ITRAINONLINE MMTK

البنى التحتيّة المعتمدة على نظام التشغيل لينكس – كراسة المتدرّب

إعداد: توماس كراغ، wire.less.dk
النسخة العربية: أنس طويلة، www.tawileh.net/anas

1 ITRAINONLINE MMTK
1. عن هذا المستند 2
1.1. معلومات حفظ الملكية الفكرية 2
3.1. المتطلبّات المسبقة 2
3.1. درجة الصعوبة 2
2. مقدّمة 2
3. دور لينكس ضمن البنى التحتيّة للشبكات اللاسلكية 3
4. الإفتراضات 4
1.4. البرمجيّات Software 4
2.4. التجهيزات Hardware 5
5. المثال الأول: نقطة الولوج القادرة على التقنيع Masquerading Access Point 5
1.5. الخطوة 0: الإعداد الأولي 5
2.5. الخطوة 1: إعداد منافذ الشبكة 6
3.5. الخطوة 2: إعداد التقنيع ضمن نواة نظام التشغيل لينكس 7
4.5. الخطوة 3: إعداد مخدّم بروتوكول الإعداد التلقائي للمضيف DHCP 8
5.5. الخطوة 4: زيادة الأمن عبر إعداد جدارٍ ناريٍّ 9
6. المثال الثاني: نقطة ولوج التجسير الشفّاف Transparent Bridging Access Point 9
1.6. الخطوة 0: الإعداد الأولي 10
2.6. الخطوة 1: إعداد منافذ الشبكة 10
3.6. الخطوة 2: بدء تشغيل الجسر 11
7. الوصفة السهلة للمثال الأول الثاني! 12
8. المثال الثالث: جدارٌ ناريٌّ مركزيٌّ مع وظائف التحقق من الهويّة 12
1.8. لمحة موجزة عن الإعداد 13
1.81.. التجهيزات المطلوبة 13
2.8. الخطوة 0: إعداد البرمجيّات الأساسيّة 14
3.8. الخطوة 1: إعداد Apache ليدعم SSL 15
4.8. الخطوة 2: إعداد ChilliSpot 16
5.8. الخطوة 3: إعداد البرمجيّات 16
5.81.. إعداد الشبكة والجدار الناري 16
5.82.. ملف إعداد ChilliSpot 17
5.83.. إعداد FreeRADIUS 18
5.84.. تخصيص النص البرمجي hotspot login 19
5.85.. إستخدام ChilliSpot 19
9. الخلاصة 20

1.عن هذا المستند

تشكّل 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-ShareAlike 2.5. 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-sa/2.5/

3.1 المتطلبّات المسبقة

للحصول على أقصى فائدةٍ ممكنةٍ من هذه الوحدة ينبغي أن يكون القارئ ملمّاً بنظام التشغيل لينكس Linux من وجهة نظر المستخدم، كما ينبغي أن يكون قادراً على تثبيت توزيعة غنو/لينكس GNU/Linux التي يختارها. تتطلّب هذه الوحدة أيضاً الإلمام بأساسيّات واجهة سطر الأوامر Command Line Interface (CLI)).

يتطلّب إعداد نقطة الولوج حسب ما هو مشروحٌ في هذه الوحدة توفّر حاسبٍ يعمل بنظام التشغيل لينكس ويحتوي على بطاقة شبكةٍ لاسلكيةٍ أو أكثر. تستخدم الأمثلة المشروحة في هذه الوحدة بطاقة شبكةٍ معيّنةٍ وبرنامج التعريف الخاص بها، إلا أنّه يمكن تحقيق نفس الهدف باستخدام عددٍ من البطاقات المختلفة. راجع وحدة "إعداد زبائن الشبكة اللاسلكية" لمزيدٍ من المعلومات عن كيفية تركيب بطاقة شبكةٍ لاسلكيةٍ ضمن نظام التشغيل لينكس.

ينبغي أن يمتلك القارئ أيضاً دراية بمبادئ شبكات TCP/IP (راجع وحدة "التشبيك المتقدّم").

3.1 .درجة الصعوبة

درجة صعوبة هذه الوحدة: متقدّم.

2. مقدّمة

تقدّم هذه الوحدة لمحةً عن الأدوار المختلفة ضمن الشبكة والتي يمكن أداؤها باستخدام حاسبٍ يعمل بنظام التشغيل لينكس. تحتوي الوحدة على ثلاثة أمثلةٍ مختلفةٍ سيتم التعريف بها بشكلٍ موجزٍ وشرح خطوات الإعداد مع ذكر بعض الأمثلة عن حزم البرمجيّات المستخدمة.

تستهدف هذه الأمثلة الثلاث:

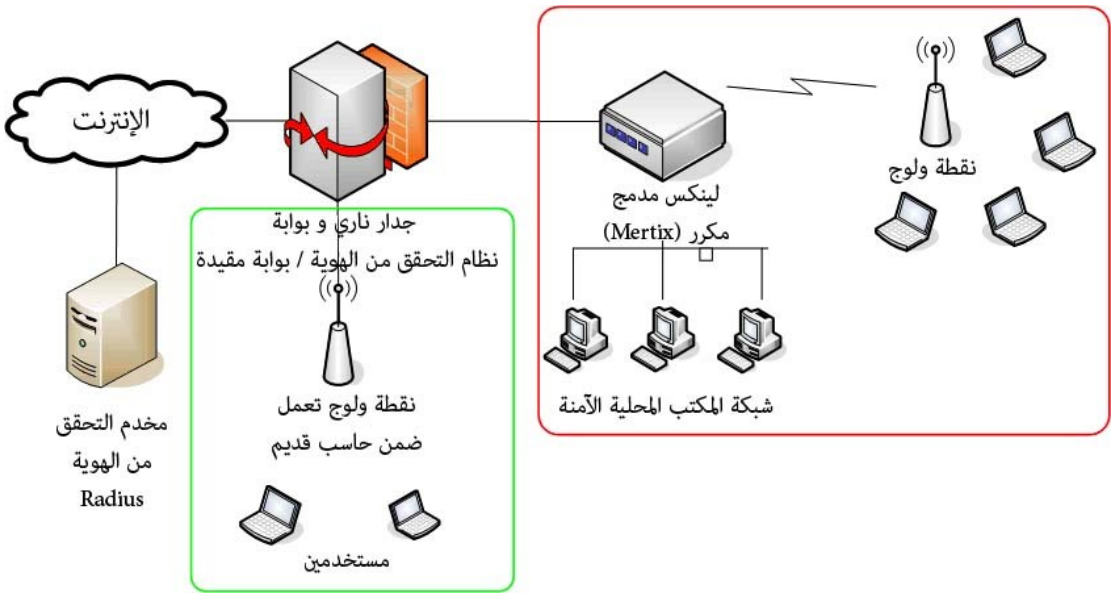
1. تقنيع نقطة الولوج Access Point Masquerading.
2. نقطة ولوج الجسر الشفّاف Transparent Bridge Access Point.
3. جدار النار / البوابة المركزيّة Central Firewall / Gateway.

