

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE



## RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de  
*Post-Graduation Spécialisée en Sécurité Informatique*

Préparé par :

**Brahim LAIB et Djillali TALBI**

Sous la direction de :

**Abdlouahab AMIRA** (Encadreur)

**Amine BOULEMTAFES** (Co-Encadreur)

# HONEYPOTS & HONEYNETS POUR LA DETECTION D'ATTAQUES

**Soutenu le :13/01/2022. Devant le jury composé de :**

**Président :**

Mr. Nabil DJEDJIG

**Examineurs :**

Mr. Samir HADJAR

Mr. Ahmed SAIDI

Année Universitaire : **2019 - 2020**

# HONEYPOTS & HONEYNETS POUR LA DETECTION D'ATTAQUES



**Brahim LAIB et Djillali TALBI**

Mémoire soumis en vue de l'obtention du diplôme de  
*Post-Graduation Spécialisée en sécurité informatique*

## **Remerciements**

*Nous remercions en premier lieu, Allah le tout puissant, de nous avoir accordé le courage et la volonté, pour achever ce travail.*

*Nous adressons nos plus profonds remerciements à nos encadreurs Abdleouahab AMIRA et Amine BOULEMTAFES, pour nous avoir encadré tout au long du stage pratique de notre PGS, pour leurs conseils et leurs orientations.*

*Nous tenons ensuite à remercier Dr. NOUALI Omar, le responsable chargé de la formation PGS sécurité informatique au CERIST.*

*Nous remercions tous les enseignants de la formation PGS sécurité informatique CERIST- Benaknoun et tous les responsables qui ont participé dans la bonne démarche de nos études durant cette période de formation PGS.*

*Nous remercions tous nos collègues stagiaires de la formation PGS sécurité informatique CERIST, pour l'environnement de travail très agréable durant cette année de formation PGS.*

*Enfin, nous remercions toutes les personnes qui ont lu et relu ce mémoire et en particulier les rapporteurs.*

# *Abstract*

*Nowadays, attacks on computer systems are becoming more and more complex, and cybercriminals are constantly improving their techniques. This leads to the need for continuous improvement of prevention and detection methods.*

*In this sense, Honeypots and Honeynets are considered among the most effective methods of learning and detecting new attacks.*

*A Honeypot is a vulnerable resource that is intentionally set up. It is a kind of decoy similar to a resource in the production system. A Honeypot can be a single file, a file system, an entire operating system, a server, or even a set of systems or a segment of a network. A Honeynet is simply an environment containing several Honeypots.*

*The purpose of this work is as follows:*

- 1. Setting up a Honeynet: deploying a set of Honeypots probes on the network.*
- 2. The collection and analysis of different types of captured data (logs, traffic, ... etc.) captured.*
- 3. Experimenting the use of artificial intelligence in the analysis of the collected data.*

*To do this, the recommended work plan is as follows:*

- State of the art on Honeypots/Honeynets,*
- Study on the different types of Honeypots and existing deployment architectures,*
- Design of the architecture and deployment,*
- Analysis of the results using different techniques,*
- Experimentation of an artificial intelligence techniques for analysis.*

***Keywords: Honeypots, Honeynets.***

# Résumé

De nos jours, les attaques sur les systèmes informatiques sont de plus en plus complexes, et les cybercriminels ne cessent d'améliorer leurs techniques. Ceci amène à la nécessité de l'amélioration continue des méthodes de prévention et de détection.

Dans ce sens, les Honeypots et Honeynets sont considérés parmi les méthodes les plus efficaces permettant d'apprendre et de détecter les nouvelles attaques.

Un Honeypot est une ressource vulnérable intentionnellement mise en place. C'est une sorte de leurre semblable à une ressource dans le système de production. Un Honeypot peut être un simple fichier, un système de fichiers, un système d'exploitation complet, un serveur, ou même un ensemble de systèmes ou un segment d'un réseau. Un Honeynet est simplement un environnement contenant plusieurs Honeypots.

