The Journal of *Philosophical -Theological Research* (JPTR)
Vol.20, No. 2, Summer 2018, Issue 76 (pp. 71-94)
DOI: 10.22091/PFK.2017.1803.1575

پژوهش‌های فلسفی کلامی
سال بیستم، شماره دوم، تابستان ۱۳۹۷، شماره پیاپی ۷۶ (ص ۹۴-۷۱)

An Ethical Study of Teaching Malware Writing, Hacking Skills and System Infiltration

Alī Rezā Ālebūyeh[*]
Zaynab Ālebūyeh[**]

Received: 10/07/2017 | Accepted: 06/10/2018

Abstract

Nowadays, the number of courses teaching hacking skills is increasing and has encountered a very warm reception. In some countries, teaching hacking and writing malware has been considered as part of course credits for students of the fields of computer and information technology. According to some, since teaching hacking and malware writing may lead people to criminal activities and people may misuse this expertise, it is in detriment to the society and based on this, it is unethical; but some others agree with this instruction and believe that in order to confront cyber criminals, we must be able to think like them. According to this group, security experts need to learn hacking skills and malware writing in order to better understand the weakness in the security of systems and to deal with malware and therefore, they consider it ethical. Thus, considering the increase in the number of malware and hacking courses being held, and also the importance of the security of computers, this article delves into the explanation, analysis, critique and study of the ethical arguments for and against malware writing and hacking skills education and some measures for the ethical use of these skills will also be presented.

Keywords:

hacking instruction, career ethics, information technology ethics, malware, hacker, infiltration test.

* Assistant professor, Islamic Culture and Science Research Center | alireza.alebouyeh@gmail.com
** Master's student of Computer Engineering (software), researcher at Jāmi'at al-Zahrā' (corresponding author) | z.alebouyeh@gmail.com

پژوهش‌های فلسفی کلامی
سال بیستم، شماره دوم، تابستان ۱۳۹۷، شماره پیاپی ۷۶ (ص ۹۴-۷۱)

The Journal of *Philosophical -Theological Research* (JPTR)
Vol.20, No. 2, Summer 2018, Issue 76 (pp. 71-94)
DOI: 10.22091/PFK.2017.1803.1575

بررسی اخلاقی آموزشِ نوشتن بدافزارها و مهارتِ هک و نفوذ به سیستم‌ها

علیرضا آل‌بویه*
زینب آل‌بویه**

تاریخ دریافت: ۱۳۹۵/۱۱/۲۲ | تاریخ پذیرش: ۱۳۹۶/۰۷/۰۶

چکیده

امروزه برگزاری دوره‌های آموزشیِ مهارتِ هک کردن رو به افزایش بوده و با استقبال زیادی مواجه شده است. در برخی کشورها آموزش هک و نوشتن بدافزارها جزء واحدهای درسی دانشجویان رشته‌های کامپیوتر و فناوری اطلاعات در نظر گرفته شده است. به اعتقاد برخی، از آنجا که آموزشِ مهارت هک و بدافزارنویسی ممکن است افراد را به سمت فعالیت‌های مجرمانه سوق دهد و افراد از این مهارت سوءاستفاده کنند، به ضرر جامعه است و بر همین اساس، غیراخلاقی است، اما برخی دیگر با این آموزش‌ها موافق‌اند و بر این باوراند که برای این‌که بتوانیم با مجرمان سایبری مقابله کنیم، باید بتوانیم مانند آن‌ها فکر کنیم. به اعتقاد این افراد، کارشناسان امنیتی برای فهم بهترِ نقاط ضعف امنیتی سیستم‌ها و مقابله با بدافزارها نیازمند یادگیری مهارت هک کردن و نوشتن بدافزارها هستند و از همین رو، آن را اخلاقی می‌دانند. بنابراین، با توجه به افزایش برگزاری دوره‌های آموزشی بدافزارنویسی و مهارت هک کردن و همچنین اهمیت امنیت رایانه‌ها، در این مقاله به تبیین، تحلیل و نقد و بررسی استدلال‌های موافق و مخالف اخلاقی بودن آموزش نوشتن بدافزارها و مهارت هک کردن پرداخته می‌شود و راه‌کارهایی برای استفاده اخلاقی از آموزش این مهارت‌ها ارائه می‌شود.

کلیدواژه‌ها

آموزش هک، اخلاق حرفه‌ای، اخلاق فناوری اطلاعات، بدافزار، هکر، تست نفوذ.

* استادیار پژوهشگاه علوم و فرهنگ اسلامی | alireza.alebouyeh@gmail.com
** کارشناسی ارشد مهندسی کامپیوتر (نرم‌افزار)، پژوهشگر جامعه الزهرا (نویسنده مسئول) | z.alebouyeh@gmail.com

مقدمه

امروزه با گسترش روزافزون فناوری اطلاعات و اینترنت، مشکلات امنیتی در این حوزه به‌شدت افزایش یافته است. مسئولان فناوری اطلاعات و کارشناسان امنیتی سازمان‌ها برای حفظ امنیت و برقراری صحت اطلاعات در سیستم‌ها باید به‌طور مداوم ابزارهای دفاعی و امنیتی خود را به‌روز کرده و توسعه دهند، در غیر این صورت، با یک طوفان واقعی از مشکلات امنیتی مواجه خواهند شد.

وظیفهٔ برقراری امنیت در زیرساخت‌ها و سیستم‌های رایانه‌ای به عهدهٔ کارشناسان امنیت فناوری اطلاعات است. بسیاری از اساتید و متخصصان حوزهٔ فناوری اطلاعات معتقدند که دانشجویان و کارشناسان این حوزه برای این‌که بتوانند با حملات و چالش‌های امنیتی مقابله کرده و راه‌کارهای دفاعی مؤثرتری ارائه دهند، باید به شیوهٔ هکرها[1] فکر کرده و با ماهیت انواع حملات و بدافزارها و طریقه نفوذ آن‌ها به سیستم‌ها آشنا شوند (Logan, 2005, p. 1). بسیاری از شرکت‌ها و سازمان‌ها به منظور آگاهی از چگونگی نفوذ هکرها به شبکه آن‌ها و کشف نقاط ضعف امنیتی سیستم‌ها خواستار آنند که کارشناسان امنیتی‌شان با طرز فکر و شیوه عملکرد هکرها آشنا شوند (Pashel, 2006, p. 1) و به همین منظور در سراسر دنیا و به‌طور گسترده دوره‌های آموزشی با عنوان «هکر اخلاقی[2]» و «تست نفوذ[3]» به صورت قانونی و در اغلب موارد با مجوز از مراجع قضایی برگزار می‌شود.

علاوه بر مؤسسات خصوصی، بسیاری از دانشگاه‌ها نیز برای تربیت متخصصان امنیت فناوری اطلاعات و آموزش مهارت‌های دفاعی، اقدام به برگزاری دوره‌های امنیتی کرده‌اند (Livemore, 2005, p. 1)؛ دوره‌هایی از قبیل آموزش هک، آموزش نوشتن بدافزارها و ویروس‌ها و آشنایی با جاسوس‌افزارها و هرزنامه‌ها از مباحثی هستند که در سال‌های اخیر و در برخی دانشگاه‌ها جزء واحدهای درسی دانشجویان رشتهٔ علوم کامپیوتر و فناوری اطلاعات قرار گرفته‌اند (Pashel, 2006, p. 1; Curbelo, 2013, p. 1; Aycock, 2006, p. 1 Aycock, 2005, p. 1; Livemore, 2007, p. 2).

بسیاری از افراد به دلیل مزایای زیاد آموزش مهارت هک و نوشتن بدافزارها برای دانشجویان و کارشناسان امنیتی با این‌گونه آموزش‌ها موافق بوده و معتقدند برای این‌که بتوانیم با مجرمان سایبری مقابله کنیم، باید قادر باشیم مانند آن‌ها فکر کنیم. به اعتقاد آنان زمانی که کارشناسان امنیتی،

---

۱. مراد از هک نفوذ به سیستم‌ها و دسترسی به اطلاعات آنهاست و هکر هم کسی است که به سیستم‌ها نفوذ کرده و به اطلاعات آنها دسترسی پیدا می‌کند.

2. Ethical Hacking
3. Penetration Testing

اطلاعات فنیِ لازم را در مورد بدافزارها و هک و نفوذ به سیستم‌ها نداشته باشند، نمی‌توانند به‌طور مؤثری جلوی بدافزارها و حملات هکرها را گرفته و امنیت سیستم‌ها را تأمین کنند.

