ITRAINONLINE MMTK

كشف أعطال الشبكات اللاسلكية – كراسة المتدرّب

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

ITRAINONLINE MMTK.....1
1. عن هذا المستند.....1
1.1. معلومات حفظ الملكية الفكرية.....1
2.1. درجة الصعوبة.....1
2. مقدّمة.....2
3. المنهجيّة Methodology.....2
1.3. كشف الأعطال من الأعلى باتجاه الأسفل Top-Down Troubleshooting.....3
2.3. كشف الأعطال من الوسط باتجاه الأعلى أو باتجاه الأسفل Middle-Top, Middle-Down Troubleshooting. 3
3.3. مثال عملي.....3
4. أدوات كشف الأعطال 5
5. المثال 1: التشويش على الإشارة اللاسلكية، القنوات المشغولة؟ 5
6. المثال 2: الشبكة المكتظّة؟ طوفان الشبكة؟ 6
7. المثال 3: لماذا توقفت هذه الخدمة عن العمل؟ لماذا يتم رفض الإتصال؟ 7
8. الخلاصة.....9

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: متوسّط.

2. مقدّمة

تقدّم هذه الوحدة أسلوباً منهجيّاً لكشف أعطال الشبكات اللاسلكية. يتجلّى التحدي الأكبر أثناء محاولة كشف الأعطال في أي شبكةٍ إتصالات في تحديد ماذا جرى عند وقوع المشكلة. ننصحك عوضاً عن إعادة تشغيل كل التجهيزات المتصلة بالتيار الكهربائي أو إلقاء اللوم على الأحوال الجويّة أن تتبع نموذج OSI المعياري لمحاولة إيجاد سبب المشكلة.

نموذج OSI (Open Systems Interconnection) المعياري (والذي أعدّته منظمة المعايير الدولية International Standards Organisation) هو توصيفٌ نظريٌّ لتصميم بروتوكولات شبكات الحواسب (والإتصالات). يفصل هذا النموذج وظائف الإتصال إلى سبع طبقاتٍ مختلفةٍ يمكنها العمل بشكلٍ مستقلٍّ عن بعضها البعض.

يتبع تصميم بروتوكول الإنترنت Internet Protocol بنيةً مشابهةً لنموذج OSI المعياري. تستخدم كلّ طبقةٍ من طبقات البروتوكول خدمات الطبقة التي تقع أسفلها مباشرةً فقط وتقدّم خدماتها للطبقة التي تعلوها مباشرةً فقط. تملك هذه البنية فائدةً جمّةً أثناء محاولة تحديد المشكلة لأنّها ستساعد على عزل موقع المشكلة. ينبغي علينا عند كشف مشاكل الشبكة أن نبدأ على الدوام بتحديد الطبقة التي تظهر ضمنها هذه المشكلة والطبقة التي تسببت بها.

على سبيل المثال، يشتكي المستخدمون عادةً من أنّ التطبيق (س) لا يعمل! (الطبقة السابعة من نموذج OSI) لكنّ سبب المشكلة قد يكمن في أيٍّ من الطبقات التي تقع أسفل هذه الطبقة. قد تكون المشكلة مثلاً عدم توفّر إشارةٍ لاسلكيةٍ (الطبقة الأولى من نموذج OSI) أو عدم توفّر عنوان إنترنت IP Address (الطبقة الثالثة من نموذج OSI.

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

جدول 1: نموذج OSI المعياري في مقابل مجموعة بروتوكولات TCP/IP

3. المنهجيّة Methodology

يمكننا بناءً على المعلومات المتوفّرة لدينا إنتهاج أحد الأسلوبي التاليين:

1.3 كشف الأعطال من الأعلى باتجاه الأسفل Top-Down Troubleshooting

عند ظهور مشكلةٍ ما يبدأ كشف الأعطال من الأعلى باتجاه الأسفل بتفقّد إعدادات التطبيقات وينتهي بالتحقق من وجود تشويشٍ على الإشارة اللاسلكية أو مستوى إشارةٍ ضئيلٍ في جهاز الإستقبال.