3. دورلينكس ضمن البنى التحتيّة للشبكات اللاسلكية

يتيح نظام التشغيل لينكس لمدير الشبكة(على عكس منافسه ويندوز) بشكلٍ عامٍ إمكانيّة الوصول إلى كامل كدسة الشبكة Network Stack. يمكن مثلاً الوصول إلى حزم البيانات ضمن كلٍّ من طبقة وصل البيانات الفرعيّة Data Link Sublayer، طبقة الشبكة Network Layer وبالتأكيد طبقة التطبيقات Application Layer.

أضف ذلك إلى مرونة لينكس المعهودة من حيث قابليته للعمل ضمن طيفٍ واسعٍ من التجهيزات لتعرف سبب شعبيّة لينكس كأداةٍ فائقة القوّة تستطيع لعب الكثير من الأدوار في البنى التحتيّة للشبكات.

يظهر الشكل التالي المثال الذي ستعتمد عليه هذه الوحدة (ينبغي الإنتباه إلى أنّ هذا الشكل يظهر فقط بعض الأدوار المختارة ضمن الشبكة). يمكن من حيث المبدأ دمج جميع الأدوار الموضّحة بالشكل في حاسبٍ واحدٍ أو تقسيمها بطرقٍ عدّةٍ. سنقوم بفصل الأدوار عن بعضها البعض لتسهيل الشرح.



شكل 1: بنيّة الشبكة التي ستعتمد عليها أمثلة هذه الوحدة

يوضّح هذا الشكل شبكةً محليّةً تحتوي على جزئين منفصلين، جزءٌ مفتوحٌ وجزءٌ مغلقٌ يتطلّب الوصول إليه التحقق من الهويّة Authentication. تحتوي الشبكة أيضاً على ثلاثة وحداتٍ تؤلّف البنيّة التحتيّة للشبكة اللاسلكية (يختلف شكل هذه الوحدات في الرسم لتوضيح سعة الخيارات المتاحة، أي أنّ نقطة الولوج قد تكون وحدةً متكاملةً مثل وحدة Linksys WRT54G، جهازاً مخصصاً يعمل بنظام التشغيل لينكس مثل جهاز Metrix MkII، أو حاسباً شخصيّاً قديماً أعيد استخدامه بمساعدة نظام التشغيل لينكس.

سنلقي في هذه الوحدة نظرةً على كيفية إعداد نظام التشغيل لينكس للقيام بالأدوار التالية:

1. نقطة ولوجٍ لاسلكيةٍ تملك إمكانيّة التقنيع Masquerading / ترجمة عناوين الشبكة NAT (تدعى أيضاً بالبوابة اللاسلكية).
2. نقطة ولوجٍ لاسلكيةٍ تقوم بدور جسرٍ شفاف Transparent Bridge ويمكن استخدامها كنقطة ولوجٍ بسيطةٍ أو كمكررٍ يحتوي بطاقتين للشبكة اللاسلكية.
3. موجّهٌ مركزيٌّ يحتوي على نظامٍ بسيطٍ للتحقق من الهويّة لإتاحة التحقق من هويّة المستخدمين المتصلين بعدّة نقاط ولوج.

4. الإفتراضات

1.4 البرمجيّات Software

تعتمد هذه الوحدة (بغاية التبسيط) على بعض الإفتراضات المتعلّقة بالبرمجيّات والتجهيزات التي سيتم استخدامها. يرحب المؤلف بأيّة ملاحظاتٍ أو أفكارٍ عن استخدام توزيعات لينكس أخرى أو برمجيات تعريف مختلفة (t@wire.less.dk).

ينبغي أن تعمل هذه الأمثلة أيضاً باستخدام توزيعات لينكس الحديثة الأخرى، لقد قمنا في بعض المواضع بإيضاح التغييرات الضروريّة ضمن توزيعتي ماندريك Mandrake وفيدورا Fedora Core، لكننا لم نتأكّد من هذه التغييرات عبر تجربتها ضمن التوزيعات المذكورة.

تعتمد الأمثلة على الإصدار 5.10 توزيعة أوبونتو Ubuntu (Breezy Badger) مع بطاقة شبكةٍ لاسلكيةٍ تدعمها برامج التعريف hostap أو madwifi (راجع "مصادر إضافيّة للمعلومات" لوصلات مواقع الإنترنت الموافقة).

يمكن إجراء هذه الإعدادات باستخدام برمجيّات تعريفٍ أخرى مادامت تدعم نمط السيّد Master Mode (أو نمط نقطة الولوج AP Mode). من الممكن أيضاً (إلا أنّه من غير المستحب) القيام بنفس الإعدادات ضمن النمط الخاص Ad-hoc Mode والذي تدعمه غالبيّة برمجيّات التعريف.

سنحتاج إلى البرمجيّات التالية (والتي تعمل ضمن نظام التشغيل لينكس) لإتمام الأمثلة الثلاثة:

1.أدوات الشبكة اللاسلكية (تعليمات iwlist ،iwconfig)
2.الجدار الناري iptables firewall
3.dnsmasq (مخدّم التخزين المؤقت للـــ DNS ومخدّم بروتوكول الإعداد التلقائي للمضيف DHCP).

2.4التجهيزات Hardware

تحتاج هذه الأمثلة لبعض التجهيزات: حاسبٌ قياسي (شخصي أو محمول) يحتوي على منفذ شبكة إيثرنت السلكية وبطاقةٍ للشبكة اللاسلكية (أو بطاقتين للشبكة لاسلكية) لإعداد كلٍ من نقطة الولوج ونقطة الولوج القادرة على التقنيع. لا تحتاج هذه التجهيزات إلى أيّة متطلّباتٍ خاصّةٍ من حيث سرعة المعالجة. يمكن تطبيق هذه الإعدادات ضمن أجهزة مدمجة Embedded Boxes، حواسب اللوحة الواحدة Single-Box Computers أو حتى بعض نقاط التشغيل المعدّلة والتي تعمل بنظام التشغيل لينكس (مثل نقطة الولوج Linksys WRT54G).

تحتوي وثيقة "مصادر إضافيّة للمعلومات" على وصلاتٍ لمواقع بعض منتجي التجهيزات المقترحين (لا يعني ذلك أننا ننصح بأيٍّ منهم) على الإنترنت والذين تلائم تجهيزاتهم هذه الغايات.

يحتاج مثال الجدار الناري / التحقق من الهويّة بعض التجهيزات الإضافيّة، لكنّه سيعمل بشكلٍ جيّدٍ ضمن معالج x86 بسرعة 500 ميغاهرتز مع قرص صلبٍ سعته 10 غيغابايت (أو حتى بطاقة ذاكرة من نمط Compact Flash بسعة 2 غيغابايت) وذاكرة مؤقتة RAM بسعة 128 ميغابايت. تعتمد هذه المواصفات على الضغط المتوقع على النظام (يعتمد على ضغط المستخدمين).

