Published Researches
الأبحاث المنشورة

Title عنوان البحث	**Man In The Middle attacks against SSL/TLS: Mitigation and defeat** هجمات الرجل في الوسط ضد برتوكولSSL/TLS : التخفيف والهزيمة
Author الناشر	Muneer Alwazzeh, Sameer Karaman and Mohammad Nur Shamma م. منير الوزة، أ.د.م سمير كرمان، أ.د محمد نور شمه
Source Title اسم المجلة	**Journal of cyber security and mobility** مجلة الأمن السيبراني والتنقل
ISSN	22454578, 22451439
Q	3
Link رابط البحث من موقع المجلة	https://journals.riverpublishers.com/index.php/JCSANDM/article/view/406
Abstract خلاصة	Network security and related issues have been discussed thoroughly in this paper, especially at transport layer security network protocol, which concern with confidentiality, integrity, availability, authentication, and accountability. To mitigate and defeat Man-in-the-middle-attacks, we have proposed a new model which consists of sender and receiver systems and utilizes a combination of blowfish (BF) and Advanced Encryption Standard (AES) algorithms, symmetric key agreement to distribute public keys, Elliptic Curve Cryptography (ECC) to create secret key, and then Diffe Hellman (DH) for key exchange. Both SHA-256 hashing and Elliptic Curve Digital Signature Algorithm (ECDSA) have been applied for integrity, and authentication, respectively. تمت مناقشة أمن الشبكات والقضايا ذات الصلة بشكل مستفيض في هذه الورقة، خاصة فيما يتعلق ببروتوكول شبكة أمان طبقة النقل، والذي يهتم بالسرية والنزاهة والتوافر والمصادقة والمساءلة. للتخفيف من هجمات الرجل في الوسط وهزيمتها، اقترحنا نموذجاً جديداً يتكون من أنظمة المرسل والمستقبل ويستخدم مزيجاً من خوارزميات السمكة المنتفخة (BF) ومعيار التشفير المتقدم (AES)، واتفاقية المفاتيح المتماثلة لتوزيع المفاتيح العامة، وتشفير المنحنى الإهليلجي (ECC) لإنشاء مفتاح سري، ثم Diffe Hellman (DH) لتبادل المفاتيح. تم تطبيق كل من تجزئة SHA-256 وخوارزمية التوقيع الرقمي للمنحنى الإهليلجي (ECDSA) من أجل التكامل والمصادقة، على التوالي.

Published Researches
الأبحاث المنشورة

Title عنوان البحث	**Development of Intelligent Network Defense System to enable detection and analysis of cyber-attacks using an intrusion detection and prevention system based on honeypots** **تطوير نظام دفاع ذكي للشبكات لتمكين اكتشاف وتحليل الهجمات الإلكترونية باستخدام نظام منع وكشف الاختراق المعتمد على مصائد مخترقي الشبكات**
Author الناشر	**Eng.Muneer Alwazzeh, Prof.Sameer Karaman , Prof.Mohammad Nur Shamma** م. منير الوزة، أ.د.م سمير كرمان، أ.د محمد نور شمه
Source Title اسم المجلة	**Damascus University Journal for The Engineering Sciences** مجلة جامعة دمشق للعلوم الهندسية
ISSN	2789-6854 (online)
Q	
Link رابط البحث من موقع المجلة	
Abstract خلاصة	The networks of universities and educational institutes are normally exposed to cyber-attacks, either internally or from outside the network. Sharing of knowledge associated with means of protection, which are responsible for defending the network, will effectively contribute to preventing or mitigating these attacks. We have developed a model for search, detection and analysis of network breaches and malwares by using of an intrusion prevention and detection system based on honeypots. Machine learning algorithms are implemented for classifying the attacks and discovering new threat. This system is able to capture and analyze cyber-attacks and malwares, and share the results of the analysis with other networks in real time, taking advantage of virtualization and thus saving in cost and time, since these systems are open source and free. تتعرض شبكات الجامعات والمعاهد التعليمية عادة للهجمات الإلكترونية، من داخل أو من خارج الشبكة .يساهم تبادل المعرفة المرتبطة بوسائل الحماية المسؤولة عن الدفاع عن الشبكة، بشكل فعال في منع هذه الهجمات أو التخفيف من حدتها .طورنا نموذجًا للبحث واكتشاف وتحليل خروقات الشبكة والب ا رمج الخبيثة باستخدام نظام منع وكشف الاختراق المعتمد على مصائد مخترقي الشبكات . طبقنا خوارزميات التعلم الآلي لتصنيف الهجمات واكتشاف التهديد الجديد .هذا النظام قادر على التقاط وتحليل الهجمات الإلكترونية والب ا رمج الخبيثة، ومشاركة نتائج التحليل مع الشبكات الأخرى في الزمن الحقيقي، مستفيداً من مبدأ الافتراضية وبالتالي توفير التكلفة والوقت، كون هذه الأنظمة مفتوحة المصدر ومجانية.

Published Researches
الأبحاث المنشورة

Title عنوان البحث	**Analysis and mitigate SSH Brute-force and Dictionary attacks using honeypot system** **تحليل وتخفيف هجمات القاموس والقوة الغاشمة على بروتوكول SSH باستخدام نظام مصائد مخترقي الشبكات**
Author الناشر	**Eng.Muneer Alwazzeh, Prof.Sameer Karaman , Prof.Mohammad Nur Shamma** م. منير الوزة، أ.د.م سمير كرمان، أ.د محمد نور شمه
Source Title اسم المجلة	**Damascus University Journal for The Engineering Sciences** مجلة جامعة دمشق للعلوم الهندسية
ISSN	2789-6854 (online)
Q	
Link رابط البحث من موقع المجلة	
Abstract خلاصة	Computer networks are vulnerable to cyber-attack, which has been increased rapidly and caused harm to our network security systems. It is necessary to build a system with the ability to deceive, detect and block these attacks. SSH Brute-force and dictionary attacks are ones of the most famous attacks on internet and computer networks. Honeypots are effective security system to analyze and mitigate SSH brute-force and dictionary attacks. Cowrie honeypot system was deployed to both records and analyzes SSH Brute-force and dictionary attack information and command execution after successful login to Cowrie system. Evaluation of Cowrie honeypot system can be obtained by using confusion matrix and accuracy with high percentage, which means that Cowrie honeypot system, has a good ability to protect our network from SSH attacks. تكون شبكات الكمبيوتر عرضة للهجمات الإلكترونية، والتي زادت بسرعة وتسببت في إلحاق الضرر بأنظمة أمان الشبكة الخاصة بنا. من الضروري بناء نظام لديه القدرة على خداع هذه الهجمات واكتشافها وصدها. تعد هجمات القوة الغاشمة والقاموس على بروتوكول SSHمن أشهر الهجمات على شبكات الإنترنت والكمبيوتر. مصائد مخترقي الشبكات هي نظام أمان فعال لتحليل وتخفيف هجمات القوة الغاشمة والقاموس على بروتوكول SSH. تم نشر نظام مصائد مخترقي الشبكات Cowrie لتسجيل وتحليل المعلومات والأوامر المنفذة لهجمات القوة الغاشمة والقاموس على بروتوكول SSH وذلك بعد تسجيل الدخول بنجاح إلى نظام Cowrie. تم الحصول على تقييم نظام مصائد مخترقي الشبكات Cowrie باستخدام مصفوفة الارتباك والدقة وبنسبة عالية، مما يعني أن نظام مصائد مخترقي الشبكات Cowrie لديه قدرة جيدة على حماية شبكتنا من هجمات SSH.