2.3 كشف الأعطال من الوسط باتجاه الأعلى أو باتجاه الأسفل Middle-Top, Middle-Down Troubleshooting

يبدأ هذا الأسلوب عند ظهور مشكلةٍ ما بتفقّد وصلة بروتوكول الإنترنت IP إلى الخدمة المطلوبة أو إلى موجّه البوابة وبناءً على نتيجة هذا الفحص سيتابع محاولة تحديد المشكلة ضمن الطبقات الأعلى أو الأسفل.

يعتبر هذا الأسلوب الأكثر استخداماً: <ping <the service>, ping <the router>

لكنّ هذه المعلومات ولسوء الحظ لا تساعد على تحديد المشكلة الحقيقيّة بقدر ما تساعد على تحديد الطرف الذي سيتحمّل اللوم. إذا فشل الإتصال Ping مع موجّه البوابة يمكننا توجيه اللوم إلى مزوّد خدمة الشبكة اللاسلكية، أمّا إذا فشل الإتصال مع الخدمة سنلوم حينها مزوّد خدمة الإنترنت. إذا لم نفشل في الإتصال بأيٍّ منهما سنلوم المستخدم أو نظام التشغيل.

بغضّ النظر عن الأسلوب المتبع في كشف الأعطال، لا بدّ لنا من التعرّف على الأدوات الملائمة لتحليل كل طبقةٍ من طبقات الشبكة.

يكمن الهدف الرئيس في اتباع المنهجيّة في أنّها ستتيح لك توصيف إجراءات كشف الأعطال وستمنحك القدرة على تحديد المشاكل التي تتطلّب مستويات أعلى من المهارة والخبرة.

3.3 .مثال عملي

دعنا نستخدم مثالاً عمليّاً لتوضيح الفكرة. ينبغي عليك إذا اتصل بك أحدهم وهو يصرخ "لا أستطيع قراءة بريدي الإلكتروني!" أن تمتلك أسلوباً يمكّنك من تحديد سبب المشكلة دون الإتصال بأمهر مدراء شبكتك.

سنطرح الأسئلة التالية (في حال اتبعنا الأسلوب المقترح الأول – من الأعلى باتجاه الأسفل –) لمحاولة تحديد مكمن المشكلة:

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

أمّا إذا اتبعنا الأسلوب الثاني (من الوسط باتجاه الأعلى أو الأسفل) سنطرح الأسئلة التالية:

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

في حال كانت الإجابة على كلٍ من هذين السؤالين بـ (لا):

- هل لديك عنوان إنترنت IP Address؟
- هل قمت بتسجيل الدخول إلى مخدّم التحقق من الهويّة بنجاح؟

إنّ تصنيف المشاكل ليس بالأمر السهل على الإطلاق، كما أنّ هذه المشاكل تختلف من شبكةٍ إلى أخرى، لكنّ المنهجيّة التي سنستخدمها لكشف هذه المشاكل ستبقى كما هي على الدوام.

إليك أحد الأساليب السهلة لتصنيف مشاكل الشبكة:

- لا شيء يعمل على الإطلاق (لماذا لا يستطيع جهازي – أدخل الكلمة هنا – ؟)
- بعض الأشياء تعمل في بعض الأحيان (أو أنّها تعمل بشكلٍ ردئ) (لماذا يعمل جهازي ببطءٍ شديدٍ؟)

من السهل اكتشاف مشاكل النوع الأوّل لأنّ أسبابها غالباً ما تعود إلى ميزانيةٍ خاطئةٍ للوصلة، خسارة القدرة في التجهيزات، سوء توجيه الهوائيّات، الإعدادات الخاطئة وغيرها.

