إدارة ومراقبة الشبكة

إعداد: Alberto Escudero Pascual
النسخة العربية أنس طويلة

الأهداف

- يتوجب علينامعرفة ماذانريدلنتمكن من معرفة ماذا سنحتاج
- هل تعتبر المراقبة مكافئةلإدارة الشبكة؟
- لاتتبع الأدوات، إتبعالأساليب

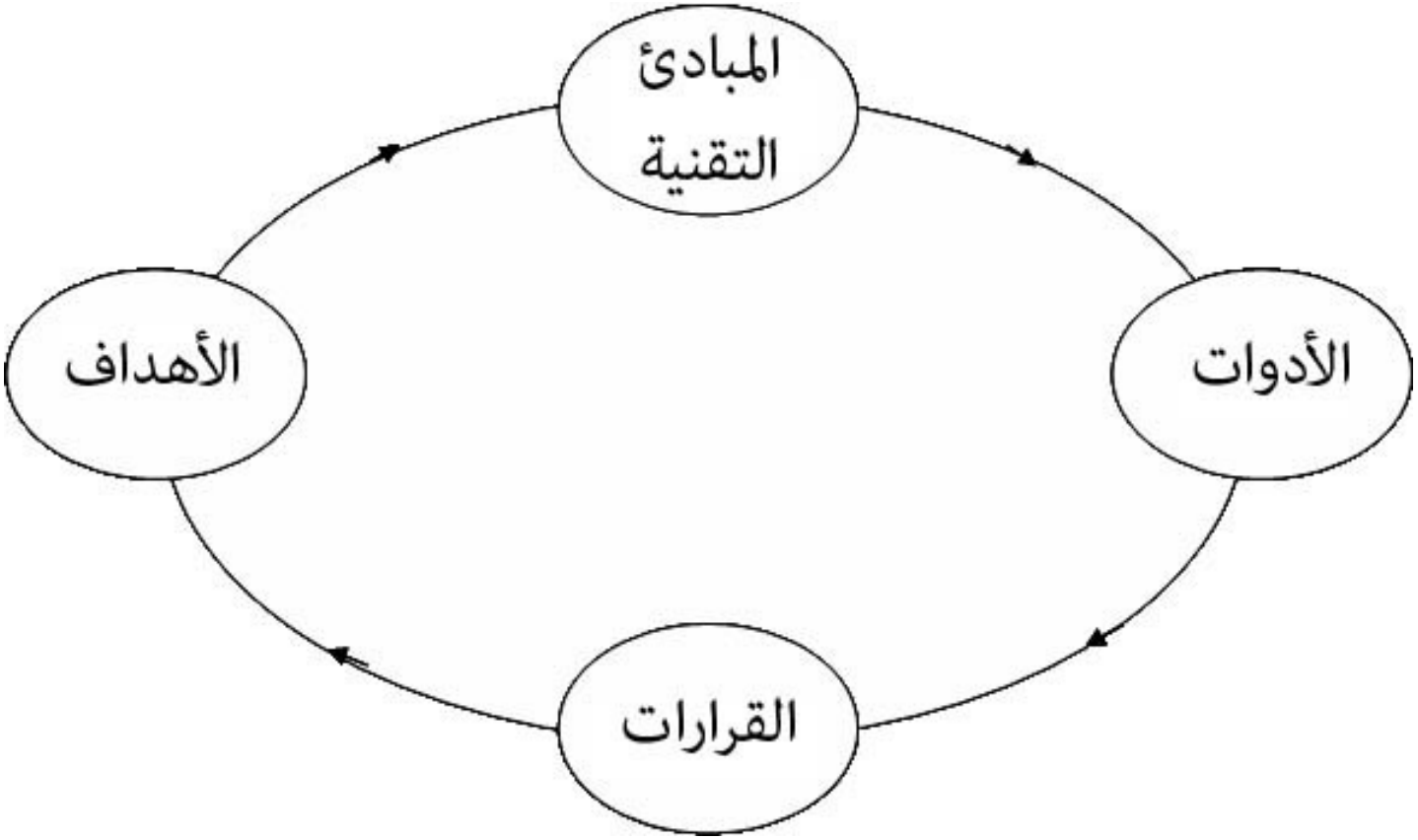
المحتويات

- منهجية الوحدة
- الأهداف مقابل مراقبةالبيانات
- أهداف خدمات المراقبة
- المبادئ التقنية
  - SNMP/MIB
  - محاسبة الحركة Traffic Accounting
  - تشذيب سيلالبيانات Traffic Shaping
  - المصافي الديكارتية Bayesian Filters
  - بصمات الفيروسات Viruses Fingerprints
- الأدوات **(MRTG, NTOP, SpamAssassin, Clam AV)**

