ITRAINONLINE MMTK

إدارة ومراقبة الشبكة – كراسة المتدرب

إعداد: ألبيرتو إسكوديرو باسكال / IT +46
النسخة العربية: أنس طويلة، www.tawileh.net/anas

ITRAINONLINE MMTK.....1
1. عن هذا المستند.....2
1.1. معلومات حفظ الملكية الفكرية.....2
2.1. درجة الصعوبة.....2
2. مقدّمة.....2
3. الأهداف في مقابل مراقبة البيانات.....3
4. مراقبة أهداف الخدمة Monitoring Service Goals.....3
1.4. توفير نفقات عرض الحزمة الدولي.....4
2.4. توفير جودة أفضل لخدمة نقل الصوت عبر بروتوكول الإنترنت VoIP.....4
3.4. إدارة الخدمة وتوسّع الشبكة.....4
5. المبادئ التقنيّة Technical Principles.....5
1.5. بروتوكول إدارة الشبكة البسيط SNMP.....5
2.5. محاسبة حركة البيانات Traffic Accounting.....6
3.5. تشذيب سيل البيانات Traffic Shaping.....7
3.51.. ضبط طوابير البيانات والتأخير Queuing disciplines and latency.....8
3.52.. إدارة عرض الحزمة عبر التحكّم باصطفاف الحزم Bandwidth Management by Packet Queuing.....9
4.5. المصافي الديكارتيّة Bayesian Filters.....10
5.5. بصمات الفيروسات Viruses Fingerprints.....11
6. الأدوات Tools.....11
1.6. مراقبة الشبكة اللاسلكية.....12
2.6. أداة MRTG.....12
3.6. مراقبة متغيرات الشبكة اللاسلكية باستخدام أداة MRTG.....12
3.61.. مراقبة عرض الحزمة Bandwidth Monitoring.....13
3.62.. مراقبة نسبة الإشارة للضجيج Signal/Noise Ratio Monitoring.....13
4.6. أداة Ntop.....17
5.6. أداة Spam-Assassin.....18
5.61.. قواعد بيانات تعريف الرسائل المرسلة عشوائيًّا التشاركيّة Collaborative Spam Identification Databases.....19
5.62.. قوائم حجب DNS DNS Blocklists.....19
6.6. أداة Clam AntiVirus (CLAM AV).....20
7. الخلاصة.....21
8. الملحق 1.....22

1.عن هذا المستند

تشكل هذه المواد التدريبية جزءاً من حزمة تدريب الوسائط المتعددة Multimedia Training Kit (MMTK). توفر هذه الحزمة مجموعةً متكاملةً من المواد التدريبية والموارد الداعمة للإعلام الإجتماعي، مراكز الوسائط المتعددة للمجتمعات، مراكز الولوج البعيد وغيرها من المبادرات باستخدام تقنيات المعلومات والإتصالات لتدعيم المجتمعات ودعم نشاطات التنمية.

1.1 معلومات حفظ الملكية الفكرية

لقد تم إصدار هذه الوحدة ضمن إتفاقية الترخيص Creative Commons Attribution-NonCommercial-ShareAlike 2.5 السويد. للحصول على المزيد من المعلومات عن كيفية استخدام هذه المواد يرجى الإطلاع على نص حماية الملكية الفكرية المضمن مع هذه الوحدة أو راجع http://creativecommons.org/licenses/by-nc-sa/2.5/se/

2.1 .درجة الصعوبة

درجة صعوبة هذه الوحدة: متقدّم.

2. مقدّمة

يتطلّب ضمان توفير خدمةٍ معيّنةٍ ضمن الشبكة القيام باستمرارٍ بمراقبة العديد من جوانب نظام الإتصالات. تعتبر القدرة على تمييز المعلومات القيّمة والحصول على البيانات من النظام شرطين أساسيين للتمكّن من اتخاذ القرارات الصحيحة.

لسوء الحظ، لن تتمكّن البيانات وحدها من حل المسألة، فالبيانات ليست بالضرورة معلومات، والحصول على المعلومات لا يعني بالضرورة أيضاً حصولك على المعرفة.

ينبغي أن يكون نظام مراقبة (إدارة) الشبكة قادراً على:

- استحصال / تجميع البيانات الضروريّة من النظام.
- معالجة وعرض البيانات.
- عرض البيانات المجمّعة بمستوياتٍ مختلفةٍ من التفصيل.
- إتخاذ القرارات تلقائيّاً عند الحاجة.

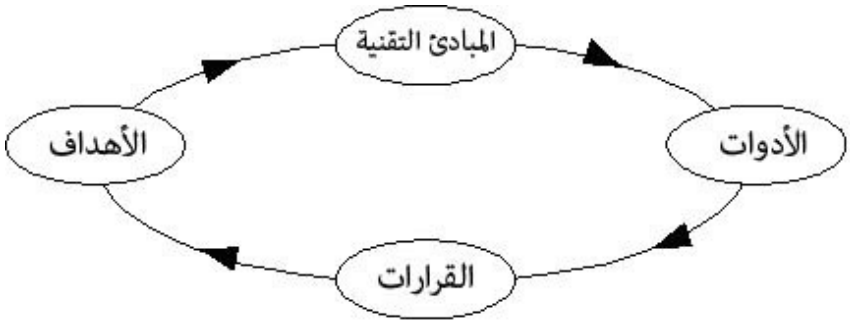
من الأخطاء الشائعة في عالم مزوّدي خدمات الإنترنت ISPs تبنّي أسلوبٍ يعتمد على الأدوات tool-centric في اتخاذ القرار. على سبيل المثال، عند تركيب أداة إدارةٍ معيّنةٍ في نظامٍ لإدارة الشبكة يتم اتخّاذ جميع القرارات بناء على إمكانيّات هذه الأداة عوضاً عن أهداف وأولويّات مزوّد الخدمة.

تعتمد هذه الوحدة أسلوباً مبنيّاً على الأهداف goal-centric في إدارة الشبكة. تقدّم هذه الوحدة (بعكس الأسلوب المعتمد على الأدوات) منهجيّةً لإدارة الشبكة تبدأ بتحديد أهدافٍ واضحةٍ لإيجاد الأدوات الصحيحة.

3. الأهداف في مقابل مراقبةالبيانات

تعتبر الخطوة الأولى والأكثر أهميّةً والتي يجب على أيّ مزوّدٍ لخدمات الإتصالات / الإنترنت اتخاذها قبل البدء بتركيب أيّ نوعٍ من أدوات المراقبة تحديد الأهداف التي يريد تحقيقها والتحديّات التي يواجهها.

يعتبر تحديد (1) **الهدف** أمراً أساسيّاً للتفكير (2)**بالمبادئ التقنيّة** المطلوبة للحصول على المعلومات الضروريّة من النظام. يمكّننا تحديد المبادئ التقنيّة من اختيار، تصميم وتركيب (3) **الأدوات** اللازمة. توفّر المعلومات التي ستقدّمها هذه الأدوات معرفةً إضافيّةً لإتخاذ (4) **القرارات** الصائبة.



شكل 1: يظهر المنهجيّة المعتمدة على الأهداف لمراقبة (إدارة) الشبكة

4. مراقبةأهداف الخدمة Monitoring Service Goals

سنحاول في سبيل استعراض هذا الأسلوب المنهجي لمراقبة الشبكة تحديد ثلاثة أهدافٍ مختلفةٍ شائعةٍ في أيّة شبكةٍ لاسلكيةٍ:

1. توفير النفقات عبر تخفيض استخدام عرض الحزمة الدولي
2. توفير جودة أفضل لخدمات نقل الصوت عبر بروتوكول الإنترنت VoIP
3. إدارة الخدمة وتوسّع الشبكة

تظهر الجداول التالية كيفيّة استخدام هذه الأهداف للمبادئ التقنيّة الأساسيّة وكيف يتطلّب كلٌ من هذه الأهداف تجميّع المعلومات من جميع طبقات نموذج OSI المعياري لنظام الإتصالات.

تؤثّر الأهداف في الشبكات اللاسلكية (تماماً كما هي الحال في أيّ نظام إتصالاتٍ آخر) على جميع طبقات نموذج OSI المعياري. لذلك يتوجّب علينا لضمان جودة الخدمة أن نستوعب جميع جوانب شبكة الإتصالات وليس تلك المتعلّقة بالشبكة اللاسلكية وحسب.

1.4 .توفيرنفقاتعرض الحزمةالدولي

الطبقة	المبدأ التقني
التطبيقات Application	التخزين المؤقت Caching، كشف / إيقاف الرسائل غير الموجّهة Spam والفيروسات (المصافي الديكارتيّة Bayesian Filters)
النقل Transport	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
الشبكة Network	التحكّم بالوصول إلى الشبكة Network Access Control (جدار النار Firewalling) تشذيب سيل البيانات محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
التحكّم بالوصول إلى الناقل Media Access Control	التحكّم بالوصول إلى الشبكة اللاسلكية Wireless Access Control تجميع بيانات الطبقة الثانية اللاسلكية (SNMP)

جدول 1: المبادئ التقنيّة (وطبقات نموذج OSI الموافقة) التي يمكن استخدامها لتوفير عرض الحزمة الدولي

2.4.توفير جودة أفضل لخدمة نقلالصوت عبر بروتوكولالإنترنت VoIP

الطبقة	المبدأ التقني
التطبيقات Application	
النقل Transport	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
الشبكة Network	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
التحكّم بالوصول إلى الناقل Media Access Control	تجميع بيانات الطبقة الثانية (SNMP) تخفيض التأخير اللاسلكي Wireless Latency

جدول 2: المبادئ التقنيّة (وطبقات نموذج OSI الموافقة) التي يمكن استخدامها لتوفير جودةٍ أفضل لخدمة VoIP

3.4 . إدارة الخدمة وتوسّع الشبكة

الطبقة	المبدأ التقني
التطبيقات Application	Virus/Spam, SQL (موازنة الخدمات Service Balancing)
النقل Transport	تجميع إحصاءات بروتوكولات TCP/UDP موازنة استخدام الجدران الناريّة Firewall Balancing
الشبكة Network	تجميع إحصاءات طبقة بروتوكول الإنترنت IP مبادئ التوجيه Routing Principles
التحكّم بالوصول إلى الناقل Media Access Control	تجميع بيانات الطبقة الثانية (SNMP)

جدول 3: المبادئ التقنيّة (وطبقات نموذج OSI الموافقة) التي يمكن استخدامها لإدارة الخدمة وتوسّع الشبكة

يؤدّي الإخفاق في إعدادٍ أيٍّ من الطبقات بشكلٍ أمثل إلى التأثير على أداء الخدمة بأكملها. على سبيل المثال: تؤثّر المستويات المرتفعة من الحزم المعطوبة في الشبكة اللاسلكية على أداء بروتوكول TCP بأكمله مما يؤدّي إلى تأخّرٍ ملحوظٍ في تخديم مستخدمي تطبيقات الزمن الحقيقي Real-time.

لا تتجلى الصعوبة في استيعاب جميع طبقات الإتصال المتعلقّة بالنظام وحسب، بل من ضرورة الإلمام بالتداخلات والتفاعلات المختلفة بين هذه الطبقات أيضاً.

تماماً كما في جميع أنظمة الإتصالات، يمكنك بناء شبكةٍ لاسلكيةٍ بسهولة، أما بناء شبكةٍ لاسلكيةٍ ذات أداءٍ جيّدٍ فيتطلّب منك الكثير من الوقت والخبرة. هذا هو المبدأ الذي بني عليه نجاح الإنترنت بأكملها!

5.المبادئ التقنيّة Technical Principles

سنقوم بشرح المبادئ التقنيّة التي تعتمد عليها أدوات مراقبة (إدارة) الشبكة قبل مناقشة هذه الأدوات. يمكن تطبيق بعض هذه المبادئ بأشكالٍ عدّةٍ لتحقيق أهدافٍ مختلفةٍ. تستخدم الأدوات عادةً مجموعة جزئيّةً من إمكانيّات مبدأٍ تقنيٍّ.

سيساعدك استيعاب المبادئ التقنية بالإضافة إلى اختيار الأدوات الصحيحة على تصميم أداةٍ جديدةٍ في حال عدم توفّر أداةٍ جاهزةٍ تلبّي كل متطلباتك.

1.5.بروتوكول إدارة الشبكة البسيط SNMP

بروتوكول إدارة الشبكة البسيط (Simple Network Management Protocol (SNMP هو بروتوكولٌ للإدارة والصيانة صمّم خصيصاً للشبكات الحاسوبيّة وتجهيزات الشبكة الإفراديّة.

طورّت النسخة الأولى من بروتوكول SNMP (SNMPv1) من قبل فريق عمل هندسة الإنترنت IETF في العام 1993. تعتمد حاليّاً النسخة الثالثة SNMPv3 إلا أنّ غالبية تجهيزات الشبكات اللاسلكية تدعم النسخ الأقدم فقط.

يعتمد تجميع المعلومات على بنيّة المخدّم / الزبون حيث يقوم برنامجٌ زبون بطلب المعلومات الإحصائيّة والبيانات الخاصّة من تجهيزات الشبكة البعيدة. SNMP هو بروتوكول طبقة التطبيقات Application Layer المستخدم لتبادل المعلومات.

يحتوي كل جهازٍ يدعم بروتوكول SNMP على قاعدة بياناتٍ تدعى MIB (قاعدة معلومات الإدارة Management Information Base). تحتوي قاعدة البيانات هذه على المعلومات التي يتم تجميعها أثناء عمل الجهاز. يمكن القول بأنّ بروتوكول SNMP يشكّل آليّة إرسال الطلبات واستقبال الردود عن معلومات الإدارة من العناصر الفعّالة في الشبكة.

تكمن أهمّ نقاط القوّة في بروتوكول SNMP والتي يعود إليها الفضل الرئيسي في شعبية وانتشار هذا البروتوكول في دعمه للتفاعل بين تجهيزات الشبكة المختلفة Interoperability. تتفاوت تجهيزات الشبكة التي تدعم وكلاء SNMP Agents من الموجّهات، الحواسب والجسور إلى المودمات والطابعات.

كما تتيح مرونة بروتوكول SNMP إمكانيّة توسيعه ليتضمنّ بياناتٍ خاصةٍ بكل جهاز. يقوم معظم منتجو التجهيزات اللاسلكية بتضمين مجموعةٍ خاصّةٍ Proprietary من معلومات الشبكة اللاسلكية في قواعد معلومات الإدارة MIB ضمن منتجاتهم, قد يعني ذلك ولسوء الحظ أنّه وعلى الرغم من قيام جميع المنتجين بتضمين دعم البروتوكول SNMP فإنّ آليّات تجميع بعض أنواع معلومات الشبكة اللاسلكية قد تختلف فيما بينها.

يوفّر منتجو تجهيزات الشبكة اللاسلكية لزبائنهم عادةً "أدوات إدارةٍ" خاصّةٍ بهم تستخدم بروتوكول SNMP للتواصل مع التجهيزات التي ينتجونها. يعتبر تركيب أدوات الإدارة المختلفة من عدة منتجين أمراً معقدّاً جدّاً لأنّ هذه الأدوات نادراً ما تكون مفتوحة المصدر. قد يتمثّل الخيار الأفضل بقيامك بكتابة نظام إدارة الشبكة اللاسلكية الخاص بك.

يحتوي بروتوكول SNMP أيضاً على نقاط ضعفٍ عدّةٍ. لا يسهل استخدام هذا البروتوكول على المبرمجين نظراً لقواعد الترميز المعقّدة التي يستخدمها كما يؤخذ عليه قلّة فاعليته وإضاعته لعرض حزمة الشبكة. تتضمّن كلّ حزمة SNMP العديد من حقول البيانات عديمة الأهميّة كما يتم ترميز متغيرات SNMP بأساليب تجعل حجم حزمة البيانات كبيراً بشكلٍ غير مبرر.

عليك الإنتباه إلى النقاط التالية عند تركيب أي نظام مراقبةٍ يعتمد على بروتوكول SNMP:

1. يؤدّي استخدام بروتوكول SNMP إلى زيادة الضغط على الشبكة. حاول تخفيض هذا الضغط باتخاذ القرارات الصائبة.

2.لا يدعم بروتوكول SNMPv1 تشفير مرحلة التحقق من الهويّة, إنتبه لكلمات السر الخاصّة بك.

3.يستهلك بروتوكول SNMP جزءاً من قدرة المعالج CPU ضمن تجهيزات الشبكة.

2.5.محاسبة حركةالبيانات Traffic Accounting

يستخدم مبدأ محاسبة حركة البيانات لمراقبة إحصاءات سير البيانات ضمن الشبكات الحاسوبيّة. تعتبر المعلومات التي يتم تجميعها من خلال محاسبة حركة البيانات ذات أهميّةٍ فائقةٍ عند اتخاذ القرارات المتعلّقة بتنظيم الشبكة، كشف الأعطال ومراقبة نشاطات الحواسب المختلفة.

من المعلومات الشائعة التي تقوم محاسبة حركة البيانات بتجميعها:

- عدد الحزم والبايتات Bytes.
- إحصاءات توزّع البروتوكولات (النوع، الأوقات، %).
- أخطاء بروتوكول الإنترنت IP Checksum Errors.
- إكتشاف الأجهزة النشطة.
- حركة البيانات بين الأجهزة.

يمكن تجميع المعلومات المتعلّقة بحركة البيانات ضمن الشبكة بطرقٍ عدّةٍ. من أكثر هذه الأساليب شيوعاً تشغيل بروتوكول SNMP في جميع موجهّات وجسور الشبكة. يستخدم بروتوكول SNMP لتجميع المعلومات المتعلّقة بالشبكة بشكلٍ **نشط Active**، لأنّ الحصول على هذه المعلومات يتطلّب تبادل حزم SNMP فيما بين الموجّهات والجسور.

يمكن أيضاً الحصول على المعلومات المتعلّقة بحركة البيانات عبر الشبكة دون الحاجة إلى زيادة الضغط على الشبكة عبر إباحة التنصّت على البيانات المنتقلة ضمن الشبكة. يعتبر التنصّت على الشبكة آليةً **خاملةً Passive** لا تتطلّب استخدام بروتوكول SNMP على الإطلاق. إلا أنّ استخدام هذا الأسلوب محدودٌ لسببين: ينبغي أن تكون قادراً على الوصول المباشر إلى البيانات المنتقلة عبر الشبكة إضافةً إلى استهلاك الكثير من قدرة المعالج CPU لتجميع واستيعاب حجم المعلومات المارّة عبر قناة الإتصال.

3.5تشذيب سيلالبيانات Traffic Shaping

وهو أسلوبٌ يستخدم للتحكّم بسير البيانات ضمن الشبكة بغية ضمان مستوىً محدد من الأداء. ينتج تشذيب سيل البيانات عن تفعيل قواعد ضبط طوابير البيانات في الموجّهات. يمكنك عبر إدارة هذه القواعد بحكمة تغيير أداء الشبكة فيما يتعلّق بـــ :

1.التأخير وإدارة الإزدحام Latency and Congestion Management

2.إدارة عرض الحزمة Bandwidth والعدالة Fairness.

يعمل تشذيب سيل البيانات عادةً في طبقة بروتوكول الإنترنت IP Layer عبر تغيير أساليب إصطفاف وتوصيل الحزم في الموجّهات. يؤثّر تشذيب البيانات ضمن طبقة بروتوكول الإنترنت على توزيع الموارد في الوصلة اللاسلكية.

من الجدير بالذكر أنّ بعض منتجي تجهيزات الشبكة اللاسلكية المعتمدة على معايير IEEE 802.11 قد حاولوا تطبيق آليّاتٍ مشابهةٍ في جسور الشبكات اللاسلكية عبر تعديل طريقة أداء طبقة IEEE 802.11 MAC التقليديّة، إلاّ أنّ غالبيّة هذه الحلول ظلّت خاصّةً بالمنتج مما لا يضمن توافقيّة هذه التجهيزات مع تلك المنتجة من قبل الآخرين.

قامت شركة Proxim على سبيل المثال بتطبيق آليّة تصويتٍ خاصّةٍ تدعى (WORP) لدعم اختناق عرض الحزمة غير المتناظر Asymmetric Bandwidth Throttling والذي يتيح تعديل سرعة استقبال أو إرسال البيانات من قبل المستخدم. تقوم آليّة WORP بتوزيع استطاعة الشبكة عبر تخصيص منافذ زمنيّةٍ وجيزةٍ لجميع المستخدمين الراغبين بإرسال أو استقبال البيانات وتعطي كلاً منهم دوراً لاستخدام عرض الحزمة.

3.51.ضبط طوابيرالبيانات والتأخير Queuing disciplines and latency

إذا أردت الحفاظ على توافقيّة التجهيزات بين المنتجين المختلفين ولم ترغب بتطبيق آليةٍ خاصّةٍ بمنتجٍ ما ضمن شبكتك يتوجّب عليك حينها تطبيق تشذيب سيل البيانات على مستوى بروتوكول الإنترنت IP.

يتم تشذيب سيل البيانات عبر التأثير على طريقة ترتيب الحزم ضمن طوابير وتوصيل هذه الحزم عبر العناصر الفعّالة في الشبكة. تطبّق قواعد ضبط طوابير البيانات على الحزم أثناء عمليّة نقل هذه الحزم. تختلف قواعد ضبط طوابير البيانات تبعاً لأولويّة حزمة البيانات، مرسل هذه الحزمة أو وضعية الطابور في تلك اللحظة.

تعتبر قواعد ضبط طوابير البيانات المطبّقة على البيانات الخارجة من الشبكة أكثر أهميّةً من تلك المطبّقة على البيانات الواردة. يتوجّب إيلاء هذه القواعد عنايةً خاصّةً لأنّ عنق الزجاجة Bottleneck (أو النقطة الأكثر ضيقاً في الشبكة) تقع غالباً عند الوصلة الخارجيّة Uplink (أو الوصلة التي تربط الشبكة بالإنترنت)، حيث يتم ضغط سيل البيانات المنتقلة ضمن الشبكة المحليّة ضمن أنبوبٍ واحدٍ.

يتألّف طابور الحزم من حاجزٍ Buffer يقوم بحفظ حزم البيانات حتى يتجاوز حجم البيانات المستقبلة في الموجّه قدرته على الإرسال. ينبغي على الموجّه إهمال الحزم التي سترد بعد امتلاء الحاجز لعدم توفّر مساحةٍ في الذاكرة تكفي لتخزينها، مما قد يؤدّي إلى إعادة إرسال هذه الحزم من حاسب المستخدم.

إذا علقت حزمةٌ ما على الحاجز لفترةٍ طويلةٍ جداً فإنّ صلاحيتها ستنتهي مما يستدعي المرسل إلى إعادة إرسال هذه الحزمة، وبالتالي زيادة الحمل على الموجّه المضغوط أساساً.

يؤدّي الضغط الشديد على الحواجز إلى ظهور تأخيرٍ شديدٍ في الشبكة عند ازدحام الوصلة الخارجيّة. تتسبب محاولات إعادة الإرسال الناتجة عن إنتهاء صلاحيّة الحزم في جعل المشكلة أكثر سوءاً.

يكمن أحد حلول مشكلة التأخير في منح بعض الحزم أولويةً أعلى من غيرها. تحصل الحزم التي تتطلب التفاعل مع المستخدم (كتطبيقات Remote Console، الألعاب والدردشة على الإنترنت ونقل الصوت عبر بروتوكول الإنترنت VoIP إلخ) على أولويةٍ أعلى من تطبيقاتٍ مثل FTP، HTTP أو SMTP والتي تعمل تفضّل الحصول على عرض حزمةٍ أوسع عن حصولها على تأخيرٍ أقل. يمكن تطبيق هذه السياسة في منح الأولويات عبر استخدام قواعد تعتمد على نوع الخدمة (ما هي بوابة TCP التي تستخدمها الحزمة).

في الحالات التي تستخدم فيها عدّة بروتوكولاتٍ نفس بوابة TCP بشكلٍ إفتراضيٍّ (مثل بروتوكولي SSH و SCP) ينبغي تطبيق سياسةٍ أخرة لتنظيم الطوابير. يستخدم كلٌّ من بروتوكولي SSH و SCP البوابة 22 بشكلٍ إفتراضيٍّ. يعتبر حجم حزم البيانات في بروتوكول SSH صغيراً جدّاً (يحتوي كلٌّ منها على بضعة أحرفٍ فقط) في حين يستخدم بروتوكول SCP حزماً ذات حجمٍ أكبر بكثير. يتطلب بروتوكول SSH (بعكس نظيره SCP) التفاعل مع المستخدم، مما قد يدعوك إلى تطبيق سياساتٍ مختلفةً لكلٍّ منهما. يمكن التأثير على الخدمات المختلفة التي تستخدم نفس البوابة عبر آليةٍ تقوم بتحديد الأولويّة بناءً على حجم الحزمة.

3.52.. إدارة عرض الحزمة عبر التحكّم باصطفاف الحزم Bandwidth Management by Packet Queuing

قد تمكنّك إدارة عرض الحزمة عبر التحكّم باصطفاف الحزم من ضمان جودة الخدمة Quality of Service (QoS) في شبكتك. تعني إدارة عرض الحزمة تحديد عرض الحزمة التي يمكن استخدامها من قبل حاسبٍ معينٍ أو لشبكةٍ فرعيّةٍ معينةٍ أو تحديد السرعة المتوفّرة لنوع محددٍ من الخدمات.

يمكن تطبيق إدارة عرض الحزمة لأسبابٍ متعددة. فقد ترغب في منع عملية نقل ملفٍ كبيرٍ من التأثير على جودة الخدمة المتوفّرة لبعض الحواسب ضمن الشبكة والتي تتطلّب عرض حزمةٍ أقل. قد ترغب أيضاً في توزيع موارد شبكتك بشكلٍ عادلٍ بحيث يحصل جميع المستخدمين على عرض حزمةٍ ملائمٍ تبعاً للثمن الذي دفعه كلٌّ منهم للحصول على هذه الخدمة.

للقيام بذلك يمكن تطبيق قواعد ضبط طوابير البيانات الفئوي Classful Queuing أو غير الفئوي Classless Queuing في الموجّهات.

يمتلك ضبط طوابير البيانات الفئوي هيكليّةٍ هرميّةٍ تحتوي على علاقات أبويّةٍ Parent / Child (تعتمد على الفئات) وميراثٌ من الخصائص. ينتمي كل مضيفٍ Host إلى فئةٍ معينةٍ يتم ضمنها تحديد الخصائص مثل عرض الحزمة الأقصى Maximum Bandwidth، خوارزمية الإصطفاف Queuing Algorithm، سقف الحد Ceiling Limit (لاستعارة عرض الحزمة) وأرقام البوابات.

يمكن باستخدام إدارة عرض الحزمة وضبط طوابير البيانات الفئوي تخصيص عرض حزمةٍ محددٍ لبروتوكولٍ ما بناءً على نوع هذا البروتوكول (بوابة TCP المستخدمة). يمكن أيضاً تخصيص عرض حزمةٍ محددٍ لعددٍ من المضيفين (بناءً على الفئة التي ينتمون إليها) لضمان عدالة توزيع موارد الشبكة.

تعتبر آليّة دلو البطاقات الهرميّة (Hierarchical Token Bucket (HTB من أكثر أساليب ضبط طوابير البيانات الفئوي شيوعاً. تستخدم هذه الآليّة لتوزيع حزم البيانات على فروعٍ مختلفةٍ لنموذج الشجرة الهرميّة تبعاً للأولويّة ولعرض الحزمة. يمكن إنشاء فئاتٍ فرعيّةٍ لإتاحة تشارك عرض الحزمة غير المستخدم بين أعضاء الفئة الواحدة (أبناء نفس هذه الفئة الفرعيّة). تستخدم هذه الآليّة أيضاً للتحكّم بعرض الحزمة الصادر ضمن وصلةٍ خارجيّةٍ. تقوم هذه الآليّة عند تطبيق قواعد ضبط الطوابير على كلّ حزمةٍ واردةٍ باستخدام وصلةٍ فيزيائيّةٍ واحدةٍ لتمثيل عدّة وصلاتٍ أبطأ وبالتالي إرسال الأنواع المختلفة من الحزم عبر وصلاتٍ إفتراضيّةٍ مختلفةٍ.

تقوم قواعد ضبط طوابير البيانات غير الفئويّة (على عكس نظيرتها الفئويّة) بمجرّد إعادة جدولة حزم البيانات، تأخيرها أو رميها.

من الآليّات الشائعة لضبط طوابير البيانات غير الفئويّة طابور العدالة العشوائيّة Stochastic Fairness Queue (SFQ) والتي تستخدم عند امتلاء الوصلة الخارجيّة. لا تقوم هذه الآليّة بأيّ تشذيبٍ لسيل البيانات بل يقتصر عملها على جدولة إرسال الحزم بحيث تحصل جميع الوصلات على حصةٍ متساويةٍ من عرض الحزمة. لا تؤثّر هذه الآليّة على حركة البيانات عندما لا تكون الوصلة ممتلئةً.

تحاول آلية طابور العدالة العشوائيّة SFQ توزيع فرص إرسال البيانات إلى الشبكة بشكلٍ عادلٍ فيما بين عددٍ إعتباطيٍّ من سيول البيانات.

4.5 المصافي الديكارتيّة Bayesian Filters[1]

من المبادئ التقنيّة الأخرى التي يمكنك استخدامها لتحسين أداء شبكتك "المصافي الديكارتيّة Bayesian Filters". تستخدم المصافي الديكارتيّة لتطبيق أنظمة مكافحة الرسائل التجاريّة المرسلة عشوائيّاً Spam والتي تقوم بحساب إحتمال كون الرسالة مرسلةٍ عشوائيّاً بناءً على محتوياتها.

تعتمد تقنيّة المصافي الديكارتيّة على فكرة أنّ تصفية الرسائل العشوائيّة ممكنٌ بناءً على احتمال وجود كلماتٍ معيّنةٍ أو مجموعاتٍ من الكلمات التي تشير إلى أنّ هذه الرسالة مرسلةٌ عشوائيّاً في حين تشير كلماتٌ أخرى إلى أنّ هذه الرسالة طبيعيّة.

المصافي الديكارتيّة قادرةٌ على التكيّف، أي أنّها قادرةٌ على التعلّم من خبرتها للتمييز بين محتوى الرسائل الجيّد والسيء مما يؤدّي إلى زيادة ذكائها ووثوقيتها مع مرور الوقت.

[1] تأتي تسميّة "المصافي الديكارتيّة" نسبةً إلى عالم الرياضيّات الإنكليزي توماس ديكارت Thomas Bayes

تعتمد المصافي الديكارتيّة (شأنها شأن غالبيّة أنظمة تصفية الرسائل المرسلة عشوائيّاً) على المحتوى. تستبدل هذه المصافي القائمة اليدويّة المستخدمة لتحديد خصائص الرسائل المرسلة عشوائيّاً Spam (وهي إحدى أهم نقاط الضعف في الأنظمة الأخرى) بقائمةٍ من الكلمات التي تقوم المصفاة بنفسها ببنائها عبر تحليل المحتوى شائع الإستخدام. يتم بناء القائمة الأوليّة عبر تحليل مجموعة من الرسائل المعروفة المرسلة عشوائيّاً ومجموعةٍ من الرسائل المعروفة الطبيعيّة للحصول على تصنيفٍ أوليٍّ للتمييز بين المحتوى الجيّد والسيء.

لا يقل تصنيف المحتوى الجيّد أهميّةً عن تصنيف المحتوى السيء. كلما تكيّفت المصافي مع طبيعة مستخدمٍ ما كلّما صعب على مرسلي الرسائل العشوائيّة تخطّي هذه المصافي.

يزداد حجم القائمة الأوليّة بعد بنائها كلما استخدمت المصفاة بشكلٍ أكبر. ستتكيّف هذه المصافي بشكلٍ شخصيٍّ مع المستخدم لأنّها ستتعلّم من خلال تعليمات هذا المستخدم لدى حدوث خطأ في تصفيّة الرسائل الواردة.

تقوم المصافي الديكارتيّة (بعكس الأنواع الأخرى من المصافي المعتمدة على المحتوى) بتفحّص محتوى الرسالة بأكملها في حين تقوم المصافي الأخرى بتفحّص ترويسة الرسالة وحقل الموضوع فقط. تتفحّص المصافي الديكارتيّة (بالإضافة إلى نص الرسالة) أجزاءً أخرى مثل:

- الترويسة (المرسل ومسار الرسالة)
- نصوص HTML المضمّنة (كالألوان وغيرها)
- أزواج الكلمات والتعابير
- المعلومات التوصيفيّة Meta Information.

ننصحك بالتفكير بتركيب أنظمة تصفيّة الرسائل التجاريّة المرسلة عشوائيّاً قبل بدء نقل رسائل البريد الإلكتروني عبر شبكتك اللاسلكية. سيوفّر عليك تركيب وكلاء تحويل البريد Mail Rely Agents ومصافي الرسائل المرسلة عشوائيّاً Spam عند نقطة الإتصال بالوصلة الخارجيّة ما قد يصل حتى 10 – 20 % من تكاليف عرض الحزمة الدوليّة.

5.5 بصمات الفيروسات Viruses Fingerprints

يمكن لبرمجيّات مكافحة الفيروسات كشف الفيروسات وغيرها من البرمجيّات الضارّة وإزالتها. يتم اكتشاف هذه الفيروسات عبر تفحّص البرمجيّات التنفيذيّة والمستندات بحثاً عن تعليماتٍ حاسوبيّةٍ خاصةٍ تستخدمها الفيروسات المعروفة.

تسمّى هذه التعليمات الحاسوبيّة أو بعض مشتقاتها بـــ "بصمة" أو "توقيع" الفيروس. يعتبر استخدام البصمات أحد المبادئ التقنيّة التي تتيح لبرمجيّات مكافحة الفيروسات البحث عن تعليماتٍ محددةٍ في البرمجيّات المشبوهة.

يتطلب نجاح برنامج مكافحة الفيروسات توفّر قاعدة بياناتٍ تحتوي على بصمات الفيروسات المعروفة وتحديثها على الدوام.

لكنّ اكتشاف البرمجيّات الضارّة ليس بالأمر السهل، فبرمجيّات الفيروسات غالباً ما تتحوّل وتعدّل نفسها لتغيير بصماتها. لذلك تستخدم خوارزميات المسح الإرشادي Heuristic Scanning Algorithms والتي تقوم بتجربة مجموعة من التحويلات على بصمات الفيروسات المعروفة للتنبأ وتحليل احتمالات تحوّل الفيروس وكشفه قبل إنتشاره على نطاق أوسع.

حاذر من التقليل من أهميّة تأثير البرمجيّات الضارّة على أداء شبكتك اللاسلكية. لا تقل أهميّة القدرة على اكتشاف وإزالة الفيروسات من رسائل البريد الإلكتروني الواردة أو منع الإتصال من الحواسب المصابة عن أهميّة الحصول على نسبةٍ جيّدةٍ للإشارة إلى الضجيج SNR في وصلاتك اللاسلكية.

6.الأدوات Tools

يقدّم هذا الجزء نظرةً أكثر قرباً إلى بعض الأدوات البرمجيّة الحرّة ومفتوحة المصدر التي يمكن استخدامها لمراقبة الشبكة. تتضمّن بعض هذه الأدوات آليّاتٍ قادرةٍ على اتخاذ إجراءاتٍ مباشرةٍ عند حدوث أيّ مشكل.

من الأدوات التي سنقوم باستعراضها: أدوات مراقبة الشبكة (ntop, MRTG)، مصافي الرسائل المرسلة عشوائيّاً (SpamAssassin) وبرمجيّات مكافحة الفيروسات (CLAM AV).

1.6 .مراقبة الشبكة اللاسلكية

يقوم منتجو تجهيزات الشبكات اللاسلكية عادةً بتوفير أداةٍ لمراقبة التجهيزات التي ينتجونها. يتم إعداد ومراقبة التجهيزات باستخدام برنامجٍ معيّنٍ يعمل ضمن نظام تشغيلٍ محدد.

ستجد عند بناء وتشغيل الشبكات اللاسلكية الكبيرة بأنّ هذه الأدوات محدودةٌ جداً. لا يمكنك تشغيل الأدوات المرفقة مع التجهيزات اللاسلكية ضمن نظام إدارة الشبكة الخاص بك، وعندما تستخدم تجهيزاتٍ مختلفةٍ عند بناء الشبكة سينتهي بك المطاف مع عددٍ من الأدوات التي ستعمل على سطح المكتب سويّةً لكي تمكّنك من استيعاب ما يجري ضمن شبكتك اللاسلكية.

يمكنك تشغيل أدوات الإدارة المختلفة مع بعضها البعض وتجميعها ضمن واجهةٍ رسوميّةٍ واحدةٍ عبر محاولة الحصول على المعلومات باستخدام قواعد بيانات SNMP MIB في كلٍّ من التجهيزات المستخدمة وإظهار جميع هذه المعلومات معاً باستخدام أداةٍ إضافيّةٍ مثل MRTG.

2.6.أداة MRTG

ممثّل حركة الموجّهات المتعددة (Multi Router Traffic Grapher (MRTG هي أداةٌ لإدارة الشبكة ذات واجهةٍ تعتمد على الوب قادرةٌ على مراقبة وعرض المتغيرات المتبدّلة أثناء عمل الشبكة. تستخدم أداة

MRTG بروتوكول إدارة الشبكة البسيط SNMP لتجميع البيانات من موجّهاتٍ مختلفةٍ تدعم هذا البروتوكول بالإضافة إلى مجموعةٍ من المكتبات الرسوميّة لإظهار المعلومات بشكلٍ بياني.
لقد تم تصميم أداة MRTG بالأساس لإظهار رسوماتٍ بيانيّة توضّح ضغط حركة البيانات واستثمار عرض الحزمة إلا أنّها طوّرت لتتمكّن من تمثيل أي متغيّر ضمن الشبكة يتبدّل مع مرور الوقت.

3.6.مراقبةمتغيرات الشبكة اللاسلكية باستخدام أداة MRTG

سنشرح في المثال التالي المبادئ الأساسية لبناء نظام مراقبة الشبكة الخاص بك باستخدام بروتوكول SNMP وأداة MRTG. يعتمد هذا المثال على عائلة منتجات Orinoco لكّن المنهجيّة المستخدمة قابلةٌ للتطبيق على أيّ جهازٍ لاسلكيٍّ آخر.

لنفترض أنّ لدينا وصلةً لاسلكيةً بين نقطتي PtP ونرغب بمراقبة مدى استثمار عرض الحزمة الكلّي (الطبقة الثالثة Layer 3) ووضعيّة الوصلة اللاسلكية (الطبقة الثانية Layer 2).

تعتبر مراقبة جسر الشبكة اللاسلكية للحصول على مدى استخدام عرض الحزمة بسيطاً كبساطة مراقبة استخدام عرض الحزمة في أيّ جهازٍ يدعم بروتوكول SNMP (موجّه، مبدّل إلخ).

يمكن تلخيص خطوات إعداد MRTG بما يلي:

1. تأكّد من حصولك على جميع المتطلّبات الضرورية: مخدّم للوب، أداة MRTG، عنوان الإنترنت IP وكلمات السر لبروتوكول SNMP للجهاز الذي ترغب بمراقبته.
2. قم بكتابة ملفٍ لإعدادات MRTG. يمكن القيام بهذه الخطوة يدوياً أو باستخدام أدواتٍ إضافيّةٍ مثل cfgmaker.
3. قم بإعداد مهمّة Cron ضمن نظام التشغيل لينكس لتشغيل أداة MRTG باستخدام ملف الإعدادات المحدد بشكلٍ دوريٍّ.

3.61..مراقبةعرض الحزمة Bandwidth Monitoring

بعد تثبيت (1) أداة MRTG ومخدّم الوب أباتشي Apache Web Server سنستخدم أداة cfgmaker لبناء (2) ملف إعدادٍ إفتراضيٍّ للأداة MRTG:

يمكن الحصول على ملف الإعدادات الإفتراضي باستخدام:

```
aep@it46-d505 mrtg2]$ cfgmaker password@IP > /etc/mrtg_b.cfg]
```

حيث (password) و (IP) هي كلمة سر القراءة فقط لبروتوكول SNMP وعنوان الإنترنت IP للجسر اللاسلكي.

يتوجّب القيام بتغييرٍ وحيدٍ ضمن ملف الإعدادات للإشارة إلى الموقع الذي ترغب في توفير صفحات الوب للأداة MRTG ضمنه.

على سبيل المثال:

WorkDir:/var/www/mrtg

يشير إلى أنّ جميع صفحات الوب والأشكال البيانيّة للأداة MRTG ستوضع ضمن الدليل / var/www/mrtg.

ينبغي علينا في النهاية إنشاء مهمّة دوريّة عبر إضافة السطر التالي إلى ملف /etc/crontab:

root /usr/bin/mrtg_b.cfg****5/*

ستقوم أداة MRTG بطلب المعلومات من جسر الشبكة اللاسلكية كل خمس دقائق.

3.62..مراقبة نسبة الإشارةللضجيج Signal/Noise Ratio Monitoring

لمراقبة نسبة الإشارة للضجيج في جهازٍ لاسلكيٍ ما يتوجّب علينا الوصول إلى قاعدة معلومات الإدارة MIB لهذا الجهاز. ستعلمنا قاعدة البيانات هذه بمواقع المعلومات التي نبحث عنها.

لا يعتبر الوصول إلى قاعدة معلومات الإدارة لجهازٍ لاسلكيٍّ أمراً سهلاً على الدوام. تتوضّع غالبيّة المتغيرات اللاسلكية التي قد ترغب في مراقبتها ضمن قاعدة معلومات الإدارة الخاصّة Proprietary MIB، وهي تطويرٌ لقاعدة البيانات الأساسيّة يتم تصميمه من قبل المنتج ونادراً ما يكون موثقّاً بشكلٍ جيّدٍ للعامّة.

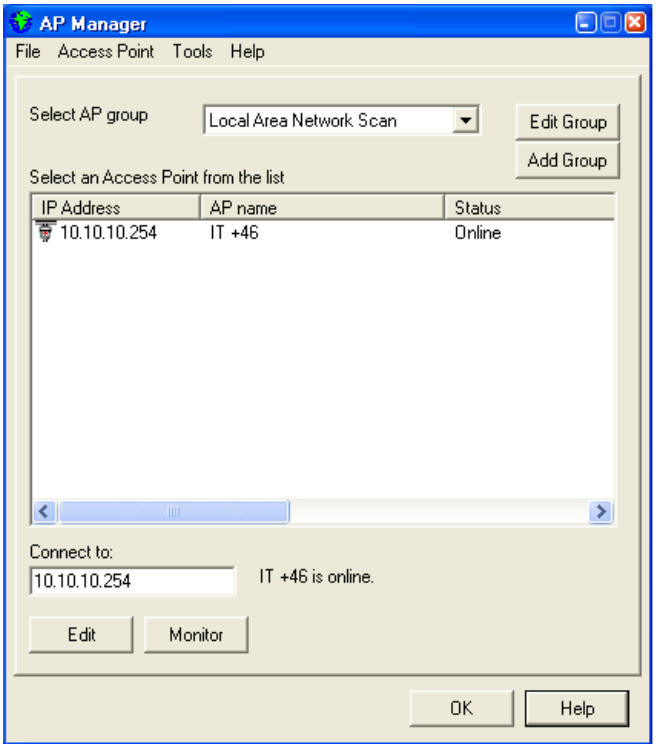
إذا لم تتمكّن من الوصول إلى قاعدة معلومات الإدارة MIB عليك حينها إيجاد ما تريد بنفسك (باستخدام الهندسة العكسيّة Reverse Engineering).

يتوجّب علينا إيجاد معرّفات الأشياء Object Identifiers (OIDs) المستخدمة في قاعدة معلومات الإدارة MIB للمعلومات التي نريد مراقبتها. معرّف الشيء OID هو رقمٌ يحدد موقع شيءٍ ما في قاعدة المعلومات MIB. يستخدم هذا المعرّف للإشارة إلى مواقع محددةٍ ضمن قاعدة بيانات الإدارة.

تقوم أداة مراقبة الشبكة عند طلب المعلومات من جهازٍ لاسلكيٍّ بإجراء مجموعةٍ من عمليات SNMP باستخدام معرّفات OID محددة. تقوم معرّفات OID بتحديد الأجزاء من قاعدة المعلومات MIB التي نريد قراءة أو كتابة البيانات ضمنها.

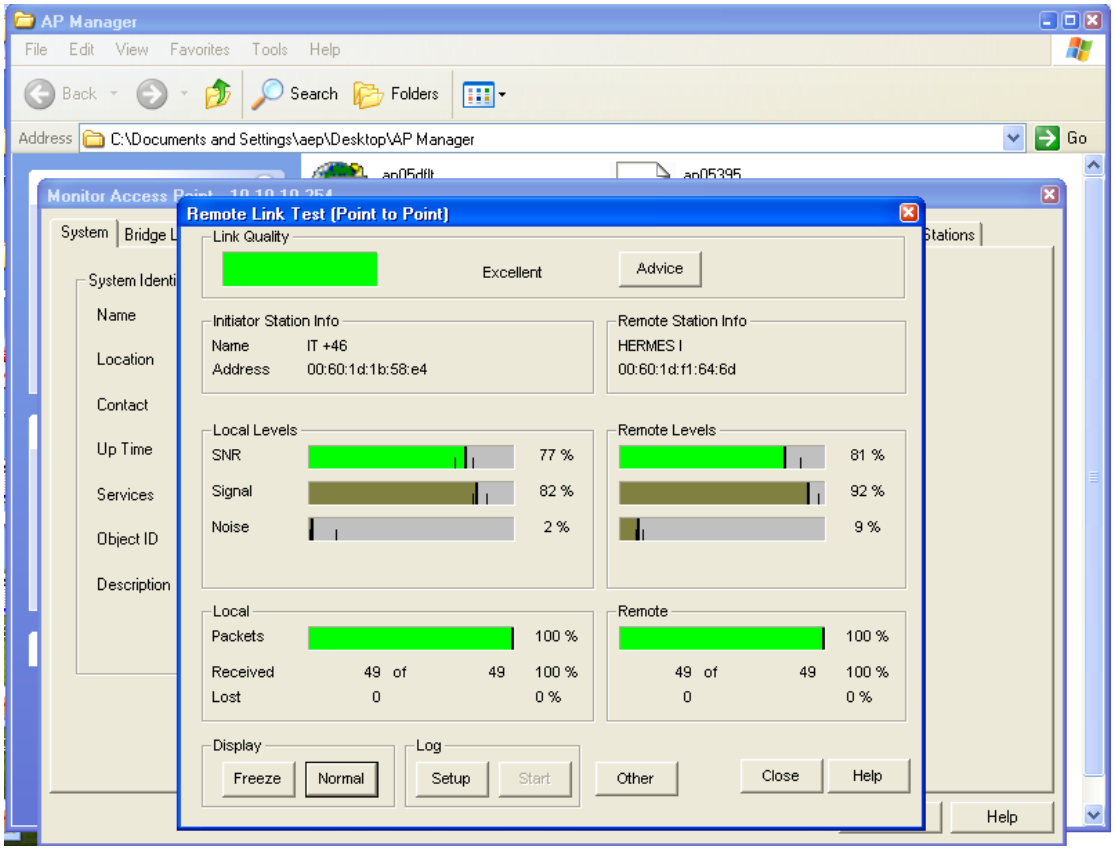
يعتبر الأسلوب الأمثل للحصول على معرّفات OID التي نبحث عنها هو استخدام أداة إدارة الشبكة المرفقة مع المنتج ومراقبة جميع المعلومات التي يتم تبادلها بين أداة الإدارة والجهاز اللاسلكي.

في هذا المثال، سنستخدم أداة Orinoco AP Manager:



شكل 2: استخدام أداةٍ تعمل ضمن نظام التشغيل ويندوز لمراقبة نقطة ولوج

بعد الإتصال بنقطة الولوج سنختار "القيام بفحصٍ للوصلة Perform a link-test" ونقوم بتسجيل جميع المعلومات الواردة من نقطة الولوج إلى أداة المراقبة.



شكل 3: تفحّص وصلةٍ بين نقطتين يظهر قياسات نسبة الإشارة للضجيج وخسارة الحزم

يمكننا الحصول المعلومات المتبادلة بين نقطة الولوج وأداة المراقبة باستخدام أدوات تحليل الحركة Traffic Analysis Tools (tcpdump, ethereal إلخ) والتي تظهر على الشكل التالي:

```
19:41:21.448323 10.10.10.12.1260 > 10.10.10.254.snmp:  GetRequest(29)  .1.3.6.1.4.1.762.2.1.7.0
0x0000   4500 0048 77b2 0000 8011 99d5 0a0a 0a0c        E..Hw...........
0x0010   0a0a 0afe 04ec 00a1 0034 64bb 302a 0201        .........4d.0*..
0x0020   0004 0670 7562 6c69 63a0 1d02 0201 0302        ...public.......
0x0030   0100 0201 0030 1130 0f06 0b2b 0601 0401        .....0.0...+....
0x0040   857a 0201 0700 0500                            .z......
19:41:21.448854 10.10.10.254.snmp > 10.10.10.12.1260:  GetResponse(30)  .1.3.6.1.4.1.762.2.1.7.0=2 (DF)
0x0000   4500 0049 0037 4000 4011 1150 0a0a 0afe        E..I.7@.@..P....
0x0010   0a0a 0a0c 00a1 04ec 0035 62b5 302b 0201        .........5b.0+..
0x0020   0004 0670 7562 6c69 63a2 1e02 0201 0302        ...public.......
0x0030   0100 0201 0030 1230 1006 0b2b 0601 0401        .....0.0...+....
0x0040   857a 0201 0700 0201 02                         .z.......
```

تستخدم قاعدة معلومات الإدارة MIB الخاصّة بشركة لوسنت Lucent والتي تقوم بتجميع المعلومات المتعلّقة بالشبكة اللاسلكية متغيّرات 1.3.6.1.4.1.762.2.5.* . تستخدم قاعدة المعلومات هذه في الكثير من نقاط الولوج اللاسلكية مثل Apple Airport و Lucent RG 1000.

يمكننا الحصول على **عدد المستخدمين المتصلين بنقطة الولوج** عبر القيام بعمليّات SNMP التالية:

```
Write Integer 50 in OIDs:
1.3.6.1.4.1.762.2.5.5.1,  1.3.6.1.4.1.762.2.5.5.1,  1.3.6.1.4.1.762.2.5.5.3
Write Integer 3 in OIDs:
 1.3.6.1.4.1.762.2.5.4.1,  1.3.6.1.4.1.762.2.5.4.2, 1.3.6.1.4.1.762.2.5.4.3
Retrive the OID:
1.3.6.1.4.1.762.2.5.1.0
```

يمكننا أيضاً الحصول على متغيّرات **الإشارة والضجيج للجهاز** اللاسلكي عبر القيام بما يلي:

```
Write Integer 1500 in OID
1.3.6.1.4.1.762.2.5.2.1.27.n
Write Integer 25 in OID
1.3.6.1.4.1.762.2.5.2.1.26.n
Write Integer 80 in OID
1.3.6.1.4.1.762.2.5.2.1.25.n
The signal can be retrieved by reading the OID
1.3.6.1.4.1.762.2.5.2.1.32.n
The noise can be retrieved by reading the OID
1.3.6.1.4.1.762.2.5.2.1.33.n
```

يتوجّب علينا بعد الحصول على معلومات MIB/OIDs المطلوبة كتابة نص برمجيٍّ Script للقيام بنفس المهام التي تقوم بها أداة إدارة نقطة الولوج ضمن نظام التشغيل ويندوز (تذكّر بأنّ الفكرة الأساسيّة تكمن في التخلّص من أداة إدارة نقطة الولوج والحصول على إمكانيّة تضمين البيانات في نظامٍ واحدٍ لإدارة الشبكة!).

يتضمّن ملحق هذه الوحدة نصاً برمجيّاً كتب باستخدام أداة snmp-tools ضمن لينكس للحصول على معلومات فحص الوصلة.

يقوم هذا النص بتجميع قيم الإشارة / الضجيج باستخدام بروتوكول SNMP ويعيد هذه القيم بتنسيقٍ يمكن استخدامه ضمن أداة MRTG:

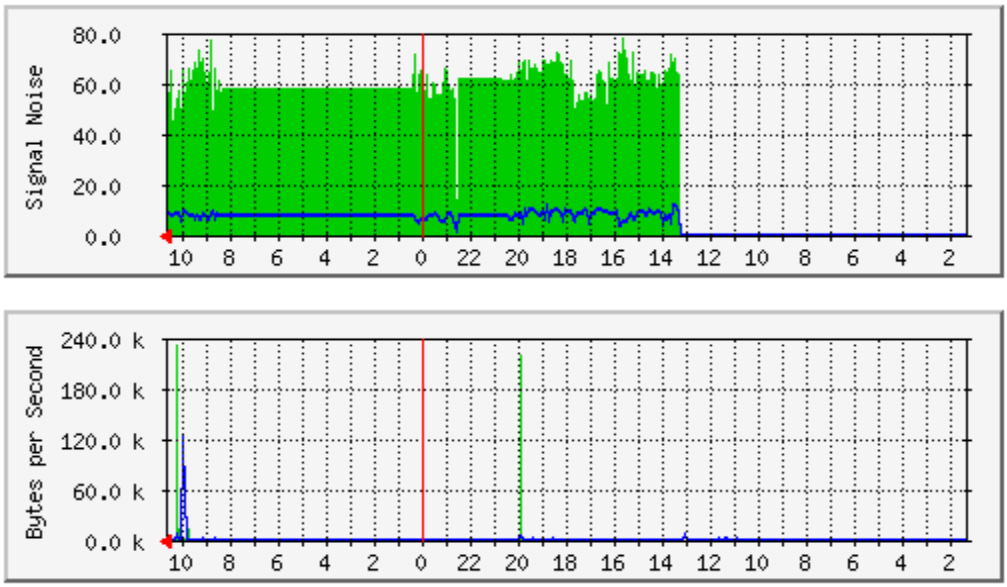
```
aep@it46-d505 etc]$ /usr/local/bin/monitoring_PtP.sh]
79
12
2:596
aep
```

هذه القيم الأربعة هي الإشارة (79)، الضجيج (12)، علامة زمنيّة (Timestamp (2:596 واسم المضيف (aep).

نستطيع الآن تجميع بيانات عرض الحزمة (معلومات بروتوكول الإنترنت IP) وبيانات نسبة الإشارة للضجيج (معلومات الوصلة اللاسلكية) ضمن واجهةٍ واحدةٍ.

يعطينا تمثيل كلٍّ من عرض الحزمة ونسبة الإشارة للضجيج بياناً ضمن واجهةٍ واحدةٍ لنظام إدارة الشبكة صورة أكثر شمولاً عن حالة الشبكة.

يظهر الشكل التالي **تجميع** بيانات مراقبة الشبكة اللاسلكية مع بيانات مراقبة حركة بروتوكول الإنترنت IP باستخدام أداة MRTG.



شكل 4: استخدام MRTG لعرض نسبة الإشارة للضجيج في وصلةٍ لاسلكيةٍ مع استخدام عرض الحزمة في آنٍ واحدٍ.

ملاحظة: ناقش المعلومات التي يمكن استخلاصها من هذه الرسوم البيانيّة.

4.6. أداة Ntop

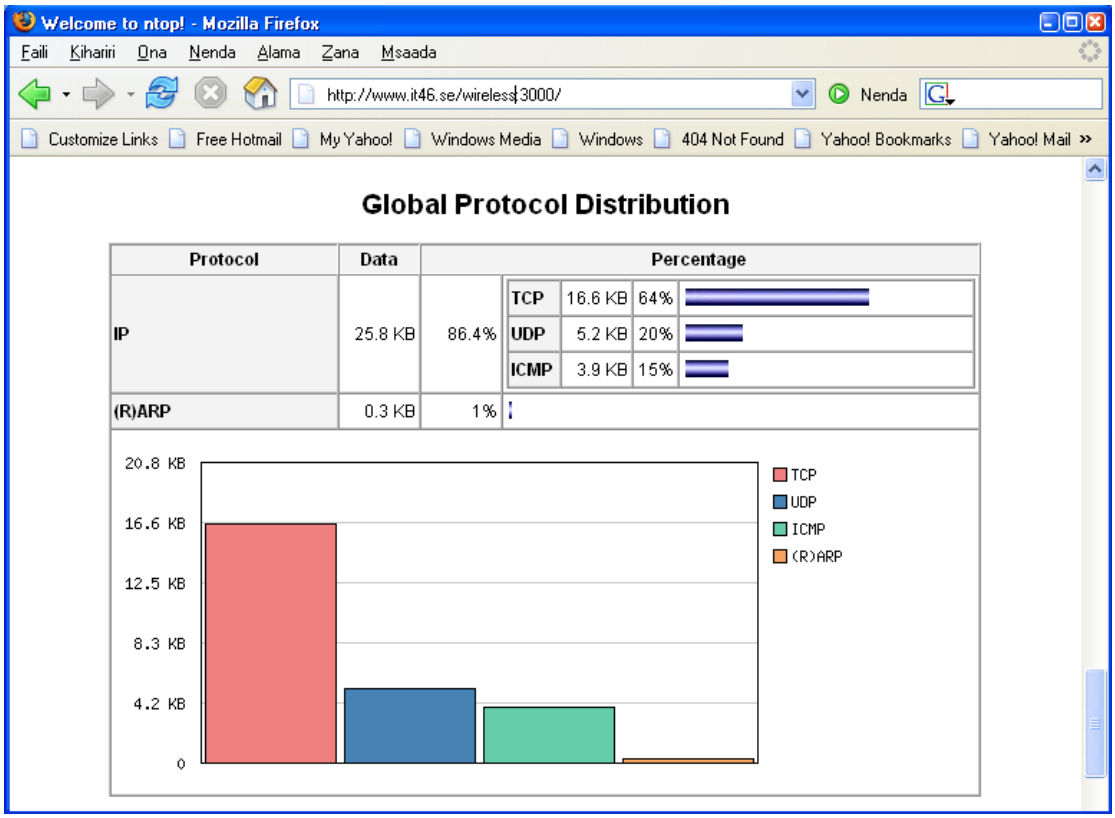
Ntop هي أداةٌ حرّةٌ ومفتوحة المصدر لمراقبة وقياس حركة بروتوكول الإنترنت IP تعمل ضمن أنظمة التشغيل المتعددة. يمكن تشغيل جميع ميزات هذه الأداة (الإعداد والمراقبة) عبر واجهةٍ تعتمد على الوب.

تعني تسمية أداة قياس حركة بروتوكول الإنترنت IP بأنّ هذه الأداة لن تقوم بتجميع أيّة معلوماتٍ متعلّقةٍ بالشبكة اللاسلكية (مثل نسبة الإشارة للضجيج، عدد المحطات المرتبطة بنقطة الولوج ..إلخ). يجب استخدام أداة Ntop جنباً إلى جنب مع أداة مراقبةٍ تعمل ضمن الطبقة الثانية Layer 2 كتلك المذكورة في الفقرة السابقة.

تركّز وظائف أداة Ntop على ما يلي:

- قياس الحركة ضمن الشبكة
- توصيف ومراقبة الحركة
- كشف محاولات إختراق الشبكة
- تحسين الأداء وتخطيط الشبكة

يتضمّن ملحق هذه الوحدة شرحاً تفصيلياً لميزات الأداة Ntop.



شكل 5: استخدام أداة Ntop لمراقبة توزيع البروتوكولات ضمن الوصلة

5.6. أداة Spam-Assassin

تتضمّن هذه الوحدة قسماً خاصّاً بمكافحة الرسائل التجاريّة المرسلة عشوائيّاً Spam والتي أصبحت كابوساً حقيقياً للعاملين في مجال إدارة الشبكة. تعتبر حماية المستخدمين من الرسائل المرسلة عشوائيّاً هدفاً أساسيّاً لأيّ مزوّد خدمة.

تعتبر أداة Spam-Assassin من أكثر أدوات مكافحة الرسائل المرسلة عشوائيّاً شهرةً واستخداماً. أداة Spam-Assassin هي مصفاةٌ ذكيّةٌ للرسائل المرسلة عشوائيّاً تستخدم عدّة أساليب للتمييز بين هذه الرسائل والرسائل الطبيعيّة. يمكن استخدام أداة Spam-Assassin في كلٍّ من زبائن أو مخدمات البريد الإلكتروني لتفحّص البريد الصادر والوارد.

لا تقوم أداة Spam-Assassin عادةً لمنع مرور الرسائل المرسلة عشوائيّاً، بل تقوم بوسم هذه الرسائل ومنحها علامةً تعتمد على محتواها. كلّما ارتفعت العلامة التي تحصل عليها الرسالة كلّما ازداد احتمال كونها مرسلةً عشوائيّاً Spam. يعود القرار النهائي في جميع الأحوال للمستخدم فيما إذا أراد حذف هذه الرسائل أو الإحتفاظ بها.

من أهم نقاط القوّة في أداة Spam-Assassin بنيتها المرنة والقابلة للتوسّع Modular مما يتيح إضافة التقنيّات الجديدة إلى المصفاة بالإضافة إلى إمكانيّة تركيبها ضمن أي نظامٍ للبريد الإلكتروني.

تستخدم أداة Spam-Assassin الأساليب الأساسيّة التالية لتحليل رسائل البريد الإلكتروني وتحديد إحتمال كونها مرسلةً عشوائيّاً:

- تفحّص الترويسة (حقل المرسل، الموضوع)
- تفحّص العبارات الواردة ضمن نص الرسالة باستخدام مجموعات قواعد مطورّةٍ من قبل جهاتٍ أخرى (الكلمات المفتاحية Keywords، نصوص HTML، عناوين بروتوكول الإنترنت IP، عناوين URL)
- المصافي الديكارتيّة
- قوائم العناوين البيضاء / السوداء اليدويّة
- قواعد بيانات تعريف الرسائل المرسلة عشوائيّاً التشاركيّة Collaborative Spam Identification Databases
- قوائم حجب DNS (قوائم الثقوب السوداء في الزمن الحقيقي RealTime Blackhole Lists – RBL)
- مجموعات المحارف والإعدادات المحليّة

5.61.. قواعدبيانات تعريف الرسائل المرسلة عشوائيًّاالتشاركيّة Collaborative Spam Identification Databases

تعتبر قواعد بيانات تعريف الرسائل المرسلة عشوائيّاً التشاركيّة إحدى آليّات كشف الرسائل المرسلة عشوائيّاً، وهي عبارةٌ عن قاعدة بياناتٍ متوفّرة عبر الإنترنت تحتوي على معرّفات Checksums عددٍ كبيرٍ من الرسائل المرسلة عشوائيّاً يمكن استخدامها من قبل أيٍّ كان للإستعلام وتحديد هذه الرسائل.

يمكن بحساب معرّف رسالةٍ مشبوهةٍ بعد وصولها إلى مخدّم البريد الإلكتروني التحقق فيما إذا كان هذا المعرّف قد تم إدخاله إلى قاعدة البيانات سلفاً كمعرّفٍ لرسالةٍ مرسلةٍ عشوائياً. في هذه الحال ستزداد العلامة الممنوحة للرسالة.

تدعم أداة Spam-Assassin ثلاثة قواعد بياناتٍ مختلفةٍ لتعريف الرسائل المرسلة عشوائياً:

- Razor, http://razor.sourceforge.net
- Pyzor, http://pyzor.sourceforge.net
- DCC (Distributed Checksum Clearinghouse), http://www.rhyolite.com/anti-spam/dcc

5.62.. قوائمحجب DNS DNS Blocklists

من قواعد البيانات الأخرى المستخدمو لكشف الرسائل المرسلة عشوائيّا قوائم حجب DNS، وهي تعرف أيضاً بقوائم DNS السوداء (DNS Blacklists (DNSBLs والتي تحتوي على عناوين مخدّمات البريد الإلكتروني المعروف (أو المشكوك) بأنّها تستخدم من قبل مرسلي الرسائل العشوائيّة.

فيما يلي بعض إعدادات مخدّم البريد الإلكتروني التي تتفاعل معها قوائم DNSBL لتحديد الرسائل المرسلة عشوائيّاً:

- محوّل SMTP المفتوح Open SMTP Relay
- الوكيل Proxy المفتوح
- بوابات إرسال البريد الإلكتروني عبر إستمارات HTML المفتوحة
- مجموعات عناوين إنترنت IP الديناميكية

إنّ محوّل SMTP المفتوح هو مخدّم بريدٍ إلكتروني تم إعداده بشكلٍ (خاطئٍ) يتيح لأيّ شخصٍ كان تحويل (إرسال) البريد عبره.

لقد توقفّ غالبية مزوّدي خدمات الإنترنت ISPs حاليّاً عن استخدام المحوّلات المفتوحة لإتاحة ميزة الوصول عن بعد لزبائنهم. لقد أصبحوا يستخدمون عوضاً عن ذلك حلولاً مثل POP أو SMTP AUTH قبل إتاحة الوصول إلى خدمات إرسال البريد SMTP. إلا أنّ ذلك يعني بأنّ مرسلي الرسائل العشوائيّة قد تأقلموا مع ذلك وابتكروا أساليباً جديدةً لبلوغ مرادهم.

يحتوي الموقع التالي على معلوماتٍ مفيدةٍ عن قوائم DNSBL:
http://www.scconsult.com/bill/dnsblhelp.html

6.6. أداة Clam AntiVirus (CLAM AV)[1]

تملك الفيروسات القدرة على إيقاف تشغيل الشبكة اللاسلكية بالكامل خلال دقائق معدودة. تقوم غالبيّة الفيروسات الحاسوبيّة بإجراء مسحٍ للشبكة أو هجماتٍ لإيقاف الخدمة Denial of Service، وتتجلّى النتيجة الأولى في إزدحام الشبكة اللاسلكية. بإمكان الفيروسات تعطيل وصلة إنترنت تعمل عبر الأقمار الصناعيّة ما لم يتّم استخدام قوائم إتاحة الولوج بسرعة.

أداة Clam AntiVirus هي مجموعة أدواتٍ متاحةٌ ضمن إتفاقيّة الترخيص العموميّة GPL تعمل ضمن نظام التشغيل يونيكس UNIX صممت خصيصاً لتفحّص رسائل البريد الإلكتروني ضمن بوابات البريد. تدعم هذه الأداة التحديث التلقائي لبصمات الفيروسات، يتم تحديث قاعدة بيانات البصمات عبر الإنترنت.

فيما يلي بعض ميزات Clam AntiVirus:

- مسحٌ سريعٌ للأدلّة والملفّات
- اكتشاف ما يفوق 30000 فيروس، دودة أو حصان طروادة (بما فيها فيروسات الماكرو في ملفّات Microsoft Office و MacOffice)
- مسح الملفّات المضغوطة باستخدام دعمٍ مضمّنٍ لخوارميّات الضغط مثل .Zip, RAR (2.0) TAR. Gzip, Bzip2, MS OLE2, MS Cabinet Files, MS CHM (Compiled HTML), MS SZDD
- دعم الملفّات التنفيذيّة المحمولة المضغوطة باستخدام UPX, FSG, Petite
- برنامج تحديثٍ متطوّرٍ يدعم التواقيع الإلكترونيّة للفيروسات والإستعلام عن نسخة قاعدة البيانات باستخدام بروتوكول DNS

لا تقوم أداة Clam AntiVirus بحذف، إعادة تسمية أو تنظيف الملف المصاب. يقتصر عمل هذه الأداة على اكتشاف الفيروس وإعلام المستخدم عبر التأشير على الرسالة أو ما شابه.

7. الخلاصة

تتطلّب إدارة الشبكة (سواءٌ كانت سلكيّةً أم لاسلكيّةً) أن نبدأ بتحديد أهدافنا كمزودين للخدمة. إذا كنّا لا نعرف ما نريد تحقيقه سيصعب علينا بالتالي تحديد ماذا نريد أن نراقب. إذا لم نعرف ماذا نريد أن نراقب، من الصعب علينا إيجاد الأدوات التي ستساعدنا في اتخاذ القرار.

يمكن تلخيص الأمور الخمس الرئيسية التي ينبغي عليك تذكرها من هذه الوحدة بما يلي:

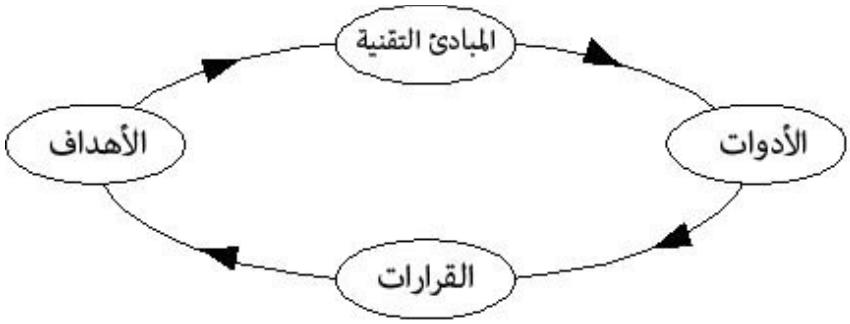
1. لا يكفي جمع البيانات الأوليّة أو تركيب الأدوات للحصول على شبكةٍ تعمل بشكلٍ جيّدٍ. لن تجد صعوبةً في إيجاد الأدوات الملائمة إذا عرفت تماماً ماذا تريد.
2. لن تكفي مراقبة وضعيّة الوصلة اللاسلكية إذا كانت شبكتك تعجّ بنشاط الفيروسات. لن يكفيك أيضاً إيقاف الفيروسات مالم تكن وصلاتك اللاسلكية ثابتةً.

[1] http://www.clamav.net/ آخر زيارة 2005/02/23

3.عند تركيب أدوات مراقبة و/أو إدارة الشبكة، يتوجّب عليك تعلّم كيفية تركيب وتشغيل الأدوات المختلفة بحيث تصبح كافّة المعلومات المطلوبة لاتخاذ القرار سهلة المنال.

4.فكّر دوماً أنّه قد يكون من الأسهل عليك في حال كانت الأدوات المتوفرة لا تلائم متطلباتك أن تقوم بكتابة أداةٍ بسيطةٍ بنفسك لتفي باحتياجاتك عوضاً عن التصارع مع أداةٍ تلائم متطلّبات شخصٍ آخر.

5.حدد أهدافك < حدد المبادئ التقنيّة < أوجد / صمم الأدوات < اتخذ القرارات



شكل 6: يظهر المنهجيّة المعتمدة على الأهداف لمراقبة (إدارة) الشبكة

8. الملحق 1

قياس الحركة باستخدام الأداة NTOP

تقوم NTOP بربط كل حزمةٍ تلتقطها بمرسل هذه الحزمة ومستقبلها. يمكن بهذا الأسلوب استحصال جميع الأنشطة المتعلّقة بمضيفٍ واحدٍ عبر معرفة إسم هذا المضيف، عنوان الإنترنت IP الخاص به أو عنوان بطاقة الشبكة NIC.

يمكن الحصول على هذه المعلومات لكل مضيفٍ باستخدام NTOP:

- البيانات المرسلة والمستقبلة: مجموع البيانات المرسلة أو المستقبلة (الحجم وعدد الحزم) مصنّفةً حسب البروتوكول المستخدم (IP, IPX, AppleTalk إلخ) وبروتوكول الإنترنت المستخدم أيضاً (FTP, HTTP, NFT إلخ)
- الإرسال المتعدد لبروتوكول الإنترنت IP Multicast: الحجم الكلّي لحركة الإرسال المتعدد المرسل أو المستقبل من قبل المضيف
- تاريخ جلسة TCP (TCP Session History): يعطي جلسات TCP الفعّالة والتي بدأها أو قبل بها المضيف بالإضافة إلى إحصاءات الحركة المتعلّقة بكل جلسة
- حركة بروتوكول UDP (UDP Traffic): الحجم الكلّي لحركة بروتوكول UDP مصنّفةً حسب البوابة المستخدمة
- خدمات TCP/UDP المستخدمة (TCP/UDP Services Used): يعطي الخدمات التي تعتمد على بروتوكول الإنترنت IP والتي يوفّرها المضيف بالإضافة إلى الزبائن الخمس الأخيرة التي استخدمت كلاً منها.
- نظام التشغيل المستخدم في المضيف
- النسبة المئويّة لعرض الحزمة المستهلك (الفعلي، الوسطي والأعظمي)
- توزّع الحركة (بين الشبكات الفرعيّة Subnets)
- توزّع حركة بروتوكول الإنترنت IP Traffic Distribution (UDP مقابل TCP، التوزّع النسبي لبروتوكولات IP)

تقوم أداة NTOP أيضاً بتجميع معلوماتٍ عامّةٍ (لا تتعلّق بمضيفٍ معيّن) عن توزّع الحركة، توزّع الحزم واستثمار عرض الحزمة.

توصيف ومراقبة الحركة باستخدام الأداة NTOP

تتطلّب مراقبة الحركة تحديد الحالات التي تحيد فيها الحركة ضمن الشبكة عن اتبّاع القواعد أو الحدود الموضوعة من قبل مدير الشبكة. بإمكان أداة NTOP إكتشاف الحالات التاليّة:

- الإستخدام المتكرر لنفس عنوان الإنترنت IP
- تحديد جميع الموجّهات الموجودة ضمن شبكةٍ فرعيّةٍ Subnet

- تحديد جميع الحواسب التي تم إعداد بطاقة الشبكة ضمنها للعمل وفق نمط
- إكتشاف الإعدادات الخاطئة للتطبيقات البرمجيّة
- إكتشاف إساءة استخدام الخدمات (كالحواسب التي لا تستخدم الأنظمة الوكيلة Proxies المحددة)
- إكتشاف الحواسب التي تستهلك عرض الحزمة بشكلٍ مفرط

إكتشاف الإختراقات الأمنيّة للشبكة باستخدام أداة NTOP

تأتي غالبيّة الهجمات الأمنيّة في الشبكة من ضمن الشبكة نفسها لا من الخارج. توفّر أداة NTOP لمستخدميها إمكانيّة ملاحقة الهجمات أثناء حدوثها وتحديد نقاط الضعف في أمن الحواسب عبر تقديم الميزات التالية:

- إكتشاف محاولات مسح البوابات "Portscan" و "Slow Portscan": تقدّم أداة NTOP تقريراً بأسماء آخر ثلاثة حواسب أرسلت حزمةً إلى كلّ بوابةٍ أصغر من 1024. يمكن اكتشاف محاولات مسح البوابات Portscan ضمن جميع الحواسب التي تقوم NTOP بمراقبتها
- إكتشاف انتحال الشخصيّة Spoofing Detection (للحزم التي تنتمي إلى نفس الشبكة الفرعيّة Subnet التي تعمل NTOP ضمنها): إنتحال الشخصيّة Spoofing يعني أن المضيف سيدّعي بأنّه مضيفٌ آخر للتمكّن من التلصص على الحزم. تقوم أداة NTOP بتنبيه المستخدم عند اكتشاف عنواني إنترنت IP مختلفين يعملان على نفس بطاقة الشبكة في الشبكة الفرعيّة Subnet.
- إكتشاف التجسس Spy Detection: يعتبر مضيفٌ ما جاسوساً إذا كانت بطاقة الشبكة الخاصّة به معدّة للعمل ضمن نمط التنصت والذي يتيح إلتقاط الحزم المارّة عبر الشبكة بغضّ النظر عن وجهتها.
- أحصنة طروادة Trojan Horses: يبدو حصان طروادة لأول وهلةٍ برنامجاً مسالماً لكنّه في الحقيقة يحتوي على برنامجٍ خفيٍ ضارٍ قادرٍ على تدمير حاسبك. تستخدم أحصنة طروادة عادةً بواباتٍ معروفةً، وبالتالي يمكن لأداة NTOP أن تكتشف وجود هذه الأحصنة عبر مراقبة الحركة على هذه البوابات.
- هجمات إيقاف الخدمة Denial of Service (DoS): وهي تصرفات المضيف الذي يقوم بإرسال حزمٍ تحتوي SYN Flag (لفتح وصلات TCP) إلى بوابات "الضحايا" دون متابعة إجراءات الوصلة. سيؤدّي ذلك في النهاية إلى امتلاء جميع منافذ الوصلات ضمن كدسة بروتوكول الإنترنت IP Stack في الضحيّة مما يمنعها من قبول أيّة وصلات إضافيّة.

تحسين أداء وتخطيط الشبكة باستخدام الأداة NTOP

يؤدّي الإعداد الردئ للحواسب والاستثمار غير الفعّال لعرض الحزمة المتوفّر إلى تدّني أداء الشبكة. تقدّم أداة NTOP الخدمات التالية لتحسين أداء الشبكة:

- تحديد البروتوكولات غير الضروريّة (الحواسب التي تستخدم بروتوكولات غير مستخدمةٍ في الشبكة).
- تحديد التوجيه غير الأمثل عبر تتبع رسائل إعادة التوجيه ICMP وتحليل قائمة الموجّهات الموجودة ضمن الشبكة.
- توصيف الحركة والتوزيع عبر دراسة أنماط الحركة Traffic Patterns.
- الإستخدام الحكيم لعرض الحزمة: تساعد دراسة توزّع الحركة بين البروتوكولات مدير الشبكة على تحديد التطبيقات التي تحتاج إلى وكلاء Web Proxies.

تدعم أداة NTOP قواعد بيانات SQL في حال أراد المستخدم حفظ البيانات التي تمّ تجميعها خلال جلسة المراقبة.

/etc/mrtg_b.cfg

```
#######################################################################
# Multi Router Traffic Grapher – Orinoco PtP signal/noise monitoring
#######################################################################

# Global configuration
WorkDir: /var/www/mrtg
WriteExpires: Yes

Interval: 5
Target[load]: `/usr/local/bin/read_signal_noise.sh <password> <IP>`
Title[load]: SIGNAL NOISE
PageTop[load]: <H1>Signal Noise PtP</H1>
Options[load]: gauge,nopercent,integer
YLegend[load]: Signal Noise
ShortLegend[load]: -dbm
MaxBytes[load]: 100
LegendI[load]: Signal
LegendO[load]: Noise
```

read_signal_noise.sh <password> <IP>

```
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.5.1 i 50 >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.5.2 i 50 >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.5.3 i 50 >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.4.1 i 3  >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.4.2 i 3  >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.4.3 i 3 >/dev/null
users=`snmpget -c public -v 1 10.10.10.254 1.3.6.1.4.1.762.2.5.1.0 | awk '{print $4}'`
#echo The number of users is $users
#echo "TESTING LINK...."
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.27.1 i 1500 > /dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.26.1 i 25 > /dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.25.1 i 8000 > /dev/null
signal=`snmpget -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.32.1 | awk '{print $4}'`
noise=`snmpget -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.33.1 | awk '{print $4}'`

#Return values for MRTG
echo $signal
echo $noise
UPTIME=`uptime | awk '{print $3$4}' | sed -e "s/,//g"`
echo $UPTIME
```