دراسة بحثية في كلية تكنولوجيا المعلومات حول نظام الكشف التعاوني عن هجومات الفيضان الموزعة للحرمان من الخدمة والتعقب المستوحى من مجتمع العناكب الاجتماعية

بينت
دراسة بحثية في كلية تكنولوجيا المعلومات اعدها الباحث عادل محمد سلمان القريشي والموسومة
بـ : " نظام الكشف التعاوني عن هجومات الفيضان الموزعة للحرمان من الخدمة والتعقب المستوحى من مجتمع العناكب الاجتماعية "
وبين
الباحث ان شبكة الانترنت الا تزال تعاني من المشاكل الأمنية التي تهم بشكل رئيسي الأشخاص الذين يستخدمون أجهزتهم للاتصال بالإنترنت، سواء كانوا أفراد أو مؤسسات كبيرة. الهجمات الموزعة للحرمان من الخدمة
لا تزال واحدة من أهم المواضيع التي يتم مناقشتها
حاليا في تهديدات أمن الشبكات للشركات التي تقدم الخدمات لعملائها.
وفي الدراسة تم اقتراح نظام الكشف التعاوني. واستند
على مرحلتين: (1) مرحلة الكشف؛ (2) مرحلة التعقب.
اعتمادا على الفكرة المستوحاة من
مجتمع العناكب الاجتماعية، تم تصنيف أجهزة التوجيه إلى نوعين
و على النحو التالي:
(1) جهاز التوجيه الذكر، الذي هو مرتبط مباشرة مع الخادم؛ (2) جهاز التوجيه الانثى
والذي هو كل جهاز توجيه غير مرتبط مباشرة مع الخادم.
ويتميز النظام المقترح بأنه حل
قائم على جهاز التوجيه وعلى فحص التدفقات.
يمكن تقسيم مرحلة الكشف إلى أربع خطوات، على النحو
التالي: (1) جمع البيانات؛ (2) معالجة البيانات واستخراج الميزات؛
(3) بناء نموذج التصنيف،
باستخدام خوارزمية شجرة القرار عالية السرعة (VFDT) كخطوة للكشف المبكر،
والتي سيتم استخدامها من قبل كل جهاز توجيه أنثى
في الشبكة؛ (4) كشف الشذوذ (الهجوم)
باستخدام خوارزمية الغابات العشوائية (RF) للتصنيف، والتي سيتم تنفيذها في كل جهاز توجيه ذكر.
الجمع بين هاتين
الخوارزميتين سوف ينتج عنه خوارزمية تصنيف جديدة تسمى هوفدينغ الغابات العشوائية (HRF).
تبدأ مرحلة تتبع مصادر الهجوم عندما يتم العثور على
بيانات الهجوم.
جهاز التوجيه الذكر القريب من الخادم الضحية سوف يتتبع مصادر الهجوم
بالاعتماد على قيمة الاهتزاز للتدفق،
ثم رفع الانذار وإرسال جميع المعلومات إلى مسؤول
الشبكة لاتخاذ الإجراءات اللازمة.
وقد استلهمت قيمة الاهتزاز من مجتمع العناكب الاجتماعية،
والذي هو قيمة تأثير جهاز التوجيه الانثى على كل تدفق يمر من خلاله.
وقد تم استخدام برنامج محاكاة شبكة NS3 لتوليد بيانات الشبكة. ثم الحصول على النتائج واختبار النظام بواسطة برنامج مبرمج باستخدام لغة C++. وعلاوة على ذلك، طبقت عدة تجارب، وتم
اعتماد تجربتين لاختبار النظام المقترح، الأول هو 90 ثانية، في حين أن الثانية هي 1200 ثانية.
أجريت هذه التجارب لتوليد البيانات العادية وكذلك توليد بيانات هجوم
الفيضان الموزع للحرمان من الخدمة للنوعين TCP و UDP.