploration, la production, le transport par canalisation, la transformation et la commercialisation des hydrocarbures et de leurs dérivés.

1.3 Présentation de la SONATRACH "Division Production"

1.3.1 Organigramme de l'entreprise

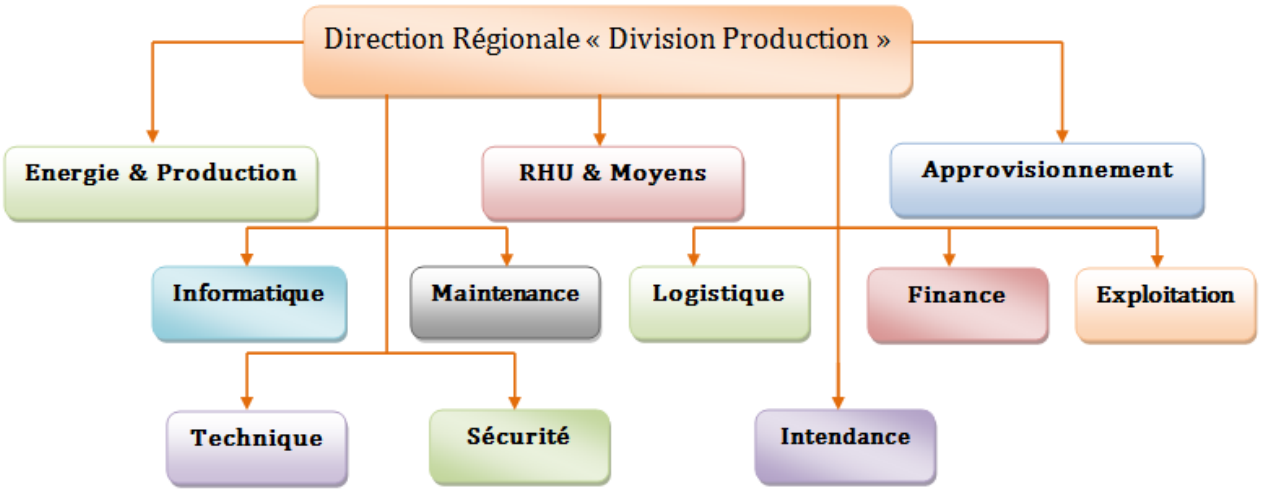


FIGURE 1.1 – Organigramme associé à la Direction Régionale "DP"

1.3.2 Définition et rôle de chaque service au sein de l'entreprise

Division Sécurité

Cette division est située au niveau de la base 24 Février, elle à pour missions principales d'assurer :

- La protection et la préservation du personnel ;
- La préservation et la conservation du patrimoine industriel ;
- La protection de l'environnement.

Division Exploitation

Les activités essentielles associées à cette division sont les suivantes :

- Traitement du brut ;
- Compression du gaz ;
- Raffinage du brut ;

– Stockage et acheminement du brut par pipes vers Haoud-El-Hamra puis vers les grands centres d'exportation.

Division Maintenance

cette division quant à elle assure ce qui suit :
– Le maintien en bon état des différents équipements pétroliers de surface.

Division Informatique

cette division assure :
– La coordination de l'activité informatique au niveau de la Direction Régionale.

Division Energie et Production

– Le développement de tout le champ Hassi-Messaoud ;
– La gestion des puits de production en s'impliquant dans les opérations de sondage pendant le forage.

Division Logistique

cette division a pour taches principales d'assurer :

– La contribution au développement de la direction régionale par l'étude, la définition, la réalisation et la maintenance des installations d'infrastructures non pétrolières.

Applications domestiques Division Technique

cette division est chargée d'assurer :
– La gestion des projets dans leurs phases d'étude et de supervision des travaux.

Division Intendance

cette division a comme tâche principale de :

– Prester les services d'hébergement et de restauration au personnel de la Direction Régionale.

Division Finance

cette division a pour tâche essentielle de s'assurer que la direction régionale dispose en temps voulu, des fonds nécessaires à sa croissance et son développement et que l'argent généré par les activités de l'entreprise soit investi de manière rentable.

Division Approvisionnement

cette division a pour mission :

– L'alimentation de toutes les structures de la Direction Régionale en consommables et en amortissables en temps voulu et au cout optimal.

Division Ressources Humaines et Moyens

cette division est chargée principalement du :

– Recyclage et la mise à niveau du personnel des différentes structures de la Direction Régionale.

1.4 Présentation de la structure concernée par l'étude "Division Informatique"

La division informatique au sein de l'entreprise a pour rôle principal d'assurer la coordination de l'activité informatique au niveau de la direction régionale et des autres régions.

1.4.1 Organigramme de la "Division Informatique"

La division informatique rassemble une trentaine de personnes qui se chargent d'accomplir les différentes tâches à exercer afin d'assurer le bon fonctionnement de cette division. Nous allons à présent, illustrer l'organigramme associé à la division informatique, afin de prendre connaissance des divers services et activités qui y contribuent.

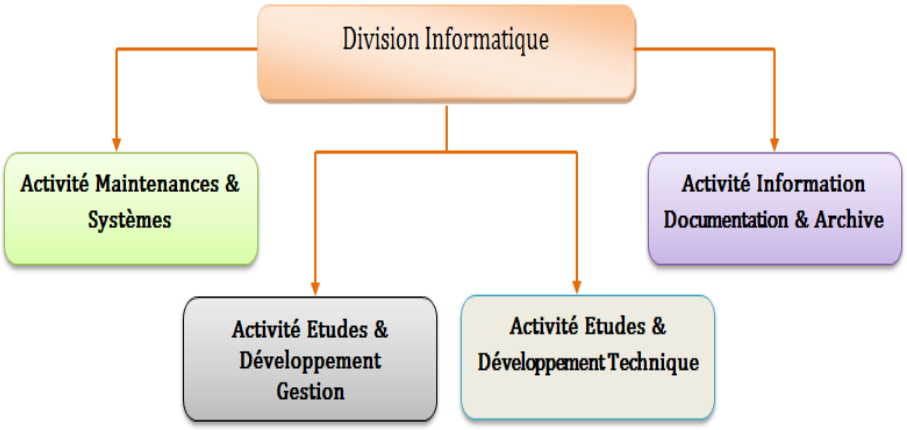


FIGURE 1.2 – Organigramme de la "Division Informatique"

1.4.2 Description et rôle du centre informatique

La Division Informatique participe en grande partie à l'élaboration de logiciels destinés aux différentes structures pour l'amélioration des systèmes et procédures de gestion. Ces applications (logiciels) sont :

- CHAMPS (Gestion de La Maintenance Assistée par Ordinateur).
- SGRH (Système de Gestion des Ressources Humaines).
- SGS (Système de Gestion des Stocks).
- SGF (Système de Gestion des Finances).

La division est munie du matériel suivant :

1. Equipement DIGITAL :
   - (02) DEC 4000 destinés à l'exploitation de l'application Champs.
   - (01) DEC 3000 destiné au développement.
   - (01) Micro Vax destiné à la messagerie électronique.
2. Station MX 300 travaillant sous unix.
3. Micro-ordinateurs destinés au développement bureautique.

4. Imprimantes (laser et matricielles).
5. Scanner.

Un réseau local est mis en place au niveau de la direction régionale, qui est de type ETHERNET. Ce réseau local relie cinq sites principaux :

- Base Irara.
- Base 24 février.
- CINA.
- CIS.
- El-Gassi.

1.5 Définition de l'architecture réseau et système

Afin de régir des activités informatiques collectives et centraliser ou répartir les ressources et les tâches à travers le système, SONATRACH DP dispose d'un ensemble d'équipements matériels et logiciels organisés fonctionnant en réseaux interconnectés, formant ainsi une infrastructure réseau et une infrastructure système, illustrées par les schémas suivants :

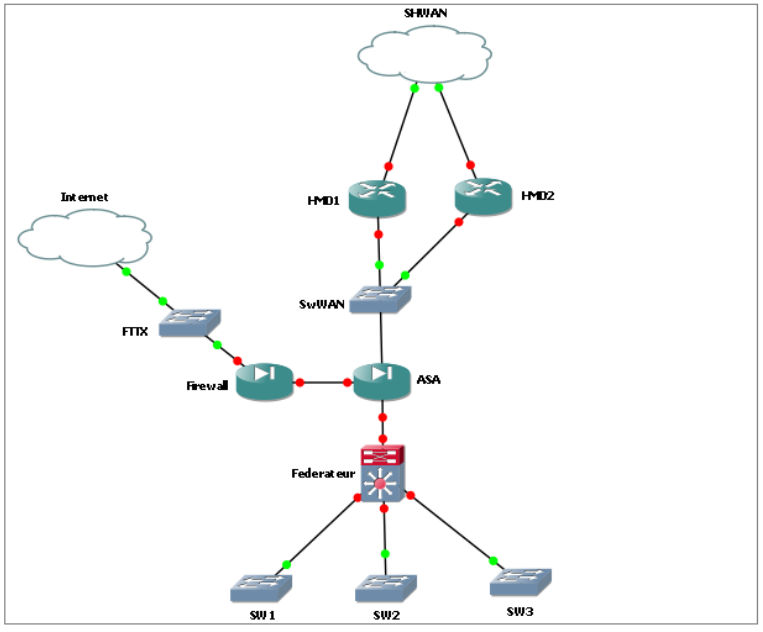


FIGURE 1.3 – Schéma simplifié de l'infrastructure réseau.

Pour offrir une meilleure conception et configuration matérielle et logicielle, SONATRACH DP dispose d'une infrastructure système illustrée dans la figure ci-dessous :

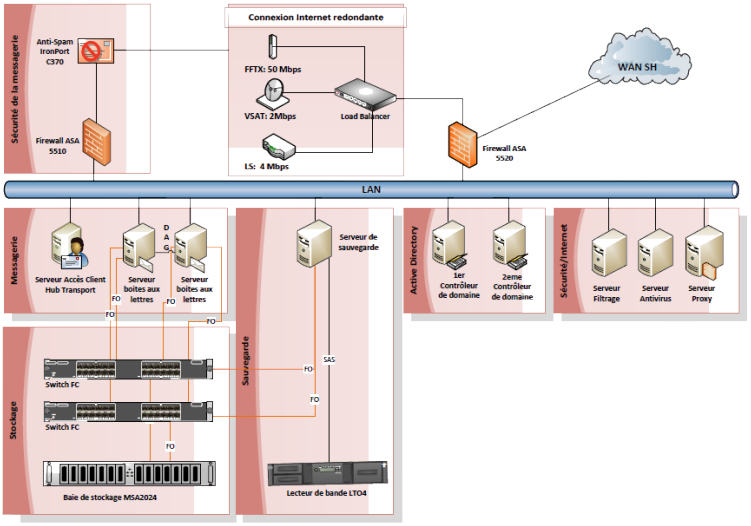


FIGURE 1.4 – Schéma simplifié de l'infrastructure système.

1.5.1 Présentation des équipements réseaux

Cette partie consiste à définir les différents équipements réseaux utilisés au sein de l'entreprise " Division Production ", nous distinguons ainsi deux sections diverses associées aux matériels :

- **Eléments actifs :** regroupe les équipements d'interconnexion et de sécurité du réseau de l'entreprise, on cite parmi eux : Les commutateurs, les routeurs, les pare-feu, les VPN, les modems...

- **Eléments passifs :** regroupe quant à eux les différents types de câbles utilisé pour interconnecter les équipements réseau de l'entreprise, on cite parmi eux : la fibre optique, les câbles UTP, STP, etc.

1.5.1.1 Eléments actifs

Nous présenterons dans ce qui suit les équipements qui constituent l'actif du réseau de l'entreprise sous ses différents aspects :

a) **Aspect réseau**

– **La gamme Catalyst Cisco 3750 :** La gamme Cisco Catalyst 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée, disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de

construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel [1].

– **La gamme Catalyst Cisco 6500 :**La gramme Catalyst6500 Cisco établit un nouveau standard pour les communications IP et la distribution d'applications sur les réseaux de campus d'entreprise et de fournisseurs de services. Premier commutateur modulaire multicouche intelligent de Cisco, la gamme Catalyst 6500 fournit des services sécurisés intégrés de bout en bout du local technique au cœur du réseau, au centre de données et à l'extrémité WAN [2].

Maintenant que l'on a décrit les différentes gammes Cisco Catalyst associées aux commutateurs qui existent au sein de la SONATRACH, nous allons indiquer ci dessous, la classification des commutateurs selon leurs rôles.

- **Commutateur d'accès :** un commutateur d'accès à pour rôle principal de fournir un moyen de connecter des périphériques au réseau, ainsi que de contrôler les périphériques qui sont autorisés à communiquer sur le réseau.

- **Commutateur de distribution :** un commutateur de distribution regroupe les données reçues à partir des commutateurs de couche d'accès, avant qu'elles ne soient transmises vers la couche cœur de réseau, en vue de leur routage vers la destination finale.

- **Commutateur cœur de réseau "fédérateur" :** un commutateur fédérateur est essentiel à l'inter-connectivité entre les périphériques de la couche de distribution. Il a aussi la capacité de regrouper le trafic de quantités importantes provenant de tous les périphériques de couche de distribution afin de le réacheminer rapidement vers la destination [8].

– **La gamme Cisco 7200 :** le routeur de gamme "7200" offre une performance et évolutivité accentue avec un large éventail d'options de déploiement avec des vitesses de traitement allant jusqu'à 400 000 de paquets par seconde [3].

b) **Aspect système :** L'infrastructure système de l'entreprise dispose d'un ensemble de serveurs définis ci-dessous :

– **Contrôleur de domaine "Active Directory" :** Active Directory est le premier service d'annuaire d'entreprise évolutif qui, représente alors la base idéale à long terme pour le partage des informations de l'entreprise et la gestion commune des ressources réseau, parmi lesquelles des applications, des systèmes d'exploitation réseau et des services liés à l'annuaire [4].

– **Serveur de messagerie "Microsoft Exchange" :** Il s'agit d'une application de serveur

de messagerie collaborative. Son rôle initial est le stockage de courrier électronique. Son utilisation est étendue au calendrier, aux listes de tâches, à la gestion des contacts et bien d'autres données qui sont partagées entre les utilisateurs [5].

c) **Aspect sécurité**

- **La gamme Cisco ASA 5500**(Adaptive Security Appliance) : Les Serveurs de Sécurité Adaptatifs Cisco+ ASA 5500 combinent les meilleurs services de VPN et de sécurité, pour constituer une solution de sécurité spécifique. Cisco ASA 5500 permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible [6].

L'entreprise SONATRACH "DP" utilise les différents équipements de sécurité associés à la gamme Cisco ASA 5500 qui répondent aux besoins de sécurité du réseau de l'entreprise, ces équipements sont illustrés ci-dessous :

- **Pare-feu ASA 5520 :** Le firewall Cisco ASA, assure une protection optimale, grâce à de nombreuses fonctionnalités qui sont : le contrôle d'applications, la protection en temps réel contre les attaques des applications DOS, détection et filtrage de l'activité réseau des vers et des virus, détection des spywares, l'inspection avancée des protocoles voix, les signatures IPs spécifiques, services IPSec et SSL protégés, services SSL avec client ou avec portail [6].

- **VPN IPsec/SSL :** La solution Cisco ASA série 5500 VPN Edition permet aux entreprises de profiter des avantages d'Internet en termes de connectivité et de coût, sans compromettre l'intégrité des règles de sécurité d'entreprise. En faisant converger les services Cisco WebVPN, composés des services VPN IPSec (IP Security) et SSL (Secure Sockets Layer), avec les technologies complètes de défense contre les menaces, la gamme Cisco ASA série 5500 propose un VPN totalement sécurisé avec une sécurité complète au niveau du réseau et du point d'extrémité [6].

- **Proxy "ISA Serveur" :** ISA Server est une passerelle de haute sécurité qui protège le réseau informatique d'une entreprise contre les menaces en provenance d'Internet, tout en offrant aux utilisateurs un accès à distance rapide et sécurisé aux données et aux applications [7].

- **Antivirus Symantec :** Symantec AntiVirus Corporate protège les ordinateurs contre les infections virales de toutes sortes qui se propagent à partir des disques durs, des disquettes et des pièces jointes à des courriers électroniques, et contre les virus transmis sur les réseaux. Symantec réagit à la présence de fichiers infectés en exécutant des opérations principales et secondaires. C'est pour ces raisons là, que l'entreprise SONTARACH "DP" à employé cet anti virus au sein de son réseau afin de renforcer et de prévenir toutes menaces voulant

affecter le fonctionnement du réseau de l'entreprise [8].

– **Serveur de filtrage "Websence Triton" :** websense est la solution de référence en matière de gestion de l'utilisation d'Internet par les employés, chargé du filtrage de sites. Elle protège les entreprises et les employés utilisant Internet des nouvelles menaces émergentes telles que les logiciels espions et les codes malveillants [9].

– **Serveur Cisco NAC :** c'est un Serveur de Contrôle d'Admission Réseau (Network Admission Control) facile à déployer qui permet à l'administrateur réseau d'authentifier, d'autoriser, d'évaluer et de corriger les équipements filaires, sans fil et distants avant de donner à leurs utilisateurs un accès au réseau. Il détermine si les équipements en réseau : ordinateurs portables ou fixes, etc sont conformes aux politiques de sécurité de l'entreprise et répare les éventuelles vulnérabilités avant de leur permettre l'accès au réseau [10].

1.5.1.2 Eléments passifs

Dans cette partie nous sommes appelés à parler de deux types de câblage distincts : le câblage horizontal et le câblage vertical.

- **Le câblage horizontal :** ce type de câblage désigne les câbles qui connectent les armoires de répartition aux zones de travail. La longueur maximale d'un câble reliant un point de terminaison de l'armoire de répartition à la terminaison de la prise de la zone de travail ne doit pas dépasser 90 mètres. Cette distance de câblage horizontal maximale est appelée liaison permanente car elle est installée dans la structure même du bâtiment. Le support horizontal chemine entre un tableau de connexions de l'armoire de répartition et une prise téléphonique murale dans chaque zone de travail. Les connexions aux périphériques sont effectuées au moyen de cordons de raccordement [11].

- **Le câblage vertical :** Le câblage vertical désigne le câblage utilisé pour connecter les armoires de répartition aux salles d'équipements, dans lesquelles se trouvent souvent les serveurs. Le câblage vertical interconnecte également plusieurs armoires de répartition dans l'ensemble du bâtiment. Ces câbles sont parfois acheminés en dehors du bâtiment vers la connexion du réseau étendu ou le FAI.

  Le câblage vertical est utilisé pour le trafic agrégé comme le trafic en direction et en provenance d'Internet et l'accès aux ressources de l'entreprise sur un site distant. Une grande partie du trafic provenant des différentes zones de travail utilise le câblage vertical pour accéder aux ressources en dehors de la zone ou du bâtiment. Par conséquent, les câbles verticaux nécessitent généralement un support de bande passante important [11].

  Afin de distinguer clairement l'emploi du câblage horizontal par rapport au vertical, nous avons ci-dessous une figure qui récapitule ce que l'on a cité précédemment.

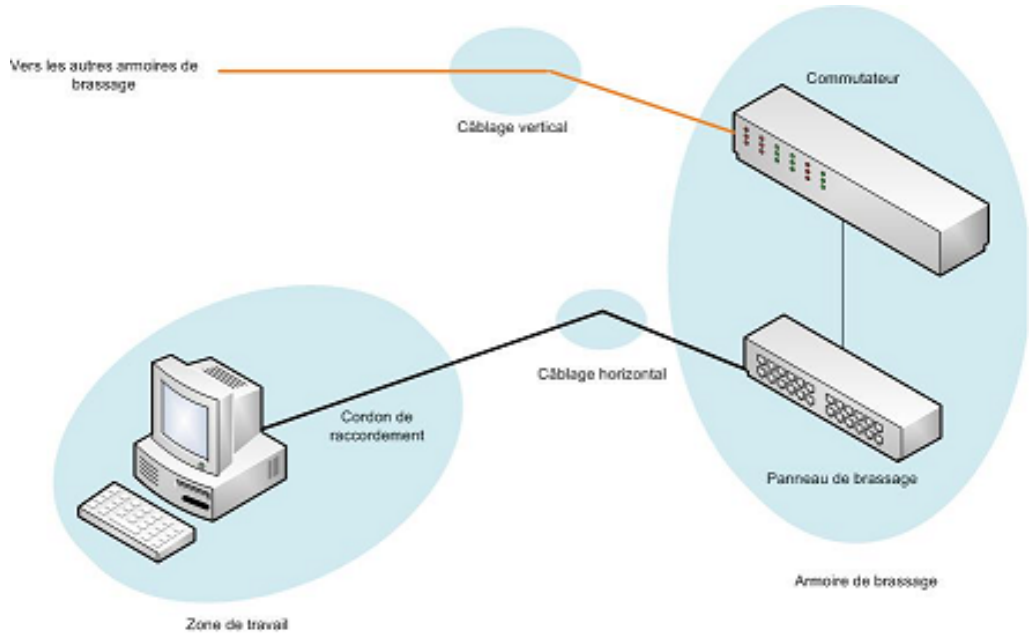


FIGURE 1.5 – Zones de câblage de réseau local

1.5.2 Définition des différents types de support

La sélection de câbles nécessaires à l'établissement correct d'une connexion de réseau local ou de réseau étendu implique de prendre en compte différents types de supports. Il existe différentes implémentations de couche physique qui prennent en charge plusieurs types de supports, à savoir : les câble en cuivre, la fibre optique, le Sans fil.
Le choix d'un support de transmission dépend de certains facteurs qui sont les suivants :
– Le cout ;
– La résistance aux perturbations électromagnétique ou radioélectriques potentielles ;
– La facilité d'installation et de maintenance ;
– La bande passante ;
– La portée du câble [11].

1.5.2.1 Supports de transmission de données

Le support le plus souvent utilisé pour les communications de données est le câblage qui utilise des fils de cuivre pour la transmission de bits de données et de contrôle entre les périphériques réseau. Le câblage employé pour les communications de données se compose généralement d'une série de fils de cuivre individuels formant des circuits dédiés à des fins de signalisation spécifiques [11].
a) **Support en cuivre**

- **Le câble coaxial :** La conception du câble coaxial a été adaptée à différentes fins. Le câble coaxial est un type couramment utilisé dans les technologies sans fil et d'accès par câble. Il permet de relier des antennes à des périphériques sans fil et de transporte de

l'énergie en radiofréquence (RF) entre les antennes et le matériel radio [11].

- **Câble à paires torsadées :** on distingue deux catégories associées à ce premier [11] :
  - **Câble "UTP" :** Le câblage UTP, terminé par des connecteurs RJ-45, est un support en cuivre courant pour l'interconnexion de périphériques réseau. Les principaux types de câbles obtenus en utilisant des conventions de câblage spécifiques sont les suivants : Ethernet direct, Croisement Ethernet, Renversement. Les catégories de câbles UTP utilisé par SONATRACH sont de 3, 4, 5, 5e, 6, 6a et 7.
  - **Câble à paire torsadées blindées "STP" :** la norme STP utilise deux paires de fils enveloppées dans un revêtement tressé, afin d'offrir une meilleure protection parasitaire que le câblage UTP, mais à un prix relativement plus élevé.

b) **La fibre optique :** Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre optique prend en charge des débits de bande passante de données brutes très élevés, l'inconvénient réside seulement dans le cout élevé de la fibre optique ainsi que sa manipulation qui est délicate et qui demande plus de compétences et de maitrise [11].

Les types de fibre optique utilisées au sein de l'entreprise SONATRACH "DP" sont :

- **La fibre optique monomode**"OS1" et "OS2" : les fibres "OS" sont classées selon leur atténuation maximum :1.0dB/km pour OS1 et 0.4dB/km pour OS2.

- **La fibre optique multi modes**"OM1", "OM2", "OM3", "OM4" : les fibres multi modes "OM" sont classées selon leurs bandes passantes, avec une bande passante allant de 200MHz/Km pour l'OM1 à 3500 MHz/km pour l'OM4.

c) **Sans fil :** technologie qui utilise les ondes radio pour la transmission des données au sein de l'entreprise [11].

1.5.3 Autres équipements réseaux

Armoire de brassage : une armoire de brassage appelée aussi "baie de brassage" est conçue pour héberger et protéger les différents équipements et composants du système de câblage du réseau informatique.
Le choix d'une baie de brassage informatique s'effectue après avoir déterminé les équipements à intégrer (nombre de panneaux de brassage, commutateur Ethernet...), ceux-ci sont standardisés : en largeur la norme 19 "482,6 mm" est le seul système accepté et utilisé dans le monde entier, la hauteur quant à elle s'exprime en "U" tel qu'un U = 44,45mm. Il suffit donc d'additionner les hauteurs en U de chaque élément à intégrer pour déterminer l'armoire de brassage selon les besoins spécifiques [50].

Au niveau de la SONATRACH "DP" le nombre maximal de "U" dans une armoire de brassage est de "9".

1.6 Conclusion

Les réseaux sont devenus un pilier de l'économie mondiale. Les besoins et les enjeux de ces technologies ne cessant d'augmenter à engendrer l'évolution de la sécurité informatique, afin d'apporter une garantie de fiabilité et de sureté.
A présent, nous avons pris connaissance de l'architecture réseau associée à l'entreprise SONATRACH "Division Production".

Dans le chapitre qui suit nous allons présenter les différents concepts liés à la sécurité et les politiques de sécurité, nous aborderons par la suite les attaques essentielles qui peuvent dégrader le fonctionnement d'un réseau ainsi que les différentes contre-mesures pour y remédier.

CHAPITRE 2

ATTAQUES ET POLITIQUE DE SÉCURITÉ

2.1 Introduction

La sécurité du transport de l'information est une préoccupation primordiale dans le domaine des réseaux. Pendant de longues années, la sécurité d'un équipement demandait une isolation complète de l'environnement extérieur, et aucune communication avec une machine externe n'était possible. Avec la généralisation d'Internet et des moyens de communication modernes, une nouvelle forme d'insécurité s'est répandue, qui s'appuie sur l'utilisation de codes informatiques pour perturber ou pénétrer les réseaux et les systèmes qui les composent.

Au cours de ce chapitre, nous abordons principalement les différents aspects liés à la sécurité des réseaux informatiques. C'est pourquoi nous définissons dans un premier temps le concept d'une politique de sécurité, puis dans un second temps nous analysons ce que nous appelons "l'anatomie d'une attaque" ainsi que les différentes attaques existantes, enfin nous présentons les différentes parades qui peuvent faire face à ces attaques.

2.2 Notions de politique de sécurité

Compte tenu de la nouvelle importance accordée à la sécurité et à la manière stratégique et globale de l'appréhender, une politique de sécurité, devient l'expression de la stratégie sécuritaire des organisations. Elle constitue pour les organisations un outil indispensable non seulement à la gouvernance de la sécurité mais aussi à la réalisation du plan stratégique de sécurité.

2.2.1 définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Elle s'occupe de la prévention d'actions non autorisées par les utilisateurs d'un système informatique, afin d'assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information traitée [12].

2.2.2 Définition d'une politique de sécurité

Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Elle spécifie les moyens (ressources, procédures, outils) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité [13].
Elle découle des grands principes de sécurité qui permettent de protéger le système d'information en évitant qu'il ne devienne une cible d'attaques [14].

2.2.3 Objectifs d'une politique de sécurité

Quelle que soit la nature des biens produits par l'entreprise, sa politique de sécurité réseau vise à satisfaire les critères suivants :

- **Authentification :** L'authentification a pour objectif de vérifier l'identité des processus communicants. Plusieurs solutions simples sont mises en oeuvre pour cela, comme l'utilisation d'un identifiant et d'un mot de passe.

- **Autorisation :** Information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié et autorisé a accès, ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise.

- **Confidentialité :** Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer leur confidentialité des données.

- **Intégrité :** Ensemble des mécanismes garantissant qu'une information n'a pas été modifiée par une personne non autorisée.

- **Disponibilité :** Ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.

- **Non-répudiation :** Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

- **Traçabilité :** Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure.

2.3 Les différents types d'attaques

L'informatique étant un domaine très vaste, le nombre de vulnérabilités présentes sur un système peut donc être important. Ainsi, les attaques visant ces failles peuvent être à la fois très variées et très dangereuses.
Le nombre d'attaques possibles est bien trop grand pour que nous puissions les citer toutes. De plus, de nouvelles procédures d'attaques s'inventent chaque jour, pour cela nous avons choisi de présenter quelques-unes [15].