المنهجية

- ركز على الأهداف، لا الأدوات
- استوعب المبادئ التقنية التي تعتمد عليها هذه الأدوات
- تعرف على المبادئ التقنية اللازمة لتحقيق أهدافك

الأهداف في مقابل مراقبةالبيانات



أهداف خدمة مراقبة الشبكة

ثلاثة أمثلة:

- تخفيض النفقات عبر تخفيض استخدام الوصلة الدولية
- توفير نوعية أفضل لخدمة نقل الصوت عبر بروتوكول الإنترنت
- إدارة الخدمات وتوسع الشبكة

الهدف 1: توفير نفقات عرض الحزمة الدولي

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

الهدف 2: جودة خدمة VoIP

الطبقة	المبدأ التقني
4	
3	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Promisc، Traffic Accounting(SNMP)
2	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Promisc، Traffic Accounting(SNMP)
1	تجميع بيانات الطبقة الثانية (SNMP) تخفيض التأخير اللاسلكي Wireless Latency

الهدف 3: إدارة الخدمة وتوسع الشبكة

المبدأ التقني	الطبقة
Virus/Spam, SQL (موازنة الخدمات Service Balancing)	4
تجميع إحصاءات بروتوكولات TCP/UDP موازنة استخدام الجدران الناريّة Firewall Balancing	3
	2
	1

المبادئ التقنية

خمسةمبادئ تقنية:

- SNMP/MIB
- محاسبة الحركة Traffic Accounting
- تشذيب سيلالبيانات Traffic Shaping
- المصافي الديكارتية Bayesian Filters
- بصمات الفيروسات Virus Fingerprints

SNMP/MIB

- بروتوكول للإدارة والصيانة صمم خصيصاً للشبكات الحاسوبية وتجهيزات الشبكة الإفرادية
- يعتمد على بنية المخدم / الزبون Client/Server
- يقوم برنامج الزبون بطلب المعلومات التالية من تجهيزات الشبكة البعيدة
  - المعلومات الإحصائية، البيانات الخاصة
- يحتوي كل جهاز يدعم بروتوكول SNMP على قاعدة بيانات تدعى MIB (قاعدة معلومات الإدارة Management Information Base)

+ دعم للتفاعل بين تجهيزات الشبكة المختلفة Interoperability

- قواعد ترميز معقدة، قلة الفاعلية

SNMP/MIB

- يؤدي استخدام بروتوكول SNMP إلى زيادة الضغط على الشبكة
  - حاول تخفيض هذا الضغط باتخاذ القرارات الصائبة
- لا يدعم بروتوكول SNMPv1 تشفير مرحلة التحقق من الهوية
  - إنتبه لكلمات السر الخاصة بك
- يستهلك بروتوكول SNMP قدراً كبيراً من قدرة المعالج CPU ضمن تجهيزات الشبكة

SNMP/MIB

- يقوم معظم منتجو التجهيزات اللاسلكية بتضمين مجموعة خاصة Proprietary من معلومات الشبكة اللاسلكية في قواعد معلومات الإدارة MIB ضمن منتجاتهم
- تختلف آلية تجميع بعض المعلومات المتعلقة بالشبكة اللاسلكية
- ترفق التجهيزات اللاسلكية مع أدوات إدارة خاصة بكل منها
- يعتبر تركيب أدوات الإدارة المختلفة من عدة منتجين أمراً معقداً جداً لأن هذه الأدوات نادراً ما تكون مفتوحة المصدر
- قم بكتابة نظام إدارة الشبكة اللاسلكية الخاص بك!