5. المثال الأول :نقطةالولوج القادرةعلى التقنيع Masquerading Access Point

وهو أبسط الأمثلة، ويفيد بشكلٍ خاصٍّ في الحالات التي تحتاج فيها إلى نقطة ولوجٍ واحدةٍ لمكتب حيث:

1.يتوفّر بالأساس جدارٌ ناريٌّ وبوابةٌ مخصصين يعملان بنظام التشغيل لينكس، وكل ما تريد عمله هو إضافة منفذ للشبكة اللاسلكية.
2.لديك حاسبٌ شخصيٌّ أو محمولٌ قديمٌ ترغب باستخدامه كنقطة ولوج.
3.تحتاج تحكمّاً أكبر بالمراقبة، حفظ السجلات Logging أو/و الأمن من ذلك المتاح ضمن نقاط الولوج التجاريّة، لكنّك في الوقت نفسه لا تريد تكبّد تكاليف نقطة ولوجٍ مؤسساتيّةٍ Enterprise Access Point (راجع المثال 3).
4.ترغب في استخدام جهازٍ واحدٍ للعمل كنقطتي ولوج (وجدارٍ ناريٍّ) بحيث تتمكّن من توفير الوصول الآمن إلى الشبكة الداخليّة بالإضافة إلى الوصول المفتوح للضيوف (راجع أيضاً المثال 3).

1.5. الخطوة 0 : الإعدادالأولي

إبدأ بحاسبٍ معدٍّ مسبقاً يعمل بنظام التشغيل لينكس (قد تكون التوزيعة المستخدمة Ubuntu Server Installation أو Fedora Core). يجب أن يحتوي هذا الحاسب على بطاقتي شبكةٍ على الأقل للقيام بهذه المهمة، أحدها على الأقل لاسلكي. سنفترض في الشرح التالي بأنّ منفذ شبكة الإيثرنت السلكي (eth0) موصولٌ بالإنترنت (حيث يستطيع الحصول على عنوان إنترنت IP من مخدّم DHCP)، وبأنّ هناك بطاقة شبكةٍ لاسلكيةٍ (wlan0) ستوفّر وظائف نقطة الولوج. كما ذكرنا سابقاً، لقد قمنا بتجربة نمط السيّد Master Mode (أو نمط نقطة الولوج Access Point Mode) مع كلٍّ من برنامج التعريف madwifi (مجموعة رقاقات Atheros) وبرنامج التعريف hostap (مجموعة الرقاقات Intersil Prism2/2.5/3) فقط.

للتحقق فيما إذا كانت مجموعة الرقاقات المستخدمة في بطاقة شبكتك تدعم نمط السيّد Master Mode، جرّب التعليمة التالية (كمستخدمٍ جذريٍّ root):

```
# iwconfig wlan0 mode Master
```

استبدل wlan0 بإسم بطاقة الشبكة الخاصّة بك.
إذا لم تحصل على رسالة خطأ فإن بطاقتك يجب أن تعمل بشكلٍ سليمٍ.
أمّا إذا حصلت على رسالة خطأ يمكنك حينها تجربة نفس الإعداد ضمن النمط الخاص Ad-hoc mode والذي تدعمه جميع مجموعات الرقاقات. يتوجّب عليك في هذه الحالة إعداد جميع الحواسب المحمولة المرتبطة بنقطة الولوج هذه ضمن النمط الخاص أيضاً، مما قد يتسبب بأداء سيخون توقعاتك أحياناً.

تأكّد قبل المتابعة من تثبيت حزمة dnsmasq ضمن حاسبك (استخدم الأداة الرسوميّة لإدارة حزم البرمجيّات الخاصّة بتوزيعتك). إستخدم التعليمة التالي إذا ما كنت تستعمل توزيعة Ubuntu (بعد إعداد مستودعات الحزم، راجع http://www.ubuntuguide.org):

```
# sudo apt-get install dnsmasq
```

2.5. الخطوة 1 : إعداد منافذ الشبكة

قم بإعداد المخدّم بحيث يكون منفذ الإيثرنت eth0 متصلاً بالإنترنت (استخدم الأداة الرسوميّة المرفقة مع توزيعتك أو جرّب التعليمة التالية كمستخدمٍ جذريٍّ root):

```
# dhclient eth0
```

قم بإعداد منفذ الشبكة اللاسلكية ضمن نمط السيّد Master وأعطه الإسم الذي تشاء:

```
# iwconfig wlan0 essid "my network" mode Master enc off
```

تقوم تعليمة "enc off" بإيقاف عمل تشفير WEP. يتوجّب عليك لتشغيل WEP إضافة مفتاحٍ ست عشريٍّ بطولٍ محدد بعد تعليمة enc، مثال:

```
# iwconfig wlan0 essid "my network" mode Master enc 1A2B3C4D5E
```

حدّد الآن عنوان الإنترنت IP لمنفذ الشبكة اللاسلكية ضمن نطاق شبكةٍ فرعيّةٍ خاصةٍ Private Subnet، تأكّد بأنّ هذا العنوان لا يقع ضمن نفس الشبكة الفرعيّة لمنفذ شبكة الإيثرنت:

```
# ifconfig wlan0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255 up
```

3.5. الخطوة 2 : إعداد التقنيع ضمن نواة نظام التشغيل لينكس

لا بدّ لنا لكي نتمكّن من ترجمة العناوين بين منفذي الشبكة ضمن الحاسب من تشغيل وظيفة التقنيع Masquerading / ترجمة عناوين الشبكة NAT ضمن نواة نظام التشغيل لينكس. سنقوم بدايةً بتحميل وحدة النواة الملائمة:

```
# modprobe ipt_MASQUERADE
```

سنتخلّص الآن من جميع قواعد الجدار الناري الموجودة مسبقاً لضمان أنّ الجدار الناري لن يمنعنا من إعادة توجيه الحزم بين منفذي الشبكة. إذا كنت تستخدم جداراً نارياً تأكّد من أنّك تعرف كيفيّة إستعادة الإعدادات الحاليّة لاحقاً.

```
# iptables –F
```

شغّل وظيفة ترجمة عناوين الشبكة NAT بين المنفذين:

```
# iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
```

علينا أخيراً تمكين النواة من توجيه الحزم بين المنفذين:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

يمكن تحقيق هذه الغاية أيضاً ضمن التوزيعات التي تعتمد على ديبيان Debian (ومنها أوبونتو Ubuntu) بتحرير الملف التالي:

```
/etc/network.options
```

وتغيير السطر:

```
ip_forward = no
```

إلى:

```
ip_forward = yes
```

ينبغي الآن إعادة تشغيل منافذ الشبكة باستخدام:

```
# /etc/init.d/network restart
```

أو:

```
# /etc/init.d/networking restart
```

4.5. الخطوة 3: إعداد مخدّم بروتوكول الإعدادالتلقائيللمضيف DHCP

لدينا الآن فعليّاً نقطة ولوجٍ تعمل بشكلٍ جيّد، ويمكننا تجربتها عبر الربط لاسلكيّاً مع جهازٍ منفصلٍ ومنح هذا الجهاز عنوان إنترنت IP ضمن نفس نطاق العناوين المستخدم لمنفذ الشبكة اللاسلكية في المخدّم (في هذا المثال 10.0.0.0/24).

