République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida

Faculté des sciences

Département informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de master en informatique

Spécialité : Sécurité de système d'information

Thème :

MISE EN ŒUVRE D'UN SYSTEME DE MONITORING POUR LA CYBER SECURITE

Mémoire présenté par :

- Hakimi Yacine

Promotrice : Mme Djeddar Afrah Encadré par : Dr. Zeghache Linda

Date de la Soutenance le : **juillet2019**

2018/2019

Remerciement

Je remercie en premier lieu, Allah tout puissant, de m'avoir accordé le courage et la volonté, pour achever ce travail.

J'adresse mes plus profonds remerciements à mes encadreurs Mme Zeghache Linda et Mme Djeddar Afrah qui ont assuré l'encadrement de ce travail au jour le jour et dont la disponibilité, la qualité des conseils et l'aide m'ont largement aidé à mener à bien cette étude.

Je tiens à exprimer toute ma reconnaissance envers tous mes enseignements du cycle primaire au cycle universitaire.

Il m'est très agréable d'exprimer toute ma sympathie à tous mes collègues, amis et ceux que j'ai côtoyés et appréciés.

Merci à mes parents, qu'ils voient ici le témoignage de ma profonde admiration et mon éternel amour.

Dédicaces

Je dédie ce modeste travail

A mes très chers parents

A mon très cher frère

A mes très chères sœurs

A mes amis de la promo

A tous ceux que j'aime et qui m'aiment

ملخص

مع زيادة التهديدات السيبرانية و محدودية وسائل المراقبة التقليدية ، أصبح استخدام أنظمة تلسكوب الشبكة أمرًا ضروريًا للحصول على معلومات موثوقة وفي الوقت المناسب لمواجهة التهديدات السيبرانية. تصف هذه الدراسة تصميم ونشر أول تلسكوب شبكة في الجزائر وتحليل البيانات التي تم جمعها بواسطة هذا التلسكوب.

يتم تخزين البيانات التي تم جمعها على مدى شهر واحد باستخدام مكدس Elasticsearch-Logstash-Kibana (ELK)الذي يسهل تحليل مجموعات البيانات الكبيرة.

يقدم هذا العمل عدة أنواع من تحليلات البيانات التي تم جمعها ، وهي: التحليل الأولي باستخدام NIDS ، وتنميط البيانات والتحليل الزمني باستخدام KIBANA والتحليل المتعمق باستخدام العنقدة. يتم استكشاف حركة المرور المجمعة بالتفصيل وإبرازها. كما تم تقديم مناقشة لحركة المرور المرصودة. و اقتراح نهج جديد لتصنيف حركة المرور واكتشاف الأنشطة غير العادية. لقد أظهرت نتائج العنقدة فعالية النهج المقترح ، وقدمت معلومات حول تهديدات معروفة وأخرى غير معروفة .

الكلمات المفتاحية: Cyber ، Darknet، تلسكوب الشبكة ، التهديدات ، الأمان ، الذكاء ، التهديدات السيبرانية ، NIDS العنقدة، ELK.

Abstract

With the increase of cyber threats and the limitations of traditional monitoring means the use of network telescope systems has become a necessity in order to obtain reliable and timely information to counter cyber threats. The present study describes the design and deployment of the first network telescope in Algeria and the analysis of data collected by this telescope.

Data collected over a period of one month is stored using the Elasticsearch-Logstash-Kibana (ELK) stack which facilitates the analysis of large datasets.

This work presents several types of analyzes of collected data, namely: preliminary analysis using NIDS, data profiling, temporal analysis using KIBANA and in-depth analysis using clustering. Collected traffic is explored in detail and highlighted. A discussion of observed traffic is also presented. A new approach to classifying traffic and detecting unusual activities is proposed. Clustering results have shown the effectiveness of the proposed approach, and provide information on known threats and other unknowns.

Keywords: Cyber, Darknet, Network Telescope, Threats, Security, Intelligence, Cyber-Threats, NIDS, Clustering, ELK

Résumé

Avec l'augmentation des cybermenaces et les limites des moyens de monitoring traditionnels l'utilisation des systèmes de télescope réseau est devenue une nécessité afin d'obtenir des informations fiables et au bon moment pour contrecarrer les cybermenaces. La présente étude décrit la conception et le déploiement du premier télescope réseau en Algérie et l'analyse de données collectées par ce télescope.

Les données collectées sur une période d'un mois sont stockées en utilisant le stack ELK(Elasticsearch-Logstash-Kibana) qui facilite l'analyse de grands ensembles de données.

Ce travail présente plusieurs types d'analyses des données collectées à savoir : une analyse préliminaire en utilisant les NIDS, le profilage de données, une analyse temporelle en utilisant KIBANA et une analyse approfondie en utilisant le clustering. Le trafic collecté est exploré en détail et mis en évidence. Une discussion relative au trafic observé est également présentée. Une nouvelle approche pour classifier le trafic et détecter les activités inhabituelles est proposé. Les résultats du clustering ont montré l'efficacité de l'approche proposée, et donnent des informations sur des menace connus et d'autres inconnues.

Mots clés : Cyber, Darknet, télescope réseau, Menaces, Sécurité, Intelligence, Cyber-menaces, NIDS,Clustering, ELK

Sommaire