در کنار مزایایی که آموزش هک اخلاقی و بدافزارها برای امنیت سیستم‌ها دارند، آشنایی با این مهارت‌ها ممکن است مشکلاتی را نیز برای جامعه به وجود آورد. به همین دلیل، برخی افراد با آموزش این مهارت‌ها کاملاً مخالف بوده و نگران گسترش این آموزش‌ها در جامعه هستند. این افراد معتقدند که آموزش این مهارت‌ها، به دلیل این‌که ممکن است افراد را به سمت فعالیت‌های مجرمانه سوق دهد و آن‌ها از این مهارت سوء استفاده کنند، به ضرر جامعه است و بنابراین، عملی اخلاقی و عاقلانه نیست (Livemore, 2007, p. 1).

بنابراین، با توجه به رشد روزافزون برگزاری دوره‌های آموزش بدافزارنویسی و مهارت هک کردن و همچنین اهمیت امنیت رایانه‌ها و فضای مجازی، بررسی اخلاقی آموزش این مهارت‌ها اهمیت بسزایی دارد که در این مقاله به مسائل اخلاقی آموزش هک و بدافزارها و بیان و تحلیل دلایل موافقت و مخالفت با این امر پرداخته می‌شود. برای روشن‌تر شدن بحث، ابتدا مطالبی در خصوص آشنایی با بدافزارها و دوره‌های آموزشی «هک اخلاقی» و «تست نفوذ» ذکر می‌شود و سپس چالش‌های اخلاقی مربوطه به آموزش بدافزارنویسی و هک مطرح شده و پس از آن به دفاع از اخلاقی بودن آموزش این‌گونه مهارت‌ها پرداخته می‌شود. در بخش بعدی راه‌کارهایی برای استفادهٔ اخلاقی از آموزش هک و بدافزارنویسی ارائه می‌شود و در پایان نیز پیشینه‌ای دربارهٔ آموزش این مهارت‌ها در دانشگاه‌های دنیا مطرح می‌گردد.

هک اخلاقی و تست نفوذ

امروزه عموماً تصور بر این است که هکر کسی است که بدون اجازه به رایانه‌ها و اطلاعات ذخیره‌شده درون آن‌ها دسترسی پیدا می‌کند. در واقع، در عرف جوامع هکرها افرادی هستند که بدون این‌که حق دسترسی مجاز به سیستم‌ها و داده‌های آن‌ها را داشته باشند، به سیستم‌ها نفوذ کرده و به اطلاعات آن‌ها دسترسی پیدا می‌کنند (Curbelo, 2013, p. 2)، اما دیدگاهی که در جامعه در مورد هکرها وجود دارد، دیدگاهی درست و جامع نیست. در دنیای فناوری اطلاعات نخستین هکرها دانشجویان نخبه و اساتید برجسته دانشگاه MIT بودند که در دهه ۱۹۶۰م با هدف کشف

نقـاط ضـعف امنیتی سـیسـتم‌ها به آن‌ها نفوذ می‌کردند. در آن زمان این افراد اسـم خود را هکر گذاشـتند[1] و این واژه بار معنایی مثبت داشـت، اما پس از مدتی برخی از این نام سـوءاستفاده کرده و با نیت‌های سـوء و با قصـد تخریب و سـرقت به سیستم‌های رایانه‌ای نفوذ می‌کردند و به آن‌ها آسیب می‌رسـانند، این افراد نیز خود را «هکر» نامیدند (Clarke, 2003, p. 1)و بدین ترتیب پس از مدتی واژۀ «هکر» بار معنایی منفی پیدا کرد. به همین دلیل بعدها برای مشـخص‌شـدن مرز بین هکرهایی که با نیت سـوء به سـیسـتم‌ها نفوذ می‌کنند و هکرهایی که نیت سـوء و مغرضـانه‌ای ندارند، آن‌ها را دسته‌بندی کرده و بر اساس نیت‌شان یک رنگ کلاه به آن‌ها اختصاص‌دادند.

هکرها انواع مختلفی دارند که اعمال برخی از آن‌ها اخلاقی و برخی دیگر غیراخلاقی اسـت. یکی از انواع هکرها، هکرهای کلاه سـفید اسـت. این گروه هکرهایی هسـتند که از دانش و توانایی خود به صـورت کاملاً مجاز و اخلاقی بهره می‌برند و به بالابردن سـطح امنیتی سـیستم‌ها و سازمان‌ها کمک می‌کننـد، امـا در مقـابـل هکرهـای کلاه سـیاه افرادی هسـتند که از دانش و مهارت خود برای انجام کارهای مجرمانه و سـوءاسـتفاده از سـیسـتم‌ها و اطلاعات آن‌ها استفاده می‌کنند (Pashel, 2006, p. 1) نوع دیگر هکرها، هکرهای کلاه خاکسـتری هسـتند که از دید خودشـان، نفوذهایشان اخلاقی است چون معتقـدنـد هیچ آسـیبی بـه سـیسـتم‌ها نمی‌رسـانند. اخلاقی بودن یا نبودن اعمال هکرهای کلاه خاکستری بحثی است که در مقاله دیگری بدان پرداخته شده است (نک: آل‌بویه، ۱۳۹۴).

در واقع، هکرهای کلاه سـفید کارشـناسـان امنیتی هسـتند که با اجازۀ مدیر سـازمان به شبکۀ آن سـازمان حمله کرده تا نقاط ضـعف امنیتی آن را بدسـت آورند و به رفع این نقاط ضـعف و افزایش امنیت سیستم‌های سازمان کمک کنند. (Pashel, 2006, p. 2). به این کار برای کشف نقاط ضعف امنیتی سـیسـتم‌ها، «هک اخلاقی» یا «تسـت نفوذ» گفته می‌شـود. هکرهای اخلاقی برای انجام تسـت نفوذ از همـان ابزارهـا و تکنیـک‌های نفوذگرها اسـتفاده می‌کنند، اما نه آسـیبی به رایانه‌ها می‌رسـانند و نه اطلاعات را سـرقت می‌کنند (Curbelo, 2013, p. 2). این افراد از دانش و مهارت خود برای ارتقای امنیت رایانه‌ها بهره می‌برند و با پیدا کردن نقاط ضـعف امنیتی سـیستم‌ها و گزارش آن به مدیران سـازمان، راه‌کارهایی برای توسـعه امنیت ارائه می‌دهند. تنها تفاوت کسـی که تسـت نفوذ انجـام می‌دهـد بـا هکر در این اسـت کـه او پیش از انجام کار از رئیس سـازمان اجازه کتبی دریافت

1. https://www. helpnetsecurity. com/2002/04/08/the-history-of-hacking/(14 july 2016)

می‌کند. انجام تست نفوذ برای تأمین امنیت سیستم‌ها و شبکه‌ها حیاتی است و بسیاری از سازمان‌ها و شرکت‌ها برای شناسایی نقاط ضعف امنیتی سیستم‌های خود از هک اخلاقی و تست نفوذ بهره می‌برند.

چیستی بدافزار[1]

بدافزارها یا نرم‌افزارهای مخرب[2] کدها یا برنامه‌های رایانه‌ای هستند که توسط مجرمان سایبری برای صدمه‌زدن به عملیات رایانه‌ها، سرقت رمزهای عبور، جمع‌آوری اطلاعات حساس و محرمانه، ارسال هرزنامه‌ها[3] و دیگر مقاصد مغرضانه و آسیب‌رسان استفاده می‌شوند (Mariotti, 2014, p. 4) زمانی که بدافزاری روی سیستمی نصب می‌شود، هکرها می‌توانند بسته به نوع بدافزار تا اندازه‌ای کنترل سیستم هدف را به‌دست گرفته و اطلاعاتی که می‌خواهند را از آن استخراج کنند (Zeltser, 2014, p. 1).

بدافزارها انواع مختلفی دارند که معروف‌ترینِ آن‌ها ویروس‌ها، کِرم‌ها[4]، تروجان‌ها[5]، باج‌افزارها[6] و جاسوس‌افزارها هستند. بسیاری از افراد این تصور اشتباه را دارند که بدافزارها مختص رایانه‌های مبتنی بر ویندوز هستند، در حالی که بدافزارها می‌توانند هر سیستم محاسباتی از قبیل گوشی‌های تلفن همراه، تبلت، تلویزیون‌های هوشمند و ... را آلوده کنند (Zeltser, 2014, p. 1).

