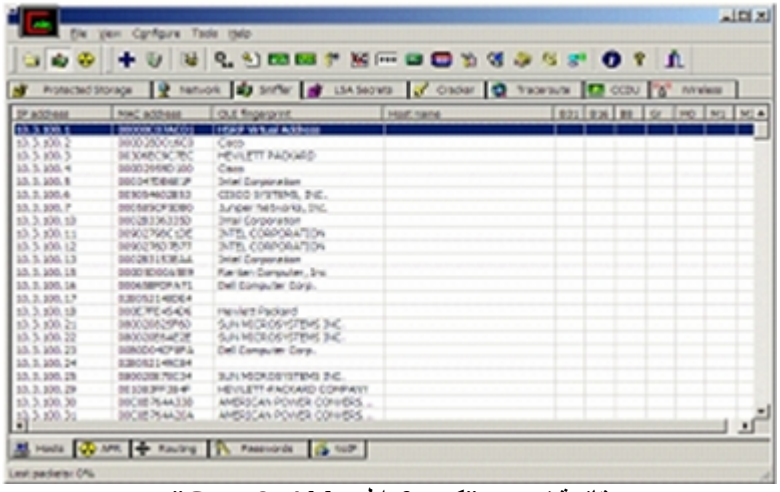
الأنترنت اللاسلكي بالمجان في المطارات والنقاط العامة

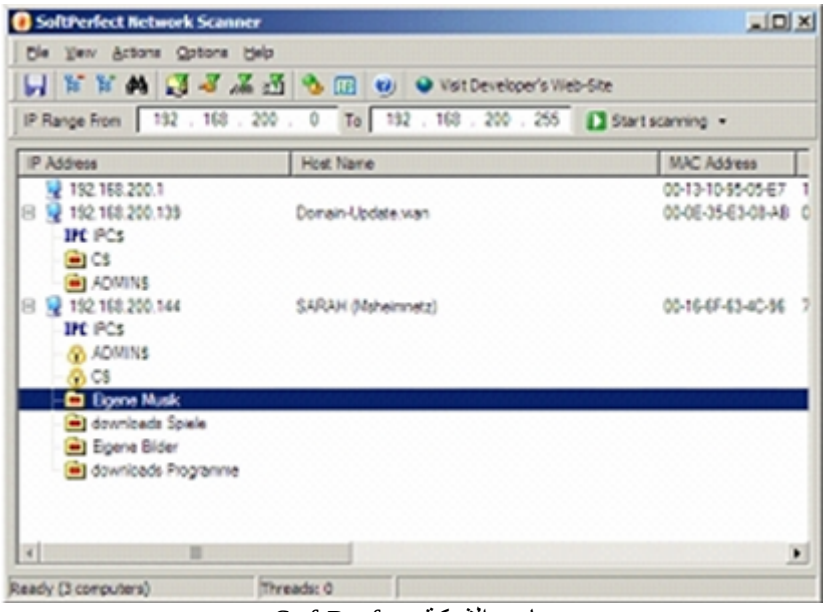
Brian Wilson الكاتب
CCNA, CCSE, CCAI, MCP, Network+, Security+, JNCIA
Slimjim100@gmail.com
anti-hacker.info
www.ethicalhacker.net
Translated by medfox2010@hotmail.com ترجمت
medfox2010@gmail.com

تنويه : هذه المقالة والمواضيع الواردة فيها هي لأغراض تعليمية ، ولا ينبغي أن تجرب على اي شبكة دون إستشارة مالكها . لا أتحمل أي مسؤولية عن الإجراءات أو الأضرار التي قد تتسببون فيها بمحاولتكم تطبيق ما في هذه المقالة . " لا تجربوا هذا في البيت يا أطفال " ، التطفل قد يضر بصحتكم .

مؤخرا أثناء سفري لاحظت مكانا توجد به طغتية ورغبت في تصفح الأنترنت ، عندما قمت بالإتصال بالحساب المدفوع لاحظت أنهم يريدون مني مقابل 8 دولارات في اليوم ، هذا كان بالنسبة لي مقابلا مبالغا فيه لإتصال قصير بالأنترنت و عندي فقط 3 ساعات توقف بين الرحلات الجوية ، لذلك قررت أن أرى مايمكن أن أقوم به للحصول على إتصال بالحساب. توجهت إلى الشاشة ومن خلالها أستطيع تصفح صفحتهم و الصفحة الرئيسية لمزود الخدمة المحلي (مزود خدمة الانترنت المحلي كان هو راعي المشروع) ، ولكن لا يمكن تصفح أي موقع آخر وعند محاولتي فعل ذلك يعود المتصفح رغما عني إلى صفحة دفع 8 دولارات . تجربتي مع إنشاء محتوى البوابات للحسابات المدفوعة مكنتمي من ملاحظة أن هذه البوابة تعمل مثل Monowall (www.m0n0.ch) ، بما أنني أعرف كيف تعمل الخصائص الأمنية ل Monowall (بإستخدام عناوين ماك MAC لمنع المحتوى) تساءلت عن مدى قدرتي على تجاوز الجدار الناري للبوابات دون دفع رسوم الخدمة ، أردت فعل ذلك فقط لأعرف مدى جدواه و لسبر أغوار أمن هذه الشبكة . أول ما فعلته هو مسح الشبكة الفرعية التي أنا عليها لأرى مايمكن الوصول إليه ، لهذا إستخدمت برنامج "كين & ابل "Cain & Able (www.oxid.it) وكذلك ماسح الشبكة ل SoftPerfect (www.softperfect.com) . سبب إستخدامي ل "Cain & Able" أنه يقدم وصلة سهلة الإستخدام ورغبتي في معرفة إمكانية مشاهدة المتواجدين معي على الشبكة الفرعية وإمكانية تلقي رد منهم .

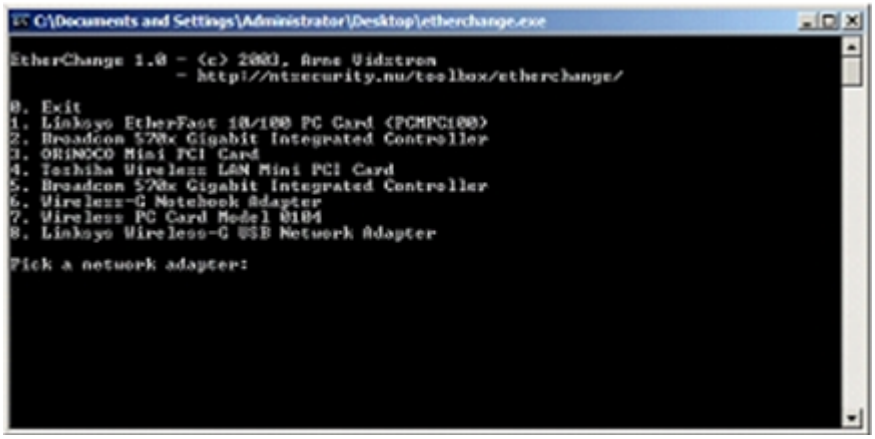


قائمة تنصت "كين & ابل Cain & Able"



ماسح الشبكة SoftPerfect

عندما تلقيت نتائج عملية المسح للشبكة الفرعية و مشاهدة كل الحواسيب الأخرى المتواجدة معي أشرت للمحتوى المفلتربالجدار الناري لكل "الأيبيهات" الغير مستخدمة لكنني تمكنت من رؤية الإختلاف من الجدران النارية MAC و MAC الحواسيب الأخرى . حاولت بعد ذلك القيام بإختبار ping وتلقيت ردودا عليه ، وقد تمكنت من التحقق من الحواسيب النشطة ومع قليل من التنصت لاحظت من يقوم بسحب البيانات خارج قيود الجدران النارية . حتى الآن وجدت أن الجدار الناري لا يسمح لي بالتصفح بحرية ولكنني استطيع أن أفعل ما أشاء داخل الشبكة الفرعية دون أي تفاعل ، أستطيع أن أتنصت وأن أقوم بعملية المسح للشبكة الفرعية والجدار الناري لا يحول بيني وبين الحواسيب الأخرى المتواجدة على الشبكة الفرعية . حان الوقت الآن لنرى مدى إمكانية التحايل بإستخدام عنوان MAC حاسوبي مع حاسوب آخر دفع قيمة الإشتراك لتصفح الإنترنت ، لذلك إستخدمت EtherChange (www.ntsecurity.nu/toolbox) لأنسخ عنوان بطاقة الشبكة لدي MAC ليماثل أحد الحواسيب الأخرى التي لاحظت أنها تقوم بسحب بيانات كثيرة .



" إذرتشينج " من موقع www.NTSecurity.NU

كان هذا هو مفتاح تجاوز فلترت الجدار الناري وبمقدوري تصفح الأنترنت بحرية . كي أتأكد من أن الحاسوب الرائع الذي أعارني عنوان MAC مازال مرتبطا بالأنترنت ، قمت بعملية تنصت sniffer مجددا والخبر السار هو أن الجدار الناري سمح لكلينا بتصفح الأنترنت ب IP مختلف وبنفس عنوان MAC . إستنتجت من ذلك أن عملية منع التصفح مرتبطة بعنوان

MAC وبمجرد دفعك لرسم الإشتراك يضاف عنوان بطاقة الشبكة لحاسوبك MAC إلى اللائحة البيضاء ، وكل حاسوب بنفس العنوان يمكنه كذلك تصفح الإنترنت بحرية . هذا النوع من أمن MAC كذلك نجده في العديد من الحسابات المنزلية المدفوعة التي تضلل الزبائن بقول ان شبكتهم آمنة ، وأرى في هذا عيبا حقيقيا حيث أن أي شخص لديه مهارات أساسية يستطيع الإلتفاف حول هذا الأمر .

والحالة هذه في شبكة المطار أتمنى فقط منهم تأمين شبكتهم الداخلية على نحو أفضل ، و أنا الآن جاهز لإختبار الحساب المدفوع التالي الذي يمنعني من التصفح لأرى مدى تأمينه . يرجى ملاحظة اني دفعت الرسم بعد عملية الإختبار هذه ، ولم أقم بكسر تشفير أي شيء ، على كل حال هذا كان سيحدث لأي شخص حاسوبه لديه نفس عنوان MAC لشخص دفع الرسوم فالساعات 24 الماضية .

في الأيام القليلة القادمة سوف يدرك الناس أهمية تأمين الشبكة وسوف يصبح الأنترنت مكانا آمنا . تذكر أن خداع الخدمة المدفوعة لإستخدامها بالمجان يعتبر سرقة ولها عواقب لذلك كن مستعدا لدفع الثمن إذا تم ضبطك ، لذلك فأنا لا أوصي بتجربة أي شيء شرحته هنا دون أخذ الإذن من صاحب الشبكة .