Le but de ce travail est comme suit :

1. La mise en place d'un Honeynet : déploiement d'un ensemble de sondes Honeypots sur le réseau.
2. La récolte et l'analyse des différents types des données capturées (logs, trafic, ...etc.) capturées.
3. Expérimenter l'utilisation de l'intelligence artificielle dans l'analyse des données récoltées.

Pour ce faire, le plan de travail recommandé est le suivant :

- État de l'art sur les Honeypots/Honeynets,
- Étude sur les différents types Honeypots et les architectures de déploiement existantes,
- Conception de l'architecture et déploiement,
- Analyse des résultats en utilisant différentes techniques,
- Expérimentation d'une technique d'intelligence artificielle pour l'analyse.

**Mots-clés: Honeypots, Honeynets.**

# Table des matières

<b>Abstract</b> .....	iv
Résumé .....	v
Table des matières .....	vi
Annexes .....	viii
Liste des figures.....	ix
Liste des tableaux .....	x
<b>Introduction</b> .....	1
<b>Objectif</b> .....	2
<b>CHAPITRE 1</b> .....	3
<b>Honeypots et Honeynets</b> .....	3
I.1- Définition.....	3
I.2- Taxonomie des Honeypots/Honeynets .....	3
I.2.1- Classification des Honeypots .....	4
I.2.1.1- Classification des Honeypots par Objectif.....	4
I.2.1.2- Classification des Honeypots par Type d'Interaction .....	6
I.2.2- Classification des Honeynets.....	9
I.2.2.1- Honeynets 1ère génération .....	9
I.2.2.2- Honeynets 2ème génération .....	11
I.2.2.3- Honeynets 3ème génération .....	12
I.2.2.4- Honeynets virtuels.....	12
I.3- Conclusion .....	14
<b>CHAPITRE 2</b> .....	15
<b>Déploiement d'une solution de détection d'attaque basée sur un Honeynet</b> ...	15
II.1- Méthodologie .....	16
II.1.1- Ensembles d'outils .....	16
II.2- Système de Monitoring du Honeynet .....	17
II.3- Conclusion .....	20

<b>CHAPITRE 3</b> .....	21
<b>Tableaux de bords, visualisation et discussion</b> .....	21
III.1- Intégration des données Cowrie dans ELK .....	21
III.2- Intégration des données Tanner dans ELK.....	23
III.3- Intégration des données Tshark dans ELK .....	24
III.4- Intégration des données Snort dans ELK.....	25
III.5- Conclusion .....	26
<b>CHAPITRE 4</b> .....	27
<b>Détection et visualisation d'attaques à l'aide du machine Learning</b> .....	27
VI.1- Algorithmes de Machine Learning .....	27
VI.2- Paradigme d'apprentissage .....	27
VI.2.1- Modèles non-supervisés .....	28
VI.2.2- Modèles supervisés.....	28
VI.3- Application d'algorithme de Machine Learning sur les données de déttection d'intrusion.....	30
VI.3.1- Pré-processing et exploration de données .....	30
VI.3.2- Implémentation et méthodologie.....	34
VI.3.3- Résultats et discussion.....	36
VI.4- Visualisation des données de sortie dans ELK.....	38
VI.5- Conclusion .....	38
<b>CONCLUSION GENERALE</b> .....	39
<b>Bibliographie</b> .....	71

## Annexes

ANNEXE A.....	40
<b>Commandes d’installation de SNARE .....</b>	<b>40</b>
ANNEXE B .....	41
<b>Commandes d’installation de TANNER.....</b>	<b>41</b>
ANNEXE C .....	43
<b>Commandes d’installation de COWRIE.....</b>	<b>43</b>
ANNEXE D.....	49
<b>Commandes d’installation de SNORT 3 .....</b>	<b>49</b>
ANNEXE E .....	54
<b>Commandes d’installation ELK .....</b>	<b>54</b>
ANNEXE F .....	59
<b>Configuration Filebeat-Cowrie.....</b>	<b>59</b>
ANNEXE G.....	60
<b>Configuration Filebeat-Snort.....</b>	<b>60</b>
ANNEXE H.....	61
<b>Configuration Filebeat-Tanner.....</b>	<b>61</b>
ANNEXE I .....	63
<b>Configuration Logstash .....</b>	<b>63</b>
ANNEXE J.....	69
<b>Configuration Tanner .....</b>	<b>69</b>