بسیاری از افرادی که امروزه بدافزارهای پیچیده و مخرب را تولید می‌کنند، نوشتن بدافزارها و توسعهٔ آن‌ها شغل اصلی آن‌هاست و این کدهای مخرب را به سازمان‌ها و افراد مختلف به قیمت‌های بالایی می‌فروشند (Zeltser, 2014, p. 2). در واقع، بدافزارها منبع درآمد آن‌ها بوده و به دلیل گسترش استفاده از دستگاه‌های محاسباتی و رایانه‌ای هیچ سیستمی از هجوم این بدافزارها مصون نیست.

چالش‌های آموزش بدافزارنویسی و هک

چند سالی است که متخصصان فناوری اطلاعات و برخی از مسئولان این حوزه به این نتیجه

1. malware
2. malicious software
3. spam
4. worm
5. trojan
6. ransomware

رسیده‌اند که بخش مهمی از درس‌ها و مباحث مربوط به امنیت اطلاعات و شبکه باید در خصوص‌شیوه عملکرد بدافزارها و روش‌های نفوذ به سیستم‌ها باشد؛ در غیر این صورت شکاف بزرگی بین دانش فارغ التحصیلان و نفوذگران ایجاد خواهد شد (Cook, 2012, p. 1). به همین دلیل مدتی است که برخی دانشگاه‌ها و مؤسسات خصوصی به منظور تربیت متخصصان امنیت فناوری اطلاعات به ارائه دروس و مباحث هک، بدافزارنویسی، آشنایی با هرزنامه‌ها، جاسوس‌افزارها پرداخته‌اند. صرف‌نظر از مزایایی که آموزش این مباحث برای دانشجویان و متخصصان امنیت فناوری اطلاعات دارد، آموختن این مهارت‌ها نگرانی‌هایی را نیز در برخی افراد ایجاد کرده که این نگرانی‌ها موجب مخالفت عده‌ای با فراگیر شدن این آموزش‌ها شده‌اند.

افرادی که با آموزش این مهارت‌ها مخالف هستند در واقع، از یادگیری این مهارت‌ها احساس خطر می‌کنند و اعتقاد دارند که در این دوره‌ها مهارت‌هایی به دانشجویان آموزش داده می‌شود که بالقوه خطرناک هستند (Grobert, 2008, p. 5; Ledin, 2005; Cook, 2012, p. 1). به عقیدهٔ برخی مخالفان، آموزش هک و بدافزارنویسی دو خطر عمده به همراه دارد، خطری که در اثر سوءاستفاده دانشجویان از این مهارت‌ها برای جامعه به وجود می‌آید و خطری که این برنامه آموزشی برای خودِ دانشجو دارد و ممکن است مهارت‌های کسب شده او را به سمت فعالیت‌های مجرمانه سوق دهد (Pike, 2013, p. 3). درست است که هدف آموزش این مهارت‌ها تربیت متخصصان امنیت فناوری اطلاعات است، اما این تنها یک روی سکه است و ممکن است دانشجویان از مهارت‌های کسب شده در جهت سوء، استفاده کرده و برای کسب منافع شخصی و نیت‌های مغرضانه از آنها بهره ببرند.

به گفتهٔ مخالفان، درست است که در بسیاری از موارد ممکن است این آموزش‌ها ضروری باشند، اما با وجود تلاش‌های بسیار مدرسان و مربیان این دوره‌ها برای به‌کارگیری صحیح این مهارت‌ها، غیر قابل انکار است که برخی از دانشجویان از این مهارت‌ها به صورت نادرست و غیرقانونی استفاده می‌کنند (Cook, 2012, p. 1). به اعتقاد این افراد برخی از دانشجویان با پس‌زمینه‌های کیفری و یا مشکل‌دار ممکن است کاندیداهای مناسبی برای پذیرش در کلاس‌های هک و بدافزارنویسی نباشند.

ولف[1] آموزش مهارت هک به دانشجویان مقطع کارشناسی را با دادن تفنگ پر به آن‌ها مقایسه

1. Wulf

کرده است، (Livemore, 2007, p. 2)؛ زیرا دانشجویان کارشناسی ممکن است قادر به تصمیم‌گیری درست در خصوص استفاده از این مهارت‌های خطرناک نباشند. بسیاری از افرادی که این مهارت‌ها را یاد می‌گیرند از آن در جهت صحیح استفاده می‌کنند، اما نگرانی اصلی مخالفان در خصوص آموزش این مهارت‌های خطرناک به افرادی است که پایبند به مسائل اخلاقی نیستند و در صورت یادگیری این مهارت‌ها از آن‌ها سوءاستفاده کرده و به جامعه، افراد و سیستم‌ها آسیب‌های بعضاً جبران‌ناپذیر وارد می‌کنند.

در گذشته مهارت‌های هک و بدافزارنویسی با تمرین بسیار و یا با آموزش از طرف یک متخصص خبره و یا هکر دیگری به دست می‌آمد که مطمئناً این شرایط یادگیری برای بسیاری فراهم نبود، اما امروزه برنامه‌های آموزشی برخی از دانشگاه‌ها و به‌ویژه کلاس‌های برخی مؤسسات خصوصی راه جدیدی برای آموزش این مهارت‌ها به هکرهای مشتاق باز کرده است (Livemore, 2007, p. 2). با مراجعه به برخی از این مؤسسات آموزشی متوجه می‌شویم که انگیزهٔ برخی افراد از یادگیری این مهارت‌ها صرفاً منافع شخصی، رقابت با همسالان، سرقت، انتقام و ... است. در حال حاضر و با این شرایطِ آموزشی، دیگر نیازی نیست که هکرها تخصص دانشگاهی و دانش فنیِ مرتبط با رایانه و فناوری اطلاعات داشته باشند. گواه این مطلب، متقاضیان شرکت در این دوره‌ها هستند که بسیاری از آن‌ها یا مدرک دانشگاهی ندارند و یا مدرک تحصیلی‌شان هیچ ارتباطی با فناوری اطلاعات ندارد.

حتی اگر قبول کنیم که به لحاظ فنی مطالعهٔ بدافزارها مفید است، باید اذعان کرد که کار با نرم‌افزارهای مخرّب و ابزارهای نفوذ از نظر اخلاقی خنثی نیست؛ زیرا زمانی که ما تنها تلاش می‌کنیم تا ساختار یک قطعه از برنامه مخرب را درک کنیم یا راه نفوذ هکری به سیستم را بررسی کنیم، نیازمند آنیم که در وهلهٔ نخست مانند یک مجرم فکر کنیم. از آنجا که تفکر اخلاقی مهارت است و باید آن را در افراد توسعه داد، کسی که به‌طور فعالانه تلاش کند تا غیراخلاقی فکر کند، ممکن است توانایی انتخاب‌های خوب را از دست بدهد، مانند یک پلیس مخفی که به دلیل ارتباطات گسترده با دنیای تبهکاران رفتارش به تدریج بد و نادرست می‌شود (Sullins, 2014, p. 2).

دلیل اخلاقی آموزش بدافزارنویسی و مهارت هک

در ژوئن سال ۲۰۱۰م بسیاری از رایانه‌های ایرانی مورد هجوم شدید کِرم رایانه‌ای خطرناکی به نام

«استاکس‌نت»[1] قرار گرفتند که افزون بر اطلاعات سیستم‌های کنترل صنعتی و نیروگاهی و تأسیسات هسته‌ای، اطلاعات سیستم‌های خانگی را نیز به سرقت برد. استاکس‌نت حدود ۶۰ هزار رایانه را آلوده کرد که بیش از نیمی از آن‌ها در ایران بودند (Farwell, 2011, p. 1). این بدافزار حدود ۶۰ درصد رایانه‌های ایرانیان را آلوده کرد (ibid.) پیچیدگی کرم نرم‌افزاری استاکس‌نت به حدی بود که برخی از متخصصان از آن به عنوان «تروریسم سایبری[2]» یاد کردند. تا پیش از گسترش کِرم استاکس‌نت باور بر این بود که حملات سایبری تنها به اطلاعات داخل رایانه‌ها آسیب رسانده و هیچ‌گونه صدمات فیزیکی در پی نخواهند داشت. نویسندگان این کرم آن را طوری طراحی کرده بودند که به‌جای سرقت اطلاعات موجب تخریب تجهیزات فیزیکی و در نتیجه آسیب به ساختمان‌ها و حتی مرگ انسان‌ها می‌شد (Applegate, 2013, p. 1, 9; Denning, 2012, p. 2). کِرم استاکس‌نت تنها یک نمونه از میلیون‌ها بدافزاری است که امنیت رایانه‌ها را در سراسر دنیا تهدید می‌کند.