2.3.1 Anatomie d'une attaque

Fréquemment appelés "les 5P" dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique : *Probe, Penetrate, Persist, Propagate, Paralyze* [15].

- ***Probe :*** consiste en la collecte d'informations par le biais d'outils comme whois, Arin, DNS lookup. La collecte d'informations sur le système cible peut s'effectuer de plusieurs manières, comme un scan de ports grâce au programme Nmap ou encore un scan de vulnérabilités à l'aide du programme Nessus.

- ***Penetrate :*** consiste en l'utilisation des informations récoltées pour pénétrer un réseau. Des techniques comme le brute force ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe.

- ***Persist :*** consiste en la création d'un compte avec des droits de super utilisateur pour pouvoir se ré-infiltrer ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot tel que les chevaux de Troie.

- ***Propagate :*** cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.

- ***Paralyze :*** cette étape peut consister en plusieurs actions. Le pirate peut utiliser un serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation.

Après ces cinq étapes, le pirate peut éventuellement tenter d'effacer ses traces, bien que cela ne soit rarement utile. En effet, les administrateurs réseaux sont souvent surchargés de logs à analyser. De plus, il est très difficile de supprimer entièrement des traces.

2.3.2 Les attaques réseaux

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation. Nous présenterons dans ce qui suit quelques attaques bien connues.

2.3.2.1 Les techniques de scan

Le scan de ports est une méthode pour déterminer le type d'attaque que l'on peut lancer sur une machine ciblé. Cette technique consiste à rapporter des informations sur les machines scannées, et en particulier le système d'exploitation et les services installés. On peut donc déterminer avec précision les failles de sécurités et donc les types d'attaques possibles sur la machine en question.
Les outils de scan sont généralement développés par des personnes très pointues techniquement, et ne seraient donc exploitables que par une certaine catégorie de personnes. Une fois une machine scannée, elle peut être sujette à des futures failles de sécurité non connues à ce jour puisque ces outils rapportent les différents logiciels installés sur les cibles. Ce type de détection de failles est donc effectué à grande échelle et toute machine disposant d'une adresse IP fixe peut être scannée et par la suite attaquée. Mais, aujourd'hui, avec l'expansion des solutions de hauts débits pour l'accès à Internet, les ordinateurs qui ne disposent pas d'adresse IP fixe sont concernés, car ils restent souvent connectés sans être utilisé, et quelques minutes suffisent pour trouver des dizaines de failles de sécurité.La plupart des attaques sont précédées par un scan de ports lors de la phase Probe, qui est comme nous l'avons vue, la première phase des 5Ps dans le déroulement d'une attaque [15].

2.3.2.2 IP Spoofing

L'usurpation d'une adresse IP d'une machine est utilisé pour cacher sa véritable identité, et donc de se faire passer pour quelqu'un autre, le plus souvent une machine de confiance du réseau attaqué.
Le principe de cette attaque consiste en la création des paquets IP en modifiant l'adresse IP Source. Cependant, d'autres mécanismes doivent être mis en place, sinon la réponse au paquet ne retournera pas à son émetteur, du fait de la falsification de l'adresse IP. De ce fait la réponse est retournée à la machine "spoofée".
Cette technique peut être utile dans le cas d'authentification basée sur une adresse IP. Pour ce faire, il existe des utilitaires qui permettent de modifier les paquets IP ou de créer ses propres paquets tel que "hping2". Grâce à ces utilitaires, il est possible de spécifier une adresse IP différente de celle que l'on possède, et ainsi se faire passer pour une autre machine [15].

2.3.2.3 ARP Spoofing

Le but de cette attaque est de rediriger le trafic d'une machine vers une autre. Grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate

peut rerouter les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien. La finalité est la même que l'IP spoofing mais celle-ci se déroule au niveau de la couche liaison de données. Pour effectuer cette usurpation, il faut corrompre le cache ARP de la victime. Ce qui signifie qu'il faut lui envoyer des trames ARP en lui indiquant que l'adresse IP d'une autre machine est la sienne [15].

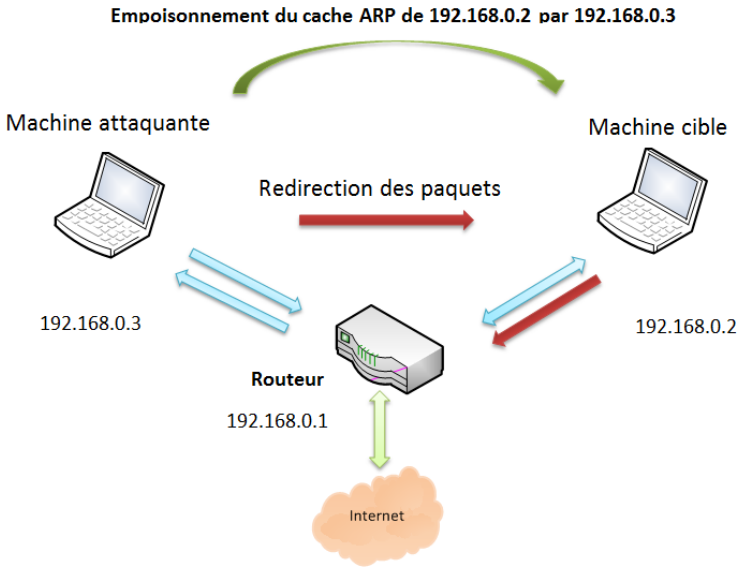


FIGURE 2.1 – Attaque ARP spoofing

2.3.2.4 Attaques DHCP spoofing

Une des possibilités pour une personne malveillante d'accéder au trafic réseau est de s'approprier les réponses envoyées par un serveur DHCP autorisé sur le réseau. Le périphérique de mystification DHCP répond aux requêtes DHCP clientes. Le serveur légitime peut lui aussi répondre, mais si le périphérique de mystification agit sur le même segment que le client, sa réponse au client peut parvenir en premier. La réponse DHCP du pirate fournit des informations de prise en charge et une adresse IP qui le désignent comme passerelle par défaut ou serveur DNS (Domain Name System). S'il s'agit d'une passerelle, les clients transmettent alors les paquets au périphérique " attaquant " qui, à son tour, les transmet vers la destination voulue. Nous parlons alors d'attaque de l'intercepteur. Ce type d'attaque peut passer complètement inaperçu puisque le pirate intercepte le flux de données sur le réseau. [16].
Cette attaque est illustrée dans la figure suivante :

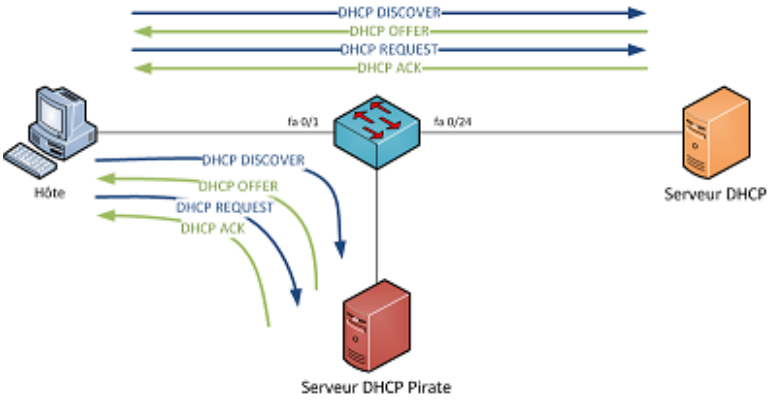


FIGURE 2.2 – Attaques DHCP spoofing

2.3.2.5 DNS Spoofing

Le but de cette attaque est de fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine afin de rediriger, à leur insu, des internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer ses informations en toute confiance tel que les identifiants. Il existe deux techniques pour effectuer cette attaque [15].

- **DNS cache poisoning :** Les serveurs DNS possèdent un cache permettant de garder pendant un certain temps la correspondance entre un nom de machine et son adresse IP. Le DNS Cache Poisoning consiste à corrompre ce cache avec de fausses informations. Ces fausses informations sont envoyées lors d'une réponse d'un serveur DNS contrôlé par le pirate à un autre serveur DNS, lors de la demande de l'adresse IP d'un domaine. Le cache du serveur ayant demandé les informations sera alors corrompu.
- **DNS ID Spoofing :** Pour communiquer avec une machine, nous devons disposer de son adresse IP. Nous pouvons toutefois avoir son nom, et grâce au protocole DNS, nous pouvons obtenir son adresse IP. Lors d'une requête pour obtenir l'adresse IP à partir d'un nom, un numéro d'identification est placé dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste à récupérer ce numéro d'identification (en sniffant le réseau) lors de la communication entre un client et un serveur DNS, puis, envoyer des réponses falsifiées au client avant la réponse du serveur DNS légitime.

2.3.2.6 Fragments attacks

Le but de cette attaque est de passer outre les protections des équipements de filtrage IP. Dans ce cas un pirate peut s'infiltrer dans un réseau pour effectuer des attaques ou récupérer des informations confidentielles. Deux types d'attaque sur les fragments IP peuvent être distingués [15].

- **Fragments overlapping :** Quand un message est émis sur un réseau, il est fragmenté en plusieurs paquets IP. Afin de pouvoir reconstruire le message, chaque paquet possède un

offset. Le but de l'attaque est de réaliser une demande de connexion et de faire chevaucher des paquets en spécifiant des offsets incorrects. La plupart des filtres analysant les paquets indépendamment ne détectent pas l'attaque. Cependant, lors de la défragmentation, la demande de connexion sera établie.

– **Tiny fragments :** Le but de cette attaque est de fragmenter une demande de connexion sur deux paquets IP : le premier paquet de taille minimum (68 octets selon la RFC du protocole IP) ne contient que l'adresse et le port de destination. Le deuxième paquet, quant à lui, contient la demande effective de connexion TCP. Le premier paquet est accepté par les filtres puisqu'il ne contient rien de suspect. Quand le deuxième paquet arrive, certains filtres ne le vérifient pas pensant que si le premier paquet est inoffensif, le deuxième l'est aussi. Mais lors de la défragmentation sur le système d'exploitation, la connexion sera établie. De nos jours, une grande majorité des firewalls sont capables de détecter et de stopper ce type d'attaque.

2.3.2.7 Attaque Mac Flooding

Flooding signifie à peu de choses près inondation. Cette attaque bien connue consiste à saturer la table MAC(Media Acces Control) du commutateur en lui envoyant plusieurs milliers d'entrées.
L'inondation MAC est réalisable au moyen d'un outil d'attaque réseau, Le pirate l'utilise sur le réseau pour inonder le commutateur d'un nombre important d'adresses jusqu'à ce que la table d'adresses se remplisse. Une fois cette table remplie, le commutateur inonde tous les ports avec le trafic entrant parce qu'il ne parvient pas à identifier le numéro de port d'une adresse MAC en particulier dans la table d'adresses. De par sa conception, le commutateur dans ce cas agit en tant que concentrateur [17].

2.3.3 Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, comme précédemment, il est possible de classifier ces attaques selon leur provenance [15].

2.3.3.1 Les problèmes de configuration

Il est très rare que les administrateurs réseaux configurent correctement un programme. En général, ils se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. D'autant plus, des erreurs peuvent apparaître lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants ou mettant en jeu l'intégrité du système d'exploitation [15].

2.3.3.2 Les buffer overflows

Les buffer overflows ou dépassement de la pile sont une catégorie de bug particulière issus d'une erreur de programmation, ils permettent l'exploitation d'un shellcode à distance. Ce shellcode permettra à une personne mal intentionnée d'exécuter des commandes sur le système distant, pouvant aller jusqu'à sa destruction. L'erreur de programmation est souvent la même : la taille d'une entrée n'est pas vérifiée, celle-ci est directement copiée dans un buffer dont la taille est inférieure à la taille de l'entrée. Ceci engendre un débordement et l'exploitant peut ainsi accéder à la mémoire [15].

2.3.3.3 Les injections SQL

Les injections SQL profitent des paramètres d'entrée non vérifiés. Comme leur nom l'indique, le but des injections SQL est d'injecter du code SQL dans une requête de base de données, ainsi, il est possible de récupérer des informations se trouvant dans une base de données ou encore de détruire des données [15].

2.3.3.4 Man in the middle

L'un des actes de piratage les plus sophistiqués qu'un utilisateur non autorisé puisse commettre est celui que l'on appelle l'attaque de l'intercepteur (Man-in-the-Middle). C'est une attaque qui a pour but de récupérer des données sensibles qui transitent sur le réseau local. Cette attaque fait intervenir trois machines : un serveur cible, un poste client et la machine où se trouve l'attaquant.
L'objectif de cette attaque est d'intercepter les communications par la machine de l'attaquant entre le serveur cible et le poste client, sans que les entités concernées ne puisse se douter de la compromission du canal de communication [18].

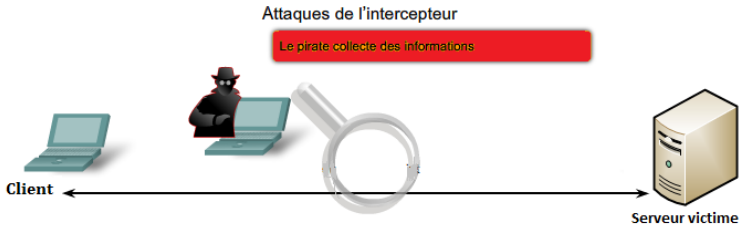


FIGURE 2.3 – Man in the middle

2.3.4 Le Déni de service

Le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières : par le biais d'une surcharge réseau rendant ainsi la machine totalement injoignable ou bien de manière applicative en crashant l'application à distance. L'utilisation

d'un buffer overflow peut permettre de planter l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie, etc.) voire un système complet. Nous présenterons dans ce qui suit quelques attaques réseaux connues permettant de rendre indisponible un service [15].

2.3.4.1 SYN Flooding

Exploite la connexion en trois phases de TCP (Three Way Handshake : SYN / SYN-ACK / ACK). Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit les SYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire, ce qui va entraîner une saturation et l'effondrement du système [15].

2.3.4.2 UDP Flooding

Le but de cette attaque consiste à envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP [15].

2.3.4.3 Smurfling

Dans ce cas le pirate fait des requêtes ICMP ECHO à des adresses de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible). La machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante [15].

2.3.4.4 Déni de service distribué

Le but de cette attaque consiste à reproduire une attaque normale à grande échelle. Pour ce faire, le pirate va tenter de se rendre maître d'un nombre important de machines. Grâce à des failles (buffer overflows, failles RPC, etc) il va pouvoir prendre le contrôle de machines à distance et ainsi pouvoir les commander à sa guise. Une fois ceci effectué, il ne reste qu'à donner l'ordre d'attaquer à toutes les machines en même temps, de manière à ce que l'attaque soit reproduite à des milliers d'exemplaires. Ainsi, une simple attaque comme un SYN Flooding pourra rendre une machine ou un réseau totalement inaccessible [15].

2.3.5 Les virus

Un virus informatique est un programme, généralement de petite taille, doté d'un ensemble de propriétés, qui sont : infection, multiplication, possession d'une fonction nocive.
La fonction d'infection permet au virus de s'introduire dans des fichiers de programmes, dans des fichiers de données utilisant un langage de script, ou dans une partie de la disquette ou du disque dur contenant un petit programme (secteur de démarrage). Lors de l'accès à ces

programmes ou secteur, le code du virus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infectera d'autres fichiers), puis visible (activation de la fonction nocive).
La fonction nocive pourra être déclenchée par des facteurs très variables selon le virus (au bout de n réplications, à une date fixe, lors de l'exécution de certaines tâches précises). Elle peut se limiter à l'affichage d'un message désagréable ou, plus généralement, conduire à des perturbations graves de l'ordinateur (ralentissement du fonctionnement, effacement ou corruption de fichiers, formatage du disque dur, etc.). Les virus sont donc des programmes parasites qui doivent être hébergés dans d'autres fichiers [46].

2.3.6 Les chevaux de Troie

Un cheval de Troie (ou Trojan Horse) est un programme qui exécute des instructions sans l'autorisation de l'utilisateur, ces instructions sont généralement nuisibles à l'utilisateur.
Le Trojan prend l'apparence d'un programme valide, mais il contient en réalité une fonction illicite cachée, grâce à laquelle il contourne la sécurité informatique.
Il pénètre ainsi par effraction dans les fichiers de l'utilisateur pour les modifier, les consulter ou même les détruire. Le cheval de Troie contrairement au ver ne se réplique pas.
Il peut rester inoffensif pendant quelques jours, semaines ou mois et se mettre en action à la date programmée. Pour éviter d'être infecté par un Trojan il est conseillé d'utiliser un antivirus et un pare-feu [47].

2.3.7 Ingénierie sociale

L'ingénierie sociale ou Social Engineering est une méthode d'espionnage répandue visant à obtenir l'accès à des données confidentielles. La cible de l'attaque est toujours la personne humaine. Pour soutirer des informations confidentielles, les arnaqueurs exploitent très souvent la bonne foi, la serviabilité, mais aussi l'insécurité des personnes. Que ce soit par téléphone, en se faisant passer pour quelqu'un d'autre, ou par Internet (attaques par hameçonnage), ils sont prêts à tout pour obtenir ce qu'ils veulent [52].

2.4 les techniques de parade aux attaques

la prise en compte des contraintes de sécurité pour faire face aux différentes attaques qui peuvent perturber ou pénétrer un réseau est une démarche capitale et primordiale pour le bon fonctionnement d'une entreprise.
Nous présentons dans ce qui suit quelques contre-mesures qui permettent de contrer les différentes attaques qui peuvent menacer un réseau.

2.4.1 Contrôle des connexions réseau avec les pare-feu

Tout accès à un réseau externe au réseau d'entreprise doit faire l'objet d'un contrôle d'accès afin de ne laisser passer que le trafic autorisé.
Le filtrage du trafic entrant et sortant du réseau d'entreprise réduit tout d'abord l'éventail des attaques possibles aux seuls services autorisés à transiter sur le réseau. D'autant plus, suivant le niveau de granularité du contrôle de filtrage mis en place, on peut se prémunir contre les attaques de type déni de service, spoofing, ainsi que contre les attaques applicatives.
Le pare-feu est le système qui a en charge de mettre en œuvre une politique de filtrage des protocoles réseau, il est l'élément de sécurité indispensable à la mise en œuvre d'une politique de sécurité. Il permet aussi de créer un périmètre de sécurité entre le réseau intranet de l'entreprise et le réseau Internet.
Une architecture à base de pare-feu offre l'avantage de concentrer les efforts de sécurité sur un unique point d'entrée. Grâce à des mécanismes de filtrage en profondeur ainsi qu'à des fonctions de journalisation des événements, les pare-feu sont en outre des éléments cruciaux pour les investigations de sécurité [14].

2.4.2 Contrôle des connexions réseau avec Les N-IPS

Les N-IPS (Network Intrusion Prevention System) incarnent une nouvelle génération d'équipements réseau qui combine les fonctionnalités des IDS (Intrusion Detection System) et celles des pare-feu. Ils présentent au minimum deux interfaces réseau (entrante et sortante) et se positionnent en passerelle/coupure de niveau 2 OSI du trafic réseau.
Bien qu'un N-IPS reste invisible pour le trafic IP, le trafic réseau est analysé en son sein afin de contrôler les données et de détecter des attaques potentielles.
Un N-PIS peut agir directement sur le trafic lors de la détection d'un trafic malicieux en agissant en coupure sur ce trafic. Cela permet de réduire la propagation de l'attaque au plus vite. L'objectif de tels équipements est ainsi d'offrir des contre-mesures en temps réel [14].

2.4.3 Contrôle d'accès au réseau avec le NAC

Cisco a annoncé une nouvelle initiative pour se connecter à un réseau. Appelée NAC(Network Access Control), elle permet de vérifier un certain nombre de points de sécurité avant d'autoriser un système à se connecter au réseau local.
Pour y parvenir, le système qui désire se connecter et le commutateur (ou le routeur) attaché au LAN doivent intégrer la fonctionnalité NAC.
Du point de vue de la sécurité, il est toujours recommandé de choisir la fonctionnalité NAC intégrée dans un commutateur, qui agit au niveau 2 OSI, plutôt que dans un routeur, lequel agit au niveau 3, pour la connexion physique au réseau. Un commutateur peut mettre en œuvre des mécanismes de sécurité de VLAN (Virtual Local Area Network), de contrôle des adresses MAC, qui sont moins permissifs que ceux d'un routeur, qui ne voit passer que des trames IP

[14].

2.4.4 Contrôle des attaques par déni de service

Les dénis de service exploitent généralement de fausses adresses IP sources afin de masquer l'origine des attaques. De telles adresses sont généralement choisies parmi les adresses IP dites réservées. Ces adresses doivent être filtrées par les opérateurs de télécommunications en périphérie de leurs réseaux afin de limiter leur exploitation à des fins de déni de service. Pour limiter les dénis de service, plusieurs mécanismes réseau sont disponibles, notamment l'URPF (Unicast Reverse Forwarding Protocol), qui permet de n'autoriser un trafic que si l'adresse source existe dans les tables de routage. Un autre mécanisme aussi s'avère efficace, il s'agit entre autre des puits de filtrage (sink hole) qui reçoivent et analysent tout le trafic et permettent dès lors de déterminer précisément les attaques à l'aide d'outils embarqués tel que Snort, Radware Defence Pro, etc [14].

2.4.5 Assurer l'authentification des connexions distante

Le laxisme qui entoure la gestion des secrets et des moyens d'authentification des accès distants a des répercutions de sécurité non négligeables sur l'entreprise. La plupart des accès distants se font à l'aide d'un ordinateur portable, qui ne contient généralement ni antivirus, ni pare-feu logiciel pour protéger les connexions des pirates qui scannent en permanence les plages d'adresses IP des opérateurs de télécommunications. De surcroît, des virus informatiques ont été spécialement développés pour rechercher sur des systèmes donnés tels que les PC(Personnal Computer) portables tous les secrets relatifs aux accès distants. L'authentification assure une protection contre toutes les attaques utilisant une usurpation d'identité, telles les attaques de type IP spoofing, les attaques visant à dérober les mots de passe, les attaques par cheval de Troie, dont l'objectif est d'offrir à l'attaquant un accès non authentifié ou dérobé [14].

2.4.6 Assurer la confidentialité des connexions

La confidentialité des informations transitant sur un réseau ne peut être assurée que par le chiffrement des données avant leur émission. Le réseau ne peut garantir par lui-même la confidentialité des données si elles ne sont pas chiffrées par un quelconque processus. Le chiffrement des données doit aussi avoir un sens, c'est pour cela qu'il doit se référer à une politique de classification des informations au sein de l'entreprise. Une telle classification a pour objectif d'établir clairement des niveaux de confidentialité des données et de définir les moyens à mettre en œuvre, ainsi que les listes de diffusion.
En s'appuyant sur cette politique de classification de l'information, le chiffrement applique aux données le niveau de confidentialité voulu au moyen d'algorithmes cryptographiques et de clés de chiffrement de longueurs adéquates.

La confidentialité des connexions permet de se prémunir d'un grand nombre d'attaques, parmi lesquelles : les attaques à l'aide de programmes d'écoute (sniffers), les attaques par virus, dont l'objectif est de copier tout fichier à caractère confidentiel, notamment les documents contenant le mot confidentiel ou les fichiers contenant les mots de passe de connexion à distance, etc.
Pour garantir une isolation des fonctions de sécurité d'un réseau, il est préférable de dédier le chiffrement des données à un équipement spécifique plutôt que d'ajouter une telle fonction à un routeur ou à un pare-feu [14].

2.5 Conclusion

Au terme de ce chapitre, nous avons fait le tour d'horizon sur les points les plus importants de la sécurité des réseaux informatiques, à savoir les notions de base d'une politique de sécurité ainsi que les différentes attaques pouvant corrompre le bon fonctionnement d'un réseau. Nous avons finis par présenter les différentes contre-mesures qui répondent le mieux aux besoins de sécurité.
Le chapitre qui suit sera consacré à la description détaillée de la démarche utilisée pour mener un audit de sécurité informatique.

CHAPITRE 3

AUDIT DE SÉCURITÉ ET APPLICATION DE LA MÉTHODE EBIOS

3.1 Introduction

L'audit a connu un développement important ces dernières années. Il est utilisé tant sur le plan interne qu'en externe, il est donc essentiel de savoir pourquoi et comment travaille l'auditeur afin de comprendre l'importance de son rôle.

Dans ce présent chapitre, nous définissons l'audit toute en illustrant ces diffèrent types, nous présentons aussi les principales normes d'audit de sécurité nécessaires pour la conduite d'une mission d'audit et sa démarche.

Nous introduisons par la suite les différentes méthodes et justifier nos choix quant à cet audit particulier. En fin , nous passons à la rédaction et au diagnostic du système d'information de la SONATRACH DP pour établir un plan d'action des différentes modifications et améliorations que nous envisageons.

3.2 Présentation d'un audit

L'audit est l'examen professionnel qui consiste en une expertise par un agent compétent et impartial et un jugement sur l'organisation, la procédure ou une opération quelconque d'une entité. L'audit est une amélioration continue, car il permet de faire le point sur l'existant (état des lieux) afin d'en dégager les points faibles et/ou non conformes (suivant les référentiels d'audit). Cela, afin de mener par la suite les actions adéquates qui permettront de corriger les écarts et disfonctionnements constatés [19].

3.2.1 Délimitation du besoin et des objectifs de l'audit

Selon l'Association Française de l'Audit et du conseil Informatique, les entreprises font appel à une procédure d'audit pour majoritairement s'assurer que les enjeux stratégiques de la direction sont correctement pris en considération à l'intérieur du système d'information de l'entreprise. En effet, l'audit permet avant tout de savoir si le système est perfectible, et dans quelles mesures, dans le but d'assurer l'adéquation du système informatique aux besoins de

l'entreprise.
Dans une période où la technologie va plus vite que l'innovation, et où la concurrence est féroce, il faut sans cesse prendre garde à ne pas être dépassé dans les moyens fonctionnels et technologiques mis en place. Cependant, chaque organisation a ses raisons qui la poussent à engager une procédure d'audit, l'important est de bien les cerner pour connaître ses objectifs. [20].

3.2.2 les principes de l'audit

Pour réaliser leur mission, les auditeurs doivent disposer d'une marge de manœuvre entière leur permettant de s'exprimer sur tout sujet ayant un impact négatif sur le fonctionnement, voire la survie de l'entreprise au regard des objectifs qu'elle s'est fixés.
Ceci nous conduit à présenter quelques principes fondamentaux [21] :

- **Le principe de la déontologie** : Il est le fondement même du professionnalisme. Ainsi ce principe suppose de l'auditeur la confiance, l'intégrité, la confidentialité et la discrétion qui en sont des éléments essentiels ;
- **Le principe de la présentation impartiale** : Ce principe oblige l'auditeur à mener sa mission d'une manière honnête et précise. C'est-à-dire que les constats d'audit, les conclusions des rapports d'audit devront refléter de manière honnête et précise les activités de l'auditeur. Les obstacles importants rencontrés pendant la mission d'audit et les questions non résolues ou les avis divergents entre l'équipe auditrice et auditée doivent aussi être consignés ;
- **Le principe de la conscience professionnelle** : Ce principe voudrait tout simplement rappeler qu'avec leurs compétences, les auditeurs agissent en accord avec l'importance des tâches qu'ils réalisent et la confiance que leur ont accordée le commanditaire de l'audit et les autres parties intéressées ;
- **Le principe de l'indépendance** : Ce principe est le fondement même de l'impartialité de l'audit et de l'objectivité des conclusions retenues dans un rapport d'audit. En respect de ce principe, les auditeurs doivent être indépendants de l'activité auditée et doivent avoir ni parti pris ni conflit d'intérêt. Ils doivent pour cela conserver un esprit objectif tout au long du processus d'audit et s'assurer que les constats et conclusions sont uniquement fondés sur les preuves d'audit ;
- **Le principe de l'approche fondée sur la preuve** : Ce principe constitue pour l'auditeur une méthode rationnelle pour parvenir à des conclusions fiables et reproductibles dans un processus d'audit systématique. Les preuves d'audit sont vérifiables et doivent s'appuyer sur des échantillons des informations disponibles, dans la mesure où un audit est réalisé avec une durée et des ressources délimitées.

3.2.3 Types d'audit existants

Du point de vu général, il existe deux types d'audit[22] :

- **Interne** :L'audit interne se base sur la tâche d'évaluation, de contrôle, de conformité et

de vérification. Il est exercé d'une façon permanente par une entreprise. Cet audit a pour mission de déceler les problèmes et de donner des solutions.

– **Externe** :L'audit externe est une opération volontaire décidée par la direction d'une entreprise pour faire apprécier la conformité de son système avec un référentiel, et ce par une firme d'audit tiers reconnu pour ses compétences et sa notoriété dans les secteurs d'activités concernés.

3.3 Présentation de l'audit de la sécurité informatique

Un audit informatique a pour objectif principal l'évaluation des risques associés aux activités informatiques, il permet également de s'assurer de l'adéquation du système informatique aux besoins de l'entreprise et de valider que le niveau de services est adapté aux activités de celles-ci. Un audit informatique est un diagnostic et un état des lieux extrêmement fin du système informatique de l'entreprise. Il est réalisé afin de définir des axes d'amélioration et d'obtenir des recommandations pour palier aux faiblesses constatées.

3.3.1 Intérêt et nécessité de l'audit

L'audit peut être envisagé à la suite de problèmes techniques, pour l'établissement d'une documentation dans le but d'évaluer les besoins en ressources en fonction de la tâche à effectuer. Mais il s'agit également souvent d'aider les entreprises à définir et à adopter un plan stratégique informatique. Ce plan identifiera les objectifs de l'entreprise à moyen terme et indiquera comment l'informatique peut aider à atteindre les objectifs posés [24].

3.3.2 Cycle de vie d'un audit de sécurité

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de vie qui est schématisé à l'aide de la figure 3.1 :
L'audit de sécurité informatique se présente essentiellement suivant deux parties comme le présente le schéma illustré dans la figure 3.1 :

– L'audit organisationnel et physique
– L'audit technique

Une troisième partie optionnelle peut être également considérée, il s'agit de l'audit intrusif "test d'intrusions". Enfin un rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de l'audit, il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées [24].

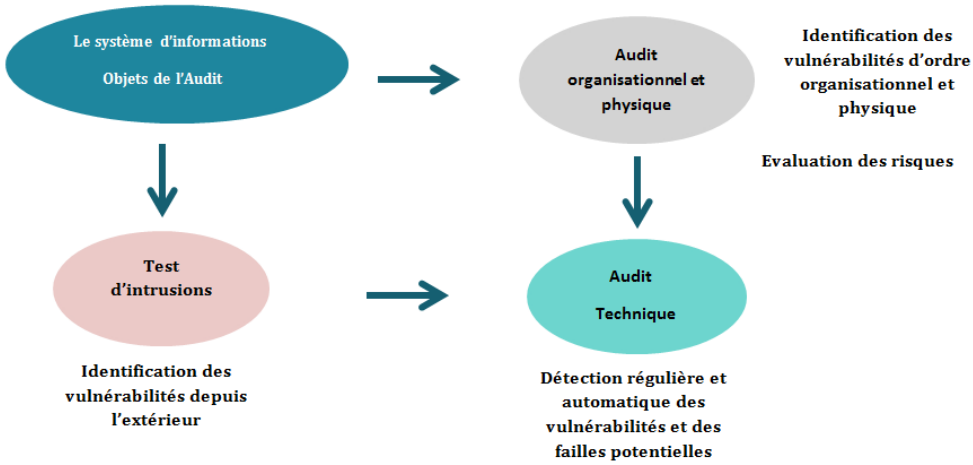


FIGURE 3.1 – cycle de vie d'audit de sécurité

3.4 les principales normes d'audit

3.4.1 Présentation de la famille ISO 27000

Issue des réflexions de groupes de travail internationaux dédiés au domaine de la sécurité de l'information, la famille des normes ISO 27000 apporte une aide indéniable dans la définition, la construction et la déclination d'un système de management de la sécurité. Nous pouvons distinguer trois types de normes dans cette famille :

- **Des normes certifiantes** : celle-ci décrivent les exigences devant être respectées si l'on souhaite viser la certification et ainsi obtenir une reconnaissance externe. L'ISO 27001, norme de définition et de mise en place d'un SMSI "Système de Management de la Sécurité de l'Information" publiée en 2005 est le pilier du système, nous retrouvons aussi la norme ISO 27006.
- **Des normes de recommandations** : ces normes proposent de bonnes pratiques à suivre pour définir les systèmes de management et sélectionner les mesures de sécurité. La plus connues est la norme ISO 27002 qui décrit les mesures de sécurité en trente et neuf (39) objectifs et cent et trente trois (133) mesures, la norme ISO 27003, ISO 27004, ISO 27005.
- **Des normes sectorielles et techniques** : l'ISO prépare aussi des "SMSI sectoriels" en sélectionnant et en adaptant les contrôles devant être mis en œuvre pour certains types d'organismes. Un des secteurs les plus avancés est celui des télécommunications avec le projet de la norme ISO 27011 [25].

3.4.2 Présentation de la norme ISO 27001

Cette norme récente, décrit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). Cela permet à une entreprise de choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise, sur un périmètre défini.

La norme ISO27001 s'appuie sur les onze (11) chapitres de la norme ISO27002 pour s'assurer de la pertinence des engagements de sécurité définis par le management. Cette norme s'adapte à tout type d'entreprise, quelque soit le secteur d'activité, sa structure, sa taille et la complexité de son système d'information. L'application de cette norme passe par une démarche qualiticienne classique : la roue de Deming (Plan, Do, Check, Act = Plannifier, Mettre en œuvre, Vérifier, Améliorer).
L'application de la norme ISO 27001, voire sa certification ne garantit pas un niveau de sécurité mais qu'un système de gestion de la sécurité informatique est en place et fonctionne (analyse des risques, pertinences des solutions,...). C'est devenu un standard international, reconnu, concret, facilement applicable et utilisé par l'ensemble des entreprises ayant souhaité une sécurisation de leur systèmes d'information. A savoir, le process "gestion de la sécurité" d'ITIL(Information Technology Infrastructure Library) v3 est une mise en œuvre opérationnelle d'un chapitre de l'ISO 27001[25].

3.4.3 Présentation de la norme ISO 27002

C'est un code de bonnes pratiques pour la gestion de la sécurité de l'information. Anciennement ISO 17799, la référence ISO 27002 va devenir la référence normative. Dans cette norme, les chapitres quatre (4) à quinze (15) listent les domaines qui peuvent être appliqués à l'entreprise : en fonction de ses contraintes légales, son domaine d'activité, sa structure, etc. Tous les points de mesure ou recommandations ne sont pas à appliquer nécessairement, cela dépend du contexte de l'entreprise [25]

3.5 Les différentes méthodes employées par l'audit informatique

3.5.1 La méthode COBIT

COBIT (Control objectives for information and technology), initié par l'ISACA (Information Systems Audit and Control Association), a été conçu pour prendre en charge la gestion des risques liés au domaine informatique.
La nécessité d'avoir un cadre de référence en matière de sécurité et de contrôle des technologies de l'information a poussé l'ISACA à créer la méthode COBIT en 1996. Cette méthode est diffusée en France par sa branche française l'AFAI (Association Française de l'Audit et du Conseil Informatique).
L'objectif était de faire le lien entre les risques métiers, les besoins de contrôle et les questions techniques en se basant sur les meilleures pratiques en audit informatique et système d'informations.
Le COBIT se destine aussi bien au management (qui doit décider des investissements à effectuer pour assurer la sécurité et la maîtrise des TI, et les ajuster suivant les risques de l'environ-

nement) qu'aux utilisateurs (sécurité, mise sous contrôle des services informatiques fournis). Cette méthode se veut le modèle de référence de la gouvernance des TI(Test d'Intrusions) et s'appuie sur cinq parties qui sont [30] :

- La synthèse : consiste en la présentation des concepts et principes de COBIT
- Le cadre de référence : se décline en check lists méthodiques couvrant quatre (4) domaines, trente et quatre (34) objectifs de contrôles généraux et trois cent et deux (302) objectifs de contrôle détaillés.
- Le guide d'audit : permet d'évaluer et de justifier les risques et les faiblesses des objectifs généraux et détaillés et de mettre en place des actions correctives.
- Le guide de management : fournit des indicateurs clés d'objectif et de performance et des facteurs clés de succès.
- Les outils de la mise en œuvre : contiennent une présentation de "success story" d'entreprises qui ont mis en place rapidement et avec succès la méthode COBIT.

3.5.2 La méthode MEHARI

MEHARI (MEthode Harmonisée d'Analyse de RIsques) est une méthode complète d'évaluation et de management des risques liés à l'information, ses traitements et les ressources mises en œuvre.
Réduire les risques impose de connaître les enjeux et les processus majeurs pour l'organisation afin d'appliquer les mesures organisationnelles et techniques de manière à optimiser les investissements. Cette démarche implique donc d'utiliser les pratiques et solutions à la hauteur des enjeux et des types de menaces pesant sur l'information, sous toutes ses formes, et les processus comme les éléments qui la gèrent et la traitent.
MEHARI, conforme aux exigences de la norme ISO/IEC 27005 pour gérer les risques, peut ainsi s'insérer dans une démarche de type SMSI promue par l'ISO/IEC 27001, en identifiant et évaluant les risques dans le cadre d'une politique de sécurité (Planifier), en fournissant des indications précises sur les plans à bâtir (Déployer) à partir de revues des points de contrôle des vulnérabilités (Contrôler) et dans une approche cyclique de pilotage (Améliorer). Ainsi MEHARI apporte une aide efficace pour manager et sécuriser l'information de toutes sortes d'organisations. MEHARI fournit un cadre méthodologique, des outils et des bases de connaissance pour :

– analyser les enjeux majeurs,
– étudier les vulnérabilités,
– réduire la gravité des risques,
– piloter la sécurité de l'information [27].

3.5.3 La méthode EBIOS

EBIOS signifie : Expression des Besoins et Identification des Objectifs de Sécurité. Cette méthode a été mise en place par la Direction Centrale de la Sécurité des systèmes d'information.

Méthode reconnue par les différentes administrations françaises, la méthode EBIOS consiste à formaliser les besoins de sécurité et les menaces, et permet de déterminer les risques pesant sur les périmètres à auditer. La méthode EBIOS se base sur Cinq axes, qui sont :
– Étude du contexte fonctionnel et technique,
– Expression des besoins de sécurité,
– Étude des menaces pesant sur le périmètre audité (fonctionnelles et techniques),
– Expression des objectifs de sécurité,
– Détermination des exigences de sécurité [28].

3.5.4 Méthode Feros

La méthode FEROS signifie : Fiche d'Expression Rationnelle des Objectifs de Sécurité des Systèmes d'Informations.Elle part du constat simple que les Responsables Informatiques sont généralement chargés de veiller sur [31] :
– le bon fonctionnement des matériels et réseaux de communication de l'entreprise,
– l'intégrité des données qui circulent. Partant de ce constat, il est donc primordial de définir des objectifs de sécurité à mettre en œuvre dans l'entreprise. Pour ce faire, il faut commencer par déterminer les besoins de la structure auditée :
– identification des données cruciales,
– détermination d'un seuil de tolérance de disponibilité ou inaccessibilité des dites données,
– identification des impératifs légaux incontournables qu'il faut respecter. La méthode FEROS s'articule autour de quatre axes principaux :
– un guide permettant à chaque structure auditée de rédiger un questionnaire qui lui sera propre,
– le questionnaire structuré qui permettra de mettre en évidence les particularités de l'entreprise,
– un glossaire qui définira précisément le sens de chaque terme technique employé pour le vulgariser auprès des décideurs non techniques,
– une synthèse des menaces potentielles qui permettra d'en prévoir les parades.

3.5.5 Méthode Marion

La méthode MARION "Méthodologie d'Analyse de Risques Informatiques Orientée par Niveau" est issue du CLUSIF.
Il s'agit d'une méthodologie d'audit, qui, comme son nom l'indique, permet d'évaluer le niveau de sécurité d'une entreprise (les risques) au travers de questionnaires pondérés donnant des indicateurs sous la forme de notes dans différents thèmes concourant à la sécurité.
Le niveau de sécurité est évalué suivant vingt et sept indicateurs répartis en six grands thèmes, chacun d'eux se voyant attribuer une note de zero à quatre, de sorte que le niveau trois étant le niveau à atteindre pour assurer une sécurité jugée correcte.
La méthode est basée sur des questionnaires portant sur des domaines permettant d'évaluer

les vulnérabilités propres à l'entreprise dans tous les domaines de la sécurité. La méthode se déroule en quatre phases distinctes :
– Préparation.
– Audit des vulnérabilités.
– Analyse des risques.
– Plan d'actions [27].

3.5.6 Critères de choix d'une méthode d'audit informatique

Afin d'effectuer le bon choix d'une méthode et pour mener à bien une démarche d'audit, nous nous basons sur les critères suivants :
– Origine géographique
– Langue
– Existence de logiciels adaptés
– Ancienneté
– Qualité de la documentation
– Facilité d'utilisation
– Comptabilité avec les normes
– Le coût (matériel et humain)
– La popularité, la reconnaissance [24].

3.6 Démarche adoptée

C'est à partir des critères ci-dessus, que nous avons porté notre choix sur la démarche EBIOS qui nous semble par conséquent, la plus adaptée en tant que méthode d'audit informatique.

3.6.1 Présentation de la démarche EBIOS

Créée en 1995 et maintenue par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) française, la méthode EBIOS "Expression des Besoins et Identification des Objectifs de Sécurité" permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information "SSI". EBIOS à la particularité d'être disponible gratuitement, pour tout organisme souhaitant mener une étude des risques SSI et mettre en place une politique adéquate de sécurité de l'information largement utilisée dans le secteur public (l'ensemble des ministères et des organismes sous tutelle), dans le secteur privé (cabinets de conseil, petites et grandes entreprises), en France et à l'étranger par de nombreux organismes en tant qu'utilisateurs ou bénéficiaires d'analyses de risques SSI [30].

3.6.2 Déploiement de la démarche EBIOS

La démarche EBIOS se décompose en cinq étapes présentant les activités à réaliser dans le cadre d'une étude des risques SSI. Il faut noter que l'ensemble des activités proposées peuvent être adaptées, afin de répondre au mieux aux besoins d'une organisation donnée vis-à-vis de son contexte et de ses caractéristiques, nous avons ci-dessous représenté sur une figure les cinq étapes associées à la démarche EBIOS [31].

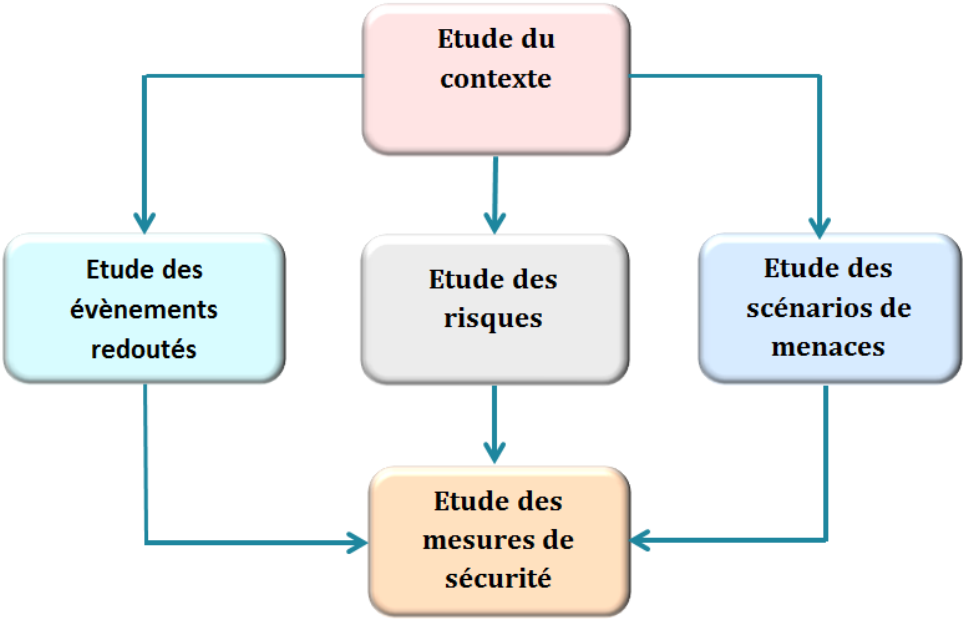


FIGURE 3.2 – La démarche EBIOS

Avant d'entamer l'explication et le déroulement de chaque étape associée à la démarche EBIOS, il est essentiel de définir certaines notions que nous rencontrerons lors du déploiement de notre démarche

– **Définition d'une vulnérabilité** Une vulnérabilité ou faille est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système [32].

– **Définition d'un risque** Un risque est un scénario qui décrit comment des sources pourraient exploiter les vulnérabilités des supports jusqu'à provoquer un incident sur les éléments à protéger et des impacts sur la vie privée [32].

– **Le niveau d'estimation d'un risque selon la méthode EBIOS [32]** Le niveau d'un risque est estimé en termes de gravité et de vraisemblance.
  - La gravité représente l'ampleur d'un risque.
  - La vraisemblance traduit la faisabilité d'un risque. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

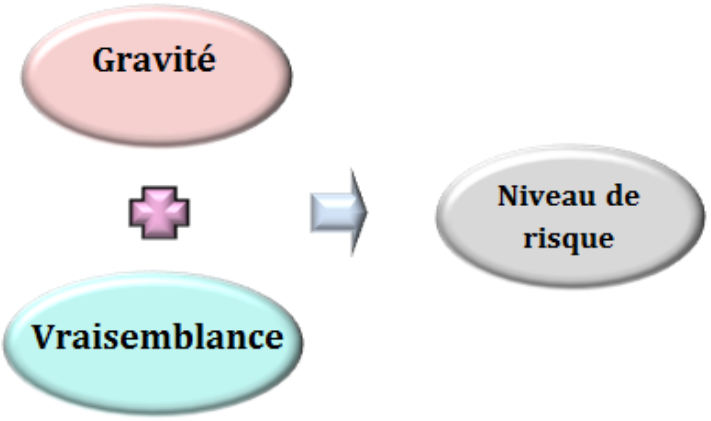


FIGURE 3.3 – Détermination d'un niveau de risque

Dans ce qui suit, nous décrivons le déroulement de chaque étape de la méthode EBIOS [33].

Etape 1 : Etude du contexte

Cette étape essentielle a pour objectif de comprendre comment réunir les éléments nécessaires pour adapter la gestion des risques au contexte particulier du sujet de l'étude, qui est le système cible. Il s'agit de l'étude du réseau de la SONATRACH DP. Pour ce faire, nous allons suivre un ensemble d'activités. Que l'on site ci-dessous :

– Etude du système cible
– Discuter des outils de sécurité présentés en répondant à un ensemble de questions.

Activité 1 : Etude du système cible

– Structure de l'entreprise : la direction régionale de l'entreprise SONATRACH DP est subdivisée en onze divisions illustrées dans le schéma présenté dans la figure1.1.

Système informatique : l'entreprise SONATRACH DP dispose d'un réseau LAN constitué d'un ensemble d'équipements matériels et logiciels, celui-ci suit une hiérarchie de commutateurs Cisco Catalyst 3750, nous citons le commutateur Core qui gère le trafic provenant des divers commutateurs d'accès connectés à ses différents ports, qui sont à leurs tour connectés aux PC d'utilisateurs ainsi qu'aux divers serveurs existants : serveur de messagerie, serveur d'annuaire Active Directory, serveur de filtrage, serveur antivirus, serveur proxy. Pour qu'une machine interne puisse accéder au réseau étendu, il est impératif qu'elle passe en premier lieu par un mécanisme de filtrage, qui représente dans notre cas le pare-feu ASA 5500 , sans omettre le réseau de l'entreprise comprend deux routeurs Cisco Catalyst 7200 qui constituent à leur tour le réseau WAN de l'entreprise et qui permettent d'acheminer le trafic provenant du réseau LAN aux différents LAN distants associés aux autres secteurs de la SONATRACH DP qui constitue un réseau de confiance permettant l'accès au LAN sans aucune mesure de sécurité envisagée.

Pour se connecter à INTERNET, le LAN de l'entreprise est connecté à un opérateur de télé-communication. ci-dessous, nous illustrons l'architecture réseau associée à l'entreprise :

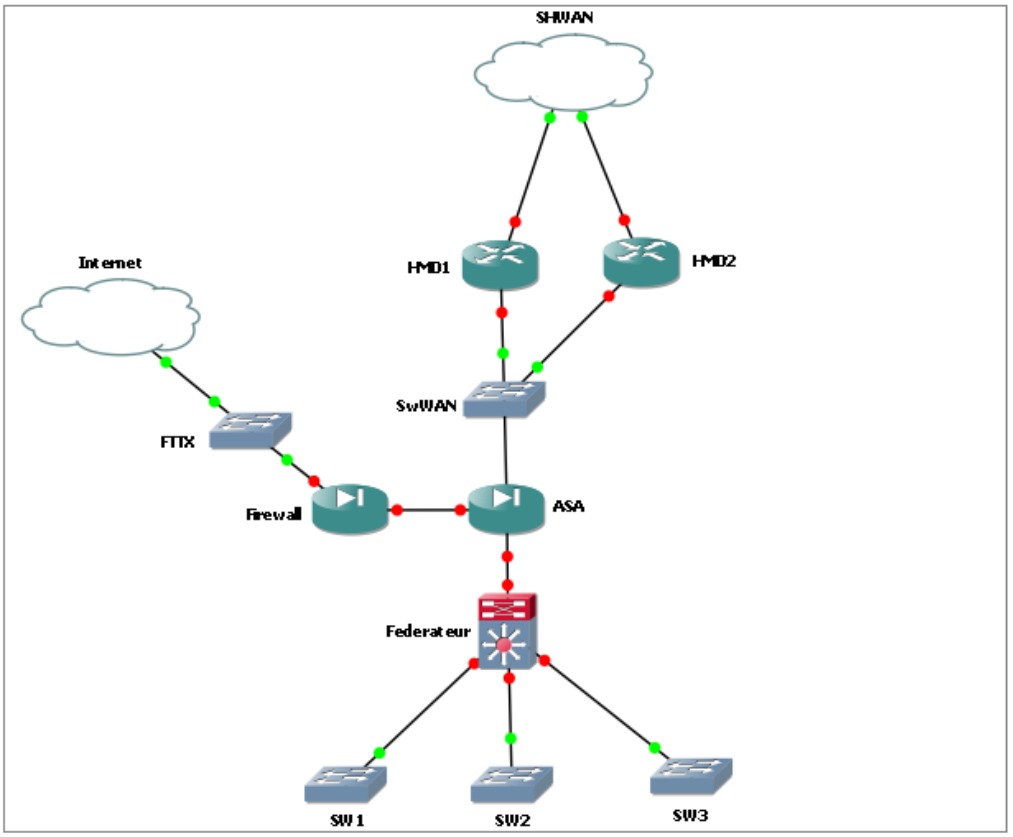


FIGURE 3.4 – Architecture du réseau de l'entreprise

– **Eléments de contexte :**
Nous avons au cours des entretiens avec le personnel de la direction ainsi que la visite des locaux recueillis les informations suivantes :

- La salle machine se situe au niveau de la division informatique.
- La salle machine dispose d'un système de reconnaissance d'empreinte digitale permettant l'accès qu'aux personnes autorisées.
- La salle machine dispose d'un système anti-incendie.
- La salle machine ne dispose pas d'une alarme anti-intrusion.
- Le réseau de l'entreprise dispose d'une alimentation de secours de type onduleur qui assure la continuité des services.
- Il existe des consignes de fermeture à clés des locaux, mais aucun moyen, ni procédure de contrôle n'ont été mis en place.

Sources de menaces retenues :

Les sources de menaces retenues peuvent être présentées sous différentes figures, il peut s'agir de sources humaines ou non humaines. Dans notre cas, nous citons les sources de menaces suivantes :

- Hacker
- Script-kiddies
- Concurrent (éventuellement en visite incognito)
- Maintenance informatique
- Employé peu sérieux
- Administrateur peu sérieux
- Client
- Partenaire
- Fournisseur d'accès Internet
- Hébergeur
- Virus non ciblé
- Panne électrique
- Incendie des locaux

Activité 2 : Discussion des outils de sécurité

Maintenant que nous avons eu une vision étendue du réseau de l'entreprise, nous sommes appelés à répondre à un ensemble de questions.

Question 1 : Quels sont les métiers de la SONATRACH DP ?

On distingue deux types de métiers :

1. Les métiers de base :
   - Les métiers de la maintenance
   - Les métiers de la sécurité industrielle
   - Les métiers de l'exploitation
   - Les métiers de l'engineering production
   - Les métiers techniques

2. Les métiers soutien et support :
   - Gestion des ressources humaines
   - Approvisionnements
   - Logistique
   - Intendance
   - Finances
   - Informatique

Question 2 : Quelles sont les axes stratégiques de la SONATRACH DP ?
Les axes stratégiques de la SONATRACH DP sont les suivants :

- Axe 1 : Exploitation, le forage, l'exploitation et la production
- Axe 2 : Chimie pétrolière, transformation des hydrocarbures, raffinage, traitement
- Axe 3 : le transport des hydrocarbures et acheminement
- Axe 4 : la commercialisation des hydrocarbures

Question 3 : Qui ou quoi est susceptible de menacer l'organisme "sources de menaces" ?

Types de sources de menaces	**Retenu**	**Non Retenu**	Exemples de source de menace
Source humaine interne, malveillante, avec de faibles capacités	Oui		Employé peu sérieux
Source humaine interne, malveillante, avec des capacités illimitées	Oui		administrateur peu sérieux, maintenance informatique, partenaire
Source humaine externe, malveillante, avec de faibles capacités	Oui		Script-Kiddies, client
Source humaine externe, malveillante, avec des capacités illimitées	Oui		Hacker, hebergeur, concurrent
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui		Emeployé peu sérieux
Source humaine interne, sans intention de nuire, avec des capacités importantes	Oui		Administrateur peu sérieux
Source humaine externe, sans intention de nuire, avec de faibles capacités	Oui		Clients
Source humaine externe, sans intention de nuire, avec des capacités importantes		Non	Fournisseur d'accès internet, hebergeur
Virus non ciblé	Oui		client, partenaire, concurrents
Phénomène naturel	Oui		Incendie
Catastrophe naturelle ou sanitaire	Oui		Séisme

TABLE 3.1 – présentation des sources de menaces

Question 4 : Quels sont les supports des éléments à protéger ?

Types de biens supports	**Biens supports**
Matériels	Ordinateurs, routeurs, commutateurs, points d'accès, serveur de messagerie, serveur d'annuaire " Active Directory ", serveur de filtrage, serveur antivirus, serveur proxy, pare-feu, téléphones IP
Logiciels	Systèmes d'exploitation, base de données, anti-X,
Canaux informatiques et de téléphonie	Câbles en cuivre, Wifi, fibre optique
Organisations	fournisseur d'accès Internet hébergeur, partenaire
Personnels	Chef de division, chefs de service, employés,
Supports papiers	Imprimantes, photocopieur, scanner
Locaux	Salle machine, bureaux d'administrateurs

TABLE 3.2 – présentation des biens support à protéger.

Question 5 :Quelles sont les sources de risques pertinentes ?

- Quelles sont les personnes internes à considérées ? Administrateur peu sérieux, maintenance informatique, employé peu sérieux, partenaire.

- Quelles sont les personnes externes à considérées ? Client, haker, concurrent, script-kiddies, fournisseur d'accès Internet, hebergeur.

- Quelles sont les sources non humaines à considérer : ? virus non ciblé, panne electrique , incendie des locaux.

Question 6 : Quelles sont les mesures de sécurité existantes ?
sur quel bien support repose chacune des mesures ?

Mesures de sécurité existantes	Bien supports lesquelles elles reposent
– Authentification centralisée et sécurisée via un contrôleur de domaine	serveur d'annuaire "Active Directory"
Solution Antivirale.	Serveur antivirus
– Stratégie de sécurité du Domaine – Solution Antivirale – Identification de trafic IP et séparation en DMZ. – Politique de gestion des ACL.	serveur de messagerie, serveur d'annuaire "Active Directory", serveur de filtrage, serveur antivirus, serveur proxy
– Accès sécurisé par mot de passe et adresse IP de l'équipement – Accès centralisé par un serveur d'authentification ACS au niveau d'Alger.	routeurs, commutateur, points d'accès,
– Sécurité Matérielle ASA 5500. – Filtrage de Contenu pour le trafic internet(ISA, websens, NAC).	pare-feu, routeur

TABLE 3.3 – mesures de sécurité existantes

Etape 2 : Etude des événements redoutés

Cette étape consiste à identifier et à estimer les éléments constitutifs des risques, en d'autre terme "les événements redoutés", pour ce faire il est essentiel d'établir un ensemble d'activités, que l'on site ci-dessous :

- Déterminer les besoins des biens essentiels en utilisant les échelles définies dans le tableau qui suit,
- Déterminer les sources les plus pertinentes en utilisant la liste des sources de menace définie auparavant,
- Imaginer les impacts si les besoins de sécurité ne sont pas satisfaits,
- Estimer la gravité en utilisant l'échelle correspondante définie dans le tableau qui suit.

Afin de répondre à ces activités, nous présentons à présent les échelles à utiliser

Echelles à utiliser :

Niveaux	Description détaillée de l'échelle
Disponibilité	
Plus de 72h	Le bien essentiel peut être indisponible plus de 72 heures.
Entre 24 et 72h	Le bien essentiel doit être disponible dans les 72 heures.
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24 heures.
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures.
Intégrité	
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
Maitrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.
Intègre	Le bien essentiel doit être rigoureusement intègre.
Confidentialité	
Public	Le bien essentiel est public.
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.
Gravité	
Négligeable	Le réseau de l'entreprise surmontera les impacts sans aucune difficulté.
Limitée	Le réseau de l'entreprise surmontera les impacts malgré quelques difficultés.
Importante	Le réseau de l'entreprise surmontera les impacts avec de sérieuses difficultés.
Critique	Le réseau de l'entreprise ne surmontera pas les impacts (sa survie est menacée).

TABLE 3.4 – présentation des echelles à utiliser

Maintenant que les échelles sont définies, nous allons énumérer les différentes sources de menaces retenues suivi des impacts vraisemblables qui peuvent atteindre le système étudié et enfin dégager les événements redoutés.

Evénements redoutés :

Biens essentiels	Critères	Besoins	Sources de menaces	Impacts	Gravité
SYS-Réseau interne	Disponibilité	Moins de 4h	administrateur peu sérieux, Script-kiddies, Concurrent, Client, Employé peu sérieux, hacker	Compromettre la disponibilité des ressources au niveau LAN	2. Limitée
SYS-Réseau interne	Intégrité	Intègre	script-kiddies, Concurrent, partenaire, client, Maintenance informatique, Employé peu sérieux	Compromettre l'intégrité des données au niveau LAN	2.Limitée
SYS-Réseau interne	Confidentialité	Limité	administrateur peu sérieux, concurrent, partenaire, Hébergeur, Maintenance informatique, Employé peu sérieux	Compromettre la confidentialité des données au niveau LAN	4.Critique
SYS-réseau WAN	Disponibilité	Entre 4 et 24h	Script-kiddies, Concurrent, Client, Partenaire, Virus nonciblé, Hébergeur	Compromettre la disponibilité des ressources au niveau LAN	2.Limitée

SYS-réseau WAN	intégrité	Maitrisé	Script-kiddies, Concurrent, Client, Partenaire,Hébergeur, maintenance informatique	Compromettre l'intégrité des données au niveau WAN	3.Importante
SYS-réseau WAN	Confidentialité	Limité	Script-kiddies, Concurrent, Partenaire,Virus non ciblé, Hébergeur, maintenance informatique	Compromettre la confidentialité des données au niveau WAN	4.Critique
SYS-réseau Wifi	Disponibilité	Entre 24 et 72h	Employé peu sérieux, concurrent, administrateur peu sérieux	Compromettre la disponibilité des ressources au niveau LAN	2.Limitée
SYS-réseau Wifi	Intégrité	Intègre	employé peu sérieux fournisseur d'accès Internet, administrateur peu sérieux	Compromettre l'intégrité des données au niveau LAN	2. Limitée
SYS-réseau Wifi	Confidentialité	Public	Employé peu sérieux, administrateur peu sérieux	Compromettre la confidentialité des données au niveau LAN	4.Critique

TABLE 3.5 – classement des évenements redoutés

Etape 3 : Etude des scénarios de menaces

L'objectif général de cette étape consiste à savoir identifier, estimer puis évaluer les différents scénarios de menaces figurant dans le réseau de la SONATRACH DP. Pour ce faire, nous devons :

- Connaitre les différents outils de sécurité de l'organisation.
- Discuter les outils présentés.
- Savoir identifier puis évaluer les scénarios de menaces

A partir des éléments fournis, nous complétons les tableaux de scénarios de menaces tout en respectant les activités suivantes :

- Déterminer les sources les plus pertinentes en utilisant la liste correspondante
- Vérifier les vulnérabilités et les compléter si besoin
- Estimer la vraisemblance des scénarios en utilisant l'échelle définie dans le tableau qui suit.

Echelle à utiliser

Vraisemblance	
1. Minime	Ne devrait pas se produire
2. Significative	Pourrait se produire
3. Forte	Devrait se produire
4. Maximale	Va certainement se produire prochainement.

TABLE 3.6 – présentation de l'echelle à utiliser

Scénarios de menaces

Selon la méthode EBIOS, nous définissons les différents scénarios de menaces comme suit :

Bien supports	**Critères de sécurité impactée**	**Source de menaces**	**Vraisemblance**
SYS-Réseau interne	Disponibilité	administrateur peu sérieux, Script-kiddies, Concurrent, Client, Employé peu sérieux, haker	3. Forte
SYS-Réseau interne	Intégrité	script-kiddies, Concurrent, partenaire, client, Maintenance informatique, Employé peu sérieux	3.Forte
SYS-Réseau Interne	Confidentialité	administrateur peu sérieux, concurant, partenaire, Hébergeur, Maintenance informatique, Employé peu sérieux	3. Forte
SYS-réseau WAN	Disponibilité	Script-kiddies, Concurrent,Client, Partenaire,Virus non ciblé,Hébergeur	3. Forte
SYS-réseau WAN	Intégrité	Script-kiddies, Concurrent,Client, Partenaire,Hébergeur, maintenance informatique	3. Forte
SYS-réseau WAN	Confidentialité	Script-kiddies, Concurrent, Partenaire,Virus non ciblé, Hébergeur, maintenance informatique	3.Forte
SYS-réseau Wifi	Disponibilité	Employé peu sérieux, concurrent, administrateur peu sérieux	1. Minime
SYS-réseau Wifi	Intégrité	employé peu sérieux,fournisseur d'accès Internet, administrateur peu sérieux	1.Minime
SYS-réseau Wifi	Confidentialité	Employé peu sérieux, administrateur peu sérieux	1. forte

TABLE 3.7 – définition des scénarios de menaces

Etude de certains scénarios de menaces du réseau de la SONATRACH DP

A partir de l'étude menée dans les étapes précédentes, nous allons affiner l'étude pour un ensemble de scénarios de menaces, que nous allons présenter ci-dessous.

1er Scénario de menace

Bien support : SYS-réseau WAN.

Critère de sécurité : confidentialité.

Sources de menaces : hacker, Script-kiddies, Concurrent, Client.
Vraisemblance : 2.Significative.
Description : Il est vraisemblable qu'un hacker, Script-kiddies, Concurrent ou Client réalisent une compromission sur le réseau WAN de la SONATRACH DP "IRARA" en accédant au réseau LAN de cette dernière et ce en passant par l'un des routeurs des différents secteurs de IRARA qui sont autorisés à accéder à son réseau LAN sans aucun dispositif de filtrage ou de contrôle d'accès.

Décomposition du réseau WAN

- Matériel : routeur Cisco Catalyst 7200
- Logiciel : IOS
- Logiciel : Windows XP
- matériel : ordinateur de l'attaquant
- Réseau : WAN

2^{eme} scénario de menace

Bien support : SYS-réseau interne
Critère de sécurité : disponibilité et confidentialité
Sources de menaces : administrateur peu sérieux, employé peu sérieux, partenaire.
Vraisemblance : 3.Forte
Description : Il est vraisemblable qu'un administrateur peu sérieux, employé peu sérieux ou un partenaire réalisent une compromission sur le réseau interne de la SONATRACH DP "IRARA" en saturant la table MAC d'un commutateur Catalyst 3750 et ce à partir de l'envoi massif de requêtes ARP en utilisant des adresses MAC aléatoires dans le but de basculer le commutateur en mode HUB qui diffusera toutes les trames reçues sur ses ports,ainsi l'intrus peut intercepter les flux de données.

Décomposition du réseau interne

- Matériel : Commutateur Cisco Catalyst 3750
- Logiciel : IOS
- Logiciel : Windows XP
- matériel : ordinateur de l'attaquant
- Réseau : interne

3^{eme} scénario de menace
Bien support : SYS-réseau interne.
Critère de sécurité : confidentialité et intégrité des données.
Sources de menaces : Concurrent, hacker, client, employé peu sérieux
Vraisemblance : 1.Minime

Description : Il est vraisemblable qu'un Concurrent, hacker, client ou employé peu sérieux prennent le contrôle d'un commutateur ou d'un routeur du réseau LAN ou WAN de la SONATRACH DP "IRARA" à partir d'un accès distant via le protocole "Telnet", ceci peut se faire du fait que le protocole Telnet est très simple et basique, car les données sont transférées en clair sur le réseau, il utilise aussi une méthode d'authentification minimale. De ce fait un intrus aurait la possibilité d'écouter le trafic du réseau LAN, et donc les données en chemin, ceci en utilisant l'un des outils de capture et d'analyse de trafic comme Wireshark, ainsi l'intrus peut facilement récupérer les données d'une session Telnet (login et mot de passe) lors de la phase de l'authentification d'un client Telnet (machine d'un administrateur) auprès d'un serveur Telnet (commutateur ou routeur).

Décomposition du réseau interne

- Matériel : Commutateur Cisco Catalyst 3750, routeur Cisco 7200
- Logiciel : IOS
- Logiciel : Windows XP
- matériel : ordinateur de l'attaquant
- Réseau : Internet

4^{me} scénario de menace
Bien support : SYS-réseau interne
Critère de sécurité : confidentialité, intégrité et disponibilité
Sources de menaces : Hacker, Concurrent, Partenaire, client, Employé peu sérieux
Vraisemblance : 4.maximale

Description : Il est vraisemblable qu'un Hacker, Concurrent, Partenaire, client ou un employé peu sérieux accèdent au réseau interne "LAN" de la SONATRACH DP "IRARA", par l'intermédiaire des points d'accès non sécurisé présent sur le réseau de l'entreprise. En effet, par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau, ainsi elle peut accéder au réseau filaire de l'entreprise (réseau interne) et éventuellement à Internet. Le réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour un intrus au réseau interne de l'entreprise. Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à Internet gratuit pour cet intrus (l'une des sources de menace) le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet, par conséquent l'entreprise risque d'être tenue responsable de l'attaque.

Décomposition du réseau interne

- Matériel : point d'accès
- Logiciel : IOS
- Logiciel : Windows XP
- matériel : ordinateur de l'attaquant
- Réseau : Internet

Analyse détaillée des menaces précédentes :

Dans le tableau qui suit, nous détaillons les différents scénarios de menaces définis auparavant.

Menaces	Exemple	Pré-requis	Vulnérabilité	Vraisemblance
Accès non autorisé au LAN de la SONATRACH DP IRARA en passant par le LAN de l'un de ses secteurs	– Accès aux données sensibles et confidentielles de l'entreprise (accès au serveur de messagerie ou serveur de bases de données,fichiers) – interception des communications circulant dans le réseau.	– Connaissance d'absence de pare-feu au niveau des secteurs de IRARA. – L'accès autorisé des secteurs de IRARA au LAN de cette dernière. – Accès au routeur de l'un des secteurs de IRARA et ce en se faisant passer pour un des employés d'un secteur X.	– Absence de mécanisme de filtrage ou de contrôle d'accès au niveau des routeurs des différents secteurs d'IRARA. – l'existence d'un réseau de confiance entre IRARA et ses différents secteurs qui permettent l'accès total de ces derniers à tout le LAN d'IRARA.	2.significative
Saturation de la table MAC du commutateur et interception non autorisée des flux de données transitant sur le réseau de la SONATRACH DP "IRARA"	Interception par un intrus d'un message qui ne lui est pas destiné.	Accès au réseau LAN de l'entreprise.	Absence de configuration permettant de sécuriser l'accès aux ports d'un commutateur (limitation du nombre d'adresses MAC autorisées sur un port donné)	3.Forte

Accès distant par " Telnet " qui n'utilise aucun mécanisme de chiffrement lors du transport des données de la session	– Interception d'un intrus des communications entre le client Telnet (administrateur réseau) et le serveur Telnet (commuutateur, routeur). – prise de contrôle d'un commutateur ou routeur du réseau.	Ecoute du trafic réseau en utlisant un sniffeur (analiseur) réseau comme wireshark	Le protocole Telnet ne dispose pas de mécanisme de chiffrement de données circulant entre le client et le serveur Telnet	1.minime
Accès au réseau LAN en passant par un point d'accès non sécurisé	– Accès non autorisé à certains serveurs ou périphériques situés dans le réseau LAN de la SONATRACH DP – interception des communications circulant dans le réseau – accès gratuit à Internet – l'entreprise risque d'être tenue responsable d'une attaque menée sur Internet à travers son réseau sans fil.	Accès à un point d'accès ouvert sur le réseau de l'entreprise.	présence d'un réseau sans fil non sécurisé au sein de l'entreprise	4.maximale

TABLE 3.8 – récapitulation des différents scénarios de menaces.

Etape 4 : Etude des risques

Cette étape consiste à connaitre les différents outils du réseau de l'entreprise "SONATRACH DP", dans le but d'apprécier les risques pesant sur le réseau de cette dernière ainsi que d'identifier les objectifs de sécurité de celle-ci, les activités associées à cette étape sont les suivantes :

- Présenter le risque à partir de la description de ses composantes.
- Discuter de la manière à évaluer les risques.
- Savoir choisir la manière dont chaque risque doit être traité et identifier les risques résiduels.
- Répondre à un ensemble de questions pour pouvoir compléter le tableau ci-dessous.

- Analyse d'un risque "identification et estimation, en tenant compte des mesures de sécurité existantes"

Echellle à utiliser

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	3.Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	4. Maximale

TABLE 3.9 – Echelle utilisée pour l'estimation des risques.

A ce niveau, nous sommes appelés à remplir les tableaux ci-contre :

Evénement redouté	**Source de menaces**	**Impacts**	**Gravité**
- Accès aux données sensibles et confidentielles de l'entreprise (accès au serveur de messagerie ou serveur de bases de données, fichiers) -interception des communications circulant dans le réseau	hacker, Script-kiddies, Concurrent, Client.	Compromettre la confidentialité des données au niveau LAN	Critique
Diffusion non autorisée d'informations	administrateur peu sérieux, employé peu sérieux, partenaire.	Compromettre l'intégrité des données au niveau LAN	Limitée
– Interception d'un intrus des communications entre le client Telnet (administrateur réseau) et le serveur Telnet (commutateur, routeur). – prise de contrôle d'un commutateur ou routeur du réseau	Concurrent, hacker, client, employé peu sérieux	Compromettre l'intégrité des données au niveau WAN	Importante

– Accès non autorisé à certains serveurs ou périphériques situés dans le réseau LAN de la SONATRACH DP – interception des communications circulant dans le réseau – accès gratuit à Internet – l'entreprise risque dêtre tenue responsable dune attaque menée sur Internet à travers son réseau sans fil.	Hacker, Concurrent, Partenaire, client, Employé peu sérieux	Compromettre l'authenticité des entités au niveau LAN	Critique

TABLE 3.10 – Identification et estimation des évenements redoutés

Scénarios de menaces	**Sources de menaces**	**Vraisemblance**
Accès non autorisé au LAN de la SONATRACH DP " IRARA " en passant par le LAN de l'un de ses différents secteurs	hacker, Script-kiddies, Concurrent, Client	2.Significative
Saturation de la table MAC du commutateur et interception non autorisée des flux de données transitant sur le réseau de la SONATRACH DP "IRARA"	administrateur peu sérieux, employé peu sérieux, partenaire	3. Forte
Accès distant par " Telnet " qui n'utilise aucun mécanisme de chiffrement lors du transport des données de la session	Concurrent, hacker, client, employé peu sérieux	1. Minime
Accès au réseau LAN en passant par un point d'accès non sécurisé	Hacker, Concurrent, Partenaire, client, Employé peu sérieux	4. Maximale

TABLE 3.11 – Estimation des menaces identifiées.

Mesure de sécurité existante	**Bien support sur lequel elle repose**	**Prévention**	**Protection**
Authentification centralisée et sécurisée via un Contrôleur de domaine.	Serveur d'annuaire " Active Directory "	X	
Accès centralisé par un serveur d'authentification ACS au niveau d'Alger.	Serveur d'authentification ACS	X	
Accès sécurisé par mot de passe et Adresse IP de l'équipement	Equipements réseau (commutateur, routeur...)	X	
Sécurité matérielle ASA 5500	Equipements de sécurité réseau (Pare-feu, VPN, Proxy...)		X
Solution antivirale	Serveur Symantec		X
Politique de gestion des ACL	Routeurs et commutateurs	X	
Filtrage de contenu pour le trafic Internet " Websence, NAC"	Serveur Websence Serveur NAC		X
Identification de trafic IP et séparation en DMZ		X	
Segmentation du réseau local en VLANs	Commutateurs	X	

TABLE 3.12 – Présentation des mesures de sécurité existantes.

Evaluation des risques

Après avoir étudier et analyser chacun des risques affectant le réseau de l'entreprise SONATRACH DP en tenant compte des mesures de sécurité existantes, nous avons pu dégager une évaluation de niveau de risques estimée par une gravité et vraisemblance.

Afin d'identifier les objectifs de sécurité du réseau de l'entreprise et de savoir choisir la manière dont chaque risque doit être traité et identifier les risques résiduels,nous répondons aux questions listées ci-dessous :

- En quoi pourrait consister chaque option de traitement concernant un risque donné ?

- Réduire un risque
- Transférer un risque
- Eviter un risque (option choisie).

- Comment fait-on le choix ?

Notre choix repose sur la solution de sécurité proposée pour chaque risque.

-Comment peut-on identifier des risques résiduels à ce niveau ?
L'identification des risques résiduels se fait à partir des tests effectués sur l'ensemble des solutions de sécurité proposées au préalable.

Etape 5 : Etude des mesures de sécurité

Cette étape consiste à savoir déterminer les traitements appropriés des risques, les planifier et suivre leur mise en oeuvre, pour cela nous devons spécifier les mesures de sécurité nécessaires et suffisantes de l'organisme, ensuite les mettre en oeuvre. Les activités associées à cette étape sont les suivantes :

- À partir d'un objectif de sécurité fourni, déterminer une ou plusieurs mesures de sécurité permettant de le satisfaire.
- Démontrer la couverture des mesures de sécurité envisagées et mettre en évidence les risques résiduels.
- À partir des mesures de sécurité présentées, formaliser le plan d'action.

Objectif de sécurité

Risque	Evitement	Réduction	Prise	Transfert
– Accès aux données sensibles et confidentielles de l'entreprise (accès au serveur de messagerie ou serveur de bases de données) – interception des communications circulant dans le réseau – accès gratuit à Internet – l'entreprise risque dêtre tenue responsable d'une attaque menée sur Internet à travers son réseau sans fil.	X			
Diffusion non autorisée d'informations	X			
– Interception d'un intrus des communications entre le client Telnet (administrateur réseau) et le serveur Telnet (commutateur, routeur). – prise de contrôle d'un commutateur ou routeur du réseau	X			

TABLE 3.13 – Définition des objectifs de sécurité

Mesures de sécurité

Mesures de sécurité complémentaires	Bien supports concernés
– Mettre en place un Pare-feu au niveau de chaque LAN des différents secteurs de IRARA interdisant ainsi à un intrus d'accéder au réseau LAN de IRARA – Mettre en place un VPN "IPsec ou SSL" qui permet de sécuriser les communications entre le LAN de "IRARA" et ses différents secteurs en assurant l'authentification de ses entités et la confidentialité des communications. – Sécuriser les points d'accès du réseau de la SONATRACH DP IRARA à partir du protocole "WPA2" qui permet l'authentification de l'accès au réseau local sans fil et le chiffrement des flux de données circulant entre les clients et le point d'accès et ce en s'appuyant sur le protocole de chiffrement "AES" utilisé par le protocole "WPA2". – mettre en place un serveur Radius permettant l'authentification des différents utilisateurs avant d'accéder à un point d'accès.	– Pare-feu ASA 5500 – VPN matériel "IPsec ou SSL" – VPN Logiciel "OpenVPN" à installer sur un routeur Cisco – Points d'accès
– Sécuriser les ports associés au commutateur en utilisant la fonction "Port Security" limitant le nombre d'adresses MAC sur un port de manière statique ou dynamique. – Activation du protocole 802.1X sur les ports associés au commutateur afin d'assurer le contrôle d'accès à celui-ci et d'empêcher la saturation de la table de correspondance par une source de menace.	Commutateur
-Remplacer le protocole "Telnet" par le protocole "SSH" afin d'assurer un accès distant sécurisé, car le protocole "SSH" prend en charge une authentification par mot de passe plus résistante, que celle proposée par le protocole "Telnet" et un chiffrement de donnés de la session via le protocole "RSA", préservant ainsi la confidentialité de l'ID, mot de passe et des détails de la session de gestion de l'administrateur.	– Equipement réseau "routeur, commutateur" – Equipement de sécurité "Pare-feu"

TABLE 3.14 – proposition des mesures de sécurité

Démonstration de couverture du risque conformément à l'objectif de sécurité
Risques résiduels
Quel est le niveau de risque après l'application des mesures de sécurité ?

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3.Importante	4. Critique
Vraisemblance	1. Minime	**2.Significative**	3. Forte	4. Maximale

TABLE 3.15 – Estimation du niveau de risque

Mise en oeuvre des mesures de sécurité au réseau de la SONATRACH DP
Echelles à utiliser

Difficulté	**Cout financier**	**Terme**
Faible	1. Nul	1. Trimestre
Moyenne	2. Moins de 1000 euro	2. Année
Elevée	3. Plus de 1000 euro	3.3ans

TABLE 3.16 – echelle à utiliser pour la mise en oeuvre des mesures de sécurité

Extrait des mesures de sécurité

Mesure de sécurité	Responsable	Difficulté	Cout financier	Terme
Mettre en place un Pare-feu au niveau de chaque LAN des différents secteurs de " IRARA " interdisant ainsi à un intrus d'accéder au réseau LAN de "IRARA".	Administrateur réseau et sécurité	1.Faible	2. Moins de 1000 euro	3.3ans
Mettre en place un VPN "IPsec ou SSL" qui permet de sécuriser les communications entre le LAN de "IRARA" et ses différents secteurs en assurant l'authentification de ses entités et la confidentialité des communications	Administrateur réseau et sécurité	1.Faible	3. Plus de 1000 euro	3.3ans
Sécuriser les points d'accès du réseau de la SONATRACH DP "IRARA" à partir du protocole "WPA2"qui permet l'authentification de l'accès au réseau local sans fil et le chiffrement des flux de données circulant entre les clients et le point d'accès et ce en s'appuyant sur le protocole de chiffrement "AES" utilisé par le protocole "WPA2"	Administrateur réseau et sécurité	1.Faible	1.Nul	3.3ans
mettre en place un serveur Radius permettant l'authentification des différents utilisateurs avant d'accéder à un point d'accès.	Administrateur réseau et sécurité	1.Faible	1.Nul	3.3ans

Sécuriser les ports associés au commutateur en utilisant la fonction "Port Security" limitant le nombre d'adresses MAC sur un port de manière statique ou dynamique.	Administrateur réseau et sécurité	1.Faible	1.Nul	3.3ans
Activation du protocole 802.1X sur les ports associés au commutateur afin d'assurer le contrôle d'accès à celui-ci et d'empêcher la saturation de la table de correspondance par une source de menace	Administrateur réseau et sécurité	1.Faible	1.Nul	3.3ans
Remplacer le protocole "Telnet" par le protocole "SSH" afin d'assurer un accès distant sécurisé, car le protocole "SSH" prend en charge une authentification par mot de passe plus résistante, que celle proposée par le protocole "Telnet" et un chiffrement de donnés de la session via le protocole "RSA", préservant ainsi la confidentialité de l'ID, mot de passe et des détails de la session de gestion de l'administrateur.	administrateur réseau et sécurité	1.Faible	1.Nul	3.3ans

3.7 conclusion

Dans ce chapitre, nous avons présenté l'audit de sécurité informatique ainsi que les différentes normes et méthodes existantes dans ce domaine, nous avons par la suite adopté la démarche EBIOS qui nous a permis de mener à bien l'audit de sécurité du réseau informatique de SONATRACH DP.
Une description des systèmes de détection d'intrusions ainsi que l'environnement de travail fait l'objet du chapitre suivant.

CHAPITRE 4

LES SYSTÈMES DE DÉTECTION D'INTRUSIONS ET ENVIRONNEMENT DE TRAVAIL

4.1 Introduction

Aujourd'hui les systèmes d'informations des entreprises sont de plus en plus ouverts sur le réseau Internet. Ainsi la mise en place des mesures sécuritaires devient une condition nécessaire, mais pas suffisante pour se protéger des risques et menaces présents sur la toile.

De ce fait les entreprises commencent à prendre conscience de l'importance de la mise en place d'une politique de sécurité informatique autour de ces systèmes d'informations et détecter d'éventuelles intrusions devient une nécessité pour estimer la complétude de cette politique de sécurité, ainsi les IDS (Intrusion Detection System) se font de plus en plus indispensables.

Au cours de ce chapitre, nous abordons principalement les systèmes de détection d'intrusions ainsi que l'environnement de notre travail. C'est pourquoi nous définissons dans un premier temps le concept des IDS, puis dans un second temps nous faisons une étude détaillée de l'IDS SNORT, enfin nous présentons l'environnement de notre travail pour la mise en place et le test de ce dernier.

4.2 Présentation générale des IDS

Un IDS est un mécanisme qui permet d'écouter le trafic réseau et de contrôler les activités réseau afin de repérer toutes activités anormales ou suspectes ainsi que de remonter des alertes sur les tentatives d'intrusion à un système informatique.
Un IDS est constitué essentiellement d'un sniffer couplé avec un moteur qui analyse du trafic selon des règles. Ces règles donnent une description des caractéristiques des trafics réseau à signaler. Ainsi un IDS remplit des fonctionnalités de contrôle réseau et réagit selon la nature du trafic.
Un IDS ne remplace en aucun cas un pare-feu ou tout autre mécanisme de sécurisation des systèmes d'informations. Cependant il renforce la sécurité en ajoutant une couche de sécurité

et permettant ainsi la mise en place d'une défense en profondeur sur l'architecture réseau.

4.2.1 Les types des IDS

La diversité des attaques utilisées par les pirates et des failles exploitées par ces attaques sur les différents niveaux des systèmes d'informations justifie l'existence de plusieurs types des IDS. En effet, pour assurer le bon fonctionnement de ces mécanismes, il faut savoir évaluer les risques encourus par un système d'information et classifier ces risques afin de déterminer le type de système de détection d'intrusion à mettre en place.
Nous présentons ci-dessous les différents types des IDS en expliquant leurs caractéristiques principales [34].

4.2.1.1 Les systèmes de détection d'intrusions réseau (NIDS)

Ce type d'IDS écoute tout le trafic réseau, analyse de manière passive les flux et détecte les intrusions en temps réel afin de générer des alertes.

4.2.1.2 Les systèmes de détection d'intrusions de type hôte (HIDS)

Un HIDS est plus lié à une machine qu'à son réseau. Il permet d'analyser, non seulement, le trafic réseau, mais aussi l'activité se passant sur la machine. Le but de ce type d'IDS est d'assurer l'intégrité des données d'un système et analyser le flux relatif à une machine.

4.2.1.3 Les systèmes de détection d'intrusions hybrides

Ce type d'IDS est utilisé dans un environnement décentralisé. Il centralise les informations en provenance de plusieurs emplacements sur le réseau. Le but de ce type d'IDS est d'avoir une vision globale sur les composants constituants un système d'informations en permettant une supervision centralisée en matières d'alertes d'intrusions remontées par les NIDS et les HIDS présents sur l'architecture du réseau supervisé.

4.3 Présentation de Snort

Snort est un NIDS provenant du monde Open Source, initialement développé par Marty Roesch en 1998, appartient actuellement à Sourcefire. Il s'est imposé comme le système de détection d'intrusions le plus utilisé. Sa version commerciale, plus complète en fonctions de monitoring, lui a donné bonne réputation auprès des entreprises.
Snort est capable d'effectuer une analyse du trafic réseau en temps réel et est doté de différentes technologies de détection d'intrusions telle que l'analyse protocolaire. Snort peut détecter de nombreux types d'attaques, comme : buffer over flows, scans de ports, etc.
Snort est doté d'un langage de règles permettant de décrire le trafic qui doit être accepté ou collecté. De plus, son moteur de détection utilise une architecture modulaire de plugins.

4.3.1 Architecture de Snort

L'architecture de Snort est modulaire et se compose des modules suivants :

1. **Un noyau de base "Packet Decoder" :** au démarrage, ce noyau charge un ensemble de règles, les compile, les optimise et les classe. Durant l'exécution, le rôle principal du noyau est la capture des paquets.
2. **Une série de pré-processeurs "Detection Engine" :** ces derniers améliorent les possibilités de SNORT en matière d'analyse et de recomposition du trafic capturé. Ils reçoivent les paquets directement capturés et décodés, les retravaillent éventuellement puis les fournissent au moteur de recherche des signatures pour les comparer avec la base des signatures.
3. **Une série de "Detection plugins" :** Ces analyses concerne principalement une comparaison entre les différents champs des headers des protocoles (IP, ICMP,TCP et UDP) par rapport à des valeurs précises.
4. **Une série de "output plugins" :** permet de traiter cette intrusion de plusieurs manières : envoi d'alertes vers un fichier log, envoi d'un message d'alerte vers un serveur syslog ou stocker cette intrusion dans une base de données SQL [36].

Un paquet subit un traitement depuis sa capture par "libpcap" jusqu'à son envoi dans la chaîne des output plugins, ce traitement passe par trois étapes : capture, décodage, détection ; Les étapes de traitement sont basées sur une architecture bien définis illustrée dans le schéma ci-contre figure 4.1 :

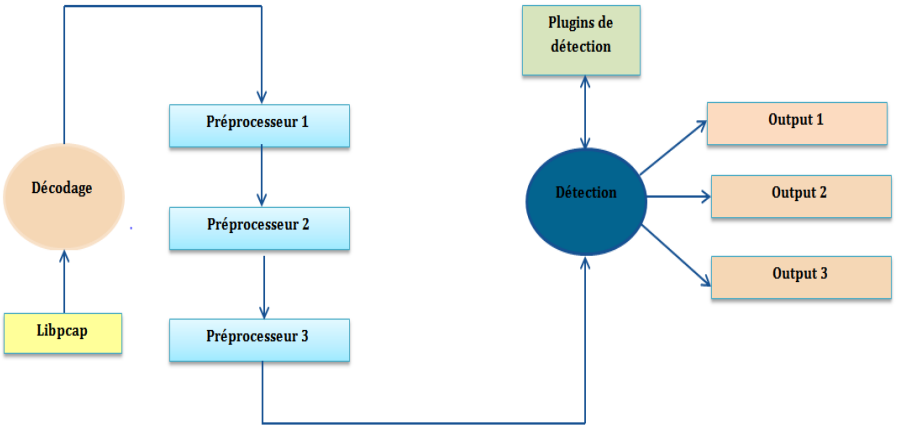


FIGURE 4.1 – architecture de Snort

4.3.2 Positionnement de Snort dans le réseau

L'emplacement physique de la sonde SNORT sur le réseau a un impact considérable sur son efficacité. Dans le cas d'une architecture classique, composée d'un Firewall et d'une DMZ, trois positions sont généralement envisageables : [36].

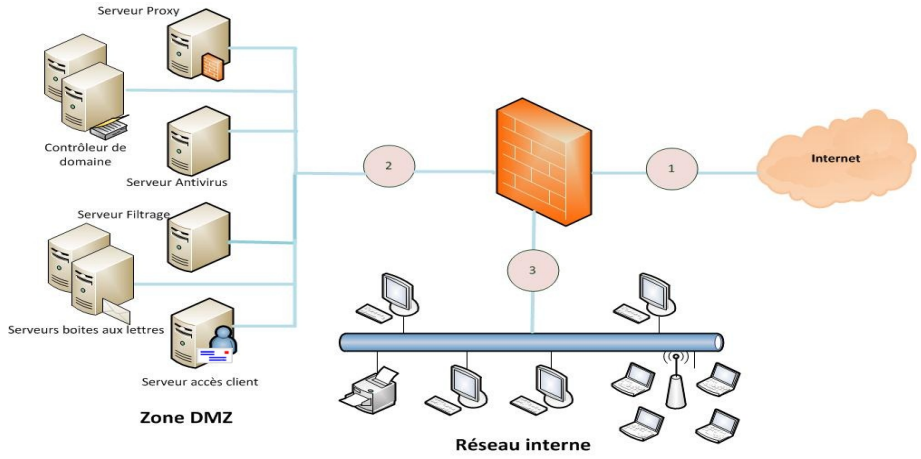


FIGURE 4.2 – Positions possibles de Snort dans le réseau

1. **Avant le Firewall ou le routeur filtrant :** Dans cette position, la sonde occupe une place de premier choix dans la détection des attaques de sources extérieures visant l'entreprise. Snort pourra alors analyser le trafic qui sera éventuellement bloqué par le Firewall. Les deux inconvénients de cette position du NIDS sont : le risque engendré par un trafic très important qui pourrait entraîner une perte de fiabilité, ainsi que sa position hors du domaine de protection du firewall qui l'expose à d'éventuelles attaques pouvant le rendre inefficace.
2. **Sur la DMZ :** Dans cette position, la sonde peut détecter tout le trafic filtré par le Firewall et qui a atteint la zone DMZ. Cette position de la sonde permet de surveiller les attaques dirigées vers les différents serveurs de l'entreprise accessible de l'extérieur.
3. **Sur le réseau interne :** Le positionnement du NIDS à cet endroit nous permet d'observer les tentatives d'intrusions parvenues de l'intérieur du réseau d'entreprise. Dans le cas d'entreprises utilisant largement l'outil informatique pour la gestion de leur activités ou de réseaux fournissant un accès à des personnes peu soucieuses de la sécurité (réseaux d'écoles et d'universités), cette position peut revêtir un intérêt primordial.

4.3.3 Mode de fonctionnement de Snort

Snort permet d'analyser le trafic réseau de type IP, il peut être configuré pour fonctionner en trois modes :

4.3.3.1 Utilisation de Snort en mode sniffer

Il s'agit d'écouter le réseau, en saisissant une ou plusieurs lignes de commandes qui indiqueront à Snort le type de résultat à afficher. En voici quelques-unes : [37]
La commande verbose affiche les en-têtes TCP/IP :

```
# snort -V
```

La commande verbose dump second layer info affiche les adresses IP et les en-têtes TCP/UDP/ICMP :

```
# snort -vde
```

4.3.3.2 Utilisation de Snort en mode packet logger

Ce mode est en tout point analogue au précédent, à ceci près que les logs ne s'affichent plus à l'écran, mais s'inscrivent directement dans un fichier de log (/var/log/snort/ par défaut).

```
# snort -de -l /var/log/snort
```

4.3.3.3 Utilisation de Snort en NIDS

Le véritable intérêt des NIDS est encore l'utilisation en mode NIDS. Snort utilise pour cela des règles afin de détecter les intrusions. Il existe aujourd'hui environ 1500 règles différentes, chacune s'adaptant à un cas particulier.

4.3.3.4 Utilisation de snort en IPS (Inline Mode)

Dans ce mode, Snort obtient les paquets d'Iptables (pare-feu Linux) au lieu de libpcap et décide le comportement du pare-feu : abandonner ou laisser passer le paquet [38].

4.3.4 Les Règles de Snort

Avec Snort, il est possible d'écrire et d'ajouter de puissantes règles de filtrage afin de tenir compte des spécificités de l'installation. Néanmoins, elles sont complexes à paramétrer : une règle Snort se présente sous la forme d'une ligne de commande et d'un langage conçus par un développeur.
Les règles Snort sont divisées en deux sections logiques, l'entête de la règle et les options de la règle. L'entête de règle contient comme informations l'action de la règle, le protocole, les adresses IP source et destination, les masques réseau ainsi que les ports source et destination. La section options de la règle contient les messages d'alerte et les informations sur les parties du paquet qui doivent être inspectées pour déterminer si l'action de la règle doit être acceptée [38].

4.3.4.1 Format des régles de snort

Les règles de Snort sont composées de deux parties distinctes : le header et les options.

- **header :** permet de spécifier le type d'alerte à générer (alert, log et pass) et d'indiquer les champs de base nécessaires au filtrage : le protocole ainsi que les adresses IP et ports sources et destination.
- **options :** spécifiées entre parenthèses, permettent d'affiner l'analyse, en décomposant la signature en différentes valeurs à observer parmi certains champs du header ou parmi les données [38].

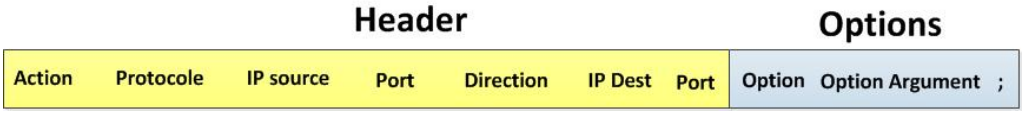


FIGURE 4.3 – format d'une règle de snort

Action : Une règle vous permet tout d'abord de définir une action, Snort exécute cette action lorsqu'il trouve une correspondance entre un paquet et les éléments dans une composition de règle. Les cinq principaux types d'actions définis par Snort sont les suivants [38].

- **alert :** génère une alerte en utilisant la méthode d'alerte sélectionnée et journalise le paquet.
- **log :** journalise le paquet.
- **pass :** ignore le paquet.
- **activate :** alerte et active une autre règle dynamique.
- **dynamic :** reste passive jusqu'à être activée par une règle **activate**, alors agit comme une règle log.

protocoles :il faut spécifier ensuite le protocole que Snort doit analyser, snort est en mesure d'analyser les protocoles TCP, UDP, ICMP et IP. Il est en outre tout à fait possible de créer des règles se rapportant aux protocoles des couches supérieures ; il suffit pour cela de spécifier le numéro de port correspondant dans le champ **any** [38].

Les adresses IP :La section suivante de l'entête de règle s'occupe comme information de l'adresse IP et du port pour une règle donnée. Le mot clé any peut être utilisé pour définir n'importe quelle adresse [39].

Les numéros de ports :Les numéros de ports peuvent être spécifiés de plusieurs manières ; en incluant any, en définissant des ports statiques ou des intervalles et des négations. Les ports any sont les valeurs génériques, signifiant littéralement tous les ports. Les ports statiques sont indiqués par un seul numéro de port, les intervalles de ports sont indiqués avec l'opérateur d'intervalle " :" [39].

Les options des règles :Les options de règle forment le cœur du moteur de détection d'intrusion de Snort. Toutes les options de règle de Snort sont séparées les unes des autres par un caractère "point-virgule". Les mots clés des options de règle sont séparés de leurs arguments avec un caractère "deux points". Quinze mots clé d'options de règle sont disponibles dans Snort, ces options portent entre autre sur les éléments définis dans le tableau suivant :

Option	**Rôle**
msg	affiche un message dans les alertes et journalise les paquets
logto	journalise le paquet dans un fichier nommé par l'utilisateur au lieu de la sortie standard.
ttl	teste la valeur du champ TTL de l'entête IP
tos	teste la valeur du champ TOS de l'entête IP
id	teste le champ ID de fragment de l'entête IP pour une valeur spécifiée
ipoption	regarde les champs des options IP pour des codes spécifiques
fragbits	teste les bits de fragmentation de l'entête IP
dsize	teste la taille de la charge du paquet contre une valeur
flags	teste les drapeaux TCP pour certaines valeurs
seq	teste le champ TCP de numéro de séquence pour une valeur spécifique
ack	teste le champ TCP d'acquittement pour une valeur spécifiée
itype	teste si la valeur du champ type ICMP est égale à une valeur spécifiée
icode	teste si la valeur du champ code ICMP est égale à une valeur spécifiée
icmp_id	teste si la valeur du champ ICMP ECHO ID est égale à une valeur spécifiée

icmp_seq	teste si la valeur du numéro de séquence ECHO ICMP est égale à une valeur spécifique
content	recherche un motif caractéristique d'une attaque (signature) dans le contenu à l'intérieur d'un paquet
content-list	recherche un ensemble de motifs caractéristiques d'une attaque dans le contenu à l'intérieur d'un paquet
offset	modifie l'option content, fixe le décalage du début de la tentative de correspondance de motif
depth	modifie l'option content, fixe la profondeur maximale de recherche pour la tentative de correspondance de motif
content-list	recherche un ensemble de motifs caractéristiques d'une attaque dans le contenu à l'intérieur d'un paquet
offset	modifie l'option content, fixe le décalage du début de la tentative de correspondance de motif
depth	modifie l'option content, fixe la profondeur maximale de recherche pour la tentative de correspondance de motif
nocase	correspond à la procédure de chaîne de contenu sans sensibilité aux différences majuscules/minuscules
session	affiche l'information de la couche applicative pour la session donnée
rpc	regarde les services RPC pour des appels à des applications/procédures spécifiques
resp	réponse active (ferme les connexions, etc)
react	réponse active (bloque les sites web)

TABLE 4.1 – Les options des règles

3.3.4.2 Mise à jour des règles de snort

L'installation et la mise à jour des règles de Snort sont disponible sur le site officiel de snort et peuvent être téléchargées à partir de l'adresse suivante : http ://www.snort.org/, cependant une inscription ultérieur doit être effectuée.

4.3.5 Déploiement de Snort dans les réseaux

Bien que Snort puisse s'utiliser dans un petit réseau ou dans le cadre d'une utilisation personnelle, son déploiement au sein de grandes entreprises peut s'avérer plus problématique. En effet, Snort ne constitue que la brique de base d'un système global de détection des intrusions et ne fournis nativement aucun mécanisme de stockage des données ou d'exploitation de la sonde. Pour remédier à ceci, il est courant d'utiliser Snort en association avec des bases de données SQL et des interfaces d'exploitation utilisant un frontal Web.

Dans ce domaine, l'association **Linux-Apache-MySQL-PHP** (ce que l'on résume par l'acronyme LAMP) a fait ses preuves [35].
Le rôle de chaqu'un des composant de LAMP est illustré dans la figure suivante :

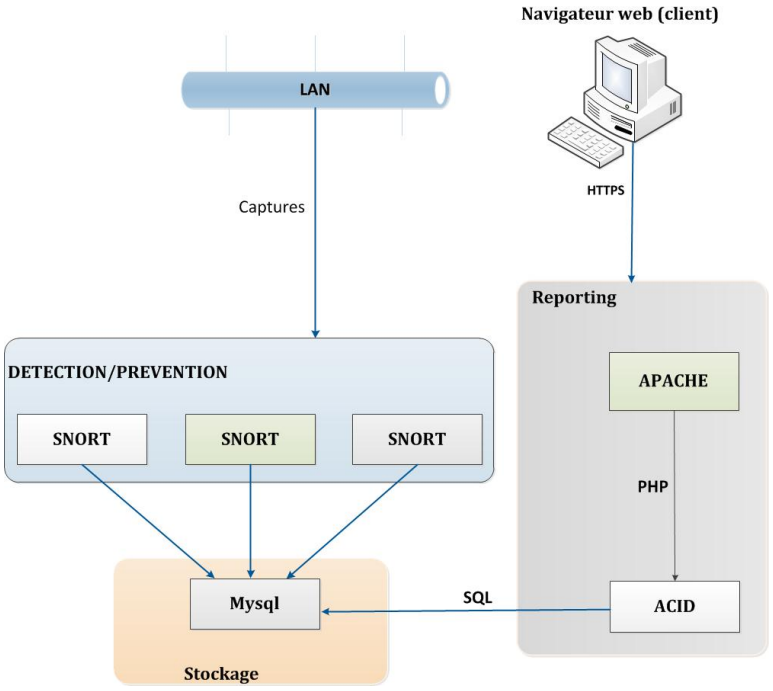


FIGURE 4.4 – exemple de déploiement de snort en entreprise

4.3.6 Définition des outils nécessaires pour Snort

Il faut être conscient que Snort ne constitue que la partie cachée de l'iceberg et qu'il est nécessaire de déployer les outils de management et de stockage des données associés. Dans ce qui suit, nous allons lister l'ensemble des outils nécessaires à déployer pour le fonctionnement de Snort.

4.3.6.1 Interface Basic Analysis and Security Engine (BASE)

Basic **A**nalysis and **S**ecurity **E**ngine est une interface web écrite en PHP permettant la gestion des alertes générées par l'IDS Snort et envoyées dans la base de données. Elle permet le classement des alertes en groupe, l'affichage des diagrammes et la recherche des alertes selon différents critères.
Pour fonctionner, BASE a besoin d'un certain nombre de dépendances :
– Un SGBD installé, comme MySQL
– Snort compilé avec le support de ce SGBD
– Un serveur HTTP, comme Apache
– La bibliothèque ADODB, qui est en fait une librairie d'abstraction de base de données pour PHP.
Afin que Snort enregistre les alertes dans la base de données, il faut modifier le fichier "snort.conf" et rajouter la ligne output database avec les informations nécessaires pour se connecter à la base de données [40].

4.3.6.2 Mysql

Le logiciel baptisé communément MySQL est un serveur de bases de données développé, distribué et supporté, à l'origine, par la société MySQL.
Il s'agit d'un logiciel de type client/serveur, constitué d'un serveur SQL multithread qui supporte différents systèmes de stockage, plusieurs programmes clients et outils d'administration, ainsi que de nombreuses interfaces de programmation.
MySQL est réputé pour sa fiabilité, ses performances et sa facilité d'utilisation. Il fonctionne sur beaucoup de plates-formes : les principales versions Unix, les distributions Linux, les systèmes Windows, Mac OS X, FreeBSD. MySQL reste disponible en tant que logiciel Open Source sous les termes de la licence GPL (MySQL Community Server). [48].

4.3.6.3 Barnyard2

Lorsqu'un comportement suspect est intercepté par Snort en fonction des signatures, Snort inscrit les événements. il est possible d'inscrire les logs en base de données directement. Néanmoins, dans un souci d'optimisation (libération de ressources), nous utiliserons Barnyard, une couche applicative qui exploite les événements générés par Snort au format "unifié". Barnyard permet de prendre en charge l'inscription des événements en base de données et libère donc des ressources à Snort qui peut davantage se concentrer sur la détection des intrusions. [49]

4.4 Tests d'intrusion

Les tests d'intrusion constituent une tentative autorisée de simuler les activités d'un pirate qui veut s'approprier des ressources qui ne sont pas les siennes, ou de nuire au bon fonctionnement d'un système d'informations. Ces tests permettent d'avoir une image claire de la sécurité globale d'une entreprise, ils correspondent à des attaques simulées d'un réseau.
Ils permettent de tester la robustesse de la sécurité, d'apprécier l'efficacité des mécanismes mis en œuvre.
Les tests d'intrusion ne peuvent pas se réduire à la simple utilisation d'un logiciel de détection automatique de vulnérabilités par balayage, mais ils nécessitent l'intervention d'une équipe de professionnels compétents pouvant identifier et qualifier les failles de manière plus réfléchie et auront à l'esprit les conséquences des tests qu'ils effectueront [41].

4.4.1 Démarche utilisée dans les tests d'intrusion

Le schéma ci-après illustre et décrit les différentes étapes de la démarche utilisé dans les tests d'intrusion qui se déroule en trois étapes

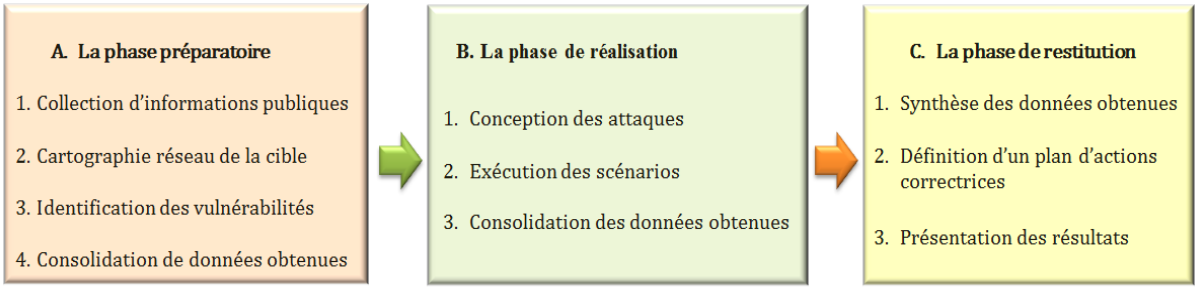


FIGURE 4.5 – la démarche utilisée dans les tests d'intrusion

Dans le cas des hackers, l'intrusion s'arrête au niveau de la phase B, tandis que dans le cas d'un audit de sécurité, il faut fermer les brèches ouvertes, puis passer à l'étape suivante.

4.4.2 Outils d'audit

Il existe de nombreux logiciels qui permettent d'automatiser la découverte de vulnérabilités, nous les appelons des scanners. Ils permettent d'évaluer les vulnérabilités présentes sur les réseaux. Ils se déclinent sous plusieurs formes et donnent des résultats avec des précisions variables, nous citons entre autre, **Internet Scanner, Satan, Saint, Retina, Nessus**. Dans notre mission d'audit nous allons simuler une attaque en utilisant Nessus pour le test d'intrusion de notre réseau[41].

4.4.3 Présentation de Nessus

Nessus est un outil d'analyse de vulnérabilités d'équipements réseaux. Il fonctionne en conjonction avec un analyseur de ports, le plus courant étant nmap. A partir d'une liste de ports disponibles, Nessus essaye toute une batterie d'actions définies dans des "plugins" (modules optionnels), ces actions peuvent conduire au "plantage" de la cible testée. En fin d'exécution, Nessus propose un rapport très détaillé. Quand c'est possible, un correctif et des liens utiles pour se renseigner sur les vulnérabilités sont proposés. Ce produit évolue constamment, les nouvelles vulnérabilités y sont ajoutées périodiquement. Il intègre sa propre gestion de base de connaissances, pour améliorer les analyses en se basant sur les données accumulées.
Il est conçu en client/serveur : un processus fonctionne sur une machine, et des clients y accèdent. Tous les échanges se font de manière cryptée, avec un niveau de cryptage élevé qui impose l'utilisation de Nessus en "local" [42].

4.5 Environnement de travail

Pour une meilleure sécurité, nous avons préféré de travailler dans un environnement Linux, qui est considéré comme le noyau le plus sûr au monde, plus précisément nous avons choisis la distribution **Ubuntu 10.04 LTS**, car il nous fournit un espace de travail unique et nous assure une fiabilité de résultat incomparable.
Ubuntu est une distribution Gnu/Linux récente, développée par la société Canonical Ltd, fondée par Mark Shuttleworth. Basée sur une Debian. ce système d'exploitation est constitué de logiciels libres, et est disponible gratuitement, y compris pour les entreprises [43].

4.6 Environnement d'attaques

Pour tester la fiabilité et la puissance de notre application, nous avons utilisé un outil d'attaques contenus dans une distribution Linux gratuite basée sur Ubuntu Lucid LTS portant le nom de Backtrack.
BackTrack est une distribution GNU/linux reconnue par les professionnels comme complète et efficace en matière d'analyse réseau et de test d'intrusion. Cette distribution est idéale pour tester l'efficacité de mesures de sécurité sur un ordinateur ou sur un réseau [44].

4.6.1 Description des différents outils de Backtrack

Backtrack est un système qui intègre une multitude d'outils pouvant monter un très grand nombre d'attaques, illustrés dans la figure suivante [45].

FIGURE 4.6 – Aperçu des différents outils d'attaque de Backtrack

Les différents outils de Backtrack sont classés dans le tableau suivant :

Outil	**Rôle**
Information Gathering	Contient tous les outils qui permettent de récupérer des informations, que ce soit concernant un protocole, une faille web, etc.
Vulnerability Assessment	Les outils qui permettent de trouver des vulnérabilités dans un protocole, un équipement, une vulnérabilité Web
Exploitation Tools	cet outil permet l'exploitation des vulnérabilités détectées.
Privilege Escalation	concerne les outils qui permettent l'élévation de privilèges.
Maintaining Access	Une fois l'accès à un système est réussi, cet outil permet de revenir facilement sur ce dernier.

Reverse Engineering	cet outil permet l'activité qui consiste à étudier un projet pour en déterminer son fonctionnement interne ou sa méthode de fabrication.
RFID Tools	outil permettant de casser une identification
Stress testing	outil permettant de tester les équipements contre la surcharge de données.
Forensics tools	outil permettant l'analyse de données sur le réseau (données hachées ou chiffrées).
Reporting Tools	Outil permettant de fournir un rapport
Services	cette outil concerne les services pouvant aider dans le Pentest.
Miscellaneous	concerne quelques outils malicieux pour le réseau et le web

TABLE 4.2 – Les différents outils de Backtrack.

4.7 Conclusion

A présent, nous avons pris connaissance des notions de base des IDS tout en se basant sur l'IDS Snort, nous avons par la suite définis l'environnement de notre travail pour mettre en place notre solution de sécurité.

Dans le chapitre qui suit nous décrierons la politique de sécurité que nous suggérons afin de remédier aux différentes vulnérabilités du réseau de l'entreprise, nous finissons par mettre en place l'une des solutions proposées qui est l'IDS Snort.

CHAPITRE 5

DÉFINITION D'UNE POLITIQUE DE SÉCURITÉ ET MISE EN PLACE DE SNORT

5.1 Introduction

Après avoir présenté dans le chapitre trois les menaces et les risques qui pèsent sur le réseau de l'entreprise "SONATRACH DP" suivant la démarche adoptée "EBIOS" et vu le nombre de vulnérabilités que l'on a rencontré durant le suivi de ce processus, nous décrivons à présent la politique de sécurité réseau à élaborer afin de mener à bien la gestion des risques et d'apporter ainsi les différentes solutions et contre-mesures pour faire face aux différentes vulnérabilités constatées, nous choisissons par la suite l'une des solutions à mettre en place, qui est l'IDS Snort dont nous détaillons toutes les étapes d'installation et de configuration, nous finissons par un test d'intrusions permettant de tester le bon fonctionnement de notre IDS, ceci en lançant une attaque de scan de ports avec l'outil Nessus intégré dans Backtrack.

5.2 Définition d'une politique de sécurité

Dans ce qui suit, nous présentons les différentes solutions propsées pour définir une politique de sécurité robuste afin de corriger les différentes failles de sécurité constatées dans l'étape d'analyse de la démarche EBIOS.

5.2.1 Solution pour les commutateurs via l'option port-security

Comme il s'agit dans notre cas d'étude des commutateurs de la gamme CISCO Catalyst 2960, la contre mesure proposée par CISCO afin de contrer à une attaque MAC flooding est l'utilisation de la commande *Switchport port-security* qui permet de limiter le nombre d'adresses MAC sur un port, de réagir en cas de dépassement de ce nombre, elle permet aussi de fixer une adresse MAC sur un port donné.
Pour réaliser cette configuration, nous devons suivre les étapes suivantes :
Activation de la fonction port-security au niveau d'une interface, soit Fa0/1 :

```
Catalyst2960 (config) # interface fa0/1
Catalyst2960 (config-if) # switchport port-security
```

Renseignement du mode d'apprentissage des adresses MAC associées à l'interface fa0/1 : Lorsqu'il s'agit d'attribution d'adresses à certains équipements tels que les serveurs, imprimantes, etc., nous attribuons ces adresses de façon statique :

```
Catalyst2960 (config-if) # switchport port-security mac-address address_mac
```

Dans le cas échéant, c'est l'attribution dynamique que nous utilisons par le biais de l'option 'sticky :

```
Catalyst2960 (config-if) # switchport port-security mac-address sticky
```

Nous indiquons par la suite au commutateur, le nombre maximal d'adresses qu'il tolèrera sur le port spécifique :

```
Catalyst2960 (config-if) # switchport port-security mac-address maximum nbr_adr_max
```

Enfin, nous indiquons au commutateur, la façon dont il réagira en cas de dépassement du nombre d'adresses MAC autorisé, en spécifiant l'un des trois modes disponibles :
– Rejet des adresses en dépassement sans notification : *mode protect*.
– Rejet des adresses en dépassement avec notification : *mode restrict*.
– Fermeture du port : *mode shut down* (mode par défaut).

Dans notre cas, nous recommandons le mode *restrict* :

```
Catalyst2960 (config-if) # switchport port-security violation restrict Spanning-tree portfast
```

5.2.2 Adoption d'une solution 802.1X pour l'authentification des utilisateurs

Utilisation du protocole 802.1X sur les commutateurs CISCO Catalyst 2960, dans le but d'imposer à tout utilisateur connectant son ordinateur au réseau local de s'authentifier avant d'entamer toute activité, en cas de succès d'authentification, l'utilisateur reçoit un profil réseau (TCP/IP et VLAN) ainsi qu'un assortiment de règles de sécurité.
La solution 802.1X s'appuie sur le protocole EAP pour assurer le transport d'un protocole d'authentification et fait appel à la configuration des trois entités suivantes :
– Le client : est typiquement un PC.

– Le commutateur : l'authentificateur
– Le serveur d'authentification : qui représente le serveur RADIUS

5.2.3 Adoption d'une Solution SSH pour sécuriser l'accès à distance

Implémentation du protocole "SSH" qui offre la possibilité de se connecter en toute sécurité à un hôte distant, en chiffrant toute la communication y compris la séquence d'authentification, ceci dans le but de palier aux vulnérabilités que présente le protocole " Telnet" définis pour assurer l'accès distant à un équipement.
Dans ce qui suit nous allons présenter la configuration de SSH sur un commutateur "CISCO Catalyst 2960" :

```
Catalyst2960 (config)#  ip domain name  nom_du_domaine

Catalyst2960 (config) # crypto key generate rsa general-keys modulus modulo

Catalyst2960 (config)#  ip ssh version 2

Catalyst2960 (config)# live vty 0  4

Catalyst2960 (config-line)# transport input ssh

Catalyst2960 (config-line)# login local

Catalyst2960 (config-line)# exec-timeout 0 30

Catalyst2960 (config)# access-class 10 in

Catalyst2960 (config-line)#exit

Catalyst2960 (config)# username nom_d'utilisateur  password  mot_de_passe

Catalyst2960 (config)# service password-encryption

Catalyst2960 (config)# enable secret mot_de_passe
```

5.2.4 Solution WPA2 pour les points d'accès non sécurisés

Mettre en œuvre la méthode de sécurité WPA2, qui assure les fonctions d'un système de sécurité, notamment renforcer la sécurité d'accès au réseau local sans fil tout en assurant la confidentialité et l'authenticité des données.
WPA2 impose l'utilisation du mécanisme d'authentification 802.1x entre le client, le point d'accès et un serveur d'authentification, généralement un serveur Radius (Remote Authentication Dial-In User Service). Le 802.1x tire parti du protocole EAP (Extensible Authentication Protocol, une extension de PPP).

5.2.5 Solution pour sécuriser l'accès au LAN d'IRARA à partir de ses différents secteurs

– Mise en place d'un pare-feu ASA 5500 au niveau de chaque LAN des différents secteurs d'IRARA, interdisant ainsi l'accès de chaque entité ou trafic provenant de l'extérieur, cette entité peut être un intrus désirant pénétrer le LAN d'IRARA en exploitant l'absence de mécanismes de sécurité permettant de protéger l'accès aux différents LAN de ces secteurs.

– Mise en place d'un VPN matériel IPsec, SSL ou d'un VPN logiciel " OpenVPN" intégré au niveau du routeur, qui permet de sécuriser les communications entre le LAN d'IRARA et les LAN de ses différents secteurs, ceci en assurant l'authentification de ses entités et la confidentialité des communications à travers le chiffrement des données échangés.

5.2.6 Solution pour se protéger contre l'ingenierie sociale

Nécessité de former le personnel de l'entreprise à avoir un comportement de sécurité (*Safe Behavior*) car l'humain est toujours le maillon faible de tout système de sécuritéil. En règle générale, la seule façon de se protéger est de s'armer de bon sens. Il est généralement utile de réfléchir sur les informations que l'on est amené à révéler, et à qui. Ceci dit, il n'existe pas de mesures techniques permettant de se protéger contre le Social Engineering.

5.2.7 solution NIDS pour les détections d'intrusions

Mise en place du NIPS Snort pour détecter les différentes intrusions qui peuvent atteindre le réseau de la SONATRACH DP "IRARA".

5.3 Mise en place de Snort

Après avoir définis une politique de sécurité du réseau de l'entreprise, parmi les solutions suggérées nous avons choisis d'étudier un cas de cette politique, il s'agit de la mise en place d'un NIDS basé sur le logiciel Snort et la console BASE (Basic Analysis and Security Engine) pour

analyser et superviser les alertes remontées par notre NIDS. Le choix de Snort, en particulier, est justifié par le fait que nous trouvons que cette solution peut être adaptée à n'importe quelle entreprise, quelque soit sa taille (TPE, PME, GE). Ce qui correspond parfaitement au cas de la SONATRACH DP, qui est une grande entreprise à caractère économique.
De plus Snort dispose d'un ensemble de plugins qui aident à étendre ses fonctionnalités, notamment " Snortsam " qui ajoute des fonctionnalités permettant à Snort de jouer le rôle d'un IPS.
Les étapes suivantes montrent pas à pas la démarche que nous avons suivie afin de réussir l'installation et la configuration de notre NIDS.

5.3.1 Installation des dépendances de Snort

Pour aboutir à une installation complète et correcte de Snort il est impératif d'installer un ensemble de prérequis qui sont les suivants :

```
# sudo apt-get install libpcap0.8-dev libmysqlclient15-dev mysql-client-5.1 mysql-server-
  5.1  bison flex apache2 php5 libapache2-mod-php5 php5-gd php5-mysql libtool libpcre3-
  dev  php-pear vim ssh openssh-server
```

Cette commande permet principalement d'installer le serveur et le client MySQL que leur mise en place est primordiale pour le fonctionnement de Snort, ils permettent de stocker les alertes qu'il génère, donc permettent aussi à la console BASE de se connecter et récupérer ces alertes.
Pendant l'installation, la figure suivante apparait où nous devons saisir le mot de passe pour la base de données MySQL comme le montre la figure ci-contre :

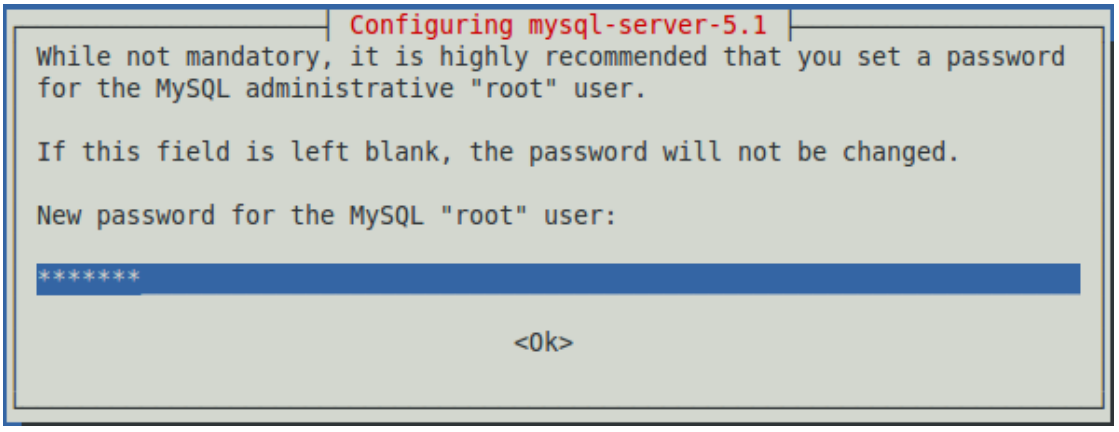


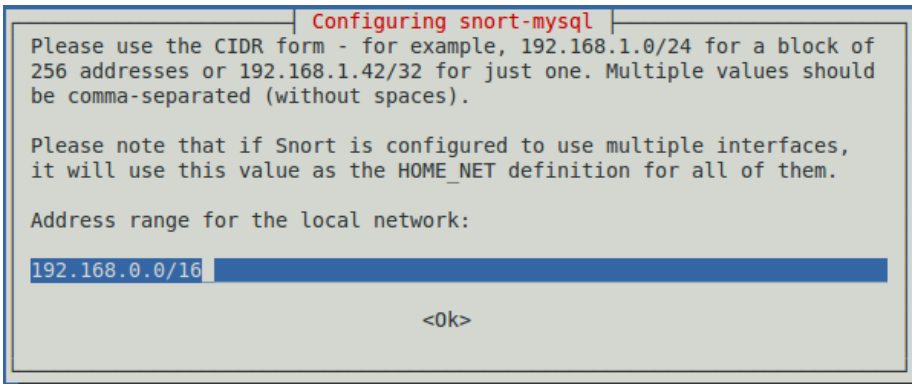
FIGURE 5.1 – création de la base de données mysql et le mot de passe pour l'utilisateur 'root'.

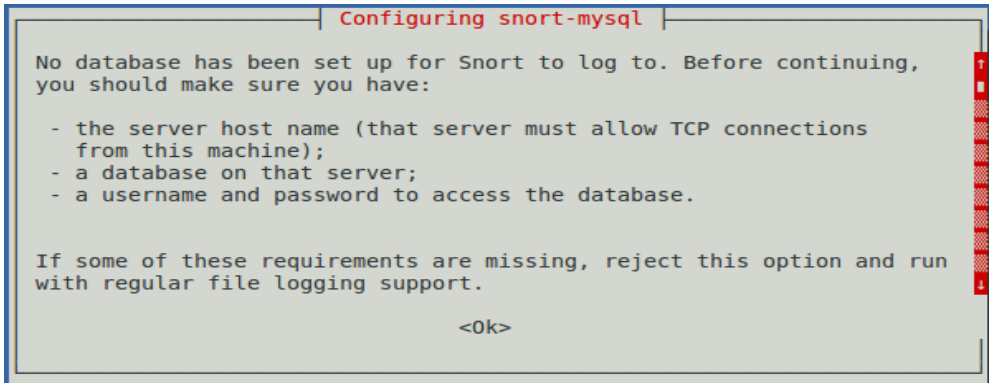
5.3.2 installation de Snort-MySQL

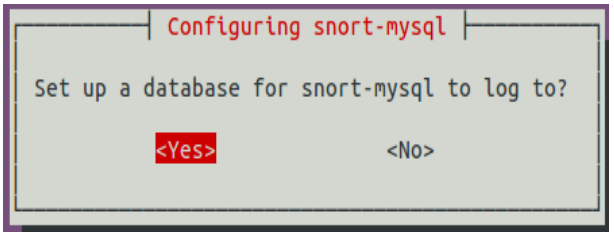
Pour que Snort puisse interagir avec le serveur MySQL afin de stocker les alertes, nous devons installer snort-mysql en utilisant la commande suivante :

```
# apt-get install snort-mysql
```

Pendant l'installation, la figure suivante apparait où nous devons autoriser la configuration et la connexion de la base de données snort pour *snort-mysql*







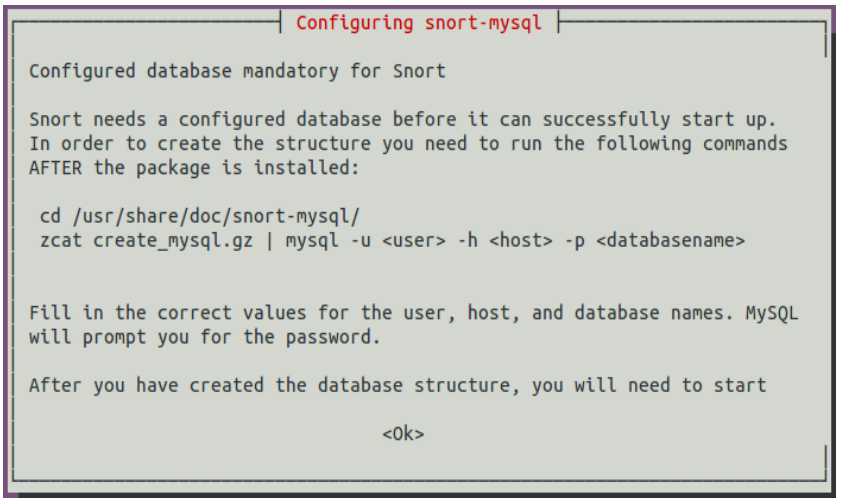


FIGURE 5.2 – paramètres de configuration "snort-mysql"

5.3.3 création de la base de données MySQL pour Snort

A présent, nous devons créer la base de données MySQL et les tables pour recevoir les logs de Snort.
Afin d'accéder à la base de données MySQL avec l'utilisateur "root", nous saisissons à partir du shell la commande suivante, puis, nous devons rentrer le mot de passe associé à la base de données définit dans l'étape illustrée par la Figure 5.2.

```
# mysql -u root -p
```

Création de la base de données "snort" et son utilisateur
Une fois Mysql lancé, nous saisissons l'ensemble de commandes suivantes pour la création de la base de données Snort et l'affectation des droits à l'utilisateur snort :

```
Mysql > create database snort;
Mysql > grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
Mysql > SET PASSWORD FOR snort@localhost=PASSWORD('snort');
Mysql > flush privileges;
Mysql > exit;
```

Maintenant, nous allons procéder à la création du schéma des données pour la base "snort", en accédant d'abord au répertoire contenant snort-mysql, ensuite, nous rapportons le schéma de snort vers la base de données MySQL en utilisant la commande suivante :

```
# cd /usr/share/doc/snort-mysql/
# zcat create_mysql.gz | mysql –u root –p
```

Afin de vérifier si la création de la base de données a été faite correctement ainsi que l'importation de schéma de données, nous utilisons les commandes suivantes :

```
Mysql > SHOW DATABASES;
Mysql > use snort;
Mysql > SHOW TABLES;
```

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| snort              |
+--------------------+
3 rows in set (0.02 sec)

mysql>
```

FIGURE 5.3 – vérification de la base de données "Snort"

```
mysql> use snort;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.00 sec)
```

FIGURE 5.4 – vérification des tables de la base de données "Snort"

5.3.4 configuration de Snort

Snort fournit des fichiers de configuration dont le principal est le fichier "snort.conf"
Le fichier "snort.conf" doit être modifié pour qu'il reflète notre configuration, cependant nous devons l'éditer avec la commande suivante :

```
# vim  /etc/snort/snort.conf
```

Une fois le fichier lancé, nous devons mettre en commentaire la ligne "var HOME_NET any" en ajoutant le symbol "♯", ensuite, nous ajoutons la ligne suivante "var HOME_NET eth0_ADDRESS" afin d'indiquer qu'il s'agit d'une interface Ethernet, dans notre cas il s'agit de "eth0".

```
# $(\Device\Packet_{12345678-90AB-CDEF-1234567890AB}_ADDRESS)
#
# var HOME_NET $eth0_ADDRESS
#
# You can specify lists of IP addresses for HOME_NET
# by separating the IPs with commas like this:
#
# var HOME_NET [10.1.1.0/24,192.168.1.0/24]
#
# MAKE SURE YOU DON'T PLACE ANY SPACES IN YOUR LIST!
#
# or you can specify the variable to be any IP address
# like this:

#var HOME_NET any
var HOME_NET $eth0_ADDRESS

# Set up the external network addresses as well.  A good start may be "any"
var EXTERNAL_NET any
#var EXTERNAL_NET !$HOME_NET
```

FIGURE 5.5 – ajout de l'interface d'écoute au fichier "snort.conf"

Maintenant, nous allons spécifier le format de fichier de sortie, dans notre cas nous avons choisi le format "unified2". Pour ce faire, nous allons en premier lieu mettre en commentaire la ligne : "Output log_tcpdump : tcpdump.log", puis insérer la ligne "Output unified2 : filename snort.log, limit 128" en second lieu.

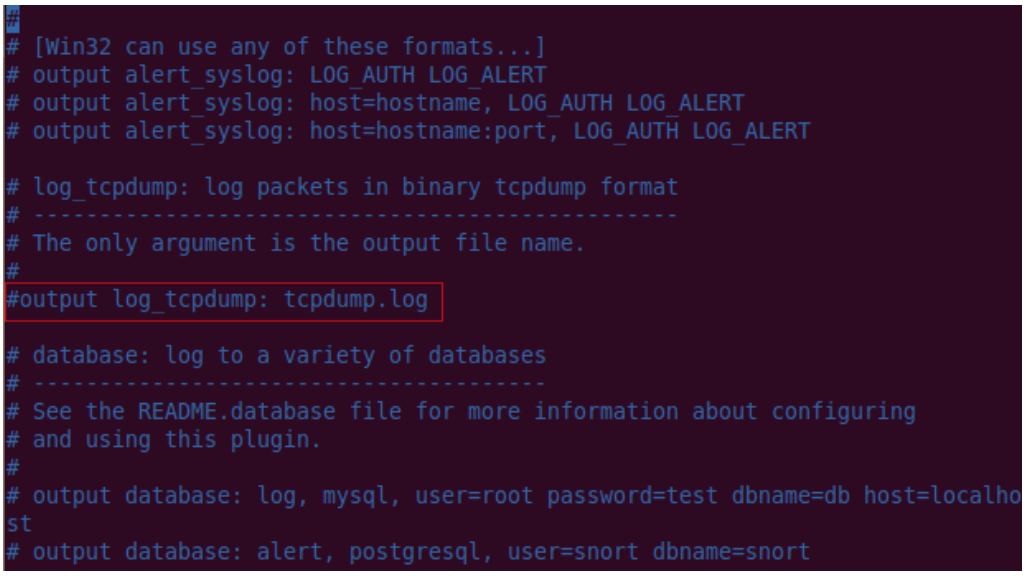


FIGURE 5.6 – modification du format de fichier de sortie

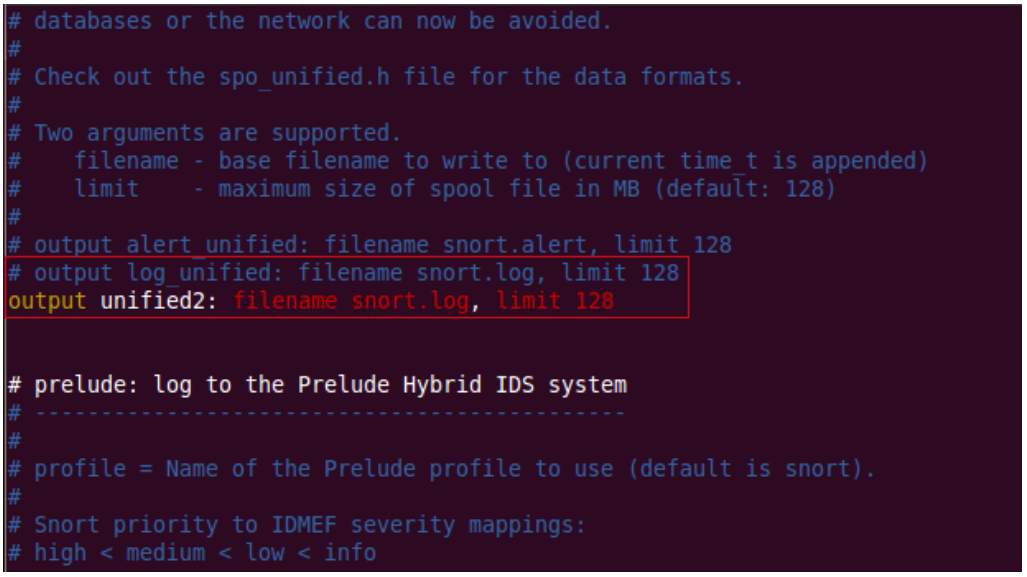


FIGURE 5.7 – spécification du format de fichier de sortie

Après avoir édité le fichier de configuration de snort, nous pouvons à présent s'assurer du bon fonctionnement de ce dernier en exécutant la commande :

```
# sudo snort -c /etc /snort/snort.conf -i eth0
```

```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.5.2 (Build 121)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snor
t-team
           Copyright (C) 1998-2009 Sourcefire, Inc., et al.
           Using PCRE version: 7.8 2008-09-05

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.11  <Build 17>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 3>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 2>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 2>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 8>
           Preprocessor Object: SF_Dynamic_Example_Preprocessor  Version 1.0
 <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 12>
           Preprocessor Object: SF_DCERPC  Version 1.1  <Build 5>
Not Using PCAP_FRAMES
```

FIGURE 5.8 – lancement de "Snort"

5.4 Mise en place de la console BASE

Pour visualiser les différentes alertes remontées par Snort et stockées dans la base de données MySQL, nous devons à présent installer un système d'interface développé en PHP, il s'agit de la console BASE.
La mise en place de BASE nécessite en premier lieu le téléchargement de certains prérequis, que nous allons installer comme suit :

```
# pear install - -alldeps Mail
# pear install - - alldeps Mail_Mime
# aptitude  install php-mail
# aptitude install php-mail-mime
```

Pour mieux organiser nos fichiers d'installation, nous créons le répertoire "snortinstall" pour procéder à l'installation de l'interface BASE :

```
# mkdir snortinstall
# cd  snortinstall
# wget -O base-1.4.5.tar.gz \http://sourceforge.net/projects/secureideas/files/BASE/base-
  1.4.5/base-1.4.5.tar.gz/download
```

Nous devons en second lieu, pour le fonctionnement de BASE installer la bibliothèque ADOdb (Active Data Objects Data Base) en téléchargeant le paquet adodb4991.tgz comme suit :

```
# wget -O adodb4991.tgz \  http://sourceforge.net/projects/adodb/files/adodb-php-4-
   and-5/ \ adodb-4991-for-php/adodb4991.tgz/download
```

A présent, nous devons décompresser les deux paquets téléchargés, puis les copier vers le répertoire /var/www :

```
# cd  /snortinstall
#  tar -xzvf adodb4991.tgz
# tar -xzvf base-1.4.5.tar.gz
# sudo mv adodb /var/www
# sudo mv base-1.4.5 /var/www
```

Une fois les deux fichiers téléchargés et décompressés, nous accédons à présent au fichier "php.ini" pour apporter les modifications nécessaires à PHP en ajoutons les extensions suivantes : Extension=mysql.so et Extension=gd.so

```
# vim  etc/php5/apache2/php.ini
```

```
;;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;;

; If you wish to have an extension loaded automatically, use the following
; syntax:
;   extension=modulename.extension
; For example, on Windows:
;   extension=msql.dll
; ... or under UNIX:
;   extension=msql.so
; ... or with a path:
;   extension=/path/to/extension/msql.so
; If you only provide the name of the extension, PHP will look for it in its
; default extension directory.
extension=mysql.so
extension=gd.so
;;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;;
```

FIGURE 5.9 – configuration du fichier "php.ini"

Nous passons maintenant à la configuration du fichier "apache2.conf", dans le but d'ajouter le nom du serveur associé, dans notre cas il s'agit de "localhost" ;

```
# vim  /etc /apache2/apache2.conf
```

Nous ajoutons alors, la ligne suivante : "servername localhost" :

```
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

#
# Define an access log for VirtualHosts that don't define their own logfile
CustomLog /var/log/apache2/other_vhosts_access.log vhost_combined


# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
Include /etc/apache2/conf.d/

# Include the virtual host configurations:
Include /etc/apache2/sites-enabled/
servername localhost
```

FIGURE 5.10 – configuration du fichier "apache2.conf"

Une fois les modifications apportées, nous allons redémarrer le service apache comme suit :

```
# /etc/init.d/apache2 restrat
```

```
root@ubuntu:/home/amel# sudo /etc/init.d/apache2 restart
 * Restarting web server apache2
 ... waiting                                                    [ OK ]
root@ubuntu:/home/amel#
```

FIGURE 5.11 – redémarrage du service apache

Nous devons à présent compiler et attribuer les droits d'écriture pour BASE :

```
# cd  /var/www

# sudo  ln -s base-1.4.5 ./base

# chmod  a+w  base
```

Pour s'assurer que le serveur Apache2 est en marche, nous introduisons sur le navigateur web l'adresse localhost "127.0.0.1", le résultat figure ci-dessous :

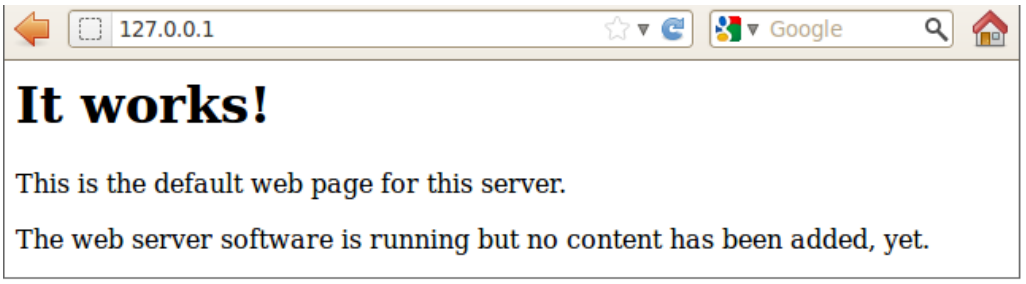


FIGURE 5.12 – vérification du fonctionnement du serveur Apache2

Une fois s'assurer du bon fonctionnement du serveur Apache2, nous pouvons à présent lancer l'assistant et procéder à l'installation de BASE en sélectionnant le dossier BASE sur l'adresse : http ://localhost/base/setup.php.
Nous obtenons la première page de l'assistant qui vérifie que les paramètres nécessaires à la configuration sont mis en place, comme le montre la figure ci-après :

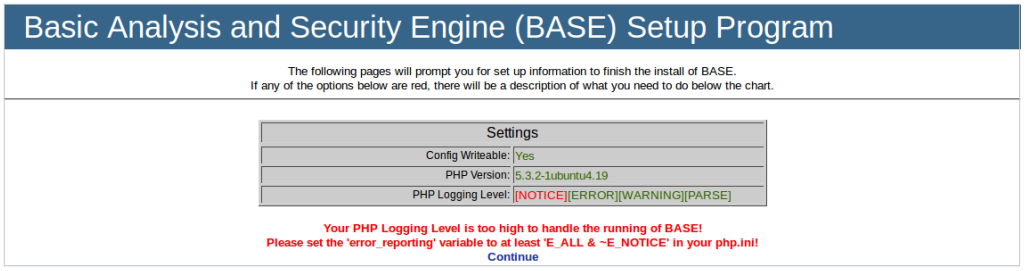


FIGURE 5.13 – configuration de BASE

Ensuite, nous devons choisir le path pour accéder à ADOdb :

FIGURE 5.14 – configuration de base "étape1"

Ensuite, l'assistant nous invite à introduire les paramètres du serveur MySQL dans la configuration :

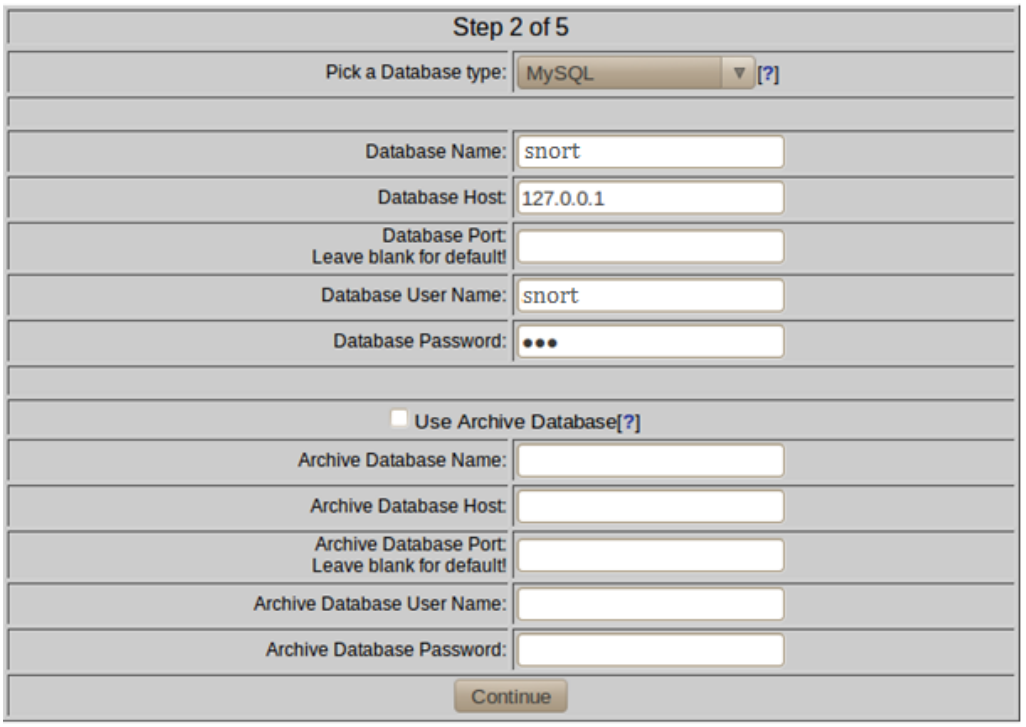


FIGURE 5.15 – configuration de BASE "étape2"

A présent, il faut paramétrer les champs d'authentification pour accéder à la console BASE :

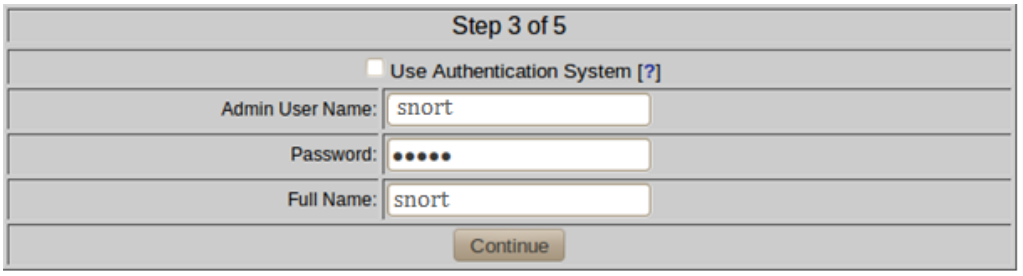


FIGURE 5.16 – configuration de BASE "étape3"

Une fois que les paramètres d'authentification sont mis en place, l'assistant nous demande de créer les tables de la base de données de BASE :

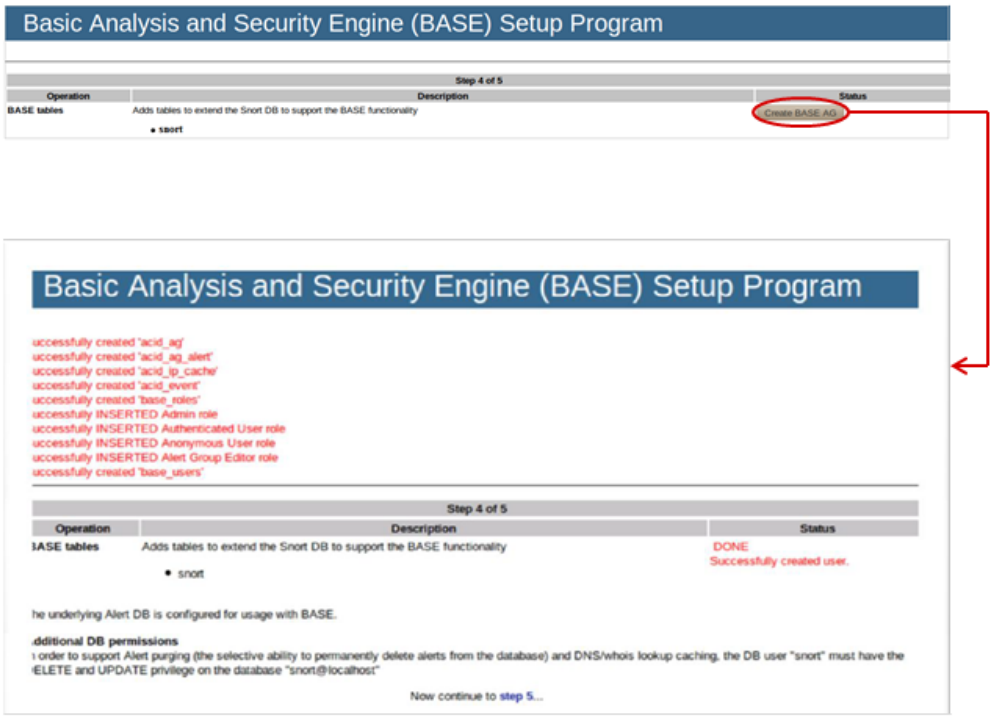


FIGURE 5.17 – configuration de BASE "étape4"

Enfin, une redirection vers la page d'authentification sera proposée afin d'accéder à la console pour superviser les alertes remontées par Snort :

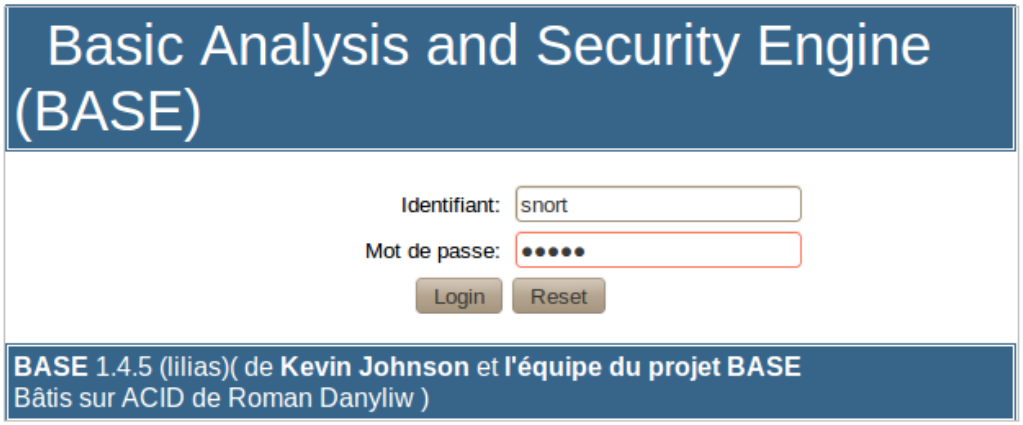


FIGURE 5.18 – configuration de BASE "étape5"

Après l'étape d'authentification, la console BASE sera enfin configurée, nous pouvons désormais accéder à son interface principale, comme le montre la figure suivante :

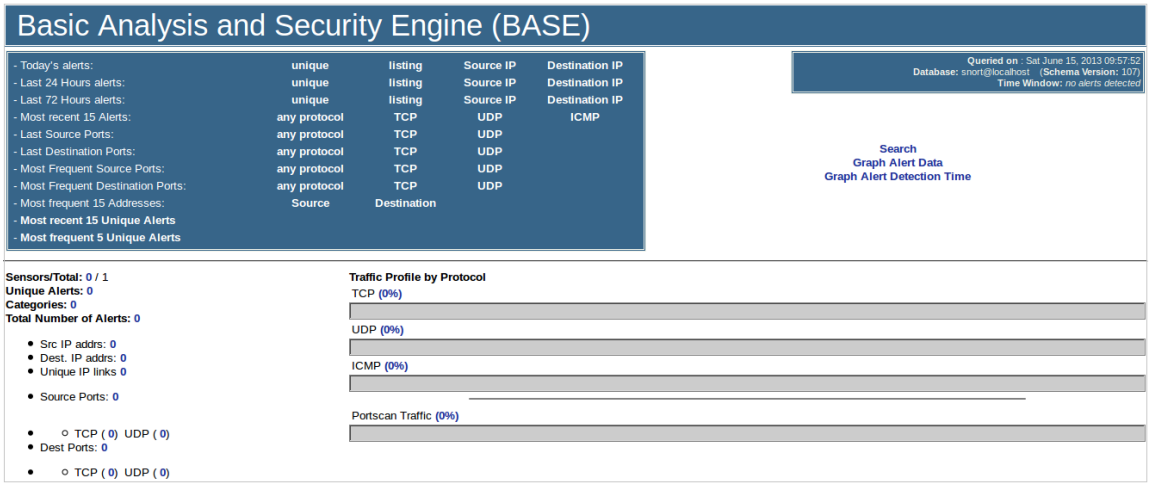


FIGURE 5.19 – l'interface principale de BASE

Enfin, nous devons donner des droits d'écriture et de lecture pour le répertoire "base", en exécutant la commande suivante :

```
# chmod og-w base
```

5.5 Mise en place de Barnyard2

Pour des raisons d'optimisation des ressources, nous procédons à présent à la mise en place de la couche applicative Barnyard2 qui exploite les évènements générés par Snort en format "unified" afin de les inscrire en base de données. Pour ce faire, nous devons tout d'abord télécharger le paquet barnyard2-1.7.tar.gz, puis le décompresser en exécutant les commandes suivantes :

```
# wget  -O barnyard2-1.7.tar.gz \ http://www.securixlive.com/download/ barnyard2/
  barnyard2-1.7.tar.gz
# tar zxvf barnyard2-1.7.tar.gz
```

Ensuite nous accédons au répertoire barnyard2-1.7 pour installer et mettre en place barnyard en exécutant dans le Shell les commandes suivantes :

```
# . /configure –with-mysql
# make
# make install
```

Enfin nous devons copier le fichier de configuration "barnyard2.conf" vers le répertoire snort afin de paramétrer Snort avec barnyard2 :

```
# cp etc/ barnyard2.conf  /etc/snort
```

Une fois terminé, nous devons créer un répertoire où barnyard2 stocke ses logs :

```
# mkdir  /var/log/ barnyard2
```

Pour vérifier l'installation adéquate de barnyard, nous exécutons la commande suivante :

```
# barnyard2 -V
```

```
root@ubuntu:/home/amel# barnyard2 -V

        -*> Barnyard2 <*-
 / ,,_  \  Version 2.1.7 (Build 225)
 |o"  )~|  By the SecurixLive.com Team: http://www.securixlive.com/about.php
 + '''' +  (C) Copyright 2008-2009 SecurixLive.

           Snort by Martin Roesch & The Snort Team: http://www.snort.org/team
.html
           (C) Copyright 1998-2007 Sourcefire Inc., et al.
```

FIGURE 5.20 – vérification de l'installation de Barnyard

Nous devons à présent apporter des modifications sur le fichier de configuration "barnyard2.conf", en ajoutons le nom de l'hôte "localhost" et l'interface "eth0" ainsi que la sortie vers la base de données comme le montre les deux figures ci-contre :

```
# vim barnyard2.conf
```

```
#   Typical options would be:
#     config hostname:  thor
#     config interface: eth0
#     config alert_with_interface_name
#
config hostname: localhost
config interface: eth0

# enable printing of the interface name when alerting.
#
#config alert_with_interface_name
```

```
#   output database: alert, postgresql, user=snort dbname=snort
#   output database: log, odbc, user=snort dbname=snort
#   output database: log, mssql, dbname=snort user=snort password=test
#   output database: log, oracle, dbname=snort user=snort password=test
#
output database: alert, mysql, user=snort password=snortuse dbname=snort host
=localhost
```

FIGURE 5.21 – configuration du fichier barnyard2.conf

Pour synchroniser Snort avec Barnyard nous devons procéder comme suit :

1) Nous créons dans un premier temps, un fichier portant le nom de "barnyard.waldo" dans le répertoire /var/log/snort.
2) Puis dans un deuxième temps, nous récupérons le dernier " timestamp " associé au format particulier des logs de Snort en exécutant la commande suivante :

```
# ls -la  /var/log/snort
```

```
root@ubuntu:/home/amel# ls -la /var/log/snort
total 312
drwxr-s---  2 snort adm    4096 2013-06-12 14:25 .
drwxr-xr-x 18 root  root   4096 2013-06-13 06:04 ..
-rw-r--r--  1 root  adm       0 2013-06-12 14:24 alert
-rw-r--r--  1 root  adm    2056 2013-06-12 02:02 barnyard.waldo
-rw-------  1 root  adm       0 2013-06-11 15:08 snort.log.1370988509
-rw-------  1 root  adm       0 2013-06-11 15:11 snort.log.1370988660
-rw-------  1 root  adm       0 2013-06-11 16:11 snort.log.1370992284
-rw-------  1 root  adm       0 2013-06-11 16:33 snort.log.1370993613
-rw-------  1 root  adm    4910 2013-06-11 16:36 snort.log.1370993647
-rw-------  1 root  adm       0 2013-06-11 17:06 snort.log.1370995574
-rw-------  1 root  adm  148634 2013-06-11 17:12 snort.log.1370995661
-rw-------  1 root  adm  145176 2013-06-12 02:02 snort.log.1371026924
-rw-------  1 root  adm       0 2013-06-12 14:25 snort.log.1371072351
root@ubuntu:/home/amel#
```

FIGURE 5.22 – récupération du dernier "timestamp" des logs de Snort

Ce dernier "timestamp" doit être ajouté dans le fichier "barnyard.waldo" comme l'illustre la figure suivante :

```
# vim /var/log/snort/barnyard.waldo
```

```
/var/log/snort
snort.log
<1273834250>
0
```

FIGURE 5.23 – configuration du fichier "barnyard.waldo"

5.6 mise en œuvre d'une attaque avec Nessus

Pour simuler une attaque, nous allons procéder à un test d'intrusions en faisant appel au scanner de vulnérabilités Nessus contenu dans la distribution professionnel Backtrack. Pour ce faire nous allons à présent configurer Nessus dans Backtrack 5 en suivant l'ensemble des étapes décrites ci-dessous.

5.6.1 Création d'un utilisateur du serveur Nesssus

Dans un premier temps, nous devons créer un nouvel utilisateur. Pour ce faire, Nous allons d'abord lancer le scanner de vulnérabilité Nessus en suivant l'ensemble des étapes illustrées dans la figure ci-contre et en sélectionnant l'option "nessus user add".

FIGURE 5.24 – création d'un nouvel utilisateur Nessus

Le shell de Backtrack s'ouvrira ensuite, où nous devons indiquer le login et le login password ainsi que le login password (again), dans notre cas, notre utilisateur portera le nom de "Nessus".

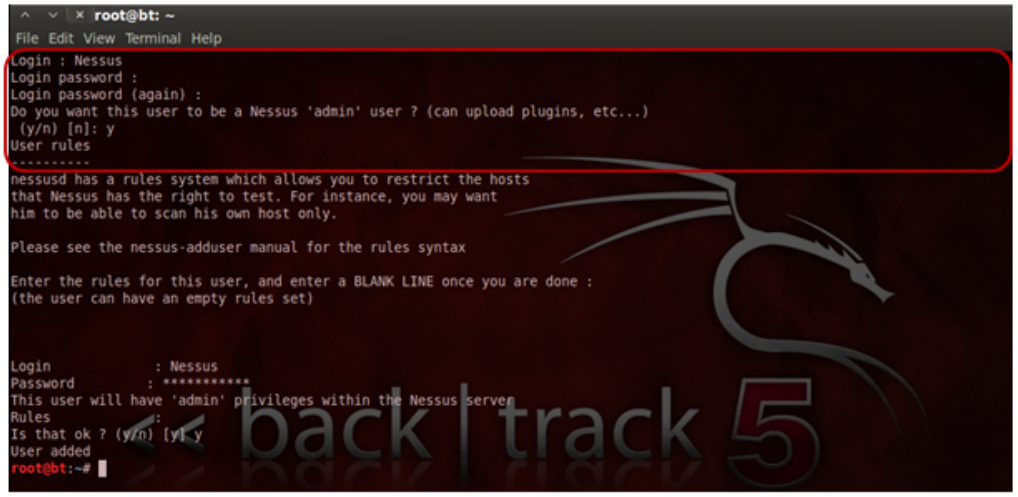


FIGURE 5.25 – définition des paramètres d'authentification de l'utilisateur "Nessus"

5.6.2 Obtention d'une clé d'activation

Afin d'obtenir une clé d'activation, nous lançant Nessus en mode "nessus register".

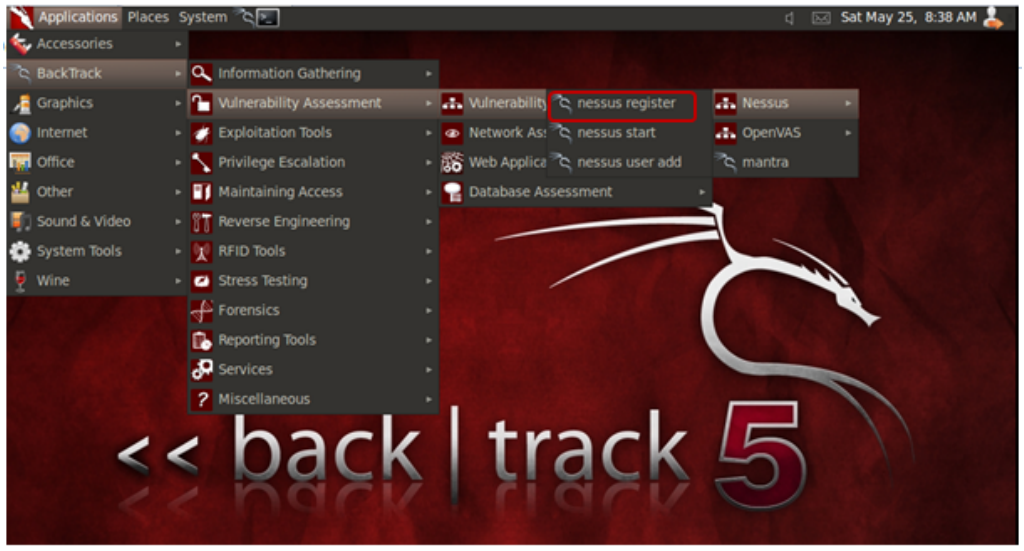


FIGURE 5.26 – obtention d'une clé d'activation pour Nessus

"nessus register" nous redirige ensuite vers le site officiel de nessus "www.nessus.org". Pour obtenir une clé d'activation, nous devons sélectionner "Using Nessus at home" et remplir les champs avec une adresse mail afin de recevoir la clé.

5.6.3 Enregistrement de la clé d'activation

Une fois cette clé obtenue, nous procédons à son enregistrement en utilisant la commande suivante à partir du shell de Backtrack,

```
# cd  /opt/nessus/bin  ./nessus-fetch --register 3FB5-BB1B-7395-9BB0-ACDE
```

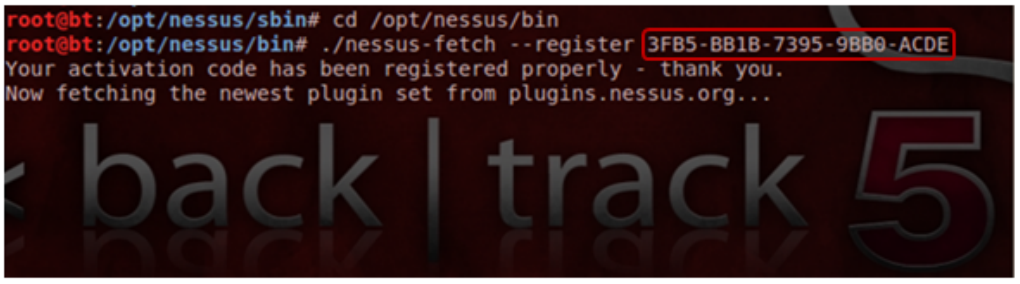


FIGURE 5.27 – enregistrement de la clé d'activation pour Nessus

5.6.4 Démarrage du serveur Nessus

A présent nous pouvons procéder au démarrage du serveur Nessus tout en lançant Nessus en mode "nessus start".

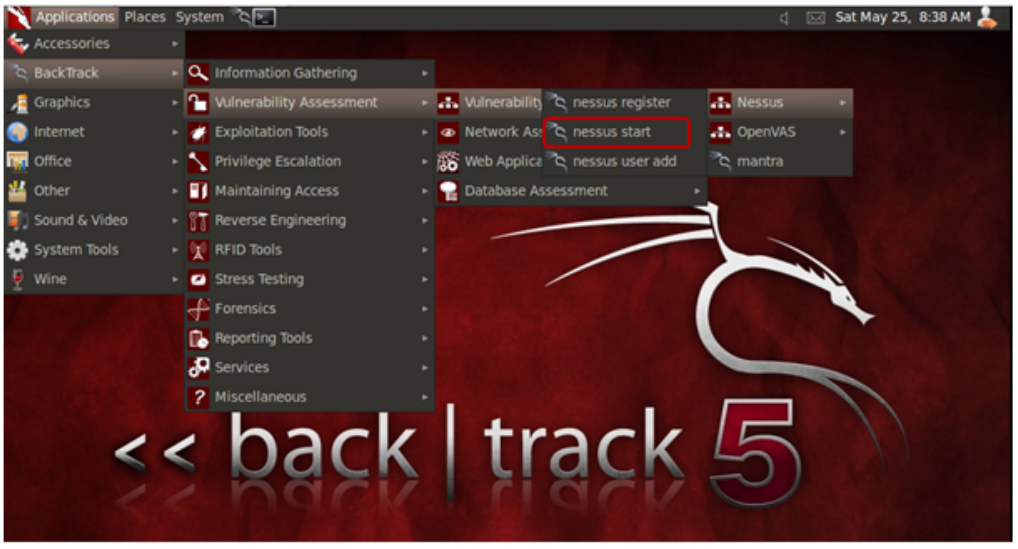


FIGURE 5.28 – démarrage de serveur Nessus

A ce niveau, si nous aurons le résultat illustré à la figure ci-dessous, c'est que Nessus est bien configuré et le serveur Nessus est démarré :

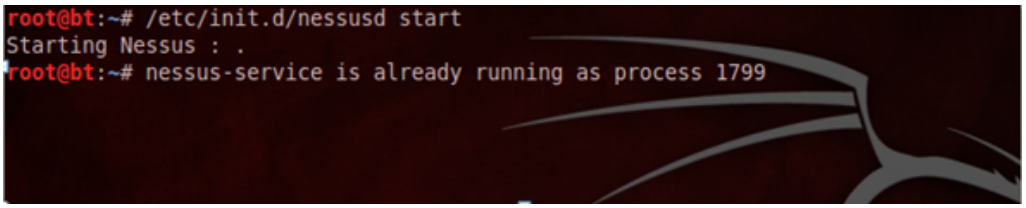


FIGURE 5.29 – lancement du serveur Nessus

Normalement le serveur est en écoute sur le port 8834, pour confirmer le numéro de port, nous utilisons la commande suivante :

```
# netstat -ntpl | grep nessusd
```

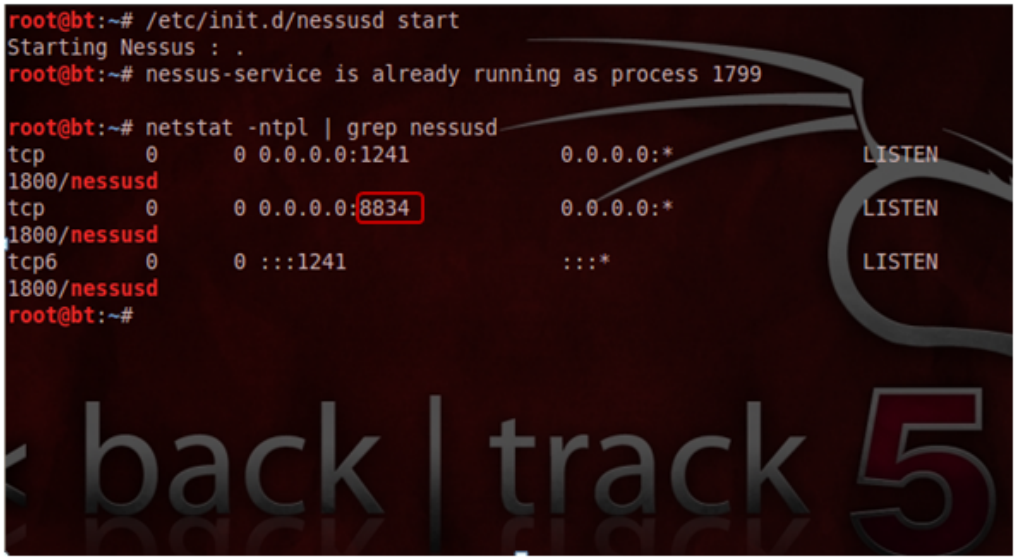


FIGURE 5.30 – vérification du numéro de port d'écoute du serveur Nessus

5.6.5 Lancement du serveur Nessus à partir du navigateur

Pour lancer Nessus, nous ouvrons le navigateur avec l'url https ://127.0.0.1 :8834.

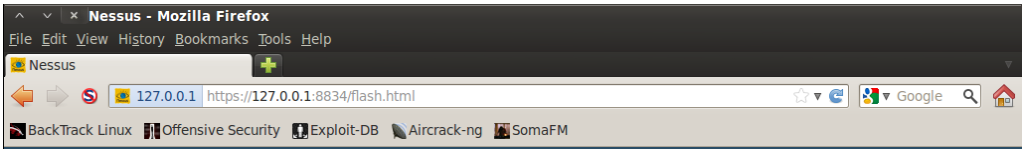


FIGURE 5.31 – Lancement du serveur Nessus à partir du navigateur

Une fenêtre d'authentification de l'utilisateur Nessus s'ouvrira par la suite, où nous devons s'authentifier en utilisant le "login" et "password" définis auparavant.

FIGURE 5.32 – authentification de l'utilisateur Nessus

Après l'authentification, l'utilisateur Nessus sera redirigé vers l'interface principale de Nessus, comme le montre la figure suivante :

FIGURE 5.33 – accès à l'interface principale de Nessus

5.7 lancement d'une attaque par scan de ports contre la machine cible "snort"

Nous allons connecter deux machines, l'une jouera le rôle de l'attaquant et l'autre jouera le rôle de la victime (machine cible).
La machine attaquante utilise BackTrack pour lancer ses différentes attaques vers la machine cible.

La machine cible essayera à son tour de détecter et de stopper les différentes attaques en utilisant le NIDS (snort) que nous avons mis en place.

5.7.1 lancement du NIDS "Snort"

Sur la machine victime, nous devons dans un premier temps lancer "Snort", puis dans un second temps, nous devons lancer barnyard2 dans un autre shell, comme l'ilustre les figures suivantes :

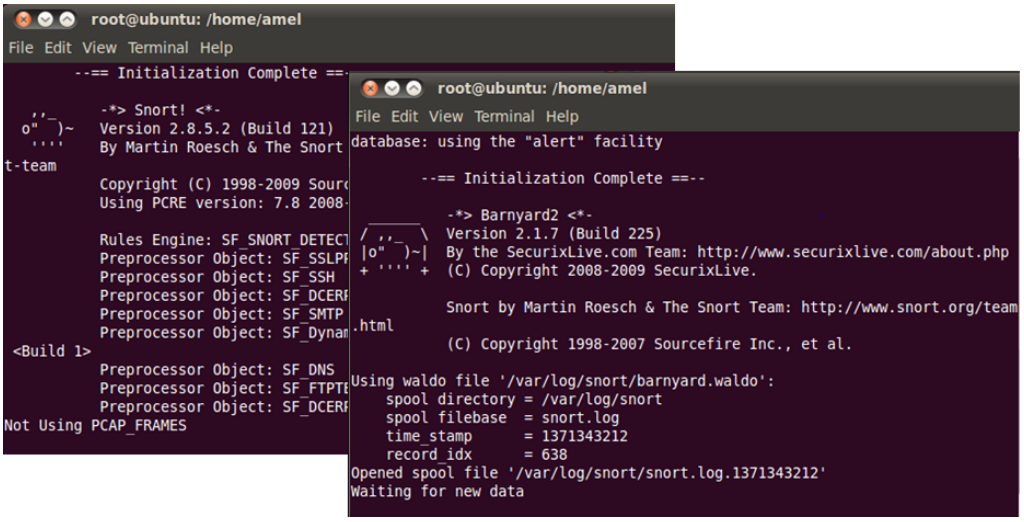


FIGURE 5.34 – lancement de 'Snort' et 'Barnyard2' pour la détection d'intrusions

5.7.2 Scan du réseau avec Nessus

Pour lancer un scan de ports contre notre machine cible où nous avons configuré Snort, nous allons suivre les étapes suivantes :

– cliquez sur l'option Scans ensuite sur add.

– à présent, il faut définir les paramètres du scan, nous allons donner un nom dans le champ "Name", puis choisir dans "Policy "l'emplacement réseau de la cible, dans notre cas il s'agit d'une machine dans le même réseau local, nous choisissons alors l'option "Internal network scan" ainsi que l'adresse IP de cette cible dans "Scan Targets".

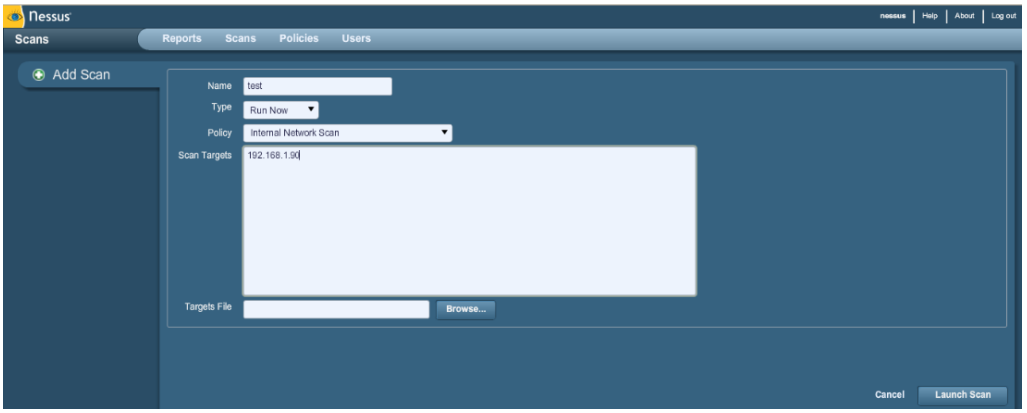


FIGURE 5.35 – lancement d'une attaque vers la machine "snort" avec scan de ports

– Ensuite, il reste qu'à cliquer sur le bouton "Launch Scan" pour lancer le scan de ports de la machine cible qui peut durer quelques minutes.

– En fin, une fois le scan est terminé, nous cliquons sur l'option "Reports" pour visualiser en détail le résultat du scan.

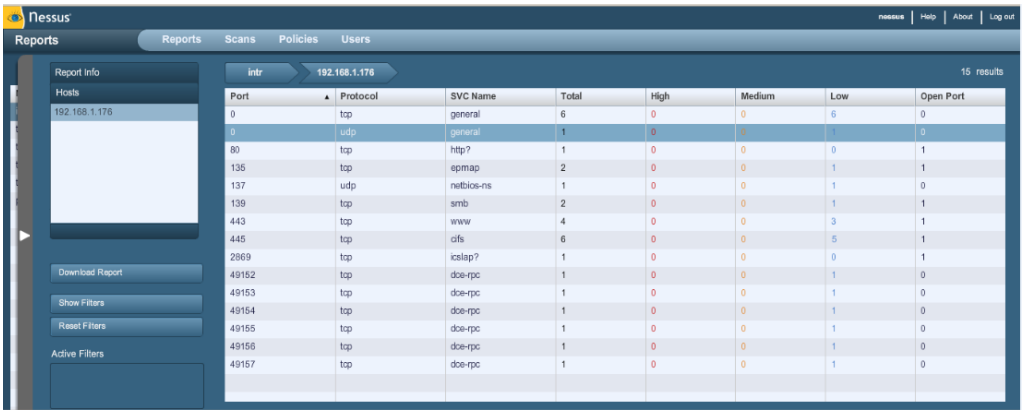
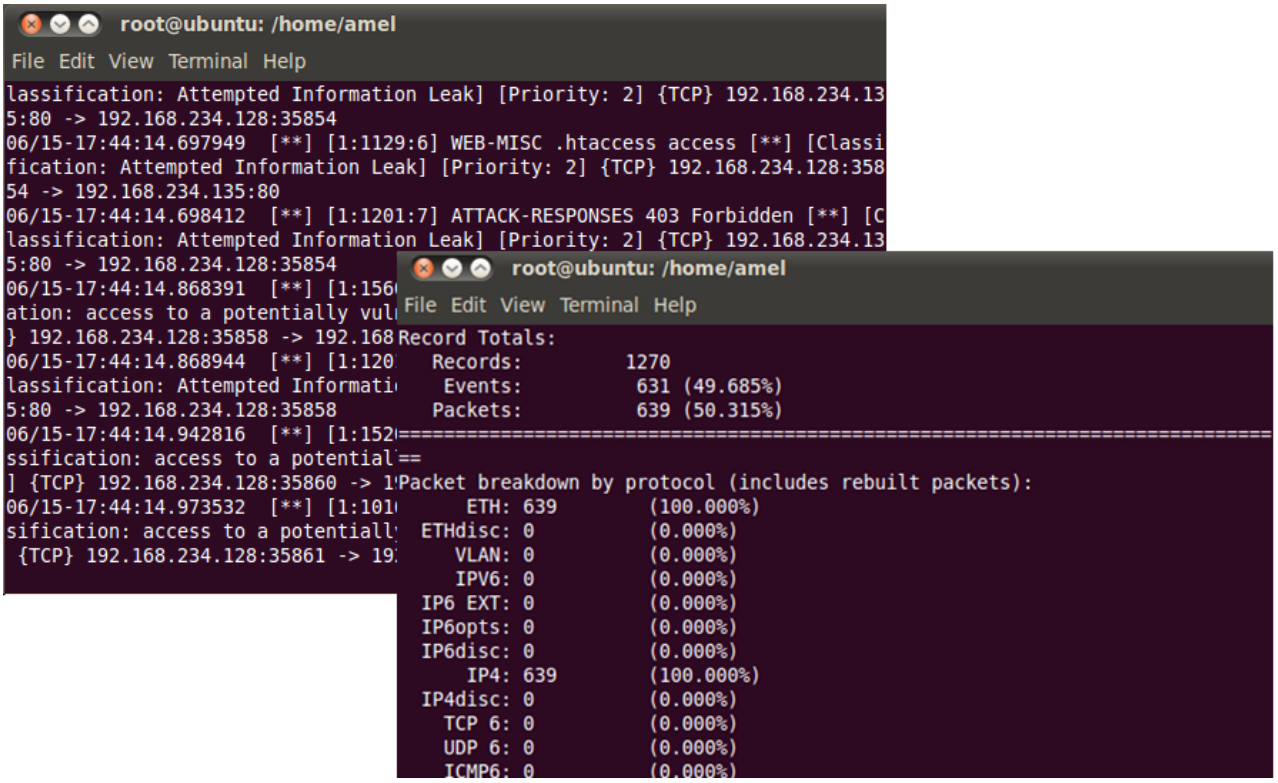


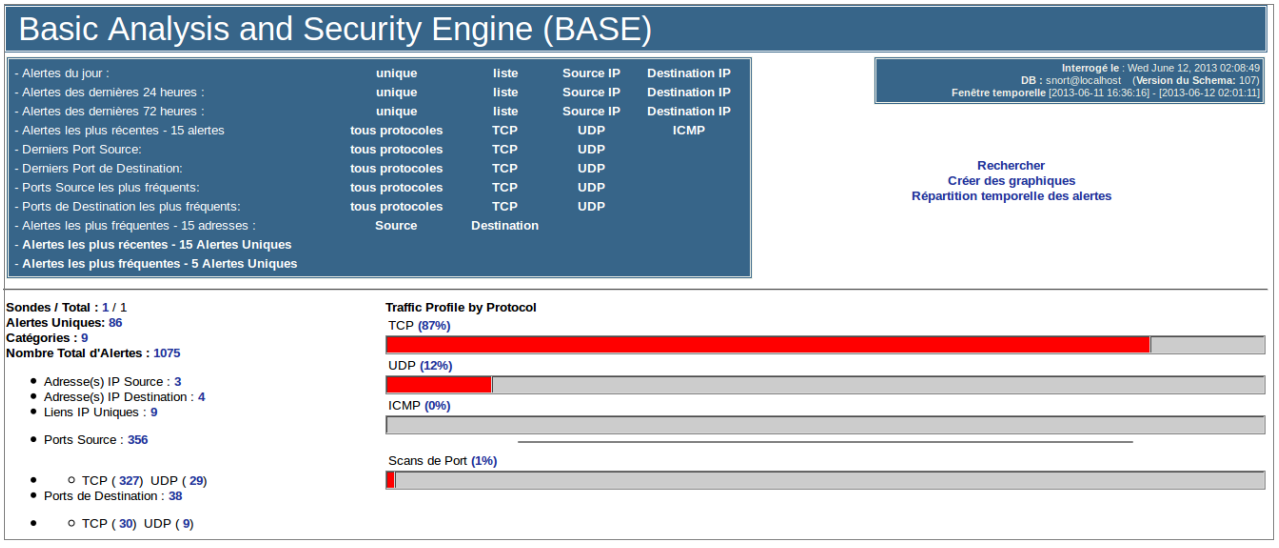
FIGURE 5.36 – résultat du scan de la machine cible "snort"

5.7.3 Détection des alertes par Snort sur BASE

Dans la machine victime, les alertes seront détectées par Barnyard comme le montre la figure suivantes :



Dans la console BASE, les alertes seront remontées comme le montre la figure ci-contre :



Pour visualiser en détails les alertes remontées, notamment, la signature, l'adresse source de menace ainsi que l'horodatage, nous cliquons sur "liste" de la figure précédente.
Le résultat est le suivant :

ID	< Signature >	< Horodatage >	< Adresse Source >	< Adresse Dest. >	< Protocole de niveau 4 >
#0-(1-1072)	[snort] portscan: TCP Portscan	2013-06-12 02:01:11	192.168.234.128	192.168.234.135	Raw IP
#1-(1-1071)	[nessus] [snort] WEB-MISC DB4Web access	2013-06-12 02:01:08	192.168.234.128:54419	192.168.234.135:80	TCP
#2-(1-1064)	[cve] [icat] [bugtraq] [snort] WEB-COLDFUSION administrator access	2013-06-12 02:01:08	192.168.234.128:54408	192.168.234.135:80	TCP
#3-(1-1069)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:08	192.168.234.128:54418	192.168.234.135:80	TCP
#4-(1-1070)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL	2013-06-12 02:01:08	192.168.234.128:54418	192.168.234.135:80	TCP
#5-(1-1066)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL	2013-06-12 02:01:08	192.168.234.128:54410	192.168.234.135:80	TCP
#6-(1-1065)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL	2013-06-12 02:01:08	192.168.234.128:54409	192.168.234.135:80	TCP
#7-(1-1067)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:08	192.168.234.128:54415	192.168.234.135:80	TCP
#8-(1-1068)	[snort] WEB-MISC /etc/passwd	2013-06-12 02:01:08	192.168.234.128:54415	192.168.234.135:80	TCP
#9-(1-1060)	[nessus] [nessus] [cve] [icat] [snort] WEB-MISC viewcode access	2013-06-12 02:01:07	192.168.234.128:54405	192.168.234.135:80	TCP
#10-(1-1058)	[nessus] [cve] [icat] [bugtraq] [bugtraq] [snort] WEB-CGI FormHandler.cgi external site redirection attempt	2013-06-12 02:01:07	192.168.234.128:54402	192.168.234.135:80	TCP
#11-(1-1059)	[nessus] [cve] [icat] [bugtraq] [bugtraq] [snort] WEB-CGI FormHandler.cgi access	2013-06-12 02:01:07	192.168.234.128:54402	192.168.234.135:80	TCP
#12-(1-1063)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL	2013-06-12 02:01:07	192.168.234.128:54407	192.168.234.135:80	TCP
#13-(1-1062)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:07	192.168.234.128:54406	192.168.234.135:80	TCP
#14-(1-1061)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:07	192.168.234.128:54405	192.168.234.135:80	TCP
#15-(1-1052)	[nessus] [snort] WEB-IIS trace.axd access	2013-06-12 02:01:06	192.168.234.128:54377	192.168.234.135:80	TCP
#16-(1-1048)	[nessus] [bugtraq] [snort] WEB-CGI faqmanager.cgi arbitrary file access attempt	2013-06-12 02:01:06	192.168.234.128:54371	192.168.234.135:80	TCP
#17-(1-1047)	[nessus] [bugtraq] [snort] WEB-CGI faqmanager.cgi access	2013-06-12 02:01:06	192.168.234.128:54371	192.168.234.135:80	TCP
#18-(1-1044)	[nessus] [cve] [icat] [bugtraq] [snort] WEB-MISC iPlanet Search directory traversal attempt	2013-06-12 02:01:06	192.168.234.128:54366	192.168.234.135:80	TCP
#19-(1-1043)	[url] [snort] WEB-PHP php.exe access	2013-06-12 02:01:06	192.168.234.128:54365	192.168.234.135:80	TCP
#20-(1-1042)	[cve] [icat] [bugtraq] [snort] WEB-IIS Directory transversal attempt	2013-06-12 02:01:06	192.168.234.128:54364	192.168.234.135:80	TCP
#21-(1-1041)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:06	192.168.234.128:54364	192.168.234.135:80	TCP
#22-(1-1055)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL	2013-06-12 02:01:06	192.168.234.128:54382	192.168.234.135:80	TCP
#23-(1-1053)	[nessus] [nessus] [cve] [icat] [snort] WEB-IIS global.asa access	2013-06-12 02:01:06	192.168.234.128:54378	192.168.234.135:80	TCP
#24-(1-1056)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:06	192.168.234.128:54396	192.168.234.135:80	TCP
#25-(1-1054)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:06	192.168.234.128:54382	192.168.234.135:80	TCP
#26-(1-1051)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:06	192.168.234.128:54375	192.168.234.135:80	TCP
#27-(1-1050)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:06	192.168.234.128:54374	192.168.234.135:80	TCP
#28-(1-1045)	[arachnids] [snort] WEB-MISC http directory traversal	2013-06-12 02:01:06	192.168.234.128:54366	192.168.234.135:80	TCP

ID	< Signature >
#0-(1-1072)	[snort] portscan: TCP Portscan
#1-(1-1071)	[nessus] [snort] WEB-MISC DB4Web access
#2-(1-1064)	[cve] [icat] [bugtraq] [snort] WEB-COLDFUSION administrator access
#3-(1-1069)	[arachnids] [snort] WEB-MISC http directory traversal
#4-(1-1070)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL
#5-(1-1066)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL
#6-(1-1065)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL
#7-(1-1067)	[arachnids] [snort] WEB-MISC http directory traversal
#8-(1-1068)	[snort] WEB-MISC /etc/passwd
#9-(1-1060)	[nessus] [nessus] [cve] [icat] [snort] WEB-MISC viewcode access
#10-(1-1058)	[nessus] [cve] [icat] [bugtraq] [bugtraq] [snort] WEB-CGI FormHandler.cgi external site redirection attempt
#11-(1-1059)	[nessus] [cve] [icat] [bugtraq] [bugtraq] [snort] WEB-CGI FormHandler.cgi access
#12-(1-1063)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL
#13-(1-1062)	[arachnids] [snort] WEB-MISC http directory traversal
#14-(1-1061)	[arachnids] [snort] WEB-MISC http directory traversal
#15-(1-1052)	[nessus] [snort] WEB-IIS trace.axd access
#16-(1-1048)	[nessus] [bugtraq] [snort] WEB-CGI faqmanager.cgi arbitrary file access attempt
#17-(1-1047)	[nessus] [bugtraq] [snort] WEB-CGI faqmanager.cgi access
#18-(1-1044)	[nessus] [cve] [icat] [bugtraq] [snort] WEB-MISC iPlanet Search directory traversal attempt
#19-(1-1043)	[url] [snort] WEB-PHP php.exe access
#20-(1-1042)	[cve] [icat] [bugtraq] [snort] WEB-IIS Directory transversal attempt
#21-(1-1041)	[arachnids] [snort] WEB-MISC http directory traversal
#22-(1-1055)	[snort] http_inspect: WEBROOT DIRECTORY TRAVERSAL
#23-(1-1053)	[nessus] [nessus] [cve] [icat] [snort] WEB-IIS global.asa access
#24-(1-1056)	[arachnids] [snort] WEB-MISC http directory traversal
#25-(1-1054)	[arachnids] [snort] WEB-MISC http directory traversal
#26-(1-1051)	[arachnids] [snort] WEB-MISC http directory traversal
#27-(1-1050)	[arachnids] [snort] WEB-MISC http directory traversal
#28-(1-1045)	[arachnids] [snort] WEB-MISC http directory traversal

5.8 conclusion

Nous avons au cours de ce chapitre définis une politique de sécurité pour le réseau de la SONATRACH DP qui permet de remédier aux différents problèmes et failles de sécurité constatées lors de la phase d'audit, nous avons choisis par la suite d'appliquer l'une des solutions proposées, il s'agit de la mise en place du NIDS Snort pour la détection et la prévention de toute intrusion qui peut atteindre et compromettre le réseau de l'entreprise. Enfin, pour tester notre produit, nous avons procédé à un test d'intrusions avec le scanner de vulnérabilités Nessus pour simuler une attaque et confirmer ainsi le bon fonctionnement de Snort.

CONCLUSION GÉNÉRALE

Dans ce travail, notre motivation fût essentiellement la mise en place d'une démarche d'audit, suivi de la définition d'une politique de sécurité pour le réseau de la SONATRACH DP, dans le but de cerner une réalité de fonctionnement de ce dernier, permettant ainsi de dégager les différentes vulnérabilités et faiblesses de celui-ci, pour en fin faire des recommandations afin d'améliorer la cohérence et la crédibilité de l'ensemble de la démarche.

Notre travail a commencé en premier lieu par une présentation de l'organisme d'accueil, afin de prendre connaissance de l'entreprise ainsi que de son environnement et l'architecture de son réseau.

Notre intérêt s'est porté par la suite sur la présentation des différents aspects liés à la sécurité des réseaux informatiques, à savoir le concept d'une politique de sécurité, ainsi que les différentes attaques existantes et leurs contre-mesures de sécurité.

Nous avons ainsi établi un processus d'audit de sécurité pour le réseau de la SONATRACH DP. Ce qui nous a permis, grâce à la démarche adoptée d'évaluer le niveau de Vulnérabilité sur ce réseau. Les résultats de notre audit permettront de consolider le niveau de sécurité sur le réseau informatique de l'organisation.

Une fois la démarche d'audit est appliquée sur le réseau de l'entreprise, nous avons ensuite présenté les systèmes de détection d'intrusions ainsi que l'environnement de notre travail.

Nous avons finalement défini une politique de sécurité et avons mis en place le NIDS Snort pour apporter une amélioration au réseau de l'entreprise et ce, dans le but de renforcer sa sécurité.

Ce travail nous a permis d'avoir une visibilité concrète sur un domaine, combien important !, qui est la sécurité informatique.

Il est clair que le stage effectué au sein de la SONATRACH DP a été très bénéfique quant à l'application de nos connaissances scientifiques et le jumelage de la théorie à la pratique.

Bibliographie

[1] A.NAIT SALEM, conception d'un protocole MAC pour la communication entre un réseau de capteur sans fil et un satellite LEO, Thèse doctorat, université A. Mira de Bejaia, mai 2008.

[2] S.Faye, Contrôle du trafic routier urbain par un réseau fixe de capteurs sans fil Sébastien Faye, Mars 2012.

[3] M.AISSANI. Optimisation du routeréseau de capteurs applications temps,Thèse en cotutelle, mars 2011.

[4] www.meas-spec.fr/sensor-types/traffic-sensors.html.

[5] M.DIOURI. Réseaux de capteurs sans fil : routage et sécurité, Thèse d'ingénieur, 2010.

[6] N. Nadim. Conception et modélisation d'un émulateur de réseaux de capteurs sans fils, Doctorat de l'université de toulouse,2012.

[7] Sciences de l'ingénieur, Les capteurs de position, NB2010.

[8] K.BEYDOUN. Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs, 2009.

[9] A.MELKI, système d'aide à la régulation et évaluation des transport multimodaux integrant les cybercars, Novembre 2008.

[10] G.Chalhoub.Routage et MAC dans les réseaux de capteurs sans fil, 8 novembre 2010.

[11] Systèmes de transport intelligents Une tentative de synthèse.

[12] A.BOUDJAADAR .Plateforme basée agents pour l'aide à la conception et la simulation des réseaux de Capteurs Sans Fil, 2010.

[13] H. Karl, A. Willig. Protocols and architectures for wireless sensor networks. Wiley, 2005.

[14] S.Sentilles. Architecture logicielle pour capteurs sans-fil en réseau,2009.

[15] Adaptation méta heuristique efficace pour le routage dans les réseaux de capteurs sans fil.

[16] F. Doetzer, F. Kohlmayer, T. Kosch and M. Strassberger, Secure communication for intersection assistance. In Proc. of the 2nd Int. Workshop on Intelligent Transportation, Hamburg, Germany, March 2005.

[17] http ://road-network-operations.piarc.org/index.php ?option=com_content&task=view&id=39&Itemid=71&lang=fr.

[18] A.Friedrich, T. Ma, F.Ramond et M.Rohani , Compléments à la présentation, PWP sur les ITS, 2005.

[19] http ://www.rapibus.sto.ca/index.php ?id=53.

[20] http ://www.developpement-durable.gouv.fr/Systemes-de-transport-intelligents,12596.html.

[21] OECD SCIENCE. Technology and industry, OUTLOOK 2012 © OECD.

[22] Province du Nouveau-Brunswick Case postale 6000 Fredericton (N.-B.) E3B 5H1, Plan stratégique 2008-2018 du Nouveau-Brunswick sur les systèmes de transport intelligents (STI).

[23] http ://road-network operations.piarc.org/index.php ?option=com_content&task =view&id=46&Itemid=71&lang=fr.

[24] http ://road-network-operations.piarc.org/index.php ?option=com_content&task =view&id=42&Itemid=71&lang=fr.

[25] BROCHURE Direction Générale des Infrastructures, des Transports et de la Mer, Les systèmes de transport intelligents (STI) en France, Juin 2011.

[26] http ://www.transport-intelligent.net/acteurs-politiques-sti/politiques-sti/.

[27] http ://www.transcore.com/pdf/Systemes-de-transport-intelligents.pdf.

[28] P.LUC et G.GIRARD, Communication inter-véhicules et route-a-véhicule Apprentissage de la communication inter-véhicules,

[29] C.Buisson,Jean, B.Lesort. Comprendre le trafic routier méthodes et calculs, avril 2010.

[30] J.ABDO. Construire de nouvelles infrastructures routières La solution à la congestion du trafic ? Par le Centre d'information sur le ciment et ses applications (CIMbéton), Décembre2011.

[31] Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques .Les temps de parcours Estimation, diffusion et approche multimodale, Éditions du Certu, GAO-12-308P, Avril2008.

[32] GAO-12-308 Intelligent Transportation Systems .Improved DOT Collaboration and Communication Could Enhance the Use of Technology to Manage Congestion, mars 2012.

[33] F.YAN. Contribution à la modélisation et à la régulation du trafic aux intersections : Intégration des communications Véhicule-Infrastructure, Mars 2012.

[34] A.Goel, S. Ray et N.Chandra.Intelligent traffic light system to prioritized emergency purpose vehicles based on wireless sensor network, February 2012.

[35] M.KAFI, Y. CHALLAL, D. DJENOURI, A.BOUABDALLAH et L.BADACHE, . A study of Wireless Sensor Network Architectures and Projects for Traffic Light Monitoring, 2012.

[36] M.Halbwachs. Des outils de gestion du trafic des feux de signalisation en particulier, 2000.

[37] http ://domotique34.com/ ?p=2987.

[38] O.Ait Said et L.Iberraken. Aménagement d'un carrefour par des feux de signalisation. Mémoire d'ingénieur, département Recherche Opérationnelle, Université A/Mira Bejaia, 1999.

[39] Modèle de file d'attente.

[40] S. de Montigny et S. Le Digabel. Introduction aux files d'attente, Ecole Polytechnique de Montréal, A2012 (v2).

[41] C.Chabriac, Processus stochastique et modélisation, Université de Toulouse, 2013.

[42] V.Phuc Do, Théorie des files d'attente, AFSF-SIE/TELECOM Nancy, 2013.

[43] I. Alioua et A.Djouder. Gestion de trac urbain à base de réseau de capteurs sans Fil : Cas de la ville de Bejaia, université A. Mira de Bejaia, 2012.

[44] L. BOUALLOUCHE-MEDJKOUNE. Modélisation et simulation des systèmes informatiques et réseaux de télécommunications, Cours Ecole Doctorale Informatique ReSyD, Département Informatique, Université de Bejaïa, 2009.

[45] http ://www.mplogic.com/gfa/index.html.

[46] A. Casadevall. introduction à MATLAB, université Paris-Dauphine, mars2004.

[47] http ://www.q-matic.com/fr-BE/be/Nos-prestations/File-dattente-lineaire/.

[48] H.Karvonen. Different aspects of trust in ubiquitous intelligent transportation systems, 2010.

[49] http ://www.lefigaro.fr/conso/2013/01/02/05007-20130102ARTFIG00455-une-appli-mobile-pour-eviter-les-longues-files-d-attente.php

[50] Razvan Stanica. Contrôle de Congestion dans les Réseaux Véhiculaires Congestion Control in Vehicular Ad-Hoc Networks, Novembre 2011.

[51] S. Faye , C.Chaudet et Is. Demeure.A Distributed algorithm for multiple intersections adaptive traffic lights control using a wireless sensor networks.

[52] B. Zhou, J. Cao, X. Zeng, and H. Wu. Adaptive traffic light control in wireless sensor network-based intelligent transportation system. In Vehicular Technology Conference Fall (VTC 2010-Fall), pages 1-5.

[53] F. Zou, B. Yang, and Y. Cao. Traffic light control for a single intersection based on wireless sensor network. In 9th International Conference on Electronic Measurement Instruments (ICEMI 2009), pages 1-1040, 2009.

Résumé

L'audit d'un système d'information est indispensable pour toute organisation qui décide de Changements au sein de son système d'information ou de s'assurer de son fonctionnement optimal. Comme toute démarche, l'audit nécessite une méthodologie rigoureuse et une communication idéale au sein de l'entreprise. Ce mémoire s'intéresse au cas de l'organisation SONATRACH "Division Production", qui désire définir une politique de sécurité pour son réseau. A travers l'audit, elle désire connaître les points faibles de son réseau et les résoudre pour une meilleure sécurité.

D'autre part, suite à notre étude sur la sécurité des réseaux informatiques ainsi que les différentes menaces auxquelles les réseaux d'entreprises sont exposés, on se rend compte qu'il n'est pas évident d'assurer une sécurité optimale à un réseau informatique et de le protéger contre d'éventuelles intrusions et menaces.

L'évolution des outils de violation de sécurité qui permettent de monter un nombre très important attaques et intrusions sur les réseaux a fait ses preuves ses dernières années, ce qui représente un véritable danger pour les réseaux d'entreprises. Avoir un réseau complétement sécurisé est concrètement irréalisable. Par conséquent, il est nécessaire de pouvoir détecter les actions malveillantes lorsqu'elles se produisent. Cela est rendu possible grâce aux mécanismes de détection d'intrusions. La détection d'intrusions consiste en la découverte d'utilisation d'un système informatique à des fins non légales. SNORT s'est imposé comme le système de détection d'intrusions le plus performant et utilisé, il est capable d'effectuer une analyse du trafic réseau en temps réel et détecter ainsi de nombreux types d'attaques.

Mot clés : Audit, Sécurité, Politique de sécurité, Attaques, Détection, Intrusion ,Snort.

Abstract

An audit of an information system is essential for any organization that wants to ensure its optimal functioning process. This thesis is interested in the case of the organization Sonatrach "Production Division" who wishes to define a security policy for its network throughout an audit allowing detection of it weaknesses and thus set areas of improvement for better security.

The evolution of tools which allow breach of security to climb (cast on) attacks and intrusions on the networks has proven itself those recent years, Having a fully secured network is concretely impossible. Accordingly it is necessary to be able to detect malicious actions. This is made possible thanks to the mechanisms of intrusions detection.

Intrusion detection is the discovery of the use of a computer system for non-legal. The SNORT has established itself as the most used and best performing system for detecting intrusions, it is able to perform an analysis of the network traffic in real time and thus detect many types of attacks.

Key words : Audit, Security, security policy, attacks, Détection, Intrusion ,Snort.