البحث الثامن

أولا: الملخص باللغة العربية

مع الزيادة المطردة في الاعتماد على شبكات الحاسب الآلي في الأنظمة الحرجة وشبكات الكمبيوتر الكبيرة والموزعة في جميع نواحي الحياة. أصبحت شبكات الحاسب الآلي أكثر عرضة للاختراقات مما يعرضها للعديد من التهديدات الكبيرة وبخاصة في السنوات الاخيرة. وعلى الرغم من وجود أنظمة مختلفة لحماية الشبكات من هذه التهديدات مثل: " الجدران النارية، ومصادقة المستخدم، وتشفير البيانات"، الا أن هذه الانظمة لم تنجح في توفير الحماية الكاملة للشبكات وأنظمتها بشكل تام من الهجمات المعرضة لها والتي تزداد تطوراً مع الوقت. ولهذا تقتضي الحاجة الى استخدام نظم كشف الاختراقات والتسلل على نطاق واسع ليكون خط الدفاع الثاني لأنظمة شبكات الحاسب الآلي جنباً إلى جنب مع تقنيات أمن الشبكات الأخرى. والهدف الرئيسي من أنظمة كشف الاختراقات هو الكشف عن الاستخدام غير المصرح به لأنظمة الحاسب الآلي من قبل كل المستخدمين لهذه الانظمة سواء من مستخدمين مصرح لهم او من المتسللين الخارجين.

تعتمد أنظمة كشف الاختراقات على مقارنة السمات المتوفرة للاستخدام المسموح به للمستخدمين والسمات التي تميز أنواع الهجمات المختلفة لتمييز إذا ما كان الاستخدام الذي يتم الآن هو استخدام آمن أم هو اختراق لأمن الشبكة. وقد قدمت العديد من أنظمة كشف الاختراقات في الكثير من الابحاث السابقة معتمدة على خوارزميات وتصاميم مختلفة ومنها ما يحقق نسب جيدة في كشف الاختراقات الا أن الابحاث الاخيرة أوضحت أن عدم اختيار السمات ذات الصلة والتي تميز الاتصال الآمن من الاتصال غير الآمن أو السمات التي تميز الاتصال المحتوى على نوع معين من التهديدات أو الاختراقات عن الاتصال الآمن يتسبب في تقليل نسب النجاح لهذه الانظمة ونسب قدرتها على كشف الاختراقات بنسب نجاح عالية، مما يحث العديد من الباحثين لمحاولة ايجاد أفضل مجموعة من السمات ذات الصلة بأنواع الهجمات المختلفة.

وأصبحت عمليات الاختراق تمثل التهديد الأكبر لشبكات الحاسب في السنوات الأخيرة لذلك يتم استخدام أنظمة كشف الاختراقات على نطاق واسع كإجراء دفاعي لشبكات الحاسب الآلي .وبالتالي، فإن بناء نظام لكشف الاختراق ذو كفاءة عالية في كشف هذه الاختراقات بشتى أنواعها هو أحد الموضوعات البحثية المطروحة بشكل كبير حالياً في مجال تأمين الشبكات .

في هذه الورقة، اقترحنا نموذج معزز لتحديد مجموعة من أهم سمات ذات الصلة لكشف التسلل/ الاختراقات بشبكات الحاسبات الآلية، واختيار الميزات الأكثر صلة التي تساعد في بناء نظام كشف التسلل/ الاختراقات بكفاءة عالية وسرعة أداء ودقة في النتائج مع أقل استهلاك للموارد مع الحفاظ على أعلى معدلات الكشف والأداء.

البحث الثامن (تابع)

وقد تم إجراء تحليل لأهم الميزات المستخدمة في قاعدة البيانات المرجعية (KDD'99)، والتي تستخدم على نطاق واسع كقاعدة بيانات قياسية لقياس فاعلية أنظمة كشف التسلل/الاختراقات. يتكون النموذج المقترح من أربع مراحل، المرحلة الأولى ما قبل معالجة البيانات، المرحلة الثانية اختيار أفضل مصنف، المرحلة الثالثة اختيار أهم الميزات/السمات واستبعاد السمات غير ذات الصلة، المرحلة الرابعة اختيار أفضل الميزات/السمات ذات الصلة بكشف أنواع الهجمات المختلفة. واقترحنا مجموعة متكاملة لتقييم الميزات /السمات ومقارنة طرق اختيار الميزات/السمات لتحديد مجموعة من أفضل الميزات ذات الصلة التي تحتوي على ١٢ ميزات/سمات فقط من إجمالي ٤١ ميزات/سمات مقترحة من خلال قاعدة البيانات المرجعية (KDD'99).

مما يقلل من حجم بيانات (KDD'99) بأكثر من ٧٠٪. وأظهرت النتائج إلى أن الميزات/السمات أرقام (١٥، ١٩، ٢٠، ٢١) ليست ذات صلة بأي نوع من الهجمات. من ناحية أخرى، أظهرت النتائج أن الميزات/السمات أرقام (١، ١٤) هي ذات أهمية كبيرة للكشف عن الهجمات من نوع (U2R)، وأن الميزات/السمات أرقام (١٠، ٣٦) هي ذات أهمية كبيرة للكشف عن الهجمات من نوع (R2L)، وأن الميزات/السمات أرقام (٢٧، ٣٨) هي ذات أهمية كبيرة للكشف عن الهجمات من نوع (PROBE). وعلاوة على ذلك، فإن الميزات/السمات أرقام (٣، ٥، ٦، ٢٣، ٣٣، ٣٥) وثيقة الصلة للغاية للكشف عن أكثر من نوع من أنواع الهجمات وتحديدا (DOS, PROBE, and R2L).

وقد قمنا بقياس أداء النموذج المقترح والتحقق من فعاليتها وجدواها من خلال مقارنتها مع تسعة نماذج مختلفة ومع النموذج الذي استخدم البيانات الكاملة لقاعدة البيانات المرجعية المستخدمة في البحث (٤١-من الميزات والسمات). وأظهرت النتائج أن يمكن للنموذج المقترح أن يعزز ويحقق ارتفاع معدلات كشف الاختراقات ويرفع من معدلات الأداء، ويخفض معدلات الانذار الكاذب، ويعطى عملية كشف للاختراقات سريعة وموثوقة وذات كفاءة.