## Liste des figures

<b>Figure 1</b> : Taxonomie des Honeypots/Honeynets .....	4
<b>Figure 2</b> : Fonctionnement d'un Honeypot à faible interaction .....	6
<b>Figure 3</b> : Fonctionnement d'un Honeypot à moyenne .....	7
<b>Figure 4</b> : Fonctionnement d'un Honeypot à forte interaction .....	8
<b>Figure 5</b> : Architecture d'un HoneyNet.....	9
<b>Figure 6</b> : Honeynet de 1ère génération .....	10
<b>Figure 7</b> : Honeynet de 2ème génération .....	11
<b>Figure 8</b> : Représentation simplifiée d'un Honeynet purement virtuel .....	13
<b>Figure 9</b> : Honeynet virtuel hybride .....	14
<b>Figure 10</b> : Architecture du réseau .....	15
<b>Figure 11</b> : Système de monitoring du Honeynet .....	18
<b>Figure 12</b> : Nombre d'attaques & adresse IP par jour qui ont tenté d'accéder à Cowrie (avec top 10 des commandes, top 10 usernames et top 10 passwords) .....	22
<b>Figure 13</b> : Cartographie de l'origine des attaques sur Cowrie .....	22
<b>Figure 14</b> : Nombre et types d'attaques utilisés sur Snare .....	23
<b>Figure 15</b> : Top 10 des chemins et agents utilisateurs les plus utilisés par les attaquants pour accéder à Snare et Cartographie de l'origine des attaques .....	24
<b>Figure 16</b> : Nombre d'attaques quotidiennes aux services ssh, http et telnet .....	25
<b>Figure 17</b> : Cartographie de l'origine des attaques (Tshark) .....	25
<b>Figure 18</b> : Top 10 messages des règles les plus provoquées par les attaquants (Snort) .....	26
<b>Figure 19</b> : Exemple pour souligner la différence entre une structure linéaire et non-linéaire .....	27
<b>Figure 20</b> : Quelques algorithmes de machine Learning et leur capacité d'apprentissage entre interopérabilité .....	30
<b>Figure 21</b> : Barplot de la variable de sortie .....	32
<b>Figure 22</b> : Visualisation multivariée des variables tcp .....	33
<b>Figure 23</b> : Valeurs propres de l'analyse en Composante Principale .....	33
<b>Figure 24</b> : Visualisation sur les deux premiers axes de l'ACP, en mettant en évidence les différentes classes de la variable de sortie .....	34
<b>Figure 25</b> : Variables importantes du modèle de données par random forest .....	35
<b>Figure 26</b> : Implémentation du système comprenant une phase d'apprentissage à partir du jeu de données (train.csv), et une phase de test en production à partir des flux capturés dans un réseau local .....	36
<b>Figure 27</b> : Validation croisée pour définir le nombre de variables .....	37
<b>Figure 28</b> : Boxplot de la variable TCP_seg_raw pour chaque classe .....	37
<b>Figure 29</b> : Nombre d'attaques extraites du numéro de port destination -tcp.dstport- aux services (ssh, telnet, http et Autres) après la prédiction .....	38

## Liste des tableaux

<b>Tableau 1</b> : Spécifications des machines pour les Honeypots utilisés .....	19
<b>Tableau 2</b> : Tableaux de bord proposés pour Cowrie .....	21
<b>Tableau 3</b> : Tableaux de bord proposés pour Tanner .....	23
<b>Tableau 4</b> : Tableaux de bord proposés pour Tshark .....	24
<b>Tableau 5</b> : Tableaux de bord proposés pour Snort .....	26