أمّا النوع الثاني فاكتشافه أكثر صعوبةً (خصوصاً عندما يتعلّق الأمر بالطبقات السفلة من مجموعة بروتوكولات TCP/IP) لأنّه يتطلّب مراقبة جميع متغيرات الشبكة اللاسلكية على مدى فترةٍ من الزمن عند محاولة تحديد سبب المشكلة.

يظهر الجدول التالي مجموعةً من الأدوات التي قد تساعدك أثناء عمليّة كشف الأعطال:

الطبقة	OSI	TCP/IP	الأدوات
7	التطبيقات Application	التطبيقات Application	nslookup
6	التقديم Presentation		
5	الجلسة Session	النقل (Transport (TCP	Ntop (ويندوز، لينكس) Visualroute, traceroute
4	النقل Transport		
3	الشبكة Network	الشبكة (Network (IP	Nmap Ntop (ويندوز، لينكس) Ethereal Etherape

2	وصلة البيانات Data Link	التحكّم بالوصول إلى الناقل Media Access Control	Ethereal (ويندوز، لينكس) Netstumbler (ويندوز) Kismet, Wavemon, Wellenreiter أدوات الإدارة الخاصة بمنتج التجهيزات
1	الفيزيائيّة Physical		

جدول 2: أدوات كشف الأعطال في كلٍّ من طبقات مجموعة بروتوكولات TCP/IP

يمكننا عند تحديد المشاكل في الشبكات اللاسلكية استخدام نوعين من الأدوات: الأدوات التي تعمل مع جميع المنتجات المتوافقة مع معايير 802.11b والأدوات التي تأتي مرفقةً مع كلّ منتجٍ على حدة.

يقوم بعض منتجو التجهيزات اللاسلكية (مثل Proxim Orinoco Outdoor Solutions) بتطوير المعيار 802.11b الأصلي مما يستدعي استخدام أدواتٍ محددةٍ جدّاً للمراقبة وكشف الأعطال.

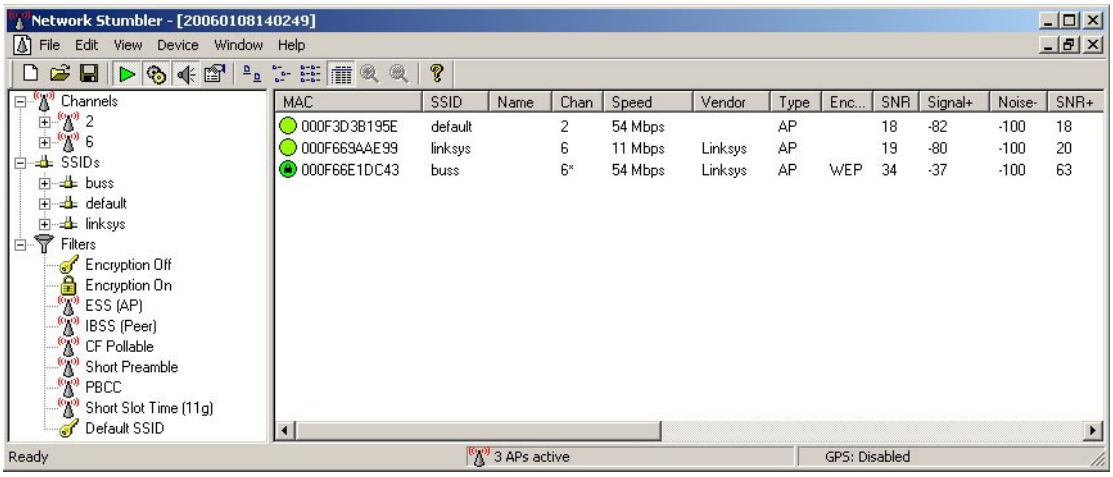
4.أدوات كشف الأعطال

1. Nslookup, dig
2. Ntop
3. Visualroute, traceroute
4. Nmap
5. Ethereal (راجع المثال 3)
6. Etherape (راجع المثال 2)
7. Netstumbler (راجع المثال 1)
8. Kismet
9. أدوات الإدارة الخاصة بمنتج التجهيزات.

