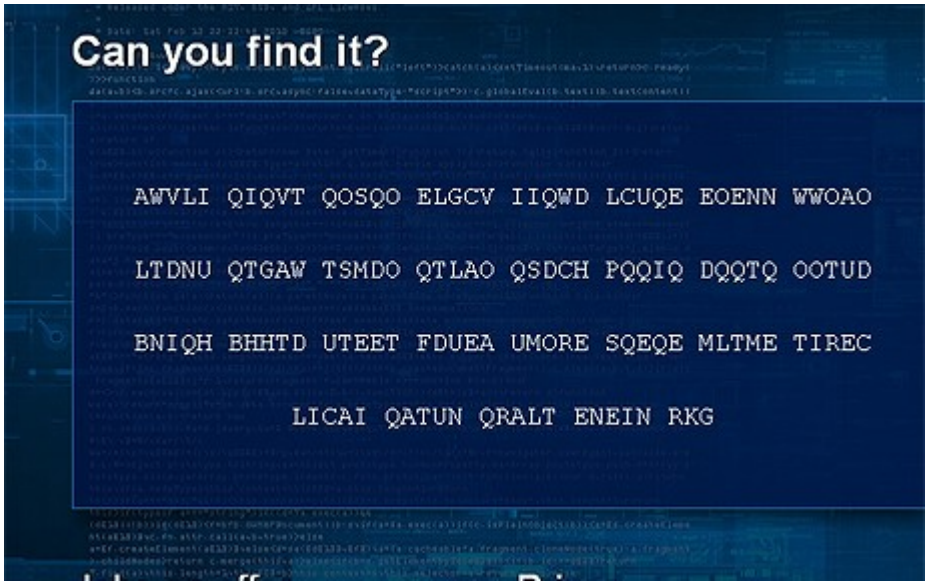
تضمين تمارين الاختراق التنافسية Competition-based Hacking Exercises في تدريس معمل مادة أمن المعلومات:
تجربة ناجحة في كلية الحاسبات بجامعة الملك عبدالعزيز

إيمان سالم الأشولي
محاضرة بكلية الحاسبات بجامعة الملك عبدالعزيز
باحثة دكتوراه في الأمن السيبراني بقسم علوم الحاسبات بجامعة أكسفورد
للمزيدعن الكاتبة: https://ealashwali.github.io

مع العدد المتزايد للاختراقات الأمنية، أصبح تدريس مادة أمن المعلومات لطلاب أقسام وكليات علوم الحاسب وأنظمة المعلومات في الجامعات أهم من أي وقت مضى. إلا أن تدريس تقنيات هجومية (اختراقات) والتي تسمح للطلاب بالتفكير كمخترق أصبح أمرا مرغوبا فيه لإعداد مهندسي أمن معلومات أكفاء يتميزون بما يعرف بـ "العقلية الأمنية". في الحقيقة، في أوساط مجتمع أمن المعلومات، من المعروف أن خبير أمن المعلومات الجيد، هو أيضا مخترق (هاكر) جيد أيضا.

عندما تذكر كلمة مخترق أو هاكر (Hacker)، فإن أول ما يتبادر للأذهان هي صورة سلبية مرتبطة بالإيذاء والاحتيال نتيجة لصورة نمطية سائدة. وهي صورة غير دقيقة حيث أن مصطلح هاكر يندرج تحته العديد من الفئات، أحد هذه الفئات هي الهاكر الأخلاقي (Ethical Hacker)، أو هاكر القبعة البيضاء (White-hat Hacker) وكلاهما يرمزان لمخترق لا علاقة له بالإيذاء أو الاحتيال، بل بالعكس، يسهم في إكتشاف الثغرات والتبليغ عنها وتحسين أمن الأنظمة بشكل عام.

اليوم، مهارات الاختراق هي مهارات ذات قيمة عالية وتقدرها الشركات والمنظمات الأمنية والتقنية على حد سواء. مثلا، أثناء فترة مراستي في بريطانيا عام 2012 قامت الاستخبارات البريطانية Government Communications Headquarters(GCHQ) بوضع إعلان توظيف على هيئة نص مشفر. كان عنوان الإعلان المسابقة الوظيفية "هل يمكن أن تجدها؟" وفقط من يستطيع كسر الشفرة سيصل لرابط التقديم وسيستطيع تعبئة نموذج الوظيفة.