خسارت‌های مالی، جانی و روانی ناشی از نفوذ بدافزارها و هکرها روز به روز در حال افزایش است و همه کشورها، سازمان‌ها و افراد در معرض این آسیب‌های بعضاً جبران‌ناپذیر قرا دارند. افراد، سازمان‌ها و کشورها تا چه حد می‌توانند آسیب‌های ناشی از نفوذها و بدافزارها را تحمل کنند؟ آیا نباید در برابر تهاجمات دشمنان و نفوذگران، از سیستم‌ها و اطلاعات خود دفاع کرد؟ آیا چنین دفاع‌هایی از اصل مسلم اخلاقی «دفاع از خود» قابل استنتاج نیست؟ چه کسانی باید چنین نفوذها و بدافزاهایی را شناسایی کرده و از سیستم‌ها و رایانه‌ها در برابر آن‌ها دفاع کنند؟ افرادی که وظیفهٔ دفاع از سیستم‌ها را به عهده دارند چه مهارت‌هایی باید داشته باشند؟

یکی از بهترین راه‌های مقابله با نفوذ هکرها و بدافزارها تربیت کارشناسان و متخصصان امنیت رایانه است. این وظیفهٔ اخلاقی متخصصان امنیتی است که از سیستم‌ها و اطلاعات آن‌ها در برابر جنگ‌های سایبری و بدافزارها محافظت کنند (ibid.). تعداد متخصصان امنیت سایبری به موازات رشد اینترنت و فناوری‌های جدید افزایش پیدا نکرده است و کمبود این متخصصان موجب شده تا از سیستم‌ها و اطلاعات در فضای سایبری به‌خوبی محافظت نشود.

بسیاری سازمان‌ها و برخی مسئولان دانشگاه‌ها معتقدند که بهترین راه برای تربیت متخصصان امنیتی آگاهی از شیوه حملاتی است که سیستم‌ها با آن مواجه می‌شوند (ibid.). غیرقابل انکار است

1. stuxnet
2. cyber terrorism

که دانشـــجویانی که شـــناخت اندکی از تکنیک‌های حمله و نفوذ دارند، قادر نخواهند بود راه‌کارهای امنیتی مناسـبی را ارائه کرده و به‌طور مؤثر از سیستم‌ها حفاظت کنند (Trabelsi, 2013, p. 8) دانشجویان علوم کـامپیوتر بـاید یاد بگیرند که چگونه بدافزارها را تشـــخیص‌داده، تحلیل کرده و غیرفعال و ســـپس حـذف کننـد. برنـامـه‌نویســـی و کار عملی برای علوم رایانه مانند کار عملی پلیس و تجربهٔ بالینی برای عمل جراحی است (Ledin, 2005, p. 1).

جرج لدین[1] یکی از دانشـــمندان علوم کامپیوتر، اظهار کرده اســـت که تحصـــیلات در زمینهٔ امنیتِ رایانه بدون واحدهای درسـی‌ای که به دانشجویان چگونگی نفوذ و نوشتن بدافزار را آموزش دهد، مانند علم پزشـــکی‌ای اســـت کـه تلاش می‌کند برای بیماری‌ها راه‌های درمان جدیدی کشـــف کند بدون این‌که در مورد بیماری‌ها و ویروس‌ها مطالعه کند (Sullins, 2014, p. 1).

در رشـــته‌هایی مانند امنیت فناوری اطلاعات، پزشـــکی، داروســـازی، شـــیمی، رشـــته‌های نظامی و ... مهـارت عملی حرف اول را می‌زنـد و خوانـدن کتـاب‌هـا و یادگیری مطالبِ نظری به‌تنهایی کافی نیســـت و اگر مباحث عملی و مهارت اســـتفاده از ابزارها در کنار دروس نظری به‌خوبی آموزش داده نشوند، مطالب نظری فراگرفته شده نیز آن‌طور که باید کارایی لازم را نخواهند داشت.

مدت‌هاســـت به علت افزایش جرائم رایانه‌ای و عدم کارایی لازم فارغ‌التحصـــیلان رشـــتهٔ فناوری اطلاعـات در حفـاظـت از ســـیســـتم‌هـا، خلاء آموزش مطـالـب عملی و کـاربردی امنیت رایانه در دانشـگاه‌ها به‌شـدت احسـاس می‌شود و به همین دلیل، در بحث امنیت فضای مجازی تحقیقات در زمینهٔ بدافزارها افزایش پیدا کرده و چند سـالی اسـت که تکنیک‌های نوشـتن بدافزار و آموزش شیوهٔ نفوذ به سیستم‌ها جزء برنامه‌های درسی دانشجویان در برخی دانشگاه‌ها قرار گرفته است.

بســیاری از طرفداران آموزش مهارت هک و بدافزارنویســی ادعا می‌کنند که دانشــجویانی که این مهارت‌ها را آموخته‌اند بهتر می‌توانند در شـرایط واقعی از سـیسـتم‌ها دفاع کنند (Grobert, 2008, p. 6)؛ زیرا در محیط‌های آزمایشـــگاهی دانشـــگاه‌ها و مؤســـســـات با انواع حملات، شـــیوهٔ عملکرد آن‌ها و هم‌چنین بـا انواع مختلف راه‌کـارهـا و ابزارهـای دفاعی آشـــنا شـــده و با ذهنی باز می‌توانند راه‌کارهای دفاعی جدیدی را طراحی کنند.

یادگیری بسـیاری از مسـائل تنها از طریق عمل به دست می‌آید. آموزش عملی مهارت‌های هک

1. George Ledin

و بـدافزارنویســی بـا موانع بســیاری روبه‌روســت که باید با موانع مقابله کرده و برای حل مشــکلات راه‌کارهای عاقلانه و منطقی ارائه داد؛ برای مثال، در گذشـته تشـریحِ اجسـاد ممنوع بود و این ممنوعیت برای قرن‌ها جلوی موفقیت پزشـکی را گرفت. اگر تشـریح اجسـاد ممنوع باشـد، پزشـکان و جراحان چگونه باید با آناتومی بدن آشـنا شـوند؟ اگر محققان نمی‌توانسـتند روی ویروس کشـنده‌ای مانند ابولا مطالعه کنند، چگونه با این ویروس مقابله و واکسن آن ساخته می‌شد؟ (Ledin, 2005, p. 1)

البته، مشـکلِ سـوءاستفاده از مهارت‌های بالقوه خطرناک، تنها مختص امنیت اطلاعات نیست. مهـارت‌هـای دیگری از قبیـل هنرهـای رزمی، آموزش‌هـای نظـامی، کلیدســازی، روان‌شــناســی، داروسـازی، مهندسـی برق، مهندسـی هسته‌ای و حتی حسابداری همه مهارت‌هایی هستند که اگر از آن‌ها سـوءاسـتفاده شـود، می‌توانند بسیار خطرناک باشند (Cook, 2012, p. 1). درسی که چگونگی نوشـتن بدافزار را آموزش می‌دهد همانند درس شیمی است که چگونگی ساخت کوکتل مولوتف را آموزش می‌دهد و یا شـبیه درس فیزیک است که چگونگی ساخت کلاهک هسته‌ای را یاد می‌دهد و این‌هـا بـه‌وضــوح نگرانی‌هـای جدّی‌ای هســتند (Ledin, 2005, p. 1). آموزش مباحث هک و بدافزارنویسی در صورتی که به‌درستی انجام نشود، خطرناک است.

زمـانی مباحث رمزنگاری در دانشــگاه‌ها و مجامع بحثی ممنوع بود و تنها تحت کنترل دولت‌ها قرار داشـت، اما با گذشـت زمان و توسـعه ابزارهای رمزنگاری این ممنوعیت برداشـته شـد و امروزه تحقیقات جدید زیادی در این زمینه در دانشــگاه‌ها انجام می‌شــود (Ledin, 2005, p. 1). نوشــتن بدافزارها و همچنین شـیوهٔ نفوذ به سیستم‌ها نیز باید به عنوان یکی از مباحث اصلی، جزء فعالیت‌های تحقیقاتی دانشــجویان قرار گرفته و کار کردن روی آن‌ها آزاد باشــد که امروزه این‌گونه نیســت و همانند رمزنگاری موانعی در برابر آن وجود دارد که باید بر آن غلبه کرد.

