بحث عن استخدام الذكاء الاصطناعي في مجال اختبار اختراق الشبكات

اعداد طلاب قسم هندسة برمجيات مستوى ثالث في جامعة سبأ

محمد حسن النجار

احمد عبدالملك العرشي

الجمهورية اليمنية _ صنعاء

1/1/2019

1/1/2021

بسم الله الرحمن الرحيم

قمنا بأعداد هذه الاوراق التي أطلقنا عليها بحث وليس ورقة علمية ، في مجال اختبار اختراق الشبكات اللاسلكية بواسطة الذكاء الاصطناعي.

قمنا بكتابته باللغة العربية لدعم المحتوى العربي في هذا الجانب .

على بساطة محتوى بحثنا ، نرجوا أن يكون دافعاً لغيرنا للدخول الى هذا الحقل والإبداع فيه.

المقدمة

١-١ دافع كتابة البحث

بسبب اتجاه العالم الى انترنت الاشياء وأن اغلب الاشياء في الحياة ستكون متصلة بالانترنت ، وسيكون لديها آي بي خاص بها – من حساس قياس الضغط المزروع داخل جسد المريض الى باب ونوافذ المنزل مروراً بالسيارة الذكية

واقع مخيف أليس كذلك.....

المشكلة البحثية ٢-١

التعامل الخاطئ مع اعدادت الشبكة

٣-١ الهدف

تصميم الشبكات بكل سهولة وأمان عالي

الانشطة ٤-١

تصميم ذكاء اصطناعي يتم تعليمه على تصميم وتشييد وادارة وصيانة انواع الشبكات الشائعة مثل

LAN , MAN , WAN

سواءً سلكيه ام لاسلكيه.

وبعد ذلك يتم تدريب هذه الآلة على طرق تأمين وحماية الشبكات من تشفير والتقنية الافتراضية وأساليب مصادقة وفلترة البيانات ومبادئ الجيل الجديد من الجدران النارية مثل

Sophose XG , PalAlto 8

وبعد ذلك يتم تدريب الآلة على أساليب أختبار الاختراق مع التركيز في البداية على الهجمات الخاصة بالشبكات اللاسلكية وبعد ذلك يتم تدريب الآلة على عدد من لغات برمجة السكربتات مثل بايثون وروبي ، وبعض اللغات المتدنية المستوى مثل لغة السي بالاضافة الى لغة الجافا

من خلال هذا نضمن بصورة كبيرة قدرة الآلة على تصميم وتنفيذ خوارزميات تساهم في أداء المراحل الثلاث السابقة بما فيها من عمليات بكل جاهزية ووثوقية وأمن وأمان.

حيث سيتم تنفيذ جميع الخطوات السابقة أو بعضها بحسب حجم الشبكة ودرجة الأمن المطلوبة

١-٥ الملخص

آلة ذكاء اصطناعي تقوم بالمهام الملقاة على عاتق مهندسي الشبكات ومختصي أمن المعلومات

٢- الاعمال السابقة

- Applications of Artificial Intelligence (AL) to Network Security
- Alberto Perez Veiga
- University of Maryland University College
- March 2018

٢-١ تناول الورقة العلمية

" الهجمات على الشبكات أصبحت أكثر تعقيداً كل يوم ، أيضاً أصبح بإستطاعة من يطلق عليهم أطفال السكربتات اختراق الشبكات !

حيث يقوم المهاجمون بالبحث للحصول على منافع جدية جراء اختراق الشبكات.

الحكومات ، الشركات الكبرى ، المنظمات الاجرامية أصبحت كلها مهتمة وبشكل متزايد بالحصول على مصادر في هذا المجال وتطوير قدراتها الحالية للتجسس وسرقة وتدمير المعلومات بكفاءة عالية.

الطرق التقليدية لحماية الشبكات أصبحت غير فعالة وأصبح التركيز الآن على التقنيات الذكية لتحديد التهديدات" (بتصرف)

Applications of Artificial Intelligence (AL) to Network Security

٢-٢ نقاط ضعف الورقة العلمية

١- لم يتم التطرق الى التعلم العميق
فيما يتعلق بتعلم الآلة لتطبيق الذكاء الاصطناعي في حماية الشبكات.
٢-لم يتم التطرق الى الشبكات المعرفة برمجيا
(SDN)

-مستويات عمل الذكاء الاصطناعي تتم في ثلاث مراحل أولاً الذكاء الاصطناعي ، ثانياً تعلم الآلة ، ثالثاً التعلم العميق .