شكل 1: إعلان وظيفة مشفر بمركز الاستخبارات البريطانية. المصدر [1].

وكذلك الكثير من الشركات التقنية من شركات قوقل، موزيلا، مايكروسوفت، فيس بوك، تويتر، أبل وغيرها الكثير، تقدّر وتكافئ المخترقين الأخلاقيين الذين يبلغون عن الثغرات الأمنية في أنظمة هذه الشركات من خلال برامج مكافئات معلنة تسمى ب " Security Bug Bounty programs"، بغض النظر عن عمر ومؤهلات وموقع الشخص جغرافيا. فذلك طفل في الخامسة استطاع اختراق حساب والده في جهاز مايكروسوفت إكس بوكس بالضغط على مسافات متتالية في خانة كلمة المرور! [2] وذلك شاب من فلسطين بجهاز محمول متهالك يخترق حساب مارك زوكيربيرق (مؤسس فيسبوك) في فيسبوك ليوضح له الثغرة التي وجدها [3] . وتتدرج المكافآت بحسب خطورة الثغرة ويصل بعضها لمئات الالوف من الدولارات. فقط في سنة 2019، شركة فيسبوك دفعت 2.2 مليون دولار مكافآت في برنامج إيجاد الثغرات [4]. بعض المشاركين يتقدمون ويتوظفون في هذه الشركات بعد ذلك.

من تجربة شخصية أيضا، خلال عملي على بحث الدكتوراه، كنت أجمع بيانات من خوادم الوب تعرف هذه البيانات بالـ Headers، ترسلها المواقع عند الإتصال بصفحاتهم. والوصول لهذا النوع من البيانات يتطلب خطوات إضافية ولا تظهر في المتصفحات العادية بشكل مباشر. إلا أن الطريف في الامر أنني حصلت عدة عروض توظيف مخفية وسط تلك البيانات. بعضها من مواقع شركات تقنية كبيرة ومعروفة. فمثلا هذا احدهم (إسم الشركة مخفي عمدا ب [company name] إذ لا معنى من وضعه كإعلان عام):

"'X-hacker': "If you're reading this, you should visit [company name]/jobs and apply to join the fun, mention this header.""

وهذا عرض آخر:

"'X-Recruiting': "If you're reading this, maybe you should be working at [company name] instead. Check out jobs.[company name]""

وهذه الأمثلة توضح لنا أهمية مهارات الاختراق اليوم.

بلا شك، تضمين تمارين عملية توضح المفاهيم النظرية التي تعطى في المحاضرات أمر في غاية الاهمية في تعليم علوم الحاسب والهندسة. والأساتذ الجيد يسعى دائما لتصميم تمارين عملية تدعم المفاهيم النظرية وفي نفس الوقت تقدم تجربة ممتعة للطلاب وقريبة للواقع واحتياج سوق العمل.

في أحد الفصول الدراسية عام 2013 قمت ببدء فكرة تضمين تمارين الإختراق في تدريس معامل أمن المعلومات للطالبات. هذه التمارين توضح مفاهيم نظرية تعطى في منهج المادة. بعض الاختراقات التي اشتملت عليها المادة ونفذنها الطالبات:

1. Cross-Site-Scripting (XSS)
2. Cross-Site Request Forgery (CSRF)
3. Click-Jacking
4. SQL-Injection
5. Network Sniffing

6. Social Engineering Attacks
7. Smart phone attacks

قمت بمشاركة التجربة في ورقة نشرت في مجلة علمية [5]، وكانت آراء الطالبات إيجابية حول هذا النوع من التمارين. بحسب علمي أنها كانت التجربة الأولى من نوعها في جامعات المملكة.

لاحظت أن تمارين الاختراق في غالبها تتكون من مهاجم وضحية، وهذه الميزة تتيح تقديم التمارين كلعبة تنافسية. لذا في الفصل الدراسي التالي قمت بعمل فكرة إضافية أخرى وهي تقديم تمارين بطريقة تنافسية بين الطالبات. التنافس كان بين فرق الطالبات، وفي تجربة أخرى بيني وبين الطالبات. وأيضا شاركنا تجربتنا بورقة علمية في مؤتمر IEEE الدولي لتعليم الهندسة IEEE Global Engineering Education Conference عام 2015، والذي أقيم في دولة إستونيا [6].

