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

Examinateurs : 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

Alger

Jan 2022

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

Annexes

Liste des figures

Liste des tableaux