لم يذكر الباحث كيف أنه سيتمكن من تطبيق الذكاء الاصطناعي في حماية الشبكات بهذه الفعالية دون تعليم الآلة بشكل عميق ، حيث سيتم تعليم الآلة بدلاً عن عشر مرات على تقسيم عناوين الشبكة

IP Subneting

١٠٠٠ مرة ، وبدل تدريبها على تحديد البرمجيات الخبيثة التي تمر عبر الشبكة ١٠٠ مرة سيتم تدريبها على ذلك مليون مرة ، وبهذا يتم بناء قاعدة معرفية كبيرة واستراتيجية تجعل هذه الآلة تستغني عن العنصر البشري.

أيضاً هناك مفهوم جديد في عالم الشبكات (الشبكات المعرفة برمجياً)

الذي سيقوم بنسف الكثير من المفاهيم والتقنيات في هذا المجال.

نقاط الانطلاق في البحث

١- تطبيق التعلم العميق في آلة الذكاء الاصطناعي

٢-جعل آلة الذكاء الاصطناعي تطبق مفاهيم

(SDN)

٣ منهجية البحث

-بسبب الاعدادات الخاطئة لأجهزة الشبكات مثل اختيار طريقة تشفير ضعيفة أو اختيار كلمة سر ضعيفة أو جعل الشبكة ظاهرة أو اعطاء تطبيقات غير موثوقة صلاحيات الجذر،

هذا يؤدي في اغلب الاحيان لاخترقا الشبكة بغض النظر عن نوعية الهجوم المستخدم وآلية عمله.

الفرضيات

الفرضية الاولى

اعداد الشبكة بشكل خاطىء(متغير مستقل) يؤدي الى اختراقها(متغير تابع)

الفرضية الثانية

عدم تدريب موظفي تقنية المعلومات على كشف ومنع هجمات

الهندسة الاجتماعية (متغير مستقل) يؤدي الى اختراقها(متغير تابع)

الفرضية الثالثة

الاعتماد على الذكاء الاصطناعي بدلاً عن العنصر البشري في مجال أمن المعلومات سيؤدي الى تقليل عوامل اختراق الشبكات بل وجعل ذلك شبه مستحيل

٤ـ التطبيق

-سيتم استخدام المنهجين الوصفي والتجريبي في اثبات الفرضيات السابقة

اولاً المنهج الوصفي:-

سنقوم بجمع استبيانات من شركات عدة توضح مدى تدريب كوادر تقنية المعلومات لديها في مجال أمن المعلومات مع التركيز على الهندسة الاجتماعية.

ثانياً المنهج التجربي:-

سيتم استخدام برمجيات الانظمة الوهمية التي سنقوم فيها بعمل اعدادت خاطئة لاجهزة الشبكات، بعد ذلك سنقوم بعمل اختبار اختراق لهذه الاجهزة .

أيضا سيتم تصميم آلة ذكاء اصطناعي بمواصفات متوسطة وذلك بشكل افتراضي وتدريبها على المجالات بالشبكات تصميمها وتشييدها وادارتها وحمايتها واختبار اختراقها

٥- النتائج

لم يتم اثبات او نفي الفرضيات السابقة (نظراً لضيق الوقت)

٥-١ التوصيات

١- ضرورة تدريب كوادر تقنية المعلومات في الشركات بالمستوى الذي يتناسب مع حجم الشركة.

٢-تصميم انظمة ذكاء اصطناعي يتم الاعتماد عليها في جانب أمن المعلومات بدلاً من العمل البشري.

٣- صعوبة تطبيق مفهوم انترنت الاشياء إلا بوجود أنظمة الذكاء الاصطناعي مساندة لجوانب أمن المعلومات

٢-٥ الاعمال المستقبلية

تطبيق البحث في جوانب الاتصالات الاخرى مثل اتصالات الاقمار الصناعية

٣-٥ معدل الخطأ

١- احتمال الوصول الفيزيائي لأجهزة الشبكة وتعطيلها

٢-احتمال تصرف الآلة بشكل غير متوقع(سلبي)

٣-احتمال وجود آلة ذكاء اصطناعي تقوم بعمل معاكس