راه‌کارهایی برای آموزش مهارت هک و بدافزارنویسی

آموزش مهـارت هـک و بدافزارنویســی مانند یک شــمشــیر دو لبه اســت. به همان اندازه که این مهارت‌ها به توسـعه امنیت سـیستم‌ها کمک می‌کنند، در صورتی که به افراد فاقد صلاحیت اخلاقی آموزش داده شـوند، می‌توانند به همان اندازه در راه نادرسـت به‌کار گرفته شـده و امنیت جامعه را بـه خطر بیانـدازنـد. عـدم آموزش این مهارت‌ها صــرفاً به دلیل این‌که بالقوه خطرناک‌اند و موجب

سوء استفاده برخی افراد می‌شوند، به لحاظ اخلاقی نادرست است؛ زیرا حفاظت از امنیت رایانه‌ها وظیفهٔ اخلاقی کارشناسان امنیت فناوری اطلاعات است و این کارشناسان تنها در صورتی می‌توانند به‌خوبی از سیستم‌ها حفاظت کنند که با شیوه نفوذ بدافزارها و هکرها آشنا شوند. آموزش مهارتِ هک مشکلاتی را با خود به همراه دارد که دانشگاه‌ها و مؤسسات با انجام یک سری اقدامات می‌توانند خطرات و مشکلات آن را تا حدی کاهش دهند. البته، در نهایت، این به عهده دانشجویان است که تصمیم بگیرند چه زمانی و کجا از مهارت‌های آموخته خود استفاده کنند، اما کمک کردن به آن‌ها و فراهم کردن ابزارها و محیط مناسب برای توسعه بلوغ و تسهیل انتخاب درست به عهده مربیان است (Cook, 2012, p. 4). اقداماتی مانند آموزش مهارت‌های هک و بدافزارنویسی در محیط‌های دانشگاهی، تدریس مسائل اخلاقی و قانونی، غربال کردن دانشجویان، تهیه و ارائهٔ منشور اخلاقی، صدور پروانه یا گواهینامه حرفه‌ای و تربیت مربیان خِبره و با اخلاق برای به حداقل رساندن فرصت سوء استفاده‌های تصادفی یا عمدی می‌تواند بسیار راهگشا باشد.

در این بخش راه‌کاری پنج مرحله‌ای برای آموزش مهارت‌های هک و بدافزارنویسی ارائه می‌شود. در صورتی که برای آموزش این مهارت‌ها همه این مراحل مد نظر گرفته شود تا حد زیادی می‌توان نگرانی مخالفان این‌گونه آموزش‌ها را برطرف کرد. البته، در صورتی که فراهم کردن همه این شرایط برای آموزش ممکن نباشد، انجام برخی از مراحل تا اندازه‌ای می‌تواند راه‌گشا باشد.

آموزش مهارت‌های هک و بدافزارنویسی در محیط‌های دانشگاهی

امروزه فعالیت هکرها و بدافزارها در فضای مجازی به‌شدت افزایش یافته است. آیا این هکرها و بدافزارنویس‌ها دانش و مهارت خود را در محیط‌های دانشگاهی فراگرفته‌اند؟ مسلماً پاسخ منفی است؛ چون در حال حاضر تنها تعداد بسیار کمی از دانشگاه‌های دنیا این مهارت‌ها را به دانشجویان خود آموزش می‌دهند، اما نکته این‌جاست که انگیزه قوی این مجرمان سبب شده تا از هر راهی به فراگیری این مهارت‌ها بپردازند. از سوی دیگر، کارشناسان امنیتی که باید جلوی نفوذ این هکرها و بدافزارها را بگیرند نه‌تنها در محیط‌های دانشگاهی مهارت لازم را کسب نکرده و دانش دفاعی لازم را به دست نیاورده‌اند، بلکه در بسیاری از موارد به دلیل نداشتن انگیزهٔ لازم، در خارج از دانشگاه نیز به دنبال فراگیری این مهارت‌ها نمی‌روند.

هـدف اکثر افراد برای ورود به دانشـگاه‌ها کسـب دانش و مهارت لازم برای ورود به بازار کار اسـت. زمانی که دانشـجویی، یک رشـته تحصـیلی مانند امنیت فناوری اطلاعات را انتخاب می‌کند تمام تلاش خود را در محیط دانشـگاه صَـرف کسـب مهارت‌های لازم در آن رشـته می‌کند تا بتواند در آینده موقعیت شـغلی بهتری به دسـت آورد. این‌گونه افراد ممکن است پس از فراغت از تحصیل موفق شـوند در موقعیت شـغلی مرتبط با رشـته خود (مثلاً به عنوان کارشـناس امنیت شـبکه سازمان) اسـتخدام شـوند. با توجه به دروسـی که این دانشـجو در دانشـگاه فراگرفته اسـت، به احتمال زیاد مهـارت لازم برای دفاع در برابر نفوذ هکرها و بدافزارها را نداشـته و نمی‌تواند به نحو احسـن انجام وظیفه کند. به همین دلیل اسـت که بارها و بارها خبر هک شـدن سـایت‌های دانشـگاه‌ها، بانک‌ها، سازمان‌ها و ... به گوش می‌رسد.[۱]

اگر هدف دانشـگاه تربیت متخصـصـانی اسـت که بتوانند بلافاصله پس از فراغت از تحصیل وارد بازار کار شـده و حداکثر کارایی را داشـته باشـند، باید مهارت‌های هک و بدافزارنویسـی به دانشجویان رشـتـه‌هـای امنیـت فنـاوری اطلاعـات، آموزش داده شـود؛ زیرا با آموزش درسـت این مهارت‌ها در دانشـگاه‌ها، امکان سـوءاسـتفاده دانشجویان از این مهارت‌ها نسبت به زمانی که این مهارت‌ها در خارج از محیط دانشـگاهی و در مؤسـسـات خصـوصی آموزش می‌بینند، بسیار کمتر است، چون اولاً، هدف دانشـجویان در دانشـگاه فراگرفتن مهارتی برای کسـب موقعیت شغلی مناسب است و تعهد دانشجویان در محیط دانشـگاهی نسـبت به مهارت‌های فراگرفته شـده بیشـتر اسـت. ثانیاً، کسـی که هدفش از گذراندن این دوره‌ها کسـب مهارت برای نفوذ و خرابکاری اسـت طبیعتاً چهار سـال از عمر خود را در دانشـگاه صـرف نمی‌کند به امید این‌که چنین واحدهای درسی‌ای را بگذراند. چنین افرادی به‌راحتی از طریق جست‌وجو در اینترنت و صرف زمان اندکی می‌توانند ابزارهای نفوذ را به‌دست آورند.

اگر مهارت‌های هک و بدافزارنویسـی در دانشـگاه‌ها آموزش داده نشـوند، با توجه به نیاز جامعه به متخصـصـان حرفه‌ای امنیت فناوری اطلاعات، مؤسـسـات خصـوصـی آموزش این مهارت‌ها را به عهده خواهند گرفت. کلاس‌های آموزشـی مؤسـسـات خصـوصـی در زمینه هک و تسـت نفوذ

---

۱. برای مثال، هک سـایت مرکز آمار ایران در چهارم خرداد ۹۵ (www. yjc. ir/fa/news/5621944) (۹۵/۶/۱۹)، هک تعدادی از سـایـت‌هـای متعلق بـه وزارت خـارجـه توسـط هکرهـای اسـتخـدامی سـعودی‌هـا در خرداد ۹۵ (www. tabnak. ir/fa/news/594370)(۹۵/۶/۱۹)، هک سـایت یکی از دانشـگاه‌های قوچان به منظور تغییر نمرات دانشـجویان مشـروطی (www. isna. ir/news/92102514875) (۹۵/۶/۱۹).

تا حد زیادی می‌تواند مهارت دفاعی لازم در برابر نفوذگران را به متقاضیان آموزش دهد، اما زمانی که این کلاس‌ها توسط مؤسسات خصوصی برگزار می‌شوند، امکان به وجود آمدن مشکلات قانونی و اخلاقی به‌دلیل سوء استفاده از این مهارت‌ها بیشتر می‌شود. احتمال این‌که متقاضیان شرکت در این دوره‌ها نیتِ سوء داشته و با هدف یادگیری این مهارت‌ها برای اهداف مغرضانه‌ای چون سرقت، تخریب، نقضِ حریم خصوصی افراد، انتقام و ... به چنین مؤسساتی مراجعه کنند بیشتر است؛ زیرا کلاس‌های این مؤسسات این امکان را فراهم می‌کنند که افراد متقاضی در مدت زمان کوتاهی مهارت‌های لازم برای هک و نفوذ را کسب کنند و ممکن است هزینه‌ای که برای شرکت در این کلاس‌ها پرداخت می‌کنند، در مدت زمان کوتاهی، از طریق نفوذهای غیرمجاز به دست آورند.

