الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de

Poste Graduation Spécialisée en Sécurité Informatique

Développement d'un système de détection d'intrusion dans une architecture réseau basée SDN

Réalisé par :

Rachid HABIB-ZAHMANI

Mourad YSSAAD

Devant le Jury :

Président :

M.KHEMISSA Hamza

Examinateurs :

M. DABAH Adel

M. KRINAH Abdelghani

L'Encadreur

Mr. Mohamed Saddek DERKI

Co-encadreur

Mr. Fateh BOUCENNA

Promotion : 2018/2019

Résumé

La réseautique définie par logiciel (SDN) est une nouvelle technologie réseau offrant la programmation nécessaire pour permettre aux opérateurs réseaux de gérer leurs infrastructures d'une façon simple et dynamique. Cependant, malgré ces avantages, ces réseaux sont très vulnérables aux attaques de déni de service (DoS) qui peuvent facilement surcharger et saturer la table des flux du contrôleur SDN, ce qui entraîne une dégradation critique des performances du réseau.

Le contrôle de la sécurité des routages des données est un concept important dans les réseaux informatiques car il est lié à la disponiblité de la donnée à tout moment qui offre une qualité de service fiable. Les garanties de qualité de service de bout en bout, en particulier, peuvent donner des garanties stables aux hôtes finaux. Avec l'émergence du Software Defined Network (SDN) et le protocle d'OpenFlow comme standards les plus populaires, nous avons l'opportunité de réintroduire le concept de contrôle de la sécurité dans les réseaux SDN à travers La nature centralisée et la programmabilité d'OpenFlow qui permettent un contrôle plus flexible et plus simple afin de serveillier le trafic du réseau et les flux malveillants.

Les vulnérabilités de sécurité réseaux associées introduites par les périphériques réseaux dans le modèle SDN émergent ainsi que le besoin urgent de détecter les effets négatifs de certains types d'attaques par déni de service (DoS) tentent d'explorer ces vulnérabilités de sécurité pour assurer un "fonctionnement normal" de l'infrastructure réseau. Notre suggestion est de créer un script "Snort Alert" qui avertit le contrôleur SDN contre les flux malveillants en collaboration avec le système de détection d'intrusion Snort IDS. Ce dernier, qui détecte automatiquement de nombreuses attaques "DoS", puis lorsqu'une attaque est détectée, alerte le contrôleur SDN via un script "Snort Alert".

La proposition actuelle applique également certaines décisions pratiques pour transférer le trafic du contrôleur SDN vers les périphériques réseau. Les résultats de l'évaluation indiquent que notre proposition détecte une attaque basée sur le DoS, ménimise son impact négatif sur les performances du réseau et garantit une livraison correcte des données de trafic normales. Notre travail met en évidence la programmation associée sur une vue abstraite de l'infrastructure réseau pour détecter le trafic malveillant à sa source et protéger le routage des données .

Mots-clés: Réseaux SDN; OpenFlow ; Sécurité des réseaux ; IDS ; attaque de Déni de Service (DoS)

Abstract

Software Defined Networking (SDN) is a new network technology that provides the programming necessary to allow network operators to manage their infrastructure in a simple and dynamic way. However, despite these advantages, these networks are very vulnerable to denial of service (DoS) attacks which can easily overload and saturate the flow table of the SDN controller, which leads to a critical degradation of network performance.

Controlling the security of data routing is an important concept in computer networks because it is linked to the availability of data at all times which provides a reliable quality of service. End-to-end quality of service guarantees, in particular, can give stable guarantees to end hosts. With the emergence of the Software Defined Network (SDN) and the OpenFlow protocol as the most popular standards, we have the opportunity to reintroduce the concept of security control in SDN networks to cross The centralized nature and programmability of 'OpenFlow which allow a more flexible and simpler control of network traffic and malicious flows.

