جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والآتمتة

تطوير نموذج أمن متكيف للوصول إلى حلول أمنية للشبكات الحاسوبية بمردود مثالي للكلفة والزمن

Developing an Adaptable Security Model to have Secure Solutions for Computer Networks with Optimal Cost-Time Efficiency

إعداد المهندس: منير محمّد الوزّة
الدكتور المشرف: أ.د.م سمير كرمان
المشرف المشارك: أ.د محمد نور شمه

الملخص

أدى التطور العلمي إلى زيادة المعلومات في الأبحاث ، وللحفاظ عليها من السرقة والاختراق، تعزز دور أمن المعلومات، ويؤدي التنسيق بين مختلف تقنيات الدفاع عن الشبكة إلى حمايتها من أي اختراق. ويسعى المهاجمون إلى اختراق شبكات الجامعات لسرقة الخصائص الفكرية والأبحاث، مستغلين الثغرات الأمنية فيها، ولما كنا جزءاً من هذا المجال التعليمي، قمنا بتطوير نموذج للبحث وتحليل الاختراقات وكشفها، باستخدام نظام منع الاختراق القائم على الاستفادة من مصائد مخترقي الشبكات ، وقادر على التقاط الهجمات الإلكترونية وتحليلها، ومشاركة نتائج التحليل مع الشبكات الأخرى، ويستفيد من تقنيات تعلم الآلة، وميزة الافتراضية، لتوفير الكلفة والزمن.

القسم النظري

ركزنا في دراستنا على أمن المعلومات وإظهار مساوئ ومحاسن تقنيات الدفاع عن الشبكة الحاسوبية، بدءاً من السياسة الأمنية، إضافةً إلى الأجهزة والبرمجيات التي تسهم في حماية الشبكة، مثل الجدر النارية، وأجهزة كشف الاختراق، وأجهزة منع الاختراق، وكذلك استخدام تقنيات الخداع متمثلة بمصائد مخترقي الشبكات. وإن تضافر الجهود بين هذه التقنيات والأجهزة والسياسة الأمنية، سيؤدي إلى الوصول إلى شبكة حاسوبية آمنة وبعيدة عن أي اختراق.

وتطرقنا إلى استخدام تقنيات تعلم الآلة واظهار المعطيات كصور، في كشف وتصنيف البرمجيات الخبيثة القديمة والحديثة.

يسهم كل ذلك في حماية الشبكة الحاسوبية، ويوفر في تكاليف وزمن تطويرها وتحديثها.

القسم العملي

طبقنا في البداية نموذج مصائد مخترقي الشبكات باستخدام بوابة Honeywall، ونشرنا مصائد مخترقي الشبكات بتفاعل منخفض وعال، واختبرنا هذه المنظومة باستخدام برنامج Hping3.

درسنا هجوم القوة الغاشمة والقاموس على بروتوكول SSH، وطورنا نموذج أمني قادر على اكتشاف هذه الهجمات، وقمنا بتحليل النتائج والتأكد من دقة هذا النموذج وفعاليته.

انتقلنا بعدها إلى تعميم نموذجنا المقترح وتطويره واستخدامه مع تقنيات الدفاع عن الشبكة، والاستفادة من تقنيات تعلم الآلة ومشاركة المعرفة، ونتائج تحليل الهجمات مع الشبكات الأخرى، وذلك بهدف الوصول إلى نموذج أمني متكيف ومتطور ويقتصد في الزمن والتكاليف.

القسم العملي

استفدنا في المرحلة الأخيرة من تقنية اظهار المعطيات كصور وتقنيات التعلم العميق، في اكتشاف وتصنيف البرمجيات الخبيثة القديمة والجديدة، وأجرينا تجارب مكثفة على بيانات التدريب للوصول للقيم المثلى للتجارب.

النتائج والمناقشة

- ❑ عدم وجود نظام دفاع عن الشبكة متكامل وقادر على اكتشاف جميع الهجمات الإلكترونية.
- ❑ استخدام مصائد مخترقي الشبكات في دراسة الهجمات وتحليلها وخاصة هجمات القوة الغاشمة والقاموس على بروتوكول SSH.
- ❑ يمتاز النموذج المطور بتكامل مكوناته وسرعته ، وقدرته على اكتشاف أنواع جديدة من الهجمات.
- ❑ يسمح النموذج المقترح بتصنيف البرمجيات الخبيثة القديمة والجديدة واكتشافها.
- ❑ يساهم النموذج المقترح في تحديث النظام الأمني ويقلل من زمن وتكاليف تطويره.

المراجع

A New Malware Classification Framework Based on Deep Learning Algorithms, Ömer Aslan, Abdullah Asım Yılmaz,IEEE Access, June 15, 2021

Malware detection based on semi-supervised learning with malware visualization , Tan Gao 1, Lan Zhao 2,*, Xudong Li 1 and Wen Chen 1 , Mathemitical Bioscience and Enginering, 02 July 2021

Implementation of Honeypot to Trap and Track Cyber Attacks, P. Nair, V. Nair, K. Nair, K.S. Charumathi, International Research Journal of Engineering and Technology (IRJET), 7 (2020) 970-974.