ملخص رسالة ماجستير بعنوان

تحسين أمن الشبكات المعرفة برمجيا بالاعتماد على الانتروبية

اسم الطالب

م.رؤى حمدان

المشرف

د.وسيم السمارة

المشرف المشارك

لايوجد

القسم والاختصاص

قسم هندسة الحواسيب والأتمتة

هندسة الحاسوب وشبكاته

الملخـــــص

في ظلّ اعتمادنا المتزايد على الأنظمة الرقميّة في أغلب مجالات الحياة، أصبحت الاختراقات الأمنيّة للأنظمة المعلوماتية أكثر خطورة. في الآونة الأخيرة نجد الكثير من الأمثلة عن اختراقات كان لها نتائج مؤثّرة جداً وخاصة في مجالات السّياسة والاقتصاد. كما أتاحت التّقنيات الحديثة في بيئات العمل الفرصة للمزيد من المخاطر الأمنيّة الجديدة بالظهور، بالإضافة إلى ظهور الجيل الجديد من الشّبكات الضخمة التي فرضت نوعاً جديداً من التحدّيات والمخاطر الأمنيّة، كما ساعد تطور التقنيّات الهائل في تزايد عدد الاختراقات بشكل أسيّ كل عدّة أشهر، أدّت كل هذه الأسباب إلى فشل نظم كشف الاختراقات التقليدية، مثل النظم المعتمدة على توقيع الاختراقات، في مجاراة هذا التطور الهائل لذلك كان لابد من تطوير مجال كشف الاختراقات ليتعامل مع بيئة معطيات كبيرة لمعالجة الكم الضخم من المعطيات والتعرف على الاختراقات الجديدة من نوعها في الزمن الحقيقي.

نسبة لأهمية هذا الموضوع فقد تناولت الدراسة مفاهيم ومنهجيات اكتشاف الحالات الشّاذة للتعرف على الاختراقات الجديدة من نوعها في بيئة الشبكات المعرفة برمجياً بشكل عام وهجوم منع الخدمة DDOS بشكل خاص عند العمل على شبكة كبيرة بتدفق عالي وسريع. يعتمد الحلّ المقترح على منهجيات وخوارزميات الانتروبية ونسبها الموزعة المهتمة بالسّياق وذلك لكشف هجوم منع الخدمة DDOS. حيث نقوم باستخراج معلومات وإحصائيات التدفق التراكمية والعشوائية في إطارات زمنية مختلفة

Master's thesis summary entitled

Improving Security of SDN based on Entropy

Student Name

Eng.Roua Hamdan

Co-Supervisor

D.Wassim Alsamarah

Supervisor

Not exist

Department

Computer and Automation Engineering

Summary

In light of our increasing dependence on digital systems in most areas of life, security breaches of information systems have become more dangerous. Recently, we find many examples of breakthroughs that have had very influential results, especially in the areas of politics and economics. Modern technologies in work environments have also provided the opportunity for more new security risks to emerge, in addition to the emergence of the new generation of huge networks that have imposed a new type of security challenges and risks. The tremendous development of technologies has also helped in the number of penetrations increasing exponentially every several months. All of these reasons led to the failure of traditional intrusion detection systems, such as systems based on intrusion signatures, to keep pace with this tremendous development. Therefore, the field of intrusion detection had to be developed to deal with a large data environment to process the huge amount of data and identify new intrusions of their kind in real time.

Due to the importance of this topic, the study addressed the concepts and methodologies of detecting anomalies to identify new intrusions of their kind in the software-defined network environment in general and DDOS attacks in particular when working on a large network with high and fast flow. The proposed solution relies on context-aware distributed entropy and entropy methodologies and algorithms to detect a DDOS attack. We extract cumulative and random flow information and statistics in different time frames.