اگر بخواهیم پیامدهای سوء استفاده از مهارت‌های هک و بدافزارنویسی کمتر شود و خطر کمتری برای جامعه به‌وجود آورد، باید تا آنجا که ممکن است آموزش این مهارت‌ها جزء سرفصل‌های درسی دانشگاه‌ها قرار داده شود تا نیاز به مؤسسات خصوصی برای آموزش چنین مهارت‌هایی کمتر شود. قابل ذکر است که به دلایل مختلفی نمی‌توان کلاس‌های آموزشی مؤسسات خصوصی را به‌طورکلی حذف کرد و برای کاهش سوء استفاده از این کلاس‌ها نیز راه‌کاری وجود دارد که در ادامه به آن خواهیم پرداخت.

آموزش مسائل اخلاقی و قانونی

آموزش مهارت‌های هک و بدافزارنویسی ممکن است برخی دانشجویان را به سمت فعالیت‌های مجرمانه سوق دهد. حفاظت از دانشجویان اهمیت ویژه‌ای دارد؛ زیرا آن‌ها اغلب از جدّی بودن اعمال خود و پیامدهای آن آگاه نیستند. هکرها به‌خوبی می‌دانند که اگر به واسطه ارتکاب اعمال مجرمانه و سوء استفاده از مهارتِ هک دستگیر شوند، ممکن است زندگی‌شان به‌طور جدّی مختل گردد، در حالی که دانشجویان دانشگاه چنین درکی از پیامدهای اعمال خود ندارند (Pike, 2013, p. 3) و قطعاً یکی از وظایف اخلاقی دانشگاه‌ها و مؤسساتی که چنین دوره‌هایی را برگزار می‌کنند این است که مسائل اخلاقی و پیامدهای قانونی چنین اعمالی را به دانشجویان آموزش دهند تا آنان به‌طور آگاهانه از این‌گونه مهارت‌ها استفاده کرده و درک روشنی از پیامدهای جدّی و بلندمدت اعمالِ خود داشته باشند.

در واقع، آموزش چگونگی هک به دانشجویان بدون آموزش مسائل اخلاقی مرتبط با آن، ممکن است آموزش جنایتکاران و تروریست‌هایی برای انجام فعالیت‌های غیرقانونی باشد. امروزه برخی دانشگاه‌ها آموزش هک اخلاقی را جزء سرفصل‌های دروس رشته‌های رایانه و فناوری اطلاعات قرار داده‌اند که مسائل اخلاقی نیز مانند مسائل فنی در این دروس پوشش داده می‌شوند (Livemore, 2007, p. 2). یکی از جنبه‌های اساسی برنامه تدریس مهارت‌های هک، باید تدریس آموزه‌های اخلاقی مرتبط با آن باشد. در حقیقت، آموزش اخلاق به دانشجویان این دوره‌ها، آن‌ها را برای اتخاذ تصمیم‌های درست و اخلاقی آماده می‌کند.

اساتید آموزش هک و بدافزارها موافق‌اند که به همراه این واحدها مسائل اخلاقی نیز باید برای دانشجویان در نظر گرفته شود، چون هک و بدافزارنویسی دانش بالقوه خطرناکی بوده و نمی‌تواند بدون در نظر گرفتن مسائل اخلاقی، در یک محیط دانشگاهی و آموزشی ارائه شود (Sullins, 2014, p. 1). آموزش مهارت هک به دانشجویان بدون آموزش مسائل اخلاقی و حقوقی منجر به آموزش کارشناسان امنیتی و هکرها در کنار هم می‌شود (Curbelo, 2013, p. 4). دانشجویان باید درک کنند که هدف از آموزش این مهارت‌ها این است که آن‌ها چگونگی عملکرد حملات را یاد گرفته و با کمک آن‌ها راه‌های دفاعی مؤثری را طراحی و پیاده‌سازی کنند (Trabelsi, 2013, p. 8).

منطقی نیست از دانشجویان توقع داشته باشیم که تمامی جزئیات رفتار غیراخلاقی و غیرقانونی خود را بدانند در حالی‌که در دانشگاه آن را فرا نگرفته‌اند. اگر دانشجویانْ ملزم به اخذ واحدهای اخلاق رایانه و حقوق شوند، احتمال این‌که از مهارت تازه‌آموختهٔ خود برای انجام اقدامی بدخواهانه استفاده کنند، به‌شدت کاهش پیدا می‌کنند. البته، باید در محتوای آموزش‌های اخلاقی‌ای که ارائه می‌شود و همچنین انتخاب اساتیدی که آموزه‌های اخلاقی را آموزش می‌دهند، دقت تمام صورت پذیرد. محتوای آموزش‌های اخلاقی باید به‌گونه‌ای باشد که افزون بر جذابیت‌های محتوایی، انگیزهٔ لازم برای اخلاقی زیستن را در دانشجویان تقویت کند. در اینجا گذری بسیار کوتاه به برخی مباحثی که می‌تواند در این زمینه مفید باشد، خواهیم داشت.

به نظر می‌رسد یکی از نکات بسیار مهمی که در اخلاقی زیستن می‌تواند تأثیر زیادی داشته باشد نوع نگاه انسان به عالم و آدم است. به بیان دیگر، نوعِ شناختی که ما از عالم هستی و انسان داریم در زیستِ اخلاقی ما می‌تواند تأثیرگذار باشد. برای مثال، از یک‌سو (نگاه هستی‌شناسانه)، اگر برای عالم هستیْ خالقی عالم، توانا، حکیم، بصیر و ناظر قائل باشیم که این عالم را بر اساس

هدفی طراحی کرده است و تمام هستی از جمله انسان به سوی او در حال شدن و حرکت‌اند و نظامی که بر این عالم حاکم کرده است، نظامی اخلاقی است و بر اساس سنن الهی اداره می‌شود و برخی از سنن الهی نیز ناظر بر رفتارهای آدمی‌اند و میان نحوه زندگی آدمی در این دنیا و سرای دیگر نه‌تنها رابطهٔ علی و معلولی برقرار است، بلکه رابطه ظاهر و باطن است و قیامت در واقع، باطن این دنیاست و این اعمال و رفتار انسان است که در قیامت ظهور و بروز می‌یابد و از سوی دیگر (نگاه انسان‌شناسانه)، اگر حقیقت آدمی تنها بدن مادی و جسمانی او نباشد و ساحت دیگری نیز به نام روح، نفس و قلب نیز در کار باشد که مستند به خود خداست و خدا این ساحت را با دو دست خود خلق کرده است و به همین واسطه نه‌تنها خلیفه الهی[۱] در زمین شده، بلکه مسجود ملائک نیز قرار گرفته است[۲] و در ایجاد آن خدا به خود تبریک نیز گفته است[۳] و به یک معنا تمام حقیقت انسان را این ساحت او تشکیل می‌دهد و این ساحتْ جاودانه بوده و با مردن نابود نمی‌شود[۴]، قابل تغییر و کمال‌پذیر است، دارای فطرت الهی[۵] و آشنا با فجور و تقوی و زشتی و زیبایی است[۶]، هدفمند خلق شده است[۷] و هدف او خود خداست[۸]، دارای اختیار[۹]، واجد موهبت عقل و تمییز میان خیر و شر است[۱۰] و به‌واسطهٔ این ویژگی‌ها این استعداد و لیاقت را یافته است که خداوند ساختن هویتش را به دست خودش بدهد و به همین دلیل بار امانت الهی را هیچ موجودی به‌جز انسان نتوانست تحمل کند[۱۱] و در نتیجه انسان با تمامی رفتارها و اعمال خود هویت و باطن واقعی و جاودانه خود را شکل داده و می‌سازد و همین هویت و باطن است که در روز قیامت ظهور می‌یابد، چنین نگاهی هستی‌شناسانه و انسان‌شناسانه بی‌شک تأثیر بسزایی در اخلاقی زیستن او خواهد گذاشت.

---

۱. سورهٔ بقره، آیهٔ ۳۰.
۲. سورهٔ بقره، آیهٔ ۳۴.
۳. سورهٔ مؤمنون، آیهٔ ۱۴.
۴. سورهٔ زمر، آیهٔ ۴۲، سجده، آیهٔ ۱۱، نحل، آیهٔ ۳۲، انفال، آیهٔ ۵۰.
۵. سورهٔ روم، آیهٔ ۳۰.
۶. سورهٔ شمس، آیهٔ ۸.
۷. سورهٔ مؤمنون، آیهٔ ۱۱۵
۸. سورهٔ انشقاق، آیهٔ ۶.
۹. سورهٔ انسان، آیهٔ ۳.
۱۰. سورهٔ ملک، آیهٔ ۱۰.
۱۱. سورهٔ احزاب، آیهٔ ۷۲.