5. المثال 1التشويش على الإشارة اللاسلكية،القنوات المشغولة؟

يقدّم هذا المثال أسلوباً منخفض الكلفة لمراقبة جميع المتغيّرات المتعلّقة "بالطبقة الفيزيائيّة" لشبكتك اللاسلكية. ستستخدم دائماً أثناء كشف أعطال الإشارة اللاسلكية أدواتٍ تتخاطب مع بطاقات الشبكة اللاسلكية وتعود إليك بمجموعةٍ محددةٍ من المعلومات التي حصلت عليها.

يمكن لبطاقة الشبكة اللاسلكية أن تعمل باستخدام برنامجٍ مثل Netstumbler كمحلل طيفٍ بسيطٍ Spectrum Analyser يقوم بمسح الشبكات اللاسلكية المتاحة، تحديد نسب الإشارة إلى الضجيج لكل شبكة Signal to Noise Ratio، تقنيّات الترميز Modulation Techniques ونمط التشغيل. يقوم برنامج Netstumbler بتجميع النتائج ضمن واجهةٍ بسيطةٍ وسهلة الإستخدام.



شكل 1: واجهة إستخدام البرنامج Netstumbler

المصدر: http://upload.wikipedia.org/wikipedia/en/9/95/Netstumbler.jpg

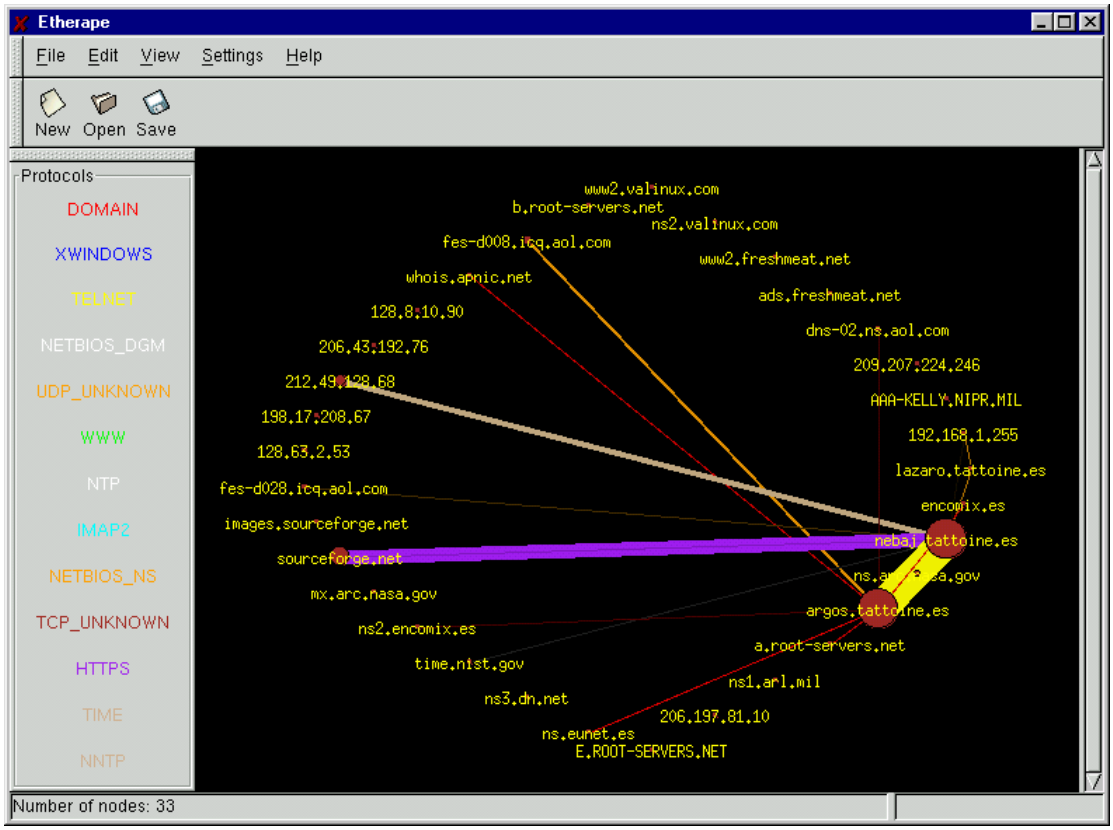
ستلاحظ في هذا المثال (شكل 1) وجود ثلاثة معرّفات لمجموعة الخدمات SSID (default, linksys, buss) ضمن قناتين فقط (2 و 6). تعمل اثنتان من نقاط الولوج بالمعيار (g) بسرعة 54 ميغابت في الثانية (default و buss) وتعمل نقطة الولوج الثالثة بالمعيار (b).

