الهدف:
سيتركز المشروع على تطبيق الأداةWifite

المتطلبات:

1. الأداة: Wifite

2. المتطلبات :

- إلتقاط مصادقة الشبكة بشكل تلقائي (handshake)
- هجمات إلغاء المصادقة
- كسر كلمة المرور (قاموس و(WPS)

3. نطاق المشروع:

يجب أن يشمل المشروع الجوانب التالية:

أ. المقدمة

في عالمنا المتصل، يعتبر أمان شبكة الانترنت يعتبر أمرًا مهماً. باستخدام اداة Wifite ، سنقوم بتقييم ثغرات الشبكة. هدفنا هو تعزيز الأمان وتقديم رؤية قابلة للتنفيذ لحماية الاتصالات الرقمية. هذا المشروع عن الاختبار الأخلاقي ويهدف إلى تعزيز إدارة الشبكة المسؤولة فقط. سنغطي تقييم الشبكة والتحليل والتقارير والتنفيذ العملي، مع عرض قدرات Wifite ضمن إطار أخلاقي.

ب. تقييم الشبكة

تنطوي هذه المرحلة على تقييم شامل لأمان الشبكة المستهدفة باستخدام .Wifite سنقوم بما يلي:

- تحديد الأجهزة المتصلة، بما في ذلك نقاط الوصول.
- تحليل هيكل الشبكة لاكتشاف نقاط الدخول المحتملة.
- تقييم معايير التشفير مثل(WPA/WPA2 ) .
- اكتشاف الثغرات من خلال هجمات إلغاء المصادقة (deauthentication) وإلتقاط مصادقة الشبكة (handshake)

ج. التحليل والتقارير

هنا، سنقوم بتحليل النتائج المستخلصة من تقييم الشبكة:

- معدل نجاح إلتقاط مصادقة الشبكة (handshake)
- فعالية كسر كلمة المرور باستخدام قاموس (dictionary)
- رسم خرائط الثغرات وتصنيفها.
- توصيات أمان عملية.

د. التنفيذ العملي

في هذه المرحلة، سنضع رؤاها في التطبيق باستخدام Wifite :

- هجمات إلغاء المصادقة (deauthentication): إظهار تقنيات إعاقة الشبكة لإلتقاط مصادقات الشبكة .(handshake)
- إلتقاط مصادقة الشبكة (handshake): تنفيذ إلتقاط مصادقة الشبكة (handshake)الناجحة للتحقق من الثغرات.
- كسر كلمة المرور: محاولة فك تشفير كلمة المرور للتأكيد على ضعف الأمان.
- الاختبار الأخلاقي: عرض ممارسات الاختبار المسؤولة التي تحترم الخصوصية وحماية البيانات.

4. المشروع:

أ. عنوان المشروع وأعضاء الفريق:
عنوان المشروع: اختبار اختراق شبكات الانترنت باستخدامWifite
أعضاء الفريق:
سلمان المفرج
حمود الراجح
فهد السعدان

ب. المقدمة:
يعتبر أمان الشبكة أمرًا بالغ الأهمية في عالمنا المترابط. تتناول هذه الوثائق اختبار اختراق شبكات الانترنت، مما يبرز أهمية حماية الشبكات اللاسلكية.

ج. وصف الأداة:
تقومWifite ، كأداة آلية، بتبسيط اختبار اختراق شبكات الانترنت. تتضمن ميزاتها إلتقاط مصادقة الشبكة (handshake)، وهجمات إلغاء المصادقة (deauthentication)، وكسر كلمة المرور، مما يساهم في تعزيز أمان الشبكة.

د. عملية تقييم الشبكة:
شرح المنهجية والخطوات المتبعة لتقييم الشبكة باستخدام الأداة المحددة ,شمل تقييمنا ما يلي:

- تعداد الأجهزة وتحليل هيكل الشبكة
- تقييم التشفير
- هجمات إلغاء المصادقة(deauthentication) وإلتقاط مصادقة الشبكة (handshake)

ه. النتائج والتحليل: قدم النتائج من تقييم الشبكة وقم بتحليل مفصل للثغرات المكتشفة.

معدل نجاح إلتقاط مصادقة الشبكة (handshake): في اختبارنا في الفصول الدراسية على شبكات الطلاب، تم تحقيق نسبة نجاح 100٪. ومع ذلك، قد تختلف السيناريوهات الحقيقية نظرًا لتنوع تكوينات الشبكة وتدابير الأمان المختلفة.

و. طرق لحد من مخاطر الاختراق:

كلمات المرور اكثر تعقيداً من المعتاد عليه

تحسين بروتوكول التشفير

نتائج كسر كلمة المرور:

باستخدام مصادقة الشبكات (handshakes) الملتقطة، كشفت اختباراتنا فعالية التشفير وأكدت ضرورة استخدام كلمات مرور قوية ومعقدة لتعزيز أمان الشبكة.

رسم خرائط الثغرات:

قمنا بتحديد الثغرات وتصنيفها حسب التأثير وقابلية الاستغلال. وهذا يوفر استراتيجيات مكافحة فعالة لتعزيز أمان الشبكة.

الاستنتاج:

يُؤكد هذا المشروع أهمية اختبار الأمان الأخلاقي للشبكات اللاسلكية. من خلال الاستفادة من أدوات Wifite، تم التركيز على نقاط الضعف والثغرات في الشبكة ، ونتمنى ان هذا يسهم في تعزيز الأمان العام للشبكات اللاسلكية ومساعدة المؤسسات على تحسين نظام الحماية لديها.