كشف أعطال الشبكات اللاسلكية

إعداد: Alberto Escudero Pascual
النسخة العربية أنس طويلة

الأهداف

- كشف الأعطال هو فن "معرفة الخطوة التالية
- كشف الأعطال هو فن اكتشاف الجهةالتي سيقع عليها اللوم

المحتويات

- المنهجية
  - من أين نبدأ؟
- تصنيف المشاكل
  - مالذي يحدث هنا؟
- الأدوات العامة لكشف الأعطال

تذكير:من الملوم؟

TCP/IP	OSI	الطبقة
Application التطبيقات	Application التطبيقات	7
	Presentation التقديم	6
(Transport (TCP النقل	Session الجلسة	5
	Transport النقل	4
(Network (IP الشبكة	Network الشبكة	3
التحكّم بالوصول إلى الناقل Media Access Control	Data Link وصلة البيانات	2
	Physical الفيزيائيّة	1

Methodology المنهجية

- من الأعلى باتجاه الأسفل
  - تبدأ بـ : إعدادات التطبيقات
  - تنتهي بـ : منافذ الشبكة اللاسلكية، نسبة الإشارة إلى الضجيج SNR
- من الوسط باتجاه الأعلى أو باتجاه الأسفل
  - تبدأ بـ: الوصول إلى الإنترنت (ping)
  - تتابع باتجاه الأعلى / الأسفل إعتماداً على النتيجة
- من الأسفل باتجاه الأعلى
  - تبدأ بـ : منافذ الشبكة اللاسلكية، نسبة الإشارة إلى الضجيج #SNR
  - تنتهي بـ : إعدادات التطبيقات

لأستطيع قراءةبريدي الإلكتروني

)Hotmail(!

)تكافئ: الطابعة لاتعمل!(

من الأعلى باتجاه الأسفل

- ماهو البرنامج الذي تستخدمه لقراءة بريدك الإلكتروني؟
  - إعدادات التطبيقات، الوكيل Proxy
- هل يمكنك الوصول إلى أيّة مواقع على شبكة الإنترنت؟
  - مشاكل مخدم أسماء النطاق DNS؟
- هل يعطيك البرنامج رسالة "إنقضاء الزمن Time Out"؟
  - مشاكل بروتوكول TCP؟
- هل قمت بتسجيل الدخول إلى مخدّم التحقق من الهويّة بنجاح؟
- هل يمكنك الوصول إلى موقعنا على شبكة الإنترنت؟
  - مشاكل التوجيه Routing؟
- هل لديك عنوان إنترنت IP Address؟

من الوسط باتجاه الأعلى أو الأسفل

- هل يمكنك الإتصال بموقع hotmail.com باستخدام أداة Ping؟
- هل يمكنك الإتصال بعنوان الإنترنت IP لموجه البوابة المتصل بمزود خدمة الإنترنت باستخدام أداة Ping؟

- على سبيل المثال، إذا كانت الإجابة على كلٍ من هذين السؤالين بـ (لا):
- هل لديك عنوان إنترنت IP Address؟
- هل قمت بتسجيل الدخول إلى مخدم التحقق من الهوية بنجاح؟

تصنيف المشاكل

- تصنيف المشاكل على طريقة X-Files!
  - مشاكل التشويش لأسباب مختلفة
  - الشبكة ليست "سريعة" كفاية
  - ضياع الحزم
  - الكثير من المستخدمين
  - الأحوال الجوية

أدوات كشف الأعطال -مستوى الوصلة

- الأدوات التي تعمل مع جميع المنتجات المتوافقة مع معايير 802.11b)تذكر:كشف الأعطال(
- الأدوات التي تأتي مرفقة مع كل منتج على حدة

أدوات كشف الأعطال

TCP/IP	الأدوات
التطبيقات Application	nslookup
النقل Transport - TCP	Ntop (ويندوز، لينكس) Visualroute, traceroute
الشبكة Network - IP	Nmap Ntop (ويندوز، لينكس) Ethereal Etherape
التحكم بالوصول إلى الناقل Media Access Control	Ethereal (ويندوز، لينكس) Netstumbler (ويندوز) Kismet, Wavemon, Wellenreiter أدوات الإدارة الخاصة بمنتج التجهيزات

ثلاثة أمثلة على كشف الأعطال

- مشاكل في مستوى الوصلة (Netstumbler)
  - مشاكل في قناة الإرسال اللاسلكي؟
- مشاكل في مستوى بروتوكول الإنترنت (Etherape)
  - إزدحام الشبكة؟ البطء؟
- مشاكل التطبيقات (Ethereal)
  - لا أستطيع قراءة بريدي الإلكتروني

Netstumbler

Network Stumbler - [20060108140249]

File Edit View Device Window Help

- Channels
  - 2
  - 6
- SSIDs
  - buss
  - default
  - linksys
- Filters
  - Encryption Off
  - Encryption On
  - ESS (AP)
  - IBSS (Peer)
  - CF Pollable
  - Short Preamble
  - PBCC
  - Short Slot Time (11g)
  - Default SSID

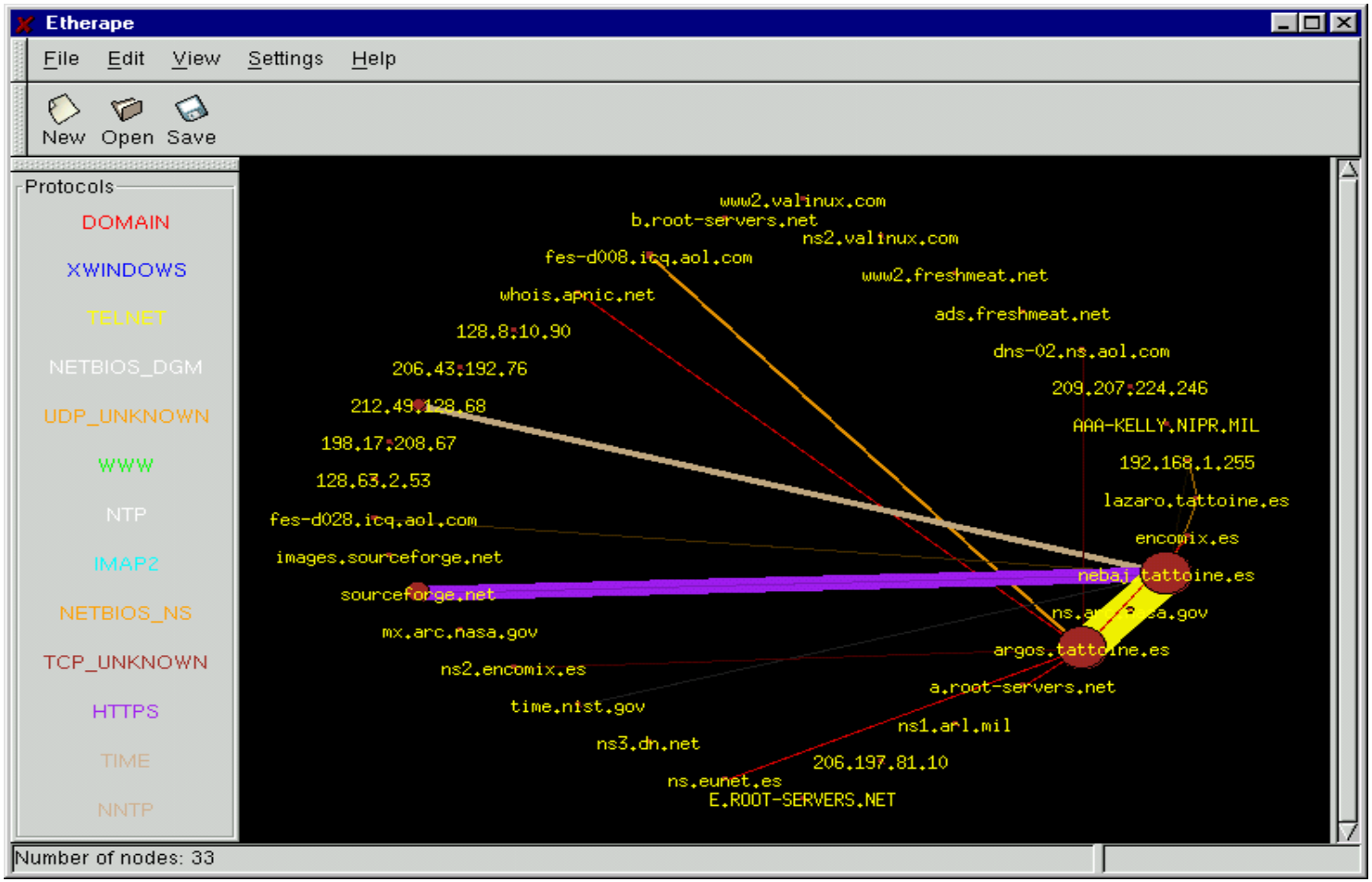
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+
000F3D3B195E	default		2	54 Mbps		AP		18	-82	-100	18
000F669AAE99	linksys		6	11 Mbps	Linksys	AP		19	-80	-100	20
000F66E1DC43	buss		6*	54 Mbps	Linksys	AP	WEP	34	-37	-100	63

Ready | 3 APs active | GPS: Disabled

Netstumbler

- تقوم بتجميع معلومات الطبقة الفيزيائية / الوصلة بشكل خامل Passivs
- j ستخدم بطاقة الشبكة اللاسلكية لمحلل لطيف الترددات
- تستطيع تحديد الشبكات المتاحة معرف مجموعة الخدمات SSID لكل منها، التشفير WEP
- تقوم بمراقبة نسبة الإشارة للضجيج SNR لكل من هذه الشبكات

EtherApe


Etherape
File
Edit
View
Settings
Help
New
Open
Save
Protocols
DOMAIN
XWINDOWS
TELNET
NETBIOS_DGM
UDP_UNKNOWN
WWW
NTP
IMAP2
NETBIOS_NS
TCP_UNKNOWN
HTTPS
TIME
NNTP
www2.valinux.com
b.root-servers.net
ns2.valinux.com
fes-d008.icq.aol.com
www2.freshmeat.net
whois.apnic.net
ads.freshmeat.net
128.8.10.90
dns-02.ns.aol.com
206.43.192.76
209.207.224.246
212.49.128.68
AAA-KELLY.NIPR.MIL
198.17.208.67
192.168.1.255
128.63.2.53
lazaro.tattoine.es
fes-d028.icq.aol.com
encomix.es
images.sourceforge.net
nebaj.tattoine.es
sourceforge.net
mx.arc.nasa.gov
argos.tattoine.es
ns2.encomix.es
a.root-servers.net
time.nist.gov
ns1.arl.mil
ns3.dn.net
206.197.81.10
ns.eunet.es
E.ROOT-SERVERS.NET
Number of nodes: 33

EtherApe

- تقوم تحديدأنواع حركةبروتوكولالإنترنت IP ضمن الشبكة وتوزع الحركةبين نقاط الشبكة المختلفة
- تتيح دراسة ديناميكية الشبكة
- تكشف البرمجيات الضارة كالفيروسات،برامج مسح البوابات، الطوفانات وغيرها.
- تفحص وصلةبروتوكولالإنترنت IP على مستوى عال (مستوى الخدمة): HTTP، DNS وخدمات البريدالإلكتروني

Ethereal

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ip.src == 194.109.209.218 | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
50	10.824243	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=48
53	10.847516	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=64
55	10.889052	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=48
58	10.942145	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=80
60	10.943307	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=32
62	10.965336	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=32
64	11.006237	194.109.209.218	85.226.127.250	TCP	ssh > 57273 [ACK] Seq=1232 Ack=512 Win=2408 Len=0 TSV=174561060 TSER=19936194
69	13.444443	194.109.209.218	85.226.127.250	TCP	pop3 > 50947 [ACK] Seq=82 Ack=11 Win=5792 Len=0 TSV=174561670 TSER=19938672
70	13.445691	194.109.209.218	85.226.127.250	POP	Response: +OK Password required for aep.
78	17.028874	194.109.209.218	85.226.127.250	TCP	pop3 > 50947 [ACK] Seq=114 Ack=21 Win=5792 Len=0 TSV=174562566 TSER=19942216
92	26.990988	194.109.209.218	85.226.127.250	POP	Response: -ERR [AUTH] "aep": access denied.
94	26.992657	194.109.209.218	85.226.127.250	POP	Response: +OK Pop server at revolware signing off.
96	27.017190	194.109.209.218	85.226.127.250	TCP	pop3 > 50947 [ACK] Seq=192 Ack=22 Win=5792 Len=0 TSV=174565062 TSER=19952247

```
▷ Flags: 0x0018 (PSH, ACK)
  Window size: 5792 (scaled)
  Checksum: 0x4695 [correct]
▽ Options: (12 bytes)
    NOP
    NOP
    Time stamp: tsval 174565056, tsecr 19942216
▽ Post Office Protocol
  ▽ -ERR [AUTH] "aep": access denied.\r\n
      Response: -ERR
      Response Arg: [AUTH] "aep": access denied.
```

```
0000  00 12 f0 62 b7 f7 00 02  17 29 b4 00 08 00 45 00   ...b.... .)....E.
0010  00 57 32 4a 40 00 36 06  a8 32 c2 6d d1 da 55 e2   .W2J@.6. .2.m..U.
0020  7f fa 00 6e c7 03 27 47  a4 fe 52 35 d3 4e 80 18   ...n..'G ..R5.N..
0030  05 a8 46 95 00 00 01 01  08 0a 0a 67 a6 c0 01 30   ..F..... ...g...0
0040  4b 48 2d 45 52 52 20 5b  41 55 54 48 5d 20 22 61   KH-ERR [ AUTH] "a
0050  65 70 22 3a 20 61 63 63  65 73 73 20 64 65 6e 69   ep": acc ess deni
0060  65 64 2e 0d 0a                                     ed...
```

File: "/tmp/etherXXXX8sCEeW" 11 KB 00:00:32 | P: 102 D: 23 M: 0 Drops: 0

Ethereal

- معلومات تفصيلية عن سيل بيانات محدد
- يمكننا تصفية المعلومات وتفحص كل حركة على حدة
- تمكننا من تحديد فيما إذا كان سبب المشكلة:
  - مشكلة وصلة (لا يمكن الوصول إلى الجهاز الآخر)
  - مشكلة خدمة (الخدمة غير متوفرة)
  - مشكلة المستخدم / المخدم (التحقق من الهوية، إعدادات التطبيقات)

تتعلق غالبية مشاكل الشبكة اللاسلكية بـ

- الطبقة الفيزيائية: النقاط الخفية، تعدد المسارات، الضجيج
- طبقة بروتوكول الإنترنت IP: تخطيط الشبكة، وجود أكثر من مخدم DHCP واحد، سرعات نقل غير متناظرة
- طبقة التطبيقات: الفيروسات، برمجيات الند للند Peer-to-Peer

الخلاصة

- كلما تعرفت أكثر على كيفية عمل الشبكة كلما ازدادت قدرتك على كشف الأخطاء بسهولة أكبر
- يختلف استيعاب المشكلة اختلافاً كلياً عن حل هذه المشكلة

تلميحات ختامية!

- يستغرق إعادة بناء نظام غير موثق زمناً أقصر من محاولة كشف الأعطال في هذا النظام
- إذا أردت الحصول على المساعدة ينبغي أن تكون مستعداً لتقديم الوثائق المطلوبة