نلاحظ أيضاً إعداد تشفير WEP ضمن الشبكة ذات المعرّف SSID = buss. تعتبر نسبة الإشارة إلى الضجيج SNR في جميع الشبكات جيّدةً < 10 ديسيبل dB.

برنامج Netstumbler هو برنامجٌ خاملٌ (Passive) يتلصص على حركة البيانات ضمن الشبكة اللاسلكية. لا تتيح جميع بطاقات الشبكة إمكانيّة استباحة مراقبة حركة الشبكة اللاسلكية، لذلك ينبغي عليك التأكّد قبل تثبيت برنامج Netstumbler من دعمه لبطاقة الشبكة الموجودة لديك.

6. المثال 2:الشبكة المكتظّة؟طوفان الشبكة؟

يمكنك استخدام برنامج EtherApe (ضمن نظام التشغيل يونيكس Unix) على بوابة الشبكة السلكيّة للحصول على صورةٍ عامّةٍ لطبيعة وصلات بروتوكول الإنترنت IP الفعّالة ضمن شبكتك اللاسلكية. يتيح لك برنامج EtherApe مراقبة الوصلات الداخلة والخارجة من وإلى شبكتك اللاسلكية. لا تقتصر فائدة هذا البرنامج على تحديد أنواع حركة بروتوكول الإنترنت IP ضمن الشبكة وتوزّع الحركة بين نقاط الشبكة المختلفة بل تتعدّاها إلى تحديد مدى ديناميكيّة الشبكة. بإمكانك عبر تتبع الأشكال البيانيّة لحركة البيانات والتي يوفّرها هذا البرنامج إكتشاف الفيروسات المنتقلة ضمن الشبكة أو وجود كمياتٍ كبيرةٍ من بيانات برامج الند للند Peer-to-Peer أو بروتوكول نقل الملفات FTP. يتوفّر عددٌ من البرمجيّات المماثلة بالإضافة إلى بعض برمجيّات تحليل البروتوكولات الأكثر تعقيداً والتي تعمل ضمن نظام التشغيل ويندوز (AirDefense, Scrutinizer, SolarWinds وغيرها) إلا أنّ غالبيّة هذه البرمجيّات ليست حرّةً أو مفتوحة المصدر.



شكل 2: واجهة إستخدام البرنامج EtherApe وتظهر عليها وصلات بروتوكول الإنترنت IP الفعّالة

نلاحظ في هذا المثال وجود كميّاتٍ كبيرةٍ من بيانات بروتوكول HTTPS (بروتوكول الإنترنت الآمن) بين نقطتي "nebaj" و "sourceforge" (الخط البنفسجي). نلاحظ أيضاً وجود وصلة Telnet بين نقطتي "nebaj" و "argos" (الخط الأصفر الثخين). يتضح أيضاً أن بروتوكول DNS يعمل بشكلٍ جيّدٍ من النقطة "argos" إلى كلٍّ من "ns.eusnet.es" و "ns2.economix.es" (الخطوط الحمراء).