محاسبة حركة البيانات

الدوافع الأساسية لمراقبة إحصاءات حركة البيانات:

- القرارات المتعلقة بالشبكة
- كشف الأعطال
- مراقبة نشاطات الحواسب المختلفة

محاسبة حركة البيانات

- عدد الحزم والبايتات Bytes
- إحصاءات توزّع البروتوكولات
- أخطاء بروتوكول الإنترنت IP Checksum Errors
- إكتشاف الأجهزة النشطة
- حركة البيانات بين الأجهزة

محاسبة حركة البيانات

- نشط Active
  - تشغيل بروتوكول SNMP في جميع موجهّات وجسور الشبكة
- خامل Passive
  - نمط التنصت
  - ينبغي أن تكون قادراً على الوصول المباشر إلى البيانات المنتقلة عبر الشبكة إضافة إلى استهلاك الكثير من قدرة المعالج CPU لتجميع واستيعاب حجم المعلومات المارة عبر قناة الإتصال

تشذيب سيل البيانات

- التحكم بكيفية سير البيانات ضمن الشبكة
- ضمان مستوى معين من الأداء
- قواعد ضبط طوابير البيانات في طبقة بروتوكول الإنترنت
  - التأخير والإزدحام
  - عرض الحزمة والعدالة

تشذيب سيل البيانات

- تطبيق آليات مشابهة في جسور الشبكات اللاسلكية عبر تعديل طريقة أداء طبقة IEEE 802.11 MAC التقليدية، إلا أن غالبية هذه الحلول تبقى خاصة بالمنتج مما لا يضمن توافقية هذه التجهيزات مع تلك المنتجة من قبل الآخرين
- قامت شركة Proxim بتطبيق آلية تصويت خاصة تدعى (WORP) لتوزيع استطاعة الشبكة عبر تخصيص منافذ زمنية وجيزة

ضبط طوابير البيانات والتأخير

- تطبق على حركة البيانات الخارجة من الشبكة
  - تشكل وصلة البيانات الخارجية نقطة اختناق في الشبكة
- إمتلاء ذاكرة الحاجز Buffer Overflow
  - إهمال حزم TCP > إعادة الإرسال
  - التأخير
- أولوية الحزم
  - التفاعل مع المستخدم (ssh, rtp)
  - نقل الملفات الكبيرة (ftp, http)

إدارة عرض الحزمة عبر التحكم باصطفاف الحزم

تضمن:

- جودة الخدمة QoS
  - سرعة نقل بيانات محددة لمضيف معين
  - عرض حزمة محدود لخدمة معينة
- الشبكة العادلة
  - يحصل الزبون / الزبونة لقاء مادفعه / دفعته

إدارة عرض الحزمة عبر التحكم باصطفاف الحزم

- قواعد ضبط طوابير البيانات الفئوي Classful Queuing
  - ذات هيكلية هرمية
  - تحدد الفئة: خوارزمية الإصطفاف Queuing Algorithm ، سرعة نقل البيانات Bit Rate سقف الحد Maximum Ceiling (تبعاً للبروتوكول المستخدم، عنوان الإنترنت IP، الشبكة الفرعية Subnet)
- آلية دلو البطاقات الهرمية HTB (فئوية)
  - تتحكم بعرض الحزمة عبر مواءمة مجموعة من الوصلات البطيئة
- طابور العدالة العشوائية SFQ (غير فئوي)
  - لتحقيق العدالة في الوصلات الممتلئة

المصافي الديكارتية

- مصفاة للرسائل التجارية المرسلة عشوائياً Spam بالإعتماد على المحتوى
  - الترويسة (المرسل ومسار الرسالة)
  - نصوص HTML المضمنة (الألوان وغيرها)
  - أزواج الكلمات والتعابير
  - المعلومات التوصيفيّة Meta Information
- قادرة على التكيف - تتعلم ذاتياً باستخدام تقارير الأخطاء
- لا تحتاج إلى قائمة كلمات يدوية Wordlist
  - يتم بناء القائمة المبدئية بتحليل المحتوى

المصافي الديكارتية

- ركب أنظمة تصفية الرسائل التجارية المرسلة عشوائياً Spam قبل دخول رسائل البريد الإلكتروني إلى شبكتك اللاسلكية
- سيوفر عليك تركيب وكلاء تحويل البريد Mail Rely Agents ومصافي الرسائل المرسلة عشوائياً Spam عند نقطة الإتصال بالوصلة الخارجية ما قد يصل حتى 10 – 20 % من تكاليف عرض الحزمة الدولية

بصمات (تواقيع) الفيروسات

- البصمات: تعليمات حاسوبية خاصة (أو مشتقاتها) تستخدمها الفيروسات المعروفة
- برمجيات مكافحة الفيروسات
  - تستخدم بصمات الفيروسات لمسح الشيفرات البرمجية
  - تستخدم قواعد بيانات متوفرة عبر الإنترنت تحدث بشكل دائم
- خوارزميات المسح الإرشادي Heuristic Scanning Algorithms
  - تقوم بتجربة مجموعة من التحويلات على بصمات الفيروسات المعروفة للتنبأ باحتمالات تحول الفيروس

أدوات المراقبة

أدوات حرة ومفتوحة المصدر Free and Open Source

- MRTG
- Ntop
- SpamAssassin
- Clam AntiVirus - Clam AV

مراقبة الشبكة اللاسلكية

- أدوات المراقبة الخاصة بالمنتج (تعمل ضمن نظام تشغيل معين)
  - ذات استخدامات محدودة
- ن منتجيًعني استخدام أداة للمراقبة
- يمكن الحصول على واجهة استخدام واحدة عبر تشغيل عدة أدوات معاً (SNMP/MIB -> MRTG)

MRTG

- ممثل حركة الموجهات المتعددة Multi Router Traffic Grapher
- تقوم بمراقبة وعرض متغيرات الشبكة (المعالج CPU، ضغط الحركة Traffic Load)
- تستخدم البيانات الواردة من التجهيزات التي تدعم بروتوكول إدارة الشبكة البسيط SNMP
- ذو واجهة استخدام تعتمد على الوب

MRTG

إعداد الأداة MRTG:

- المتطلبات الضرورية: مخدم للوب، أداة MRTG، عنوان الإنترنت IP وكلمات السر لبروتوكول SNMP للجهاز الذي ترغب بمراقبته
- قم بكتابة ملف لإعدادات MRTG (cfgmaker)
- قم بإعداد مهمة Cron ضمن نظام التشغيل لينكس لتشغيل أداة MRTG باستخدام ملف الإعدادات المحدد بشكل دوري

MRTG: مراقبة فرض الحزمة

1. قم ببناء ملف إعداد إفتراضي للأداة MRTG
>cfgmaker password@IP > /etc/mrtg_b.cfg

2. غير دليل العمل لأداة MRTG ضمن الملف mrtg_b.cfg
WorkDir: /var/www/mrtg

3. قم بـ إنشاء مهمة دورية عبر إضافة السطر التالي إلى ملف
etc/crontab/

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

MRTG: مراقبة نسبة الإشارة للضجيج

- يتوجب الوصول إلى قاعدة معلومات الإدارة MIB للجهاز اللاسلكي
- كيفية إيجاد الإستعلامات الصحيحة (OID)؟
  - الهندسة العكسية Reverse Engineering!
- استخدم أداة إدارة الشبكة المرفقة مع الجهاز لمراقبة الحركة وفحص الوصلة (link-test)

MRTG: مراقبة نسبة الإشارةللضجيج

```
snmp:  GetRequest(29)  .1.3.6.1.4.1.762.2.1.7.0.10.10.10.254 > 10.10.10.12.1260 19:41:21.448323
...........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
snmp > 10.10.10.12.1260:  GetResponse(30)  .1.3.6.1.4.1.762.2.1.7.0=2.10.10.10.254 19:41:21.448854
)(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
```

المستخدمين المتصلين بنقطةالولوج

: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

متغيرات الإشارةوالضجيج

Write Integer 1500 in OID

n.1.3.6.1.4.1.762.2.5.2.1.27

n.1.3.6.1.4.1.762.2.5.2.1.26

n.1.3.6.1.4.1.762.2.5.2.1.25

The signal can be retrieved by reading the OID

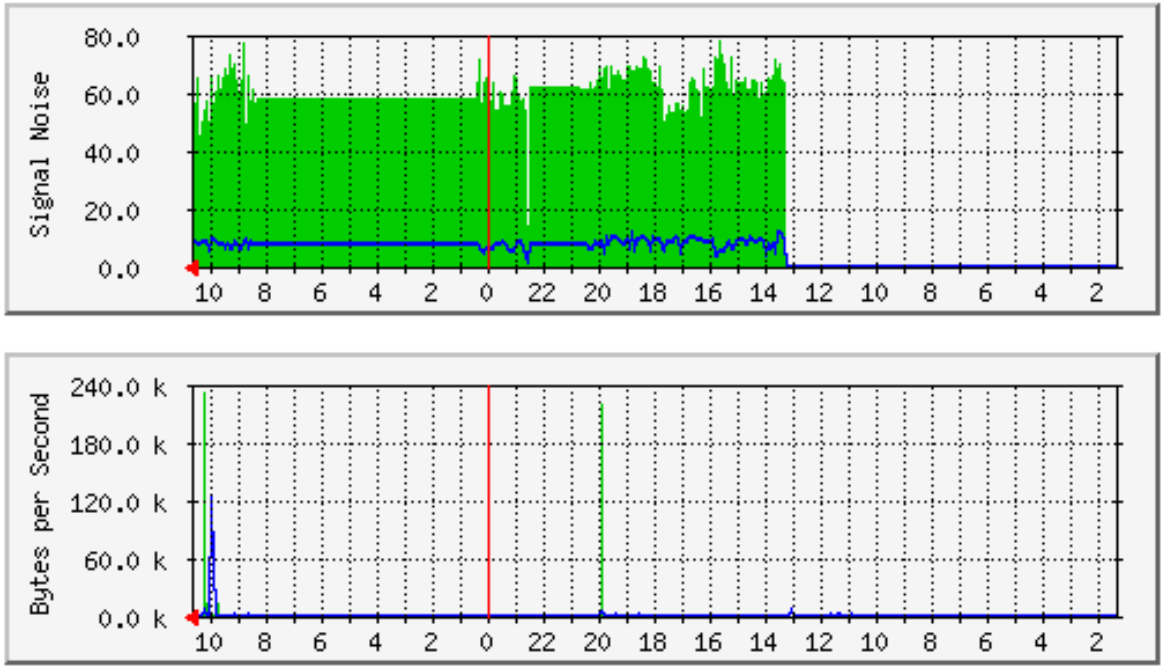
n.1.3.6.1.4.1.762.2.5.2.1.32

The noise can be retrieved by reading the OID

n.1.3.6.1.4.1.762.2.5.2.1.33

حيث >n< تشير إلى الرقم المخصص للجهاز اللاسلكي

مراقبة الشبكة اللاسلكية باستخدام الأداة MRTG



معلومات طبقةبروتوكولالإنترنت IP)الطبقة 3(معلومات الشبكة اللاسلكية)الطبقة 2(في الأداة MRTG

Ntop

أداة حرة ومفتوحة المصدر (إتفاقية ترخيص العمومية GPL)

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

قياس الحركة

- البيانات المرسلة والمستقبلةحسب البروتوكول المستخدم
- الإرسال المتعددلبروتوكولالإنترنت IP Multicast
- تاريخ جلسة TCP
- خدمات TCP/UDP المستخدمةوتوزع الحركة
- إستثمارعرض الحزمة) الفعلي،الوسطي والأعظمي(
- توزع الحركةبينالشبكات الفرعية Subnets

توصيف ومراقبة الحركة

تحديدالحالات التي تحيد فيهاالحركةضمن الشبكةعن اتباع القواعدأو الحدود الموضوعةمن قبل مدير الشبكة عبراكتشاف:

- الإستخدامالمتكررلنفس عنوانالإنترنت IP
- بطاقات الشبكةالتي تعمل ضمن نمطالتنصت Promiscuous
- الإعدادات الخاطئةللتطبيقات البرمجية
- إساءة استخدامالخدمات (الأنظمة الوكيلة Proxies .. إلخ)
- الإستهلاك المفرطعرض الحزمة

إكتشاف الإختراقات الأمنية للشبكة

إكتشاف الإختراقات الأمنية للشبكة مثل:

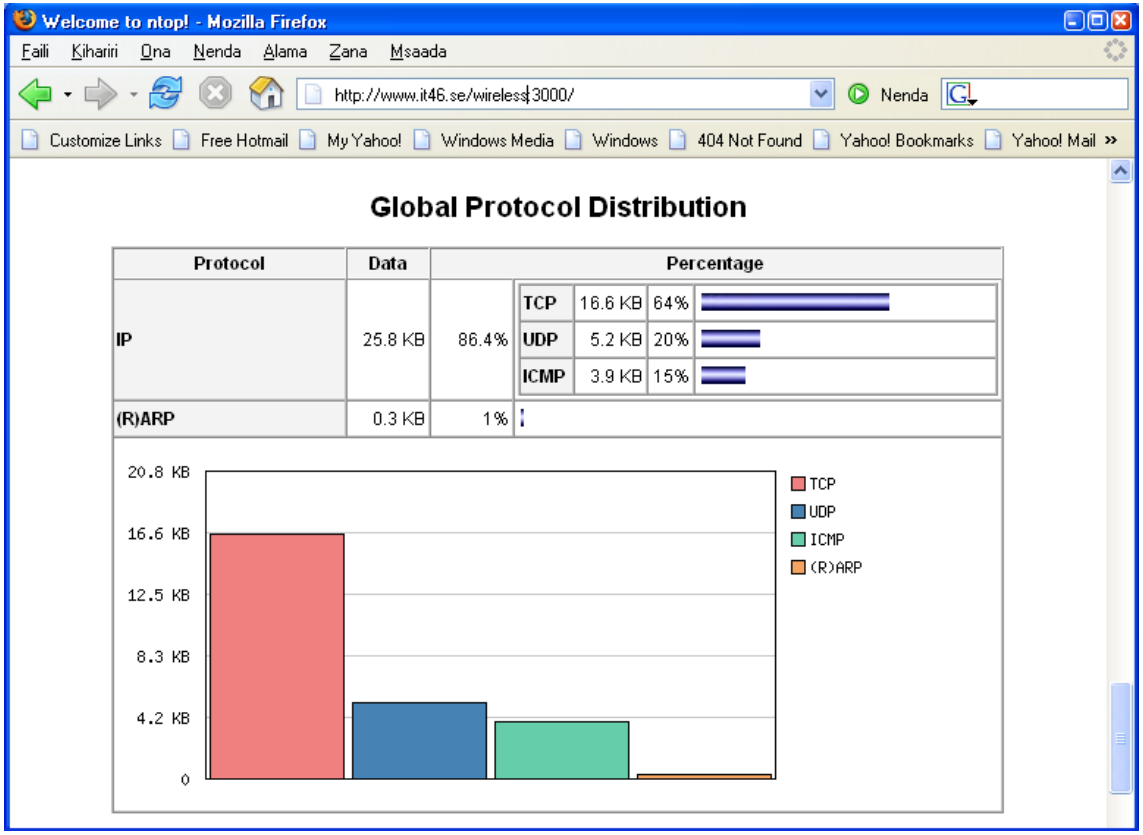
- مسح البوابات Portscan
- انتحال الشخصية Spoofing
- التجسس Spy
- أحصنة طروادة Trojan Horses
- هجمات إيقاف الخدمة Denial of Service()DoS

تحسين أداءوتخطيط الشبكة

الإعدادالردئ والاستثمار غير الفعالعرض الحزمةالمتوفر

- تحديدالبروتوكولات غير الضرورية
- تحديد التوجيه غير الأمثل (ICMP redirect)
- أنماط الحركةوالتوزيع

Ntop


Welcome to ntop! - Mozilla Firefox
Faili Kihariri Ona Nenda Alama Zana Msaada
http://www.it46.se/wireless:3000/
Nenda
Customize Links Free Hotmail My Yahoo! Windows Media Windows 404 Not Found Yahoo! Bookmarks Yahoo! Mail
Global Protocol Distribution
Protocol Data Percentage
IP 25.8 KB 86.4%
TCP 16.6 KB 64%
UDP 5.2 KB 20%
ICMP 3.9 KB 15%
(R)ARP 0.3 KB 1%
20.8 KB
16.6 KB
12.5 KB
8.3 KB
4.2 KB
0
TCP
UDP
ICMP
(R)ARP

SpamAssassin

- لا يوقف الرسائل،بل التأشير عليها فقط
- يعطي كل رسالة علامة بناء على:
  - تفحص الترويسة)حقل المرسل،الموضوع(
  - المصافي الديكارتية
  - قوائم العناوين البيضاء / السوداء
  - قواعد بيانات تعريف الرسائل المرسلة عشوائياً التشاركية
  - قوائم حجب DNS
  - مجموعات المحارف والإعدادات المحلية

Clam AntiVirus

- لاتقوم بحذف أو تنظيف الملف المصاب، بل تقوم بالتأشير عليه فقط
- مسح سريع للأدلة والملفات
- اكتشاف مليفوق 30000 فيروس، دودة أو حصان طروادة
- مسح الملفات المضغوطة
- برنامج تحديث متطور يدعم تواقيع لفيروسات

طوفان الشبكة Flooding

```
)S 1068540375:1068540375(0) win 64240 <mss 1460,nop,nop,sackOK> (DF :172.168.82.53.445 > 172.168.0.36.2231 18:12:36.432838
$....=...@..E..0   4500 0030 119f 4000 8006 3d7f aca8 00240x0000
.......?......R5     aca8 5235 08b7 01bd 3fb0 a1d7 0000 00000x0010
...............p         7002 faf0 f088 0000 0204 05b4 0101 04020x0020
)S 2018273998:2018273998(0) win 64240 <mss 1460,nop,nop,sackOK> (DF :172.168.227.122.445 > 172.168.0.23.1433 18:12:36.441460
....E..0..@...3I  4500 0030 8a9c 4000 8006 3349 aca8 00170x0000
........z....xLj      aca8 e37a 0599 01bd 784c 6ace 0000 00000x0010
...........`...p        7002 faf0 60db 0000 0204 05b4 0101 04020x0020
)S 2018316905:2018316905(0) win 64240 <mss 1460,nop,nop,sackOK> (DF :172.168.196.106.445 > 172.168.0.23.1435 18:12:36.441731
....E..0..@...RX 4500 0030 8a9d 4000 8006 5258 aca8 00170x0000
.......j....xM.i      aca8 c46a 059b 01bd 784d 1269 0000 00000x0010
..........p....M       7002 faf0 d84d 0000 0204 05b4 0101 04020x0020
arp who-has 172.168.0.247 tell 172.168.0.27 18:12:36.443252
.............[.8       0001 0800 0604 0001 0006 5ba6 3815 aca80x0000
................         001b 0000 0000 0000 aca8 00f7 0000 00000x0010
...............                  0000 0000 0000 0000 0000 0000 00000x0020
)S 767169456:767169456(0) win 64240 <mss 1460,nop,nop,sackOK> (DF :172.168.160.143.445 > 172.168.0.27.2367 18:12:36.445470
....E..0?.@....A  4500 0030 3f8b 4000 8006 c141 aca8 001b0x0000
.......-..?.....         aca8 a08f 093f 01bd 2dba 13b0 0000 00000x0010
...........p...A        7002 faf0 41cd 0000 0204 05b4 0101 04020x0020
)S 1068598455:1068598455(0) win 64240 <mss 1460,nop,nop,sackOK> (DF :172.168.217.194.445 > 172.168.0.36.2235 18:12:36.447728
$........@..E..0   4500 0030 11a0 4000 8006 b5f0 aca8 00240x0000
.......?........        aca8 d9c2 08bb 01bd 3fb1 84b7 0000 00000x0010
...............p        7002 faf0 8616 0000 0204 05b4 0101 04020x0020
)S 1068654094:1068654094(0) win 64240 <mss 1460,nop,nop,sackOK> (DF :172.168.97.176.445 > 172.168.0.36.2232 18:12:36.448124
$........@..E..0  4500 0030 11a1 4000 8006 2e02 aca8 00240x0000
.....^.?.......a      aca8 61b0 08b8 01bd 3fb2 5e0e 0000 00000x0010
...........$...p       7002 faf0 24d4 0000 0204 05b4 0101 04020x0020
```

الخلاصة

- لن تساعدك مراقبة البيانات الأولية وحسب
- يتوجب عليك مراقبة الشبكة للحصول على إدارة جيدة
- حدد أهدافك، حدد المبادئ التقنية ومن ثم قم باختيار الأدوات
- في حال كانت الأدوات المتوفرة لا تؤدي الغرض المطلوب أو تقوم بأكثر من المطلوب بكثير، فكر بكتابة أداة بسيطة بنفسك لتفي باحتياجاتك