أشارك هنا بعض المواضيع التي قد تفيد القارئ أو المستمع المهتم حول تجربتنا في تضمين تمارين اختراق تنافسية Competition-based Hacking Excercises والتي قد تكون ذات فائدة. التفاصيل موجودة في ورقة المؤتمر [6].

التنفيذ في بيئة آمنة ومراعاة الأخلاقيات والقانون

بالطبع إساءة استخدام هذه التمارين من قبل الطلاب عمدا أو بالخطأ هو أمر مقلق لمن يرغب في تدريس مهارات الاختراق للطلاب. إذ أن حماس الطلاب مع نقص الخبرة قد يؤدي إلى عواقب وخيمة اذا لم يتم أخذ بعض الاحتياطات في الحسبان. فنحن لا نريد حصول قصة مشابهة لقصة ولد المافيا (MafiaBoy) [7]. ففي عام 2000 قام الشاب ذو الـ 15 عاما بالتسبب في توقف مواقع مهمة مثل ياهو Yahoo والذي كان أحد أهم محركات البحث ومزودي خدمات البريد الالكتروني والمحادثة أنذاك، وموقع شبكة السي إن إن CNN، وإي باي ebay، وغيرهم، كل هذا بالخطأ! كان يجرب أحد الأكواد على مواقع حقيقية دون فهم تام للعواقب المتوقعة. بل كان الشاب في المدرسة أثناء توقف موقع الياهو لمدة ساعة بسببه! وبحسب تقرير أعدته مجموعة أبحاث تعرف بـ Yankee Group فإن الاختراق تسبب بخسائر اقتصادية تقدّر بأكثر من بليون دولار أمريكي [8] [7]. وهذا الشاب تعرض للمساءلة القانونية.

لذا وضعنا بعض الاحتياطات، من سابق خبرتي الشخصية في حضور مثل هذه المعامل في جامعة UCL ببريطانيا، وكذلك من قرائاتي لدراسات سابقة. منها:

1. جميع التجارب المتعلقة بالشبكات، مثل اختراقات الشبكات اللاسلكية، تتم في شبكات منفصلة تماما عن شبكة الجامعة.
2. إذا كانت التجربة تتطلب حسابات (اسم مستخدم وكلمة مرور) يجب أن تكون خاصة بالطالب أو بإذن من صاحب الحساب.
3. اختراقات الوب مثل Click-jacking, XSS, XSRF والهندسة الاجتماعية يجب أن تتم في مواقع مملوكة للطالب. هذه المواقع قد تظل داخلية، لكن في حال رغبة الطالب برفع الموقع على الشبكة العنكبوتية، يجب مراعاة أن رفع المواقع على شركة مستضيفة يجب أن يتم بحذر وأن يتم التأكد من عدم تعدي الاختراق لحدود الموقع.
4. عمل عرض مختصر عن القانون السعودي للجرائم الالكترونية (ومعظم الدول لديها قوانين مشابهة).

اختيار التمارين وتصميم المسابقات التنافسية

سأذكر هنا تمرينين على سبيل المثال فقط. لكن بالإمكان عمل أكثر من تمرين، باختراقات مختلفة. ففي أحد التمارين يتنافس الطالبات كمجموعات كل مجموعة ضد الأخرى. وفي تمرين آخر تتنافس كل المجموعات ضدي.

في التمرين الأول كل فريق يخترق كلمة المرور الخاصة بحساب فريق آخر، وفي نفس الوقت حسابهم هو الضحية لذلك الفريق المنافس. كان الهدف من التمرين فهم أهمية اختيار كلمة مرور قوية والأدوات المتاحة لاختراق الكلمات الضعيفة. السيناريو يتطلب من كل فريق عمل كلمة مرور ضعيفة في نظام وندوز سيرفر 2008 والمتوفر للطالبات على هيئة جهاز محاكاة أو ما يعرف ب (Virtual Machine). مثلا يجب أن تكون كلمة المرور موجودة في فهرس الكلمات الإنجليزية، وأن لا تزيد عن 6 أحرف. لأن كلمة المرور الضعيفة معرضة لنوع من الاختراقات يعرف ب Dictionary Attack. كل فريق سيحاول كسر كلمة المرور الخاصة بالفريق الآخر. من خلال هذا التمرين سيختبرن الطالبات كيفية اختراق نظام عبر كسر كلمة مرور ضعيفة لا تتوافق مع شروط اختيار كلمة مرور آمنة.