يتوجّب علينا بغية تسهيل الإتصال بالمخدّم دون الحاجة إلى معرفة نطاق عناوين الإنترنت IP المستخدم إعداد مخدّم بروتوكول الإعداد التلقائي للمضيف DHCP ليقوم بمنح عناوين الإنترنت IP تلقائيّاً لزبائن الشبكة اللاسلكية.

سنستخدم برنامج dnsmasq لهذا الغرض. لقد تم تطوير هذا البرنامج خصيصاً (كما يتضّح من إسمه) للجدران النارية المعتمدة على NAT، وهو يوفّر بالإضافة إلى خدمات DHCP مخدّماً للتخزين المؤقت لمعلومات أسماء النطاق DNS Caching. يعتبر وجود مخدّم التخزين المؤقت لمعلومات DNS أساسيّاً في حال كانت وصلة الإنترنت بطيئةً أو ذات تأخيرٍ كبيرٍ، كوصلات الأقمار الصناعيّة والإتصال عبر خطوط الهاتف التقليديّة. يعني وجود هذا المخدّم أنّه سيتم تلبية القسط الأكبر من طلبات DNS محليّاً مما يوفّر الكثير من الحركة على وصلة الإنترنت، وبالتالي ظهور هذه الوصلة بسرعةٍ أكبر لمستخدميها.

قم بتثبيت حزمة dnsmasq باستخدام أداة إدارة حزم البرمجيّات المرفقة مع توزيعتك، أو حمّل الشيفرة المصدريّة Source Code من موقع الإنترنت الخاص بالحزمة (راجع "مصادر إضافيّة للمعلومات").

كلّ ما يتطلّبه تشغيل dnsmasq هو تعديل بضعة أسطرٍ ضمن ملف الإعداد والذي يمكن إيجاده ضمن:

```
/etc/dnsmasq.conf
```

يحتوي ملف الإعداد على الكثير من معلومات المساعدة بالإضافة إلى كثيرٍ من الخيارات لأنواعٍ متعددةٍ من الإعدادات. يتوجّب علينا تعديل سطرين فقط لتشغيل مخدّم DHCP البسيط:

أوجد الأسطر التي تبدأ بـــ:

```
interface=
```

وعدّلها على الشكل التالي:

```
interface=wlan0
```

ثم أوجد السطر الذي يبدأ بـــ:

```
#dhcp-range=
```

وعدّله بما يتلاءم مع عناوين الإنترنت IP المستخدمة ضمن الشبكة:

```
dhcp-range=10.0.0.10,10.0.0.110.255.255.255.0,6h
```

إحفظ الملف وشغّل أداة dnsmasq:

```
# /etc/init.d/dnsmasq start
```

هذا كلّ ما في الأمر! ينبغي أن تستطيع الآن الإتصال بالمخدّم على أنّه نقطة ولوجٍ، والحصول على عنوان إنترنت IP عبر بروتوكول DHCP. أي أنّه يمكنك الإتصال بالإنترنت عبر المخدّم.

5.5. الخطوة 4: زيادة الأمن عبر إعداد جدارٍ ناريٍّ

يمكنك بعد التأكّد من نجاح الإعدادات وعمل الشبكة إضافة قواعد الجدار الناري باستخدام أيّ أداة جدارٍ ناريٍّ مضمنّةٍ في توزيعتك. إليك فيما يلي بعض أدوات إعداد قواعد الجدار الناري:

- firestarter: أداةٌ رسوميّةٌ تعمل ضمن بيئة Gnome، أي أنّها تتطلب أن يحتوي المخدّم على مدير سطح المكتب Gnome.
- KNetfilter: أداةٌ رسوميّةٌ تعمل ضمن KDE، أي أنّها تتطلب أن يحتوي المخدّم على مدير سطح المكتب KDE.
- Shorewall: مجموعةٌ من ملفات الإعداد والنصوص البرمجيّة Scripts لتسهيل إعداد الجدار الناري iptables. يوجد أيضاً واجهاتٌ رسوميّةٌ لـــ Shorewall مثل webmin-shorewall.
- fwbuilder: أداة رسوميّة قويّة (إلا أنّها معقّدةٌ بعض الشيء) تتيح لك بناء النصوص البرمجيّة للجدار الناري iptables على جهازٍ آخر غير المخدّم ومن ثمّ نقلها إلى المخدّم لاحقاً. هكذا لن تحتاج إلى تشغيل واجهةٍ رسوميّةٍ على المخدّم بالإضافة إلى كونها خياراً قويّاً للمولعين بالأمن.

لمزيد من المعلومات حول إعداد أنظمة الأمن الإضافيّة راجع المثال 3.

6. المثال الثاني: نقطة ولوج التجسير الشفّاف Transparent Bridging Access Point

يمكن استخدام هذا الحل لتركيب مكررٍ Repeater يحتوي على جهازي إرسالٍ واستقبالٍ لاسلكيين أو لنقطة ولوجٍ مربوطةٍ بشبكة إيثرنت عندما نريد لجانبي نقطة الولوج أن يقعا ضمن نفس الشبكة الفرعيّة Subnet. تتجلى فائدة هذا الحل في الحالات التي تحتوي عدداً من نقاط الولوج وعند تفضيل وجود جدارٍ ناريٍّ

مركزيٍّ واحدٍ وربما مخدّمٌ مركزيٌّ للتحقق من الهويّة. يمكن إدارة جميع زبائن الشبكة اللاسلكية من خلال مخدّم DHCP واحد وجدارٍ ناريٍّ واحدٍ كونها تنتمي جميعها إلى نفس الشبكة الفرعيّة Subnet.

يمكنك على سبيل المثال إعداد مخدّم يشبه ذلك الذي أعددناه في المثال الأول ولكن باستخدام بطاقتي شبكة إيثرنت عوضاً عن بطاقة إيثرنت وأخرى لاسلكية. تتصل إحدى هاتين البطاقتين بالإنترنت وترتبط الأخرى بمبدّل الشبكة المحليّة. يمكنك حينها توصيل العدد الذي تشاء من نقاط الولوج إلى نفس المبدّل وإعداد كلٍ منها كجسرٍ شفاف ليتمكّن جميع زبائن الشبكة من عبور الجدار الناري واستخدام نفس المخدّم لبروتوكول DHCP. نستطيع لاحقاً تتبّع المثال الثالث لإضافة التحقق من الهويّة إلى هذا المخدّم المركزي.

1.6. الخطوة 0 : الإعدادالأولي

باستثناء انتفاء الحاجة إلى تثبيت حزمة dnsmasq فإنّ الإعداد الأوليّ لنقطة ولوج التجسير الشفاف يشابه تماماً إعداد نقطة الولوج القادرة على التقنيع (راجع **الخطوة 0** في **المثال الأول**).

يحتاج هذا المثال بالإضافة إلى الإعداد الأوليّ المذكور إلى الحزمة bridge-utils. تتوفّر هذه الحزمة لتوزيعة أوبونتو Ubuntu وغيرها من التوزيعات المبنيّة على ديبيان Debian إضافة إلى توزيعة فيدورا Fedora. تأكّد من أنّ هذه الحزمة مثبّتةٌ وبأنّ التعليمة brctl موجودةٌ قبل متابعة الإعداد.

2.6. الخطوة 1 : إعداد منافذ الشبكة

يمكن إعداد منافذ الشبكة ضمن توزيعة أوبونتو Ubuntu أو ديبيان Debian كما يلي:

/etc/network/interfaces

أضف قسماً مماثلاً للقسم التالي مع تغيير أسماء المنافذ وعناوين الإنترنت IP حسب الحاجة. يتوجّب أن تتوافق عناوين الإنترنت IP وقناع الشبكة Netmask مع إعدادات الشبكة الموجودة أساساً. يفترض هذا المثال أنّك تقوم ببناء مكررٍ لاسلكيٍ باستخدام بطاقتين للشبكة اللاسلكية (wlan0 و wlan1)، ولكنّ هذا الإعداد ممكنٌ أيضاً لبطاقة شبكةٍ سلكيةٍ وأخرى لاسلكية (eth0 و wlan0).

أضف ما يلي إلى ملف الإعداد:

```
auto br0
iface br0 inet static
        pre-up ifconfig wlan 0 0.0.0.0 up
        pre-up ifconfig wlan1 0.0.0.0 up
        pre-up iwconfig wlan0 essid “client"
        pre-up iwconfig wlan1 essid “AP” mode Master
        address 192.168.1.2
        network 192.168.1.0
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.1
        bridge_ports wlan0 wlan1
```

```
post-down ifconfig wlan1 down
post-down ifconfig wlan0 down
```

قم بإضافة علامات التنصيص لجميع الأقسام الأخرى ضمن الملف والتي تشير إلى منافذ الشبكة wlan0 و wlan1 وذلك لضمان عدم تعارضها مع إعداداتك.

يختص هذا الأسلوب في إعداد الجسور باستخدام ملف /etc/network/interfaces بالتوزيعات المبنيّة على ديبيان Debian حيث يتم الإحتفاظ بتفاصيل إعداد الجسر ضمن الملفين التنفيذيين Scripts:

```
/etc/network/if-pre-up.d/bridge
/etc/network/if-post-down.d/bridge
```

وتوجد وثائق تفسير هذين الملفين ضمن الدليل:

```
/usr/share/doc/bridge-utils/
```

إذا لم يتوفّر هذين الملفين ضمن توزيعتك (كما هو الحال في توزيعة فيدورا Fedora Core) يمكنك استخدام الحل البديل عبر /etc/network/interfaces والذي يحقق نفس الهدف إنّما بقليلٍ من الجهد الإضافي:

```
iface br0 inet static
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “client”
  pre-up iwconfig wlan1 essid “AP” mode Master
  pre-up brctl addbr br0
  pre-up brctl addif br0 wlan0
  pre-up brctl addif br0 wlan1
  bridge_ports wlan0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
  post-down brctl delif br0 wlan0
  post-down brctl delif br0 wlan1
  post-down brctl delbr br0
```

3.6. الخطوة 2:بدء تشغيل الجسر

يمكن تشغيل الجسر ببساطةٍ بعد إعداده كمنفذٍ للشبكة باستخدام:

```
# ifup –v br0
```

تعني لاحقة "v–" أنّ التعليمة ستنّفذ بشكلٍ تفصيلي verbose لتخبرك بتفاصيل كلّ ما يجري.

ستحتاج إلى منح منفذ الجسر ضمن توزيعة فيدورا Fedora Core (أي التوزيعات غير المبنيّة على ديبيان Debian) عنوان إنترنت IP وإضافة مسارٍ إفتراضيٍّ لبقيّة الشبكة:

```
# ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
# route add default gw 192.168.1.1
```

يمكنك الآن وصل حاسبٍ محمولٍ إلى نقطة الولوج الجديدة والإتصال بالإنترنت (أو على الأقل بشبكتك المحليّة) عبر هذا الحاسب.

إذا أردت معرفة المزيد عن ماهيّة هذا الجسر وما الذي يقوم بعمله، ألق نظرةً على تعليمة brctl. على سبيل المثال تعرض التعليمة:

```
# brctl show br0
```

بعض المعلومات عن المهام التي يقوم الجسر بأدائها.

7. الوصفة السهلة للمثال الأول الثاني !

يمكنك عوضاً عن تثبيت توزيعة لينكس ومن ثمّ إعداد الحاسب ليعمل كنقطة ولوجٍ تقوم بمهام التقنيع Masquerading أو نقطة ولوج التجسير الشفاف Transparent Bridging أن تبحث عن توزيعاتٍ خاصةٍ من نظام التشغيل لينكس صممت خصيصاً لهذا الغرض، والتي قد تعمل بمجرّد إقلاع قرصٍ مدمجٍ CD معيّنٍ ضمن حاسبٍ يحتوي على بطاقة شبكة لاسلكية.

من أمثلة هذه التوزيعات توزيعة بيبل Pebble المبنيّة على ديبيان Debian والتي طورتها NYC Wireless (تأتي هذه التوزيعة ضمن قرصٍ مدمجٍ واحد). أو أيضاً الإصدارة المطورة من هذه التوزيعة والتي طورتها شركة Metrix Communications لتشغيل الحاسب أحادي اللوحة Single-board الذي تنتجه.

من التوزيعات أيضاً توزيعة m0nowall، وهي توزيعة جدارٍ ناريٍّ تسهّل إعداد نقاط الولوج التي تحتوي على وظائف الجدران الناريّة والتقنيع. تعمل هذه التوزيعة أيضاً على التجهيزات المخصصة كلوحات WRAP.

يمكن تشغيل لينكس (وبالتالي هذه الحلول المبنيّة عليه) على التجهيزات الخاصّة ببعض نقاط الولوج مثل Linksys WRT54G والتي يمكن تعديلها باستخدام برنامج تشغيل Firmware مخصص يتيح تركيب ميزاتٍ أكثر من تلك التي تأتي مع نقطة الولوج.

للحصول على مواقع الإنترنت لبعض توزيعات لينكس الخاصّة بالشبكات اللاسلكية راجع "مصادر إضافيّة للمعلومات".