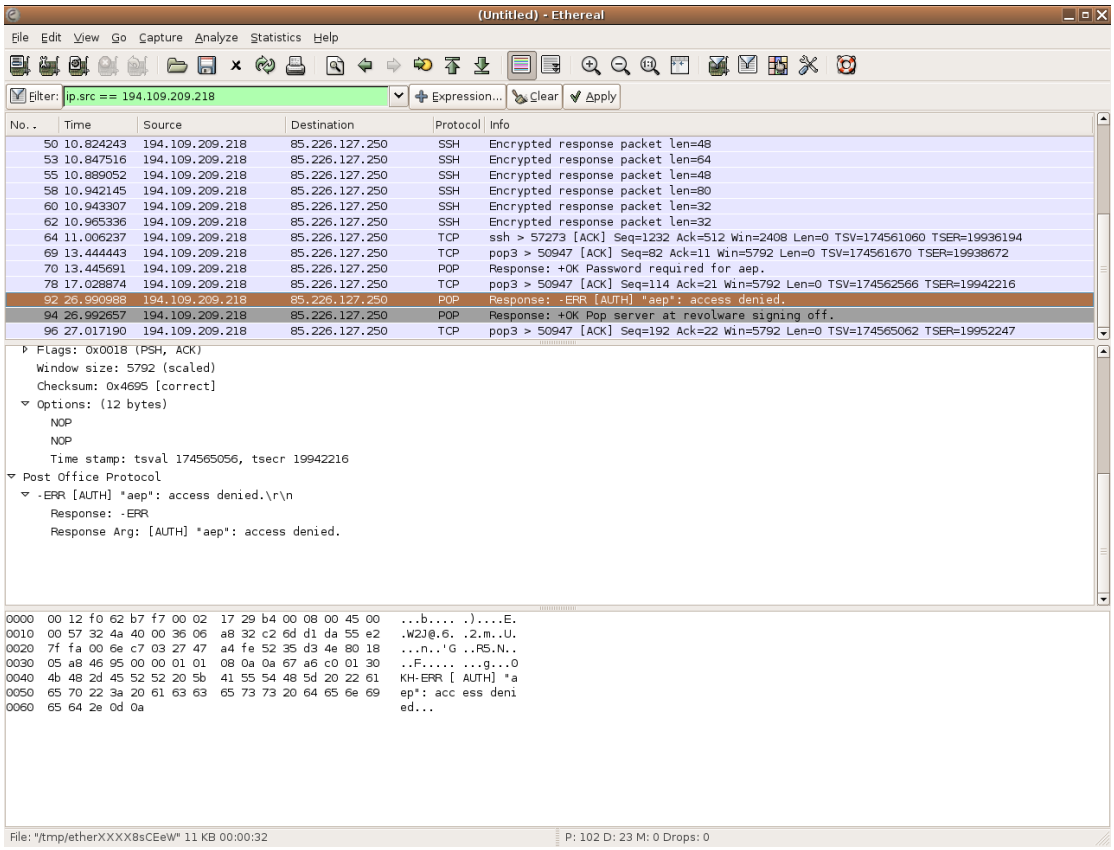
ترتبط حركة بيانات بروتوكول UDP غير المعروف (الخط البني) ببرنامج ICQ Messenger (متصلٌ مع d008.icq.aol.com).

