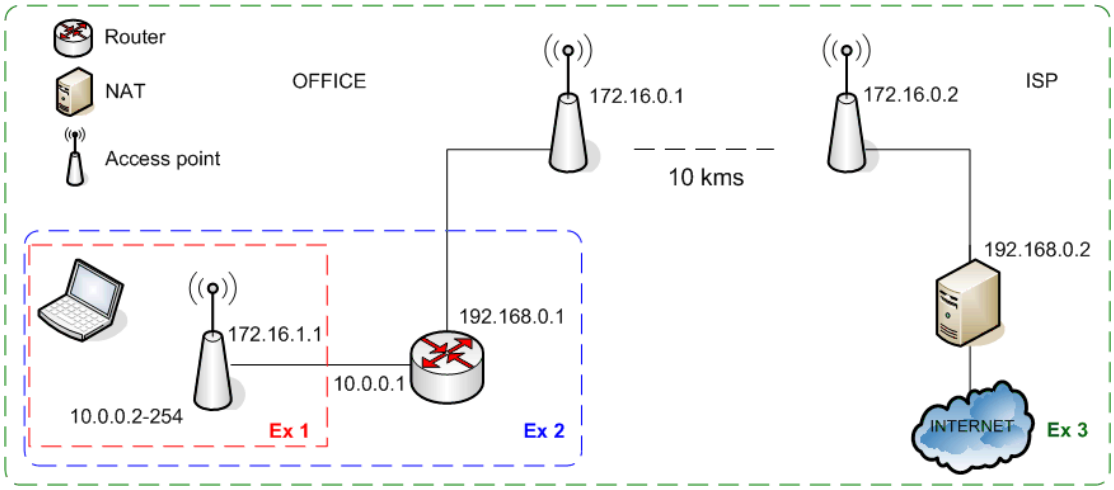
# ITRAINONLINE MMTK

# أمن الشبكات اللاسلكية – توجيهات التمارين التطبيقية

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

---




لنفترض السيناريو التالي: يتصل جهاز حاسوب محمول بشبكة أحد المكاتب (Ex 1) عبر نقطة ولوج لاسلكية. يحصل هذا الحاسوب على عنوان إنترنت من مخدم DHCP وموجّه (Ex 2).

يتصل المكتب بأكمله مع الإنترنت عبر وصلة لاسلكية مخصصة (نقطة إلى نقطة Point to Point) إلى مزود خدمة الإنترنت. تتألف هذه الوصلة اللاسلكية المخصصة من نقطتي ولوج تعملان كجسرين.

يقوم موجّه مزود خدمة الإنترنت بأداء مهام مخدم ترجمة عناوين الشبكة NAT أيضاً (Ex 3).

## التمرين الأول: سرية وكمال المعلومات

لاحظ الشكل السابق (Ex 1) حيث يرتبط جهاز الحاسوب المحمول بشبكة المكتب عبر نقطة ولوج لاسلكية.

**السؤال الأول**: كيف يمكنك ضمان سرية وأمن المعلومات؟

- ماهي الوظائف التي يمكنك تطبيقها ولماذا؟

**مقترحات للنقاش:**

قم بإعداد بروتوكول WPA2 المؤسساتي لضمان التشفير الكلي على مستوى الوصلة IEEE 802.1X
قم بإعداد بروتوكول WPA2 الشخصي وحدد سراً مشتركاً للإستخدام ضمن المكتب. ناقش فاعلية هذا الحل.
قم بتدريب موظفيك للتعرف على الخدمات الحساسة واستخدم الأمن على مستوى التطبيقات دون اعتماد التشفير على مستوى الوصلة على الإطلاق.
قم بإعداد حل يعتمد على الشبكة الخاصة الإفتراضية VPN وأجبر جميع المستخدمين على التواصل عبر مركز الـ VPN.

•ناقش جميع الخيارات المتاحة لضمان سرية المعلومات ضمن الحلقة الأولى (بين جهاز الحاسوب المحمول ونقطة الولوج).

**مقترحات للنقاش:**

ميزات وعيوب استخدام بروتوكول الوصول الآمن للشبكة اللاسلكية WPA2 مع أو بدون IEEE 802.1X. أوقف عمل التشفير، استخدم حلول الشبكة الخاصة الإفتراضية VPN (التوافقية، الكلفة)، إدارة الشبكة، إلخ.

الآن راجع الشكل مجدداً (Ex 3)

**السؤال الثالث**: كيف يمكن لمزود خدمة الإنترنت ضمان سرية وكمال المعلومات ضمن الوصلة المخصصة بينها وبين المكتب؟

•ناقش ميزات وعيوب جميع الحلول الممكنة.

**مقترحات للنقاش:**

ينبغي أن يقوم مزود خدمة الإنترنت بإعداد التحقق من الهوية ضمن الوصلة المخصصة للمكتب بغية منع اختراق هذه الوصلة.
قد يقرر مزود خدمة الإنترنت عدم تطبيق التشفير على مستوى الوصلة لعدة أسباب:

1. القوانين النافذة (هل يسمح باستخدام التشفير؟)
2. الصعوبة الفيزيائية للتنصت على الوصلة من قبل أشخاص غير مخولين (هوائيات الوصلة موجهة بشكل دقيق جداً من نقطة إلى نقطة وعلو أبراج هذه الهوائيات).
3. تخفيف متطلبات إدارة الشبكة.

## التمرين الثاني: التحقق من الهوية – التحكم بالوصول

لاحظ الشكل السابق (Ex 2): يقوم الموجّه بتزويد مستخدمي الشبكة اللاسلكية بعناوين إنترنت IP من خلال بروتوكول الإعداد التلقائي للمضيف DHCP.

**السؤال الأول**: كيف يمكنك منع المستخدمين غير المخولين من الحصول على عنوان إنترنت IP من شبكتك؟

**مقترحات للنقاش:**

قم بإعداد التحقق من الهوية ضمن نقاط الولوج باستخدام بروتوكول WPA أو WPA2.
إستخدم عناوين إنترنت IP ساكنة وراقب طلبات بروتوكول الإعداد التلقائي للمضيف DHCP الواردة (وذلك لتعقيد الأمور قليلاً على المتطفل).
لا ترسل معرّف مجموعة الخدمات SSID وقم بتحديد نطاق تغطية الشبكة اللاسلكية (وذلك لتعقيد الأمور قليلاً على المتطفل).

**السؤال الثاني**: كيف يمكنك منع المستخدمين غير المخولين من الوصول إلى الإنترنت من خلال شبكتك؟

**مقترحات للنقاش:**

إمنع مرور حزم بروتوكول الإنترنت IP عبر موجّه المكتب.
إسمح بمرور البيانات الواردة من عناوين إنترنت IP أو MAC محددة ضمن الموجّه فقط.
تطبيق حل يعتمد على بوابة مقيّدة ضمن موجّه المكتب.

راجع الشكل (Ex 3): يقوم مزود خدمة الإنترنت بتشبيك المكتب عبر مخدم ترجمة عناوين الشبكة NAT.
**السؤال الثالث**: كيف يمكن لمزود خدمة الإنترنت التأكد من أن مكتبك فقط هو المربوط مع شبكة المزود؟

**مقترحات للنقاش:**

اسمح بمرور حزم البيانات IP الواردة من عنوان الشبكة الفيزيائي MAC لموجّه المكتب.
قم بإعداد بوابة مقيّدة ضمن مخدم ترجمة عناوين الشبكة NAT وإتاحة التحقق من الهوية لكل مستخدم.
تأكد من أن الوصلة المخصصة بين المكتب ومزود خدمة الإنترنت معرّفة بالكامل.

## التمرين الثالث: التوفر وتجنب توقف الخدمة

لاحظ مخطط المكتب (Ex 1, Ex 2) ومخطط مزود خدمة الإنترنت (Ex 3).

**السؤال الأول**: إشرح احتمالات حدوث أية مشاكل لدى كل عقدة في المخطط بأكمله. ما الذي قد يتسبب في إيقاف عمل الشبكة؟

**مقترحات للنقاش:**

إزدحام الإشارات اللاسلكية ضمن كل من الوصلتين.
إرتباط مستخدمين غير مخولين بأي من نقاط الولوج لإرسال معلومات خاطئة.
إغراق الوصلات اللاسلكية من قبل برمجيات مؤذية.
انتحال شخصية الموجّه من قبل أشخاص غير مخولين (إختطاف عنوان الإنترنت IP أو MAC للموجّه).
إنتحال شخصية نقطة ولوج من قبل أشخاص غير مخولين (إختطاف القناة الراديوية).

**السؤال الثاني**: ناقش كيفية معالجة كل من هذه المشاكل الأمنية وحدد الطرف الذي ينبغي أن يكون مسؤولاً عن تطبيق هذه الإجراءات؟

**مقترحات للنقاش:**

إزدحام الإشارات اللاسلكية ضمن كل من الوصلتين: راقب وصلاتك اللاسلكية بشكل دوري، أعلم سلطات الإتصالات المختصة عند اكتشاف أية هجمات.
إرتباط مستخدمين غير مخولين بأي من نقاط الولوج لإرسال معلومات خاطئة: قم بإعداد بروتوكول WPA2، أضف سياسات تشكيل سيل البيانات Traffic Shaping ضمن الموجّه ونقاط الولوج، حدد نطاق تغطية شبكتك اللاسلكية.
إغراق الوصلات اللاسلكية من قبل برمجيات مؤذية: راقب سير البيانات عبر شبكتك، أضف أنظمة كشف التطفل (Intrusion Detection Systems (IDS، أضف سياسات تشكيل سيل البيانات Traffic Shaping ضمن الموجّه ونقاط الولوج، إفصل المحطات المصابة بهذه البرمجيات عن الشبكة .
انتحال شخصية الموجّه من قبل أشخاص غير مخولين (إختطاف عنوان الإنترنت IP أو MAC للموجّه): قم بإعداد التحقق من الهوية ضمن الوصلة المخصصة، راقب نسبة الإشارة إلى الضجيج SNR لكشف أية تغييرات ملحوظة.
إنتحال شخصية نقطة ولوج من قبل أشخاص غير مخولين (إختطاف القناة الراديوية): قم بإعداد التحقق من الهوية ضمن الوصلة المخصصة، راقب نسبة الإشارة إلى الضجيج SNR لكشف أية تغييرات ملحوظة..

**السؤال الثالث**: فكّر بمثال واقعي (مشفى، مدرسة، مركز تدريبي.. إلخ) واشرح متطلباته الأمنية. إقترح الإجراءات الأمنية الضرورية لتلبية هذه المتطلبات.