غربال کردن دانشجویان

یکی از مسائل اصلی که برگزارکنندگان دوره‌ها با آن مواجه هستند این است که آن‌ها از نیت واقعی شرکت‌کنندگان در این کلاس‌ها خبر ندارند؛ چه کسانی متقاضی شرکت در این دوره‌ها هستند؟ آیا تمام کسانی که در این کلاس‌ها شرکت می‌کنند هدفشان ارتقای امنیتی سیستم‌هاست یا قصد سوءاستفاده از این مهارت‌ها را دارند؟ به گفتهٔ برخی کارشناسان، درک نیت واقعی دانشجویان برای یادگیری مهارت هک بسیار سخت است (Curbelo, 2013, p. 3). یکی از دلایلی که آموزش چنین مهارت‌هایی در واحدهای درسی بسیاری از دانشگاه‌ها گنجانده نشده، این است که آموزش چنین مهارت‌هایی به افرادی که روحیه تخریب‌گری دارند و یا از نظر روانی ثُبات لازم را ندارند، می‌تواند پیامدهای فاجعه‌آمیزی به همراه داشته باشد. بنابراین، بررسی سوابق مجرمانهٔ دانشجویان، مصاحبه از آن‌ها و انجام تست‌های روان‌شناسی، پیش از پذیرش دانشجویان برای چنین دوره‌هایی، باید در نظر گرفته شود (Pashel, 2006, p. 3; Curbelo, 2013, p. 4).

برخی از دانشگاه‌ها و مؤسسات پیش از پذیرش و آموزش مهارت‌های مربوط به هک و بدافزارنویسی، متقاضیان را بررسی کرده و آن‌ها را غربال می‌کنند، اما برخی دیگر به این امر اعتقادی نداشته و این مهارت‌ها را به هر کس که تقاضا کند آموزش می‌دهند (Livemore, 2007, p. 3).

امروزه غربال‌گری دانشجویان متقاضی شرکت در این دوره‌ها در اکثر دانشگاه‌ها انجام می‌شود، اما مؤسسات خصوصی‌ای که این دوره‌ها را برگزار می‌کنند در اغلب موارد این غربال‌گری را انجام نمی‌دهند که این کار از نظر اخلاقی درست نیست؛ چون این مؤسسات نسبت به سوءاستفاده‌ها و پیامدهای امنیتی این‌گونه آموزش‌ها اخلاقاً مسئول هستند. به دلیل این‌که هدف اصلی برگزاری این دوره‌ها تربیت متخصصان امنیت فناوری اطلاعات است و یکی از کارهایی که این مؤسسات خصوصی می‌توانند انجام دهند این است که از متقاضیان شرکت در این کلاس‌ها معرفی‌نامه درخواست کنند و افرادی که کارشناس امنیتی سازمانی هستند تنها در صورت ارائهٔ معرفی‌نامهٔ رسمی از رئیس سازمان اجازهٔ شرکت در دوره‌های تخصصی امنیت را داشته باشند.

تهیه و ارائه منشور اخلاقی

ارائه منشور اخلاقی جامع برای هکرهای اخلاقی جهت جلوگیری از سوءاستفاده‌های احتمالی

شرکت‌کنندگان در دوره‌های آموزشی می‌تواند تا حد زیادی کمک‌کننده باشد. محتوای این منشورِ اخلاقی باید وظایف، مسئولیت‌ها و محدودیت‌های هکرهای اخلاقی را مشخص کند. از آنجا که به دلیل ماهیت کاری، هکرهای اخلاقی در زمان انجام تست نفوذ در شرکت‌ها و سازمان‌ها ممکن است به اطلاعات مهم و محرمانه‌ای دست یابند، این منشور اخلاقی باید شیوهٔ برخورد آن‌ها با چنین اطلاعاتی را مشخص کند.

این منشور اخلاقی باید به همان اندازه که روی اثربخشی کار هکرهای اخلاقی تأکید می‌کند، روی حفاظت از سیستم‌های مشتریان و اطلاعات آن‌ها نیز تأکید داشته باشد.

برخی مؤسسات معروف آموزشِ مهارت هک این منشور اخلاقی را تهیه کرده‌اند. برای نمونه، در منشور اخلاقی سایت موسسه آموزشی EC-Council[1] مواردی چون حفاظت از مالکیت معنوی افراد، نگهداری محرمانه از اطلاعاتِ به دست آمده از سازمان‌ها، عدم استفاده نادرست از گواهینامه کسب شده از موسسه، عدم شرکت در فعالیت‌های هکرهای کلاه سیاه و ... ذکر شده است.[2] اساتید این دوره‌ها باید مسائل اخلاقی این منشور را مرتباً در طول دوره یادآوری کنند تا شرکت‌کنندگان فراموش نکنند که هدف آن‌ها برای یادگیری این مهارت‌ها صرفاً ارتقای امنیتی سیستم‌ها بوده و نباید به هیچ عنوان از مهارت‌های کسب شده سوء استفاده کنند.

متقاضیان این دوره‌ها باید بدانند که باید اطلاعاتی که در کار حرفه‌ای خود به دست می‌آورند را مخفی و محرمانه نگه دارند و اطلاعات اشخاص از قبیل نام، ایمیل، آدرس و ... را بدون رضایت قبلی افراد از سیستم‌ها جمع‌آوری نکنند، نفروشند و به کسی ندهند. هکرهای اخلاقی باید پیش از هک و در حین انجام کار میزان حساسیت و محرمانه بودن اطلاعات کارفرمای خود را مشخص کنند. این کار کمک می‌کند تا در حین کار مراقبت و حساسیت بیشتری نسبت به اطلاعات حساس و محرمانه داشته باشند. پس از عملیات هک اخلاقی نیز نباید اطلاعات مشتری را فاش کنند، چون هک اخلاقی برای امنیت سیستم و شبکه مشتری انجام می‌شود و افشای اطلاعات محرمانهٔ مشتری، هک اخلاقی را بی‌اثر می‌کند.[3]

---

۱. کمیته بین‌المللی مشاوران تجارت الکترونیک (EC-Council) بزرگترین مرجع صدور گواهینامه‌های فنی در حوزهٔ امنیت سایبری است. این کمیته پس از حمله ۱۱ سپتامبر به مرکز تجارت جهانی تشکیل شد و در حال حاضر در ۱۴۰ کشور دنیا در حال فعالیت است (https://www. eccouncil. org/about) (۱۴/۹/۲۰۱۶).

2. https://www. eccouncil. org/code-of-ethics/

3. http://panmore. com/ethical-hacking-code-of-ethics-security-risk-issues. (2016/9/14)

صدور پروانه و گواهی‌نامهٔ حرفه‌ای

این راه‌کار مخصوص مؤسسات خصوصی آموزش هک و تست نفوذ است. این‌گونه مؤسسات در پایان دوره آموزشی به شرکت‌کنندگان گواهینامه حرفه‌ای معتبر ارائه می‌دهند که این گواهینامه‌ها برای کسب موقعیت‌های شغلی می‌تواند بسیار تأثیرگذار باشد. اگر به‌گونه‌ای برنامه‌ریزی شود که افراد برای کار در حوزه امنیت فناوری اطلاعات ملزم به ارائه گواهینامه حرفه‌ای مرتبط باشند، مشکلات تا اندازه‌ای می‌تواند برطرف شود. در واقع، از دست دادن مجوز و یا اعتبار گواهینامه ممکن است برای ادامه فعالیت‌های مشروع یک سوءاستفاده‌کننده مشکلاتی به وجود آورد (Livemore, 2007, p. 3). در این صورت افراد در استفاده از گواهینامه و مهارت خود بیشتر دقت خواهند کرد.

برخی مؤسسات بین‌المللی فرم‌های مخصوص گزارشِ نقض اخلاق دارند و اگر فردی در کلاس‌های این مؤسسات شرکت کرده و از آن‌ها گواهینامه گرفته باشد و به هر صورتی از مهارت کسب شده و گواهینامه خود سوء استفاده کند، این امکان وجود دارد که افرادی که از کار فرد متضرر شده و شکایت دارند به موسسه مراجعه کرده و فرم مخصوص نقضِ اخلاق را پر کنند. در این حالت، موسسه در خصوص اعتبار گواهینامه فرد خاطی تجدیدنظر خواهد کرد. برای مثال، کمیته EC-Council که توجه ویژه‌ای به اخلاق دارد، فرآیند عادلانه‌ای برای ارزیابی موارد نقضِ اخلاق در نظر گرفته است. هر کسی که بخواهد نقضِ اخلاق را از سوی دارندگان گواهینامه این موسسه گزارش کند، فرم گزارش نقضِ اخلاق را پر کرده و جزئیات و چگونگی نقضِ اخلاق را بیان می‌کند و سپس کمیته بر اساس شواهد قابل توجه و کافی، مورد را بررسی کرده و در صورت اثبات نقضِ اخلاق، دستور لازم را صادر می‌کند. تصمیم‌ها یا مجازات‌های ممکن شامل لغو اعتبار گواهینامه، توبیخ، هشدار، تعلیق گواهینامه و انتشار تخلف است.[1]

اگر تمامی مؤسسات ملزم به ارائهٔ گواهینامه حرفه‌ای معتبر تحت نظارت یک مرجع قانونی باشند و همچنین شرط لازم برای کار در حوزهٔ امنیت فناوری اطلاعات نیز ارائهٔ گواهینامه معتبر و قانونی باشد، بسیاری از مشکلاتِ به وجود آمده برطرف شده و امکان سوء استفاده‌های احتمالی نیز تا حد زیادی کاهش پیدا خواهد کرد؛ زیرا افراد می‌دانند که اگر از مهارت خود سوء استفاده کنند، گواهینامهٔ آن‌ها تعلیق شده و یا به‌طورکلی باطل می‌شود و دیگر نمی‌توانند به صورت قانونی در این

1. https://cert. eccouncil. org/images/doc/Ethics-Violation-Report-Form-v1. 1-03012012. pdf, (2016/9/14).

حوزه فعالیت کنند. البته، فراهم شدن این شرایط نیاز به همکاری مسئولان سازمان‌ها، دولت‌ها و مراجع قانونی دارد تا این روند به‌طور کامل اجرا شود.

تربیت مربیان

مربیان با اخلاق و مهذّب که دقیقاً مسائل اخلاقی را مراعات می‌کنند، هم می‌توانند بر روی دانشجویان تأثیر بگذارند و هم می‌توانند الگوهای اخلاقی خوبی برای دانشجویان باشد. دانشجویان امنیت رایانه می‌توانند بهترین رفتارهای اخلاقی را از طریق اساتید و افراد حرفه‌ای که دوره‌های آموزشی را برگزار می‌کنند فراگیرند. اگر در دوره‌های آموزشی هک و بدافزارنویسی، فضا به‌گونه‌ای فراهم شود که مدرس دوره دسترسی به شبکهٔ واقعی داشته و با وجود داشتن مهارت و امکان سوء استفاده، از ابزارها و مهارت خود به بهترین نحو و به صورت اخلاقی استفاده کند نه‌تنها به خاطر دسترسی به شبکه واقعی عمق فهم و یادگیری امنیت شبکه برای دانشجویان افزایش پیدا می‌کند، بلکه آن‌ها قدرت مهارت خود و لزوم استفاده اخلاقی از این ابزارها را نیز به‌درستی درک خواهند کرد. قطعاً اتخاذ تصمیم‌های اخلاقی از سوی مربیان می‌تواند رفتار اخلاقی را در میان دانشجویان گسترش دهد (Pashel, 2006, p. 3).

تربیت مربیان مجرّب امنیت فناوری اطلاعات می‌تواند نقش بسزایی در ارائه الگوهای اخلاقی و کاهش سوءاستفاده‌های احتمالی دانشجویان داشته باشد. مربیان دوره‌های هک و تست نفوذ باید تلاش کنند تا با رفتارهای اخلاقی و قانونی خود همگام با آموزش مطالب تخصصی امنیت رایانه رفتارهای اخلاقی و قانونی را نیز در دانشجویان نهادینه کنند و قدرت تصمیم‌گیری‌های درست و اخلاقی را در آن‌ها تقویت نمایند. در این بخش برخی از اقداماتی که مربیان می‌توانند در طول دوره انجام دهند، به‌طور مختصر ذکر می‌شود.

مربیان باید به‌طور مرتب در طول دوره دانشجویان را در استفاده اخلاقی از ابزارها و تکنیک‌ها توجیه کنند. آن‌ها باید به‌طور عمدی برای دانشجویان زمینه‌سازی کنند که چرا باید چیزهای خطرناک را یاد بگیرند. مربیان باید مسئولیت‌پذیری، کار تیمی و تصمیم‌گیری‌های سنجیده را در آن‌ها ترغیب کنند. دانشجویان این دوره‌ها باید درک روشنی از پیامدهای جدّی و بلندمدت اعمال خود داشته باشند. بیان موارد سوء استفاده دانشجویان قبلی از سوی مربیان و بحث در مورد یک

حادثه مخرب هک که در اخبار بیان شـده می‌تواند بسـیار تأثیرگذار باشد (Cook, 2012, p. 4). یکی از پیشـنهادهای مطرح شـده این اسـت که موارد سـوء استفاده از این مهارت‌ها مطرح شده و به بحث گذارده شـود تا به کمک آن دانشـجویان بتوانند درک درسـتی از رفتار مناسـب و همچنین تجزیه و تحلیل پیامدهای رفتار نامناسب داشته باشند.

نمونه‌هایی از آموزش بدافزارنویسی در دانشگاه‌ها

آموزش مهارت‌های هک و بدافزارنویسـی به دانشـجویان مقطع کارشـناسـی و کارشـناسـی ارشد در سـال‌های اخیر مورد توجه زیادی واقع شـده اسـت. هدف ارائه این دروس در سطح دانشگاه آموزش دانشـجویان برای حفاظت از سـیسـتم‌ها، اطلاعات و دارایی‌های کارفرماهای آینده آن‌هاسـت که در نهایت، این امر منجر به ارتقای امنیت فناوری اطلاعات در سطح جامعه خواهد شد.

دانشـگاه کالگری کانادا در سـال ۲۰۰۳م واحد درسـی‌ای به نام «ویروس‌ها و بدافزارهای رایانه‌ای» ارائه کرد که هدف آن را توسـعه فهم مکانیزم عملکرد ویروس‌ها، آموزش چگونگی نوشتن ویروس‌ها و دفـاع در برابر آن‌هـا بیان کرد ((Aycock, 2005, p. 1 این دانشـگاه از سـال ۲۰۰۵م هرزنامه و جاسـوس‌افزارها را نیز جزء واحدهای درسـی دانشجویان قرارداده است. در این درس دانشجویان در آزمایشـگاه‌های امن به توسـعهٔ هرزنامه‌ها و جاسـوس‌افزارها پرداخته و ابزارها و راه‌های دفاعی در برابر آن‌ها را نیز بررسی کرده و توسعه می‌دهند (Aycock, 2006, p. 1).

در شـروع این برنامهٔ درسـی افزون بر مقدمات مربوط به بدافزارها، هرزنامه‌ها و جاسـوس‌افزارها، مبـاحـث اخلاقی نیز قرار گرفتـه اسـت، مباحثی از قبیل نظریه‌های اخلاقی، شـناخت مشـکلات اخلاقی، فرآیندهای تصـمیم‌گیری اخلاقی و نمونه‌هایی از مشـکلات اخلاقی در این قسـمت مطرح می‌شـوند. پس از مباحث اخلاقی، بخشی از دوره به آموزش مباحث حقوقی تخصیص داده می‌شود و در خصـوص قانون‌های مرتبط با بدافزارها، هرزنامه‌ها و جاسـوس افزارها بحث می‌شود (Aycock, 2006, p. 2; Aycock, 2005, p. 2).

دانشـگـاه RWTH آخن نیز از سـال ۲۰۰۴م بـه آموزش روش‌هـای دفـاعی در زمینـهٔ امنیـت فناوری اطلاعات پرداخته اسـت. ایدهٔ اصـلی شـروع این آموزش‌ها دادن دید وسـیع به دانشجویان در خصـوص مسـائل امنیتی و نقاط ضعفی است که یا در کتاب‌ها نیست و یا دست‌کم گسترده نیست.

دانشگاه روهر بوخوم[1] هم از سال ۲۰۰۷م آموزش مهارت‌های دفاعی حوزهٔ امنیت فناوری اطلاعات را آغاز کرده است. واحد درسی «آزمایشگاه هک با هدف یادگیری مکانیزم‌های دفاعی» یکی از درس‌هایی است که در این دانشگاه ارائه می‌شود (Grobert, 2008, pp. 3-4).

نتیجه‌گیری

دانشجویان رشته فناوری اطلاعات و کارشناسان امنیتی برای ارائه راه‌کارهای امنیتی مناسب باید با مهارت‌ها و ابزارهای هک و بدافزارنویسی آشنایی داشته باشند. این مهارت‌ها به آن‌ها کمک می‌کند که بتوانند به‌طور مؤثرتری از سیستم‌ها و اطلاعات درون آن‌ها حفاظت کