CHAPITRE 5 : EXPLOITATION ET TESTS

Dans ce chapitre, nous parlerons en premier lieu de la conformité de nos rapports d'audit par rapport aux normes et standards internationaux et d'autre part faire des tests comme des attaques sur notre réseau interne pour montrer la fiabilité de notre solution.

5.1 Conformité de standard (ISO27001)

La norme ISO 27001 définit les exigences de sécurité d'un système de management de la sécurité d'une entreprise. Elle propose un modèle pour établir, implémenter, exploiter, surveiller, maintenir et améliorer le système de management de la sécurité de l'information(SMSI). La norme 27001se focalise sur l'implémentation d'un système de management de la sécurité basé sur une structure formalisée et des contrôles à effectuer. Elle se base sur le modèle PDCA(Plan-Do-Check-Act) qui signifie Planifier-Développer-Vérifier-Réagir) et chacune de ces étapes entraine l'autre au niveau de la solution Ossim, plusieurs normes ou standards ont été définies dont ISO27001 pour permettre à l'entreprise de se passer du travail fastidieux effectuer par les auditeurs, il génère tous les rapports de l'état du SI en fonction des standards.

La figure suivante montre comment activer ces fonctions pour qu'ils puissent générer ces rapports en fonction de la norme 27001.

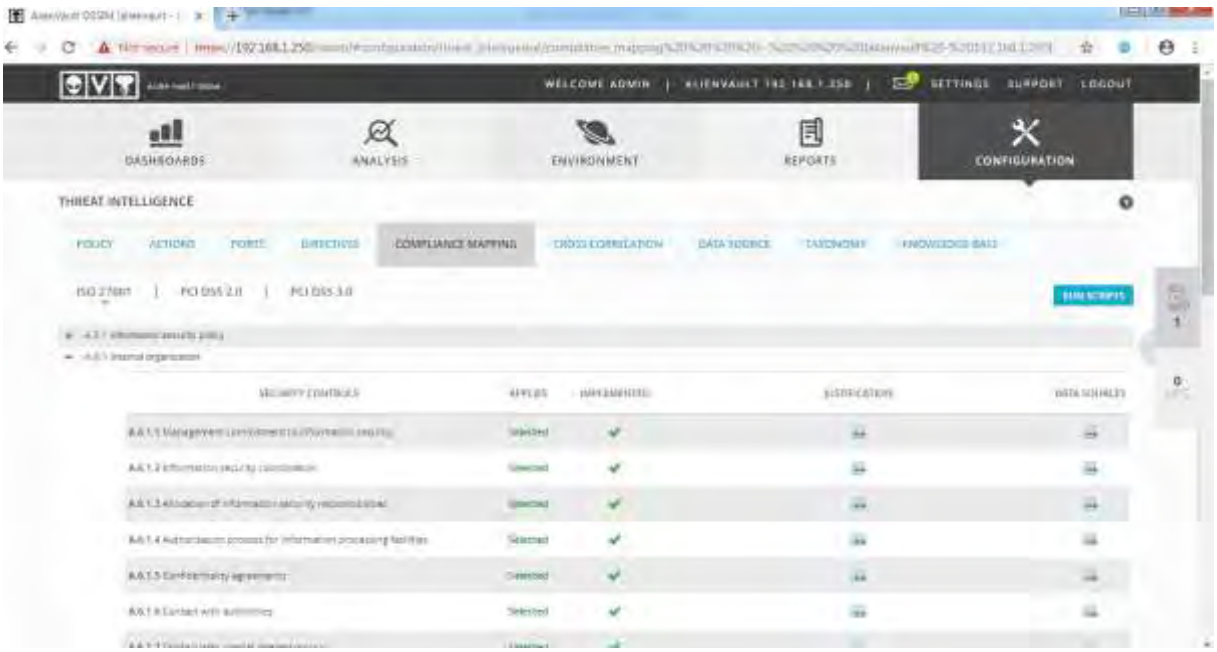


Figure 24 Conformité de OSSIM par rapport à ISO27001

Ci-dessous une partie du rapport concernant notre machine cliente ayant comme adresse **192.168.1.250,** nous allons procéder comme suit :

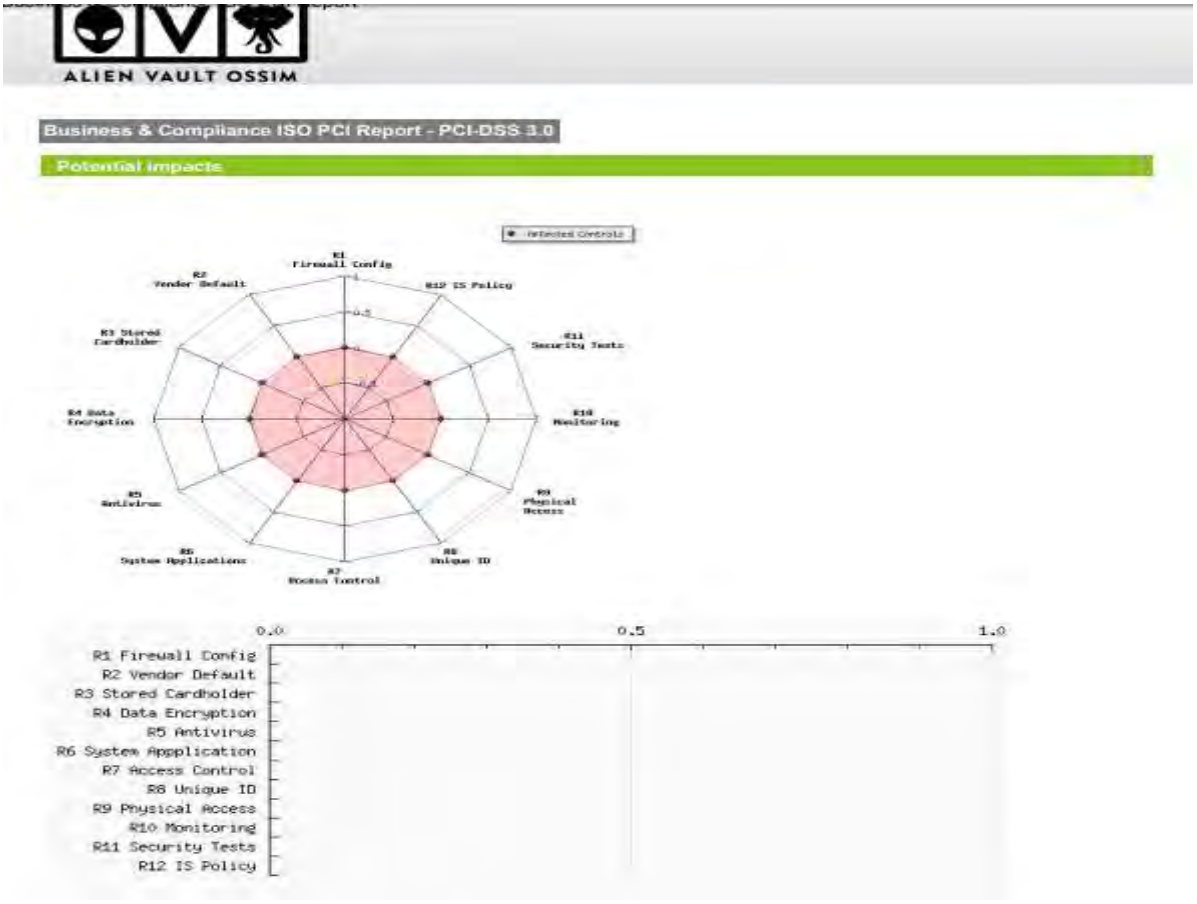


Figure 25 Rapport de conformité

5.2 Test de scan de vulnérabilités : OPENVAS

Openvas est un outil de sécurité informatique qui permet de faire un audit d'une machine ou d'un réseau entier. Openvas est sans doute le logiciel phare dans la catégorie des scanners de vulnérabilité et ce dernier est un dérivé de Nessus. Sur notre plateforme OSSIM, on fera des scans de vulnérabilité sur deux machines de notre réseau.

Machine:

- Systéme d'exploitation: Windows 10
- Adresse IP : 192.168.1.141

Sur cette figure, on voit les résultats de scans sur notre machine Windows.

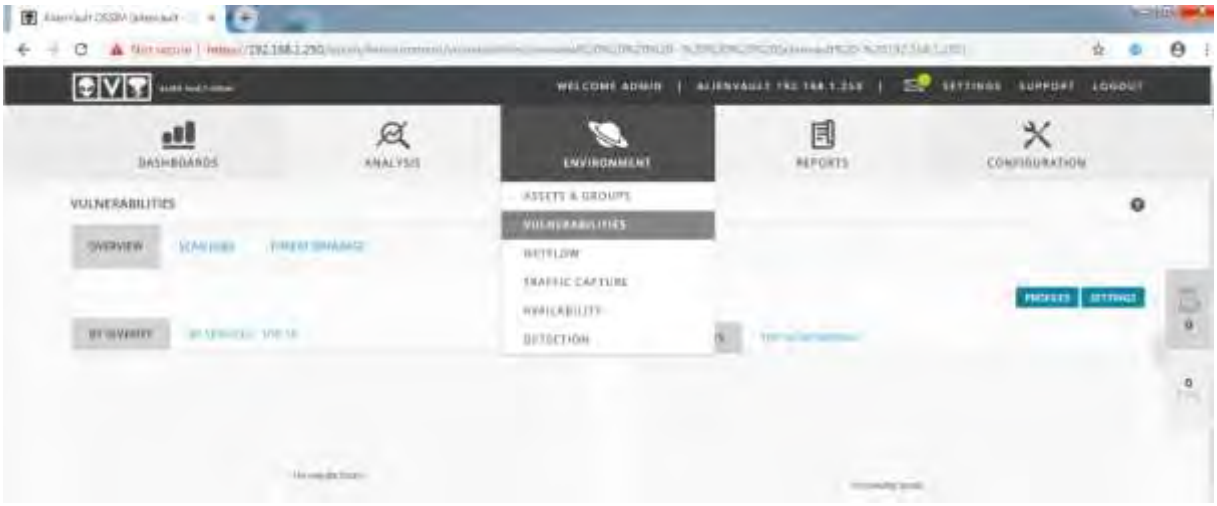
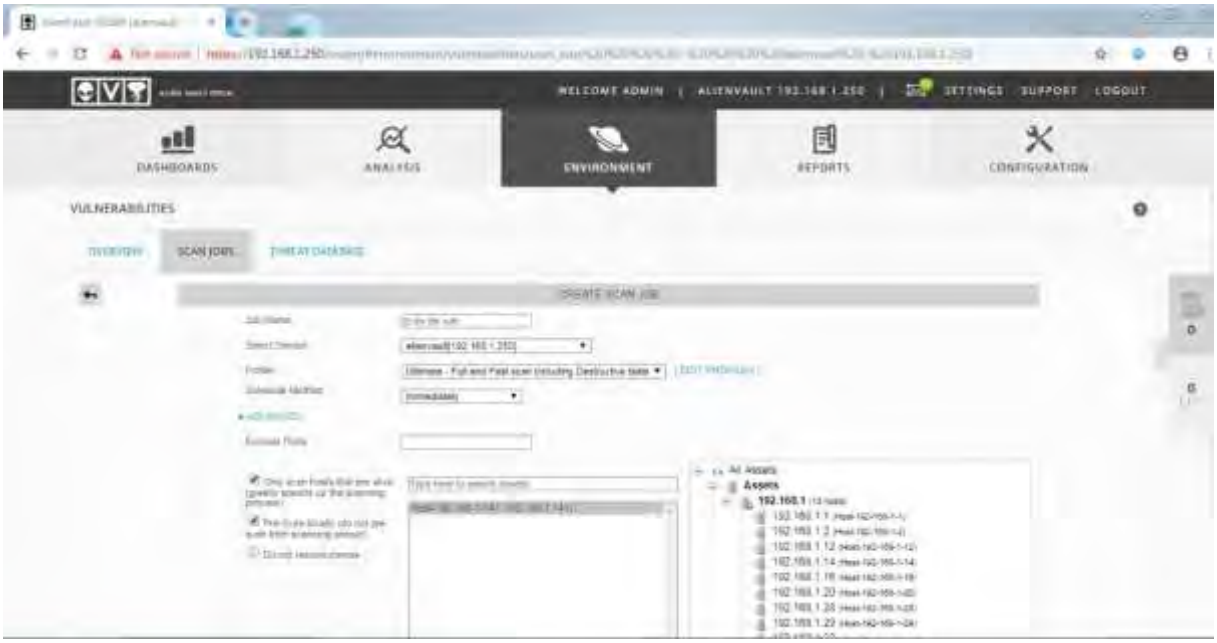
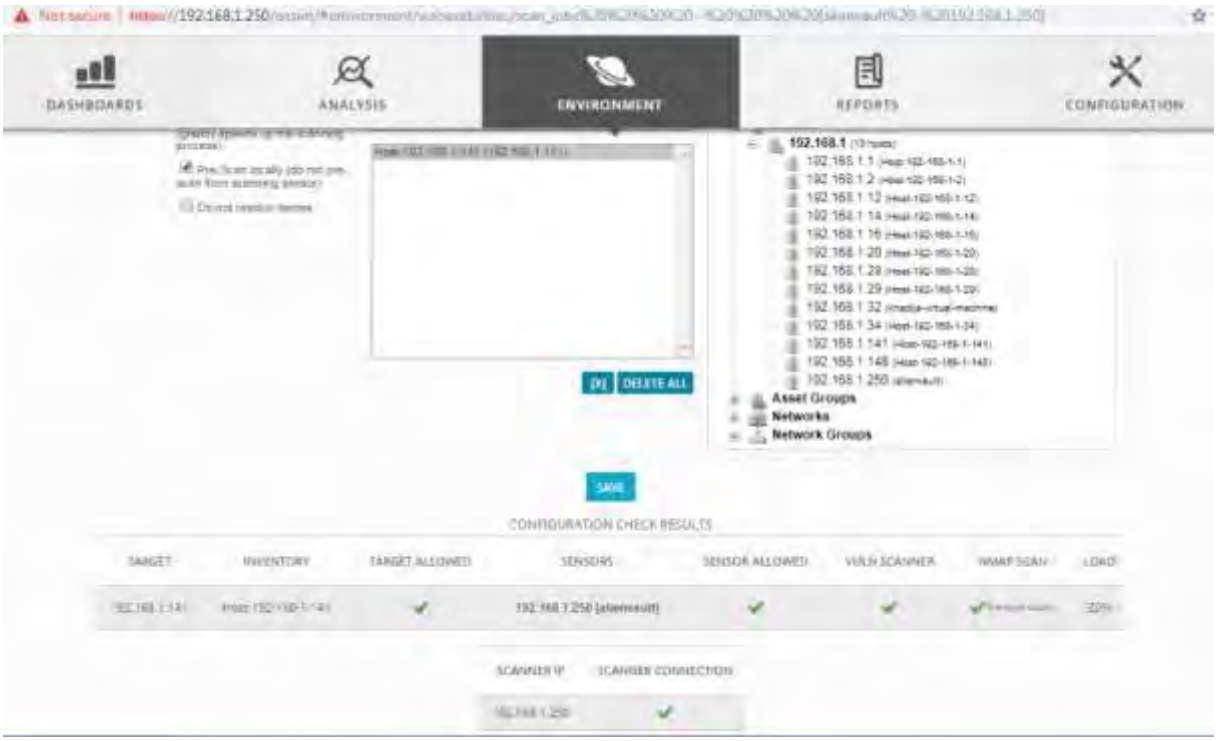