7. المثال 3: لماذا توقفت هذه الخدمة عن العمل؟ لماذا يتم رفض الإتصال؟

إذا أردت إلقاء نظرةٍ أكثر قرباً على حركة نوعٍ محددٍ من البروتوكولات يمكنك استخدام برنامج Ethereal الذي يتيح لك التقاط جميع البيانات التي ستمر عبر منفذ الشبكة الخاص بك مما يمكنّك من تفحص سير البيانات وتفاصيل جميع الحركات ضمن الشبكة. يعتبر برنامج Ethereal مفيداً جداً لمراقبة:

- خسارة الحزم في وصلات TCP Packet Loss: وهو مؤشّرٌ على احتمال ازدحام الشبكة، التصادمات وغيرها.
- زمن رحلة العودة Round trip time: ويشير إلى مستوى التأخير ضمن الشبكة, تشير القيم العالية لزمن رحلة العودة ضمن الشبكة اللاسلكية إلى مستوياتٍ عاليةٍ لاستخدام القناة أو تصادم الحزم.

- أخطاء البروتوكولات Protocol Errors: والتي لا تظهر عادةً للمستخدم مثل فشل التحقق من الهويّة Authentication، الإستخدام المتكرر لنفس عناوين الإنترنت IP، تعذّر الوصول إلى الشبكة، طوفان حزم ICMP وغيرها (راجع وحدة التشبيك المتقدّم).



شكل 3: كشف أعطال البريد الإلكتروني POP3 باستخدام برنامج Ethereal

يظهر الشكل 3 مستوى التفاصيل التي يمكن الحصول عليها من برنامج Ethereal، مما يظهر قيمة هذا البرنامج في كشف أعطال الشبكة.

- يمكننا بعد التقاط البيانات المارّة عبر الشبكة تصفية هذه البيانات (ip.src=194.109.209.118) لعرض جميع الحزم الواردة من مخدّم البريد الإلكتروني POP (الصندوق الأخضر).
- يمكننا بعد تصفية جميع الحزم مشاهدة البيانات المتبادلة بين مخدّم البريد الإلكتروني والزبون (violet). تظهر الحركة المصنّفة ضمن بروتوكول TCP مفاوضات الوصلة (والتي تعرف أيضاً بإسم مصافحة TCP Handshake)، في حين تشير حركة البيانات المصنّفة ضمن بروتوكول POP3 إلى بيانات البريد الإلكتروني "التطبيق".
- يمكننا اختيار حزمةٍ معيّنةٍ من بين حزم البروتوكول POP3 لنرى رسالة الخطأ التالية: – ("ERR (AUTH):"aep access denied.

يمكن الإستنتاج بناءً على هذه المعلومات أنّ الإتصال بين الزبون ومخدّم البريد الإلكتروني يتم بنجاح وبأنّ مخدّم البريد الإلكتروني يعمل بشكلٍ جيّدٍ وبأنّ المشكلة تظهر أثناء محاولة التحقق من الهويّة. يمكن أن تنتج مشكلة التحقق من الهويّة بسبب خللٍ من جهة المخدّم أو من جهة الزبون: إمّا أنّ كلمة السر المرسلة من قبل الزبون خاطئة أو أنّ المخدّم لم ينجح في التأكّد من كلمة السر المرسلة.

8. الخلاصة

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

1. كلّما تعرّفت أكثر على كيفيّة عمل الشبكة كلّما ازدادت قدرتك على كشف الأخطاء بسهولةٍ أكبر.
2. يختلف استيعاب المشكلة اختلافاً كلياً عن حلّ هذه المشكلة.
3. حاول اتباع منهجيّةٍ منطقيّةٍ عند حدوث عطلٍ ما عوضاً عن العمل بشكلٍ عشوائيٍّ.
4. بغضّ النظر عن الأسلوب المتّبع لكشف الأعطال ينبغي الإلمام بالأدوات الملائمة لتحليل كل طبقةٍ من طبقات الشبكة.
5. يمكن استخدام نوعين من الأدوات عند محاولة تحديد المشاكل في الشبكات اللاسلكية: الأدوات التي تعمل مع أيّ جهازٍ لاسلكيٍّ متوافقٍ مع المعيار 802.11b والأدوات التي تأتي مرفقةً مع كلّ منتجٍ على حدة.