The associated network security vulnerabilities introduced by network devices in the SDN model are emerging as well as the urgent need to detect the negative effects of certain types of denial of service (DoS) attacks attempting to explore these security vulnerabilities to ensure "normal operation" of the network infrastructure. Our suggestion is to create a "Snort Alert" script that warns the SDN controller against malicious flows in collaboration with the Snort IDS intrusion detection system. The latter, which automatically detects many "DoS" attacks, then when an attack is detected, alerts the SDN controller via a "Snort Alert" script.

The current proposal also applies certain practical decisions to transfer traffic from the SDN controller to network devices. The results of the evaluation indicate that our proposal detects a DoS-based attack, minimizes its negative impact on network performance and guarantees proper delivery of normal traffic data. Our work highlights the associated programming on an abstract view of the network infrastructure to detect malicious traffic at its source and protect data routing.

Keywords: SDN networks; OpenFlow; Network security, IDS; Denial of Service (DoS) attack.

ملخـــص

الشبكات المعرفة بالبرمجيات (SDN) هي تقنية جديدة للشبكة توفر البرمجة اللازمة للسماح لمشغلي الشبكات بإدارة بنيتهم التحتية بطريقة بسيطة وديناميكية. ومع ذلك ، على الرغم من هذه المزايا ، فإن هذه الشبكات معرضة بشدة لهجمات رفض الخدمة (DoS) التي يمكن أن تفرط وتشبع جدول تدفق وحدة تحكم SDN بسهولة ، مما يؤدي إلى تدهور خطير في أداء الشبكة.

يعد التحكم في أمان توجيه البيانات مفهومًا هامًا في شبكات الكمبيوتر لأنه مرتبط بتوافر البيانات في جميع الأوقات مما يوفر جودة موثوقة للخدمة. إن ضمانات جودة الخدمة الشاملة ، على وجه الخصوص ، يمكن أن تعطي ضمانات ثابتة للمضيفين النهائيين. مع ظهور الشبكة المعرفة بالبرمجيات (SDN) وبروتوكول OpenFlow كأكثر المعايير شيوعًا ، لدينا الفرصة لإعادة تقديم مفهوم التحكم الأمني في شبكات SDN لعبور الطبيعة المركزية وإمكانية البرمجة 'OpenFlow الذي يسمح بتحكم أكثر مرونة وبساطة في حركة مرور الشبكة والتدفقات الضارة.

تظهر ثغرات أمان الشبكة المرتبطة التي أدخلتها أجهزة الشبكة في نموذج SDN بالإضافة إلى الحاجة الملحة للكشف عن الآثار السلبية لأنواع معينة من هجمات رفض الخدمة (DoS) التي تحاول استكشاف نقاط الضعف الأمنية. لضمان "التشغيل العادي" للبنية التحتية للشبكة اقتراحنا هو إنشاء برنامج نصي "Snort Alert" يحذر وحدة تحكم SDN من التدفقات الخبيثة بالتعاون مع نظام Snort IDS لكشف التسلل. هذا الأخير يكتشف تلقائيًا العديد من هجمات "DoS" ، وعند اكتشاف هجوم ينبه وحدة تحكم SDN عبر برنامج نصي."Snort Alert" .

يطبق الاقتراح الحالي أيضًا بعض القرارات العملية لنقل حركة المرور من وحدة تحكم SDNإلى أجهزة الشبكة. تشير نتائج التقييم إلى أن اقتراحنا يكشف عن هجوم قائم على DoS ، ويقلل من تأثيره السلبي على أداء الشبكة ويضمن التسليم السليم لبيانات حركة المرور العادية.
يسلط عملنا الضوء على البرمجة المرتبطة على نظرة مجردة للبنية التحتية للشبكة لاكتشاف حركة المرور الضارة في مصدرها وحماية توجيه البيانات.

الكلمات الرئيسية: شبكات .SDN تدفق مفتوح؛ أمن الشبكة ، IDS؛ هجوم رفض الخدمة DOS

Table des matières