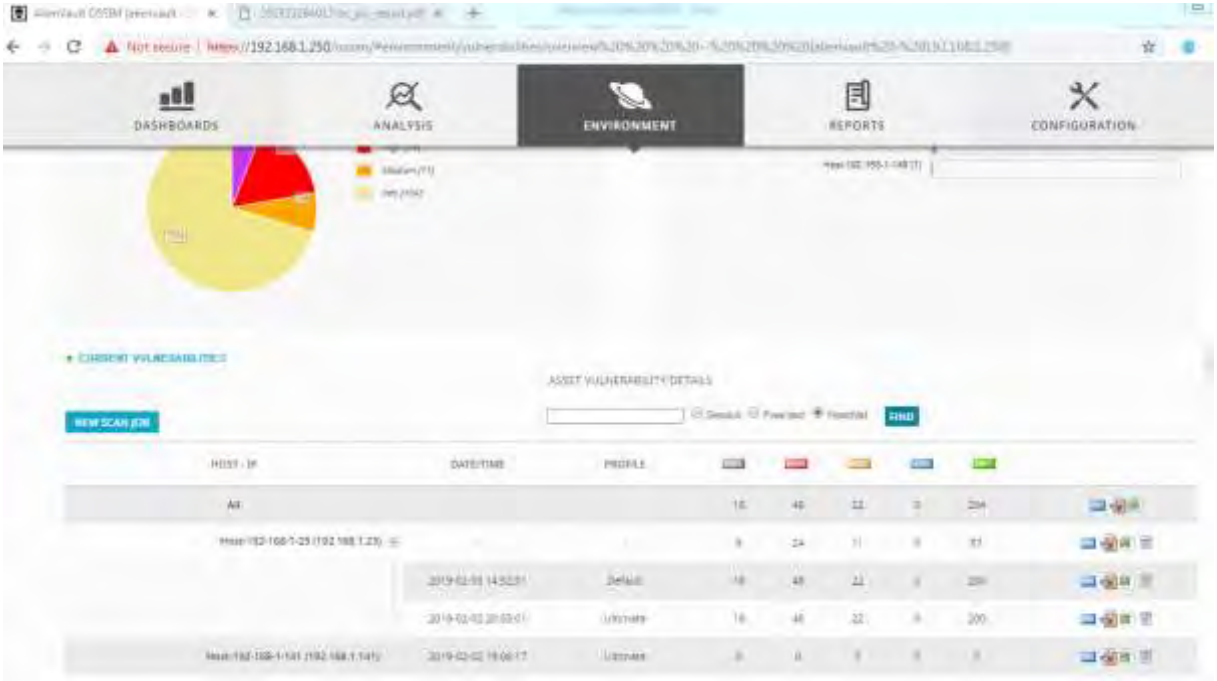
Figure 26 Scan de vulnérabilités



Scan de vulnérabilités



Scan de vulnérabilités



Interface montrant les événements et vulnérabilité de la machine Windows

Á la fin un rapport est généré sous format pdf qui va vous montrer comment faire pour résoudre les problèmes de votre système ou de votre réseau comme suit:

5.3 Supervision reseau : NETFLOW

NetFlow est une architecture de surveillance réseau développée par Cisco qui permet de collecter des informations sur les flux IP. Elle définit un format d'exportation d'informations sur les flux réseau nommé *NetFlow services export format* (format d'exportation des services NetFlow, en abrégé *protocole NetFlow*). Elle permet de superviser de façon fine les ressources du réseau utilisées. La figure suivante va montrer l'analyse du trafic réseau réalisée par NetFlow.

Figure 27 Capture d'écran du trafic réseau par Netflow

5.4 Test scan de port : NMAP

Dans la figure suivante, nous allons lancer un scan de port sur notre machine ubuntu16.04.

Interface montrant les événements et vulnérabilité de la machine Windows

Figure 28 Scan de port sur la machine Windows

Á la fin un rapport est généré sous format pdf qui va vous montrer comment faire pour résoudre les problémes de votre systéme ou de votre réseau comme suit :

Info:

Check for enabled / working Port scanner plugin
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 108323
Vulnerability Detection Result:
The host wasn't scanned due to the following possible reasons:
- No Port scanner plugin from the "Port scanners" family is included in this scan configuration. Recommended: Nmap (NASL wrapper).
- The Port scanner plugin reached a timeout during the port scanning phase. Please either choose a port range for this target containing less ports or raise the "scanner_plugins_timeout" scanner preference to a higher timeout.
Solution:
Based on the script output please:
- add a Port scanner plugin from the 'Port scanners' family to this scan configuration. Recommended: Nmap (NASL wrapper).
- either choose a port range for this target containing less ports or raise the 'scanner_plugins_timeout' scanner preference to a higher timeout.
- install the 'nmap' binary/package or make it accessible to the scanner.
Summary:
The script reports if:
- a custom scan configuration is in use without having a Port scanner from the 'Port scanners' family enabled.
- a port scanner plugin was running into a timeout.
- a required port scanner (e.g. nmap) is not installed.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
http://docs.greenbone.net/GSM-Manual/gos-4/en/performance.html#scan-performance
http://docs.greenbone.net/GSM-Manual/gos-4/en/vulnerabilitymanagement.html?highlight=scanner_plugins_timeout#general-preferences
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: Copyright (c) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 10122 $

Figure 29 Rapport de scan de port

5.5 Test attaque de type scan de port avec METASPLOIT

NMAP est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Lors de ce test, on tentera de scanner l'ensemble des ports ouverts, système d'exploitation et noyau de la machine métasploitable :

- Machine Ubuntu : 192.168.1.15
- IP : 192.168.1.23, OS : Metasploit

Dans la figure qui va suivre nous allons lancer un scan à partir de notre machine ubuntu16.04 vers la machine métasploitable

```
root@khadija-virtual-machine:/var/ossec# apt-get install nmap
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libblas3 liblinear-tools liblinear1
Paquets suggérés :
  libsvm-tools liblinear-dev
Les NOUVEAUX paquets suivants seront installés :
  libblas3 liblinear-tools liblinear1 nmap
```

Figure 30 Installation de NMAP

```
root@khadija-virtual-machine:/# nmap -T4 -A -v -Pn 192.168.1.23

Starting Nmap 6.40 ( http://nmap.org ) at 2019-02-03 17:13 GMT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 17:13
Scanning 192.168.1.23 [1 port]
Completed ARP Ping Scan at 17:13, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:13
Completed Parallel DNS resolution of 1 host. at 17:13, 0.02s elapsed
Initiating SYN Stealth Scan at 17:13
Scanning 192.168.1.23 (192.168.1.23) [1000 ports]
Discovered open port 21/tcp on 192.168.1.23
Discovered open port 445/tcp on 192.168.1.23
Discovered open port 53/tcp on 192.168.1.23
Discovered open port 80/tcp on 192.168.1.23
Discovered open port 22/tcp on 192.168.1.23
Discovered open port 25/tcp on 192.168.1.23
Discovered open port 5900/tcp on 192.168.1.23
Discovered open port 3306/tcp on 192.168.1.23
Discovered open port 111/tcp on 192.168.1.23
Discovered open port 23/tcp on 192.168.1.23
```

Lancement de scan réseau à partir d'une machine Ubuntu

```
Host script results:
| nbstat:
|   NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown
>
|   Names
|     METASPLOITABLE<00>   Flags: <unique><active>
|     METASPLOITABLE<03>   Flags: <unique><active>
|     METASPLOITABLE<20>   Flags: <unique><active>
|     \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|     WORKGROUP<00>        Flags: <group><active>
|     WORKGROUP<1d>        Flags: <unique><active>
|_    WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2019-02-02T19:39:44-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.1.23 (192.168.1.23)

NSE: Script Post-scanning.
```

Lancement de scan réseau à partir d'une machine Ubuntu

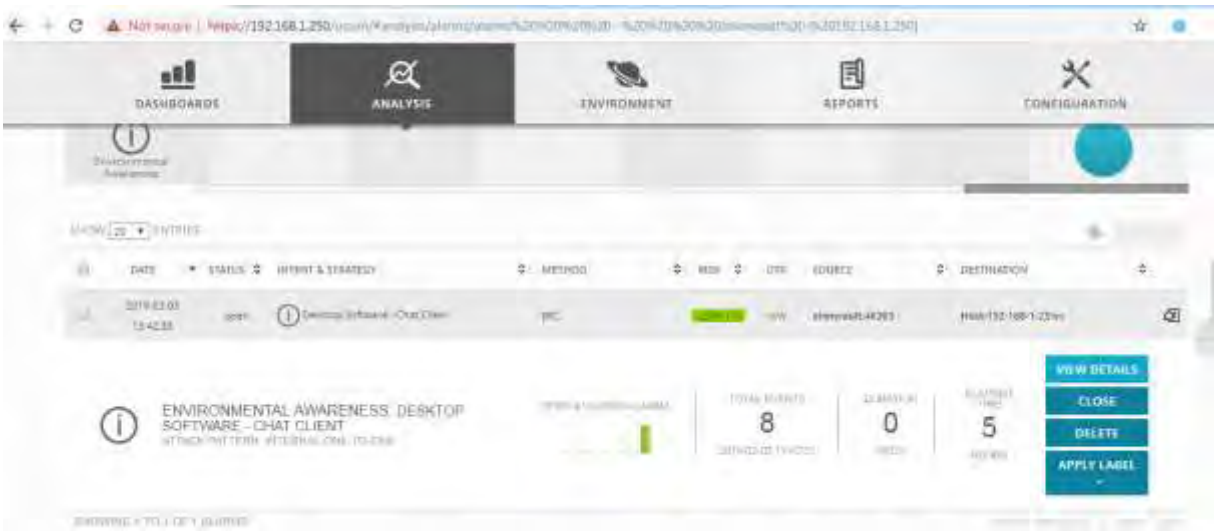


Figure 31 Détection de l'attaque par OSSIM

CONCLUSION

La sécurité d'un système d'information est une chose primordiale pour la survie d'une entreprise quel que soit son domaine d'activité.

L'étude réalisée dans le cadre de ce mémoire, m'a permis de découvrir et de comprendre des solutions de management de la sécurité de l'information.

OSSIM est une solution composée de trois briques.

- Une partie serveur : qui contient les différents moteurs d'analyse, de corrélation et les bases de données.
- Une partie agent qui prend en charge la collecte et la mise en forme des événements
- Une partie Framework : qui regroupe les consoles d'administrations et les outils de configuration et de pilotage. Le Framework assure également la gestion des droits d'accès.

Cette solution offre une grande modularité grâce à sa capacité à s'appuyer sur des outils de sécurité open-source. OSSIM est en quelque sorte le chef d'orchestre des différentes solutions déjà existante et permet de fédérer, d'agréger, d'analyser et de stocker les informations de manière centralisée et normalisée.

OSSIM est outil très fiable au niveau de l'administration du système d'information. Il permet de détecter et analyser les attaques et les menaces à son réseau et hosts.

PERSPECTIVES

Le projet a ouvert de nouvelles pistes toujours dans le domaine de la sécurité.

D'une part, nous devons poursuivre l'étude afin de nous familiariser beaucoup plus avec l'étude.

D'autre part, nous prévoyons de faire des études poussées pour faire du forensic, c'est-à-dire relier notre plateforme avec la pile elastic stack composée de elasticsearch, de logstash et de Kibana.

BIBLIOGRAPHIE

(B1) Internet

(B2) Sécurité Informatique et réseaux 1er édition DUNOD Auteur Solange Ghernaouti

(B3) Hacking, sécurité et tests d'intrusion avec Métasploit Auteur PEARSON

WEBOGRAPHIE

Mise-en-Place-d'une-Solution-SIEM-OpenSource-OSSIM.pdf
https://dumas.ccsd.cnrs.fr/file/index/docid/1066307/filename/2012.TH_18187.Bidanel_Jacques.pdf
Mise-en-place-d'un-système-de-management-des-logs-avec-OSSIM.pdf
http://www.philippe-martinet.info/ossim-project/Rapport-OSSIM-Philippe-Martinet.pdf
https://repo.zenk-security.com/Protocoles_reseaux_securisation/IDS%20intrusion%20detections%20snort.pdf
https://www.snort.org/downloads/snort/snort-2.9.11.1.tar.gz
https://www.gartner.com/reviews/customer-choice-awards/security-information-event-management
https://www.esecurityplanet.com/products/top-siem-products.html
https://fr.wikipedia.org/wiki/Security_information_management_system