8. المثالالثالث : جدارٌ ناريٌّ مركزيٌّمعوظائف التحقق من الهويّة

يهدف هذا المثال إلى إعداد بوابةٍ تجبر المستخدمين على تسجيل الدخول إلى الشبكة (عبر بوابةٍ مقيّدةٍ Captive Portal). سيحتوي الحاسب بعد الإعداد على منفذين للشبكة (سنستخدم في هذا المثال المنفذين eth0 و eth1). يتصل أحد هذين المنفذين بالإنترنت (eth0) في حين يعتبر الآخر منفذاً داخليّاً نقوم من خلاله بوصل زبائن الشبكة (eth1)، هذا المنفذ إمّا أن يكون منفذ إيثرنت متصلاً بمبدّل يمكن من خلاله توصيل عددٍ من الحواسب أو نقاط الولوج اللاسلكية (جسر شفاف يعمل ضمن الطبقة الثانية)، أو أن يكون منفذاً للشبكة اللاسلكية لتحويل البوابة تلقائيّاً إلى نقطة ولوج (راجع **المثال الأول**).

سنقوم في هذا المثال بإضافة نظامٍ للتحقق من الهويّة يتطلّب من المستخدمين تسجيل الدخول باستخدام إسم مستخدمٍ وكلمة سرٍ قبل التمكّن من الوصول إلى موارد الشبكة (كالإنترنت والطابعات وغيرها).

1.8.لمحة موجزةعن الإعداد

تتحكّم أداة ChilliSpot بالمنفذ الداخلي (eth1) باستخدام وحدة النواة vtun لتشكيل منفذٍ إفتراضي Virtual Interface (tun0), تستخدم وحدة النواة vtun فعليّاً لنقل حزم بروتوكول الإنترنت IP من النواة إلى طور المستخدم user mode بما يتيح لأداة ChilliSpot العمل دون أيّة وحداتٍ غير قياسيّة للنواة. تقوم أداة ChilliSpot بعد ذلك بإعداد مخدّم DHCP (والذي يمكن تعطيل عمله من خلال ملف إعداد ChilliSpot) على المنفذ tun0.

سيتم رفض جميع الحزم الواردة من أيّ زبونٍ متصلٍ بهذا المنفذ حتى يتم السماح له بدخول الشبكة عبر صفحة تسجيل الدخول لأداة ChilliSpot. عندما يحاول زبونٌ لم يتم التحقق من هويّته الإتصال بموقعٍ ما على الإنترت (عبر البوابة 80 أو 443) سيقوم Chilli باعتراض الطلب وإعادة توجيهه إلى نصٍ برمجيٍّ المكتوب بلغة بيرل Perl يدعى hotspotlogin.pl (يقوم بتخديمه مخدّم الوب أباتشي Apache عبر بروتوكول https الآمن).

يظهر برنامج hotspotlogin.pl للمستخدم صفحةً تحتوي على حقلٍ لإسم المستخدم وكلمة السر. يتم توجيه بيانات التحقق من الهويّة المدخلة إلى مخدّم FreeRADIUS والذي يقارنها بدوره بالمعلومات المخزّنة في قاعدة بياناته (باستخدام أحد بروتوكولي PAP أو CHAP). ستكون قاعدة البيانات مبدئيّاً ملفّاً نصيّاً Text File ولكنها يمكن أن تكون أيّاً من مجموعةٍ من الخدمات مثل Kerberos، LDAP، ملفّات كلمات السر ضمن Unix أو حتى Active Directory (ربّما!).

يقوم FreeRADIUS بعد ذلك بقبول المستخدم أو رفضه، ليوعز إلى برنامج hotspotlogin.pl بأن تظهر للمستخدم إمّا رسالة رفضٍ لمحاولة تسجيل الدخول أو صفحةٍ تحتوي على رسالة نجاح تسجيل الدخول مع وصلةٍ لتسجيل الخروج.

سنقوم بعد الإنتهاء من تركيب وتجربة هذا الحل باستخدام ملفٍ نصيٍّ باستبدال قاعدة بيانات FreeRADIUS بقاعدة بيانات MySQL والتي تتيح إضافة ميزاتٍ مثل استخدام البطاقات مسبقة الدفع للولوج إلى الإنترنت.

1.81..التجهيزات المطلوبة

أي حاسبٍ يحتوي على منفذي شبكة، لكنّه وبخلاف المثالين الأول والثاني قد يحتاج إلى قرصٍ صلبٍ أو على الأقل ذاكرةً من نمط Compact Flash بمساحة واسعة للتخزين لأنّ تشغيل قاعدة البيانات MySQL يتطلّب بعض المساحة التخزينيّة.

2.8.الخطوة 0:إعدادالبرمجيّات الأساسيّة

تعتبر هذه الخطوة تكراراً للخطوات الأولى في المثال الأول. أي أننا سنحتاج إلى حاسبٍ يحتوي على منفذي شبكةٍ يعمل بنظام التشغيل لينكس. لكننا سنحتاج أيضاً إلى بعض حزم البرمجيّات المختلفة والضروريّة لتشغيل هذا المثال.

سنبدأ هذا المثال بحاسب يحتوي على توزيعة أوبونتو Ubuntu. لقد استخدمنا هنا إصدارة Hoary من أوبونتو، لكن هذا الإعداد ينبغي أن ينطبق أيضاً على الإصدارات الأخرى وعلى توزيعات لينكس الأخرى مثل فيدورا Fedora Core، ماندريفا Mandriva وغيرها.

لقد تمت تجربة هذا الإعداد على كلٍ من إعدادي المخدّم والزبون لتوزيعة أوبونتو Ubuntu. لا تغطي هذه الوحدة المراحل الأساسيّة لتثبيت أوبونتو Ubuntu لكنّ موقع هذه التوزيعة على الإنترنت يحتوي على الكثير من تعليمات تثبيت نظام التشغيل من الصفر.

علينا بعد تثبيت أوبونتو Ubuntu تثبيت بعض حزم البرمجيّات الإضافيّة التي لا يتم تثبيتها بشكلٍ إفتراضي. إذا لم تكن معتاداً على تثبيت حزم البرمجيّات ضمن أوبونتو إقرأ الفقرة التالية قبل المتابعة، أمّا إذا كنت متمرساً باستخدام أدوات سطر الأوامر Command Line ضمن لينكس راجع صفحات دليل الإستخدام man pages لتعليمة apt-get. هناك وثيقة (كيف تعمل How To) تغطّي كيفيّة إضافة مستودع Universe إلى توزيعة أوبونتو Ubuntu التي تستخدمها، هذا المستودع Repository ضروريٌّ لعمل بعض الحزم البرمجيّة التي ينبغي تثبيتها (راجع "مصادر إضافيّة للمعلومات: دليل أوبونتو غير الرسمي Unofficial Ubuntu Guide").

قبل الإستمرار ينبغي عليك تثبيت الحزم الإضافيّة التالية (مع جميع الحزم التي تعتمد عليها) باستخدام أداة synaptic أو apt-get. قد لا تحتاج إلى بعض هذه الحزم، وقد يكون بعضها مثبّتاً بشكلٍ إفتراضيٍّ.

- mysql-server
- apache2
- freeradius
- freeradius-mysql
- phpmyadmin

عليك أخيراً الحصول على حزمة ChilliSpot (والتي لا تأتي ضمن توزيعة أوبونتو Ubuntu) من موقع ChilliSpot على الإنترنت (راجع "مصادر إضافيّة للمعلومات: ChilliSpot").

بعد الحصول على الملف المطلوب، إفتح واجهةٍ جديدةٍ لسطر الأوامر، إذهب إلى الدليل الذي يحتوي هذا الملف واكتب:

```
$ sudo dpkg –i chillispot_1.0RC3-1_i386.deb
```

باستخدام إسم حزمة ChilliSpot التي حصلت عليها.

3.8.الخطوة 1:إعداد Apacheليدعم SSL

لأسبابٍ أمنيّةٍ، نريد توفير صفحة تسجيل الدخول فقط عبر وصلةٍ مشفّرةٍ (https) لذلك علينا إعداد مخدّم الوب Apache2 لتخديم صفحات SSL المشفّرة. لقد قمنا باقتباس هذه القسم (بتصرّف) عن الموضوع التالي ضمن منتديات أوبونتو Ubuntu على الإنترنت:
http://ubuntuforums.org/showpost.php?p=19832&postcount=4

علينا بدايةً توليد شهادة SSL لمخدّم الوب Apache2:

```
$ sudo apache2-ssl-certificate
```

ستطرح عليك هذه التعليمة سلسلةً من الأسئلة عن إسم المؤسسة ومعلومات البريد الإلكتروني والتي سيتم تضمينها في الشهادة التي ستعرض على المستخدمين عند محاولة تسجيل الدخول إلى موقعك.

لتشغيل ملحقات SSL لمخدّم الوب Apace2 نفّذ التعليمة التالية:

```
$ sudo a2enmod ssl
```

قم الآن بإعداد SSL بإضافة ملف إعداد مواقع SSL. أنشئ ملفّاً جديداً باستخدام محرر النصوص المفضّل لديك (كمستخدمٍ جذريٍّ root).

```
$ sudo pico /etc/apache2sites-available/ssl
```

فيما يلي مثالٌ عن ملف إعداد SSL يقوم بتشغيل SSL ضمن الأدلّة الإفتراضيّة لمخدّم الوب Apache2 إضافةً إلى دليل cgi-bin:

```
NameVirtualHost *:443
<VirtualHost *:443>
        ServerAdmin admin@domain.com
        DocumentRoot /var/www/
        SSLEngine On
        SSLCertificateFile /etc/apache2/ssl/apache.pem

        <Directory />
```

```
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/>
        Options FollowSymLinks
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    </Directory>

    ErrorLog /var/log/apache2/error.log

    # Possible values include: debug, info, notice, warn, error, crit,
    # alert, emerg.
    LogLevel warn

    CustomLog /var/log/apache2/access.log combined
    ServerSignature On

</VirtualHost>
```

علينا الآن إخبار Apache لكي يستمع إلى البوابة 443 (https) بالإضافة إلى البوابة 80 (http).
حرّر الملف /etc/apache2/ports.conf وأضف السطر التالي إليه:

```
Listen 443
```

لتفعيل الإعدادات الجديدة يتوجّب علينا تفعيل إعدادات موقع ssl الجديدة ومن ثمّ إعادة تحميل ملفّات إعداد مخدّم الوب Apache (أو إعادة تشغيل Apache)

```
$ sudo a2ensite ssl
$ sudo /etc/init.d/apache2 force-reload
```

إنتهى.

4.8. الخطوة 2: إعداد ChilliSpot

إنسخ ملف ChilliSpot cgi إلى الدليل الإفتراضي لأباتشي Apache2 (cgi-bin):

```
$ sudo cp /usr/share/chillispot/hotspotlogin.cgi /usr/lib/cgi-bin/
$ sudo chmod +x /usr/lib/cgi-bin/hotspotlogin.cgi
```

5.8. الخطوة 3: إعدادالبرمجيّات

لقد تم اقتباس غالبيّة الأقسام التالية من دليل تثبيت ChilliSpot ضمن توزيعة Debian Sage (وبعض أجزاء تعليمات الإعداد ضمن توزيعة فيدورا Fedora Core).

5.81.. إعداد الشبكة والجدارالناري

نفترض وجود منفذين للشبكة:

- eth0 متصلٌ بالإنترنت وينبغي أن يتم إعداده لهذا الغرض (باستخدام ifconfig، /etc/network/interfaces أو الأداة الرسوميّ' لإعداد الشبكة المتوفّرة ضمن System -> Administration -> Networking).
- eth1 هو المنفذ الذي ستتصل به بقيّة الحواسب. لا ينبغي إعداد هذا المنفذ وإنّما يجب تشغيله فقط.

```
$ sudo ifconfig 0.0.0.0 up
```

يجب عليك تغيير السطر التالي في الملف /etc/network/options لتشغيل إعادة توجيه الحزم:

```
ip_forward=yes
```

ثمّ أعد تشغيل الشبكة:

```
$ sudo /etc/init.d/network restart
```

يمكنك استخدام النص البرمجي للجدار الناري "/usr/share/doc/chillispot/firewall.iptables" كنقطة بدايةٍ لإعداد الجدار الناري وترجمة عناوين الشبكة NAT. يتوجّب عليك كحدٍّ أدنى تحرير الملف والتأكّد بأنّ أسماء المنفذين تطابق الأسماء المستخدمة ضمن نظام التشغيل.
إبحث عن الأسطر التي تبدأ بـــ INTIF= و EXTIF= على التوالي وعدّلها لتطابق أسماء المنافذ المستخدمة في نظام التشغيل. INTIF هو المنفذ الذي يتصل به المستخدمون (في حالتنا هذه eth1) و EXTIF هو المنفذ المربوط بالإنترنت (eth0). يمكنك بعد التحقق من قواعد الجدار الناري تشغيل الملف باستخدام التعليمة:

```
$ sudo sh /usr/share/doc/chillispot/firewall.iptables
```

ينبغي تشغيل النص البرمجي للجدار الناري في كلّ مرةٍ يعاد فيها تشغيل الحاسب. يمكن التأكّد من حدوث ذلك بنسخ الملف إلى الدليل /etc/init.d/

```
$ sudo cp /usr/share/doc/chillispot/firewall.iptables/etc/init.d/chili.iptables
$ sudo chmod u+x /etc/init.d/chilli.iptables
$ ln -s /etc/init.d/chilli.iptables /etc/rcS.d/S40chilli.iptables
```

5.82.ملف إعداد ChilliSpot

يتوجّب عليك إخبار ChilliSpot بموقع مخدّم التحقق من الهويّة (والذي هو في هذا المثال نفس الجهاز الذي يحتوي على ChilliSpot). يمكن القيام بذلك بتعديل السطر التالي في ملف "/etc/chilli.conf":

```
uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi
```

حيث 192.168.182.1 هو عنوان الإنترنت IP الإفتراضي الذي يعطيه ChilliSpot للمنفذ الإفتراضي tun0 ويمكنك بسهولةٍ تركه على حاله دون خشية وقوع أيّة مشاكل. لزيادة أمن كلمة السر سنضيف السر المشترك بين hotspotlogin.cgi و chilli. أوجد في الملف "/etc/chilli.conf" السطر الذي يحتوي على:

```
#uamsecret ht2eb8ej6s4et3rg1ulp
```

قم بإزالة علامة التنصيص (#) من بداية هذا السطر **وغيّر** السر إلى كلمةٍ مماثلة الغرابة لكنّها مختلفة. تذكّر هذا السر لأنّ عليك إدخاله أيضاً ضمن ملف hotspotlogin.cgi (سنقوم بذلك لاحقاً).

بما أنّنا نشغّل مخدّم التحقق من الهويّة FreeRADIUS على نفس الجهاز فإننا سنحتاج إلى إيجاد وتعديل الأسطر التي تشير إلى مخدّم RADIUS ضمن الملف "/etc/chilli.conf":

```
radiusserver1 127.0.0.1
radiusserver2 127.0.0.1
```

ينبغي عليك أيضاً تغيير السطر الذي يبدأ بـــ radiussecret ضمن الملف "/etc/chilli.conf" بحيث لا يستخدم السر الإفتراضي لتشفير البيانات بين chilli و radius.

```
radiussecret somethingReallyDifficultToGuess
```

تذكّر هذا السر لأن عليك إضافته إلى ملف إعدادات FreeRADIUS أيضاً.

5.83..إعداد FreeRADIUS

يحتوي الدليل /etc/freeradius/ على جميع ملفات إعداد FreeRADIUS. بدايةً ولأغراض التجريب سنستخدم الملف النصّي "/etc/freeradius/users" لإتاحة الوصول لمستخدمٍ واحدٍ (steve). سنقوم لاحقاً بتغيير الإعدادات لاستخدام قاعدة بيانات MySQL لتخزين أسماء المستخدمين وكلمات السر، ولكن أولاً نريد أن نتأكّد من عمل النظام بأبسط شكلٍ ممكنٍ.

حرر الملف "/etc/freeradius/clients.conf".
أوجد القسم الذي يحتوي على السطر التالي:

```
client 127.0.0.1 {
```

تأكّد من إزالة علامة التنصيص (#) في بدايته، ثمّ قم بتغيير الأسطر التالية في القسم بين إشارتي } والتي تليها {:

secret = testing123

غيّر الكلمة (testing123) لتطابق السر الذي استخدمته في ملف الإعداد "/etc/chilli.conf" (إختر كلمةً يصعب تخمينها).

حرر الملف "/etc/freeradius/users" لإزالة علامة التنصيص (#) من بداية السطر التالي:

#steve Auth-Type := Local, User-Password == "testing"

هذا هو إسم المستخدم وكلمة السر الذين سيستخدمان للتأكد من أنّ كل شيء يعمل بشكلٍ صحيح.

5.84.تخصيص النص البرمجي hotspot login

يتوجّب علينا لزيادة أمان كلمة السر أن نقوم بإضافة كلمة السر "uamsecret" من الملف "/etc/chilli.conf" إلى النص البرمجي لتسجيل الدخول hotspot. حرر الملف "/usr/lib/cgi-bin/hotspotlogin.cgi".
أوجد السطر التالي:

#$uamsecret = "ht2eb8ej6s4et3rg1ulp";

قم بإزالة علامة التنصيص (#) من بداية هذا السطر وغير السر ليطابق السر الموجود ضمن الملف "/etc/chilli.conf" (سر uamsecret **وليس** كلمة سر Radius - radiussecret).

قم أيضاً بإزالة علامة التنصيص (#) من بداية السطر التالي:

#$userpassword=1;

عليك الآن أن تتأكّد من تفعيل جميع هذه التعديلات، أعد تشغيل FreeRADIUS ،Apache2 و chilli:

```
$ /etc/init.d/apache2 force-reload
$ /etc/init.d/freeradius restart
$ /etc/init.d/chilli restart
```

5.85..إستخدام ChilliSpot

ينبغي أن يكون لديك الآن مخدّمٌ للتحقق من الهويّة يتيح لحاسبٍ ما تسجيل الدخول للوصول إلى الشبكة. قم بتوصيل حاسبٍ إلى المنفذ eth1 ضمن الجهاز الذي يحوي ChilliSpot (إما باستخدام مجمّعٍ أو مبدّل، أو عبر سلك UTP متقاطع Crossover، أو عبر توصيل نقطة ولوج جسرٍ شفاف إلى المنفذ eth1). سنسمي هذا الجهاز بجهاز الزبون.

شغّل منفذ الشبكة على جهاز الزبون باستخدام DHCP، سيمنحك ChilliSpot عنوان إنترنت IP ضمن النطاق 24/192.168.182.0.

إفتح متصفح الوب وحاول الوصول إلى أي موقعٍ على الإنترنت.

يجب أن يتم تحويلك إلى صفحة تسجيل الدخول والتي تحتوي حقلاً لإسم المستخدم وكلمة السر, سجّل الدخول باستخدام إسم المستخدم "steve" وكلمة السر "testing"، يجب أن تحصل على رسالةٍ تفيد بأنّك نجحت في تسجيل الدخول. ينبغي أن تتمكّن الآن من الإتصال بالإنترنت بشكلٍ كاملٍ حتى تضغط وصلة تسجيل الخروج "logout" في صفحة ChilliSpot.

9. الخلاصة

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

1. يمنح نظام التشغيل غنو/لينكس GNU/Linux مدير الشبكة وصولاً كاملاً إلى كدسة التشبيك مما يعطي مرونةً فائقةً.
2. نظراً لطبيعة نظام التشغيل غنو/لينكس GNU/Linux فإنه قادرٌ على لعب الكثير من الأدوار ضمن البنية التحتيّة للشبكة.
3. يمكن لنقطة الولوج اللاسلكية القيام بمهام التقنيع Masquerading / ترجمة عناوين الشبكة NAT والتي تعتبر فائقة الأهميّة في الحالات التي تتطلّب مشاركة نقطة ولوجٍ واحدةٍ في مكتب.
4. يمكن لنقطة الولوج اللاسلكية أن تعمل كجسرٍ شفاف Transparent Bridge يمكن استخدامه كنقطة ولوجٍ بسيطةٍ أو كمكررٍ يحتوي على جهازي إرسالٍ واستقبال. تكمن فائدة هذا الحل بشكلٍ خاصٍّ في الحالات التي تحتوي عدّة نقاط ولوجٍ ونرغب فيها بتركيب جدارٍ ناريٍّ Firewall مركزيٍّ واحدٍ وربّما مخدّماً للتحقق من الهويّة.
5. يمكن توفير خدمات التحقق من الهويّة عبر مخدّمٍ واحدٍ يعمل كبوابةٍ تجبر المستخدمين على تسجيل الدخول عبر صفحة إنترنت لبوابةٍ مقيّدةٍ Captive Portal.