بسم الله الرحمن الرحيم

جامعة الملك سعود
كلية علوم الحاسب و المعلومات
قسم نظم المعلومات

متأخر

أنظمة كشف التطفل
(Intrusion Detection Systems)

إعداد:
محمد الرشيدي

مقدمة:

بعد أن أصبح الأتصال بالإنترنت مطلب أساسي و مهم لكثير من الشركات و المؤسسات بإختلاف أحجامها، أصبح أيضا من المهم جدا حماية الشبكات المحلية لهذه الشركات من الأخطار المحتملة من عملية الإتصال بالإنترنت. حيث يوجد في الإنترنت يوميا وفي كل لحظة آلاف الأشخاص الذين يحاولون التسلل إلى الشبكات المحلية. وغالبا ما يستهدف هؤلاء المتطفلون الموارد الخاصة بهذه الشبكات وتشمل هذه الموارد جميع المكونات البرمجية والمادية (مثل الأجهزة الخادمة، الطابعات، قواعد البيانات و ماتحتويها من بيانات سرية...إلخ).

ففي السابع من شهر أكتوبر عام 1999، تمكن مجموعة من الأشخاص من التسلل إلى شبكة وكالة ناسا الفضائية. وكان هذا التسلل يعتبر عملية ضخمة في حد ذاتها كما أنه تم بصورة خفية جدا. فقد صرح مسؤول في الوكالة أنه من الصعب معرفة مدى الأضرار التي حصلت. كما إن هؤلاء الأشخاص لم يقوموا بإغلاق أنظمة الوكالة. كل مافعلوه أنهم قاموا بالوصول إلى الملفات الموجودة في مجلدات الموظفين، بالإضافة إنهم قاموا بوضع ملفات أبواب خلفية حتى يتمكنوا من العودة لاحقا عن طريق هذه الأبواب الخلفية.
لذلك أصبح من المهم جدا الحفاظ على مستوى الأمن بقدر ما نستطيع حتى لا نصبح عرضة للأخطار القادمة إلينا. فمع التقدم في أنظمة حماية الشبكات أصبحت العملية في متناول يد الجميع، و لكن يجب أن نختار منها ما يناسب احتياجاتنا الأمنية و نستخدمه بشكل فعال و مناسب.
ويعتبر نظام إكتشاف التطفل من أحد هذه الأنظمة و سنتحدث عنه بشئ من التفصيل.

تعريف أنظمة كشف التطفل وإستخداماتها:

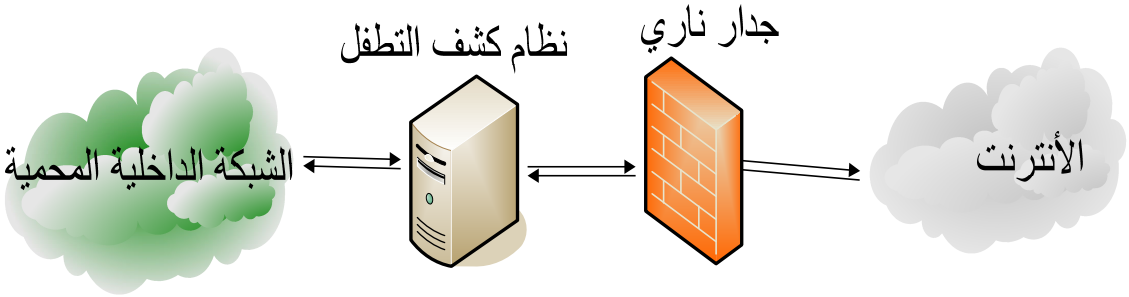
تستخدم أنظمة كشف التطفل لمراقبة أمن الشبكات الداخلية، فهي تقوم بجمع و تحليل البيانات من مناطق مختلفة من الشبكة و ذلك لمعرفة و إكتشاف ما إذا هنالك أي تسلل أو إستخدام سئ للشبكة. ويوجد هنالك نوعان لهذه الأنظمة:

أنظمة كشف التطفل المرتكزة على أجهزة الحاسوب:

يتم تحميل هذا النوع على بعض أجهزة الحاسوب المتصلة الشبكة (مثل الخوادم أو الحاسبات الشخصية) وفي بعض الأحيان يتم تحميله على جميع الأجهزة.فبعد تحميله يقوم هذا النظام بمراقبة مستمرة لملفات نظام التشغيل الحساسة، الأنشطة التي تتم على هذا الجهاز، مستوى أداء المعالج و الذاكرة الرئيسية بالإضافه إلى أنه يقوم بعملية تدقيق للبيانات الموجودة في سجلات نظام التشغيل وتشتمل هذه السجلات على الرسائل الصادرة بخصوص أخطاء في البرامج المحملة أو الرسائل الأمنية. وفي عملية المراقبة يقوم النظام بالبحث عن أي إشارة تدل على أنه يوجد نشاط مشبوه على الجهاز، فعلى سبيل المثال إذا قام أحد الأشخاص بمحاولة إختراق الجهاز عن طريق إغراقه بكمية بيانات ضخمة فإن نظام كشف التسلل سيقوم بكشف هذه المحاولة وإيقاف هذا الهجوم بإستخدام الآليات المناسبة وفي هذه الحالة يسمى النظام بنشط، أما إذا لم يقم النظام بإيقاف هذا الهجوم و أكتفى بإرسال رسالة تحذيرية إلى المستخدم فإنه يسمى بغير نشط.

أنظمة كشف التطفل المرتكزة على الشبكة:

على خلاف النوع الأول تقوم الأنظمة المرتكزة على الشبكة بمراقبة الأنشطة التي تتم في الشبكة و ليس فقط على مستوى الجهاز الواحد. وعادة مايوضع هذا النوع على مداخل الشبكة، كما يمكن وضعه في الشبكة الداخلية نفسها و ذلك لإكتشاف الإستخدام السئ للموارد من قبل المستخدمين أو الموظفين. في الشكل1 يوجد لدينا شبكة داخلية متصلة بالأنترنت عن طريق جدار ناري، ويظهر لنا نظام كشف التطفل بين الجدار الناري و الشبكة الداخلية. تقوم أنظمة الجدر النارية بترشيح حزم البيانات القادمة إلى و من الشبكة عن طريق النظر في مصدرهذه الحزم و الجهة المراد الوصول إليها أما بالنسبة لأنظمة كشف التطفل فإنها تقوم بتحليل هذه الحزم ومعرفة ما إذا كانت تهدف إلى عملية تطفل و هجوم على الشبكة.



(شكل1: مثال على إستخدام نظام كشف التطفل في شبكة محلية)

تعتمد أنظمة كشف التسلل في عملية المراقبة على طريقتين:

الطريقة الأولى: أنها تقوم بالمراقبة و البحث عن إمضاءات معرفة مسبقا تدل على وجود عملية تطفل أو هجوم، وتكون هذه الإمضاءات مخزنة مسبقا في قاعدة بيانات خاصة بالنظام (تستخدم نفس هذه الطريقة في برامج مكافحة الفيروسات). وفي حالة عدم وجود الإمضاء فإن النظام لن يتمكن من معرفة وكشف عملية التطفل.

الطريقة الثانية: أنها تقوم بالمراقبة والكشف عن أي نشاط يكون غير طبيعي في الشبكة، و تقوم بإرسال تقرير عن هذا النشاط. وغالبا ماينتج تقارير خاطئة عن هذه الطريقة.

مكونات نظام كشف التطفل:

يمكن تقسيم مكونات أنظمة كشف التسلل إلى ثلاثة أجزاء رئيسية:

1- المجسات:
تكون مهمة المجسات متعلقة بعملية جمع البيانات، وتستخدم هذه البيانات في عملية المراقبة و الكشف. وكأمثلة على البيانات المدخلة للمجسات: حزم البيانات القادمة من كرت الشبكة و الرسائل الموجودة في سجلات نظام التشغيل.

2- البرامج المحللة:
تقوم هذه البرامج من إستقبال البيانات من المجسات، ثم تقوم بتحليل هذه البيانات و تحديد ما إذا هنالك تطفل أو هجوم.

3- واجهة البرنامج للمستخدم:
تمكن واجهة البرنامج المستخدم من عرض تفاصيل مخرجات النظام. كما يمكنه من تهيئة النظام بشكل جيد و مناسب.

خاتمة:

تعتبر قضية أمن الشبكات المحلية من الأمور المهمة في الوقت الحاضر خصوصا مع إنتشار وكثرة وسائل التسلل و الهجوم على الشبكات، ولتوفيرالمستوى الأمني الذي تتطلع إليه أي منشأة يوجد هنالك العديد من الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. وقد تحدثنا هنا عن إحدى الوسائل التي يمكن تطبيقها وهي أنظمة كشف التطفل. تعتبر هذه الأنظمة مناسبة و فعالة إذا ماتم إختيارها و تهيئتها بشكل مناسب للمتطلبات الأمنية الخاصة بالمنشأة. كما يمكن الحصول على كفاءة أعلى عن طريق إستخدام هذه الأنظمة مع أنظمة أخرى مثل الجدر النارية.

المراجع:

[1] M. Ciampa, "Security+ Guide to Network Security Fundamentals", 2nd edition, Thomson, 2005.
[2] J. Brook, "Network IDS: To Tailor, or Not to Tailor", SANS Institute, 2002.
[3] D. Mathew, "Choosing an Intrusion Detection System that Best Suits your Organization", SANS Institute, 2002.
[4] T. Holland, "Network Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth", SANS Institute, 2004.
[5] K. Buonocore, "Selecting an Intrusion Detection System", SANS Institute, 2001.
[6] D. Ford, "8 Simple rules for securing your internal network", SANS Institute, 2003.
[7] T. Bradley, "Introduction to Intrusion Detection Systems (IDS) ", http://netsecurity.about.com/cs/hackertools/a/aa030504.htm
[8] J. McHugh, A. Christie, and J. Allen, "The Role of IntrusionDetection Systems", http://www.computer.org/software/so2000/pdf/s5042.pdf
[9] M. Ranum, "Coverage in intrusion detection systems", http://philby.ucsd.edu/~cse291_IDVA/papers/orig_names/Coverage-in-IDS-White-Paper-final.pdf.