في التمرين الثاني، كانت كل المجموعات تهاجم نظامي أنا، وهو عبارة شبكة لاسلكية قمت أنا بإعدادها ببروتوكول له ثغرات أمنية تمكن المخترق من سرقة كلمة المرور الخاصة بالشبكة على الرغم من انه من غير المصرح لهم بمعرفتها.

انطباعات الطالبات

من مجموع 46 طالبة وباستخدام أسئلة استبيانات مصممة بـ (five point Llikert style) لمعرفة آراء الطالبات، وجدنا أن حوالي 84,78% من الطالبات وجدن أن تمارين المعمل زادت من معرفتهم بأمن المعلومات. كما أن 86,96% وجدن أن التمارين ساعدتهم في فهم المبادئ النظرية في المادة، و 78,26% استمتعن بهذه التمارين، و 76,09% يوصون بمثل هذه التمارين للطالبات الأخريات.

بعض التحديات وكيفية التغلب عليها

أحد أهم التحديات هو أن هذا النوع من التمارين يحتاج مجهودا أكبر من التمارين العادية إعدادا، تنفيذا، متابعة، وتقييما من قبل أستاذة المعمل. وهذا قد يحد من كمية التمارين المصممة بهذا الشكل. يمكن حل الإشكال بتعيين أستاذتين يتعاونن في تقديم هذا المعمل، أو الاقتصار على عدد محدد من التمارين.

الأمر الآخر هو أن ألأسلوب التنافسي والعمل في مجموعات كأسلوب تعليم قد لا يناسب كل الطالبات. فالبعض يفضل العمل بدون تنافس مع الغير وبشكل فردي. لذا الاقتصار على بضعة تمارين تنافسية قد يكون الخيار الوسط لهذه المشكلة.

الخلاصة

من خبرتي، ومن انطباعات عدد لا بأس به من الطالبات، أستطيع القول أن تعريف طالبات المرحلة الجامعية بالاختراقات الأمنية، وخاصة بأسلوب تنافسي حيث يلعبن دور المهاجم والضحية، في معمل مادة أمن المعلومات كانت تجربة ناجحة. ولو أتيح لي تدريس معمل هذه المادة مرة أخرى فسأدرج مثل هذه التمارين للطالبات.

المراجع

1: Philipson, Alice, Can you crack the code? GCHQ unveils fiendish puzzle for new recruits, 2013, http://www.telegraph.co.uk/news/uknews/defence/10301435/Can-you-crack-the-code-GCHQ-unveils-fiendish-puzzle-for-new-recruits.html
2: BBC, Xbox password flaw exposed by five-year-old boy, 2014, https://www.bbc.co.uk/news/technology-26879185
3: Gross, Doug, Zuckerberg's Facebook page hacked to prove security flaw, , https://edition.cnn.com/2013/08/19/tech/social-media/zuckerberg-facebook-hack/
4: Facebook, A Look Back at 2019 Bug Bounty Highlights, 2020, https://www.facebook.com/notes/facebook-bug-bounty/a-look-back-at-2019-bug-bounty-highlights/3231769013503969/
5: Alashwali, Eman, Incorporating Hacking Projects in Computer and Information Security Education: an Empirical Study, 2014
6: Alashwali, Eman and Ben-Abdallah, Hanene, Design and Evaluation of Competition-based Hacking Exercises, 2015
7: Wikipedia, MafiaBoy, 2020, https://en.wikipedia.org/wiki/MafiaBoy#cite_note-11
8: Niccolai, James, Analyst puts hacker damage at $1.2 billion and rising , 2000, https://web.archive.org/web/20071112081103/http://www.infoworld.com/articles/ic/xml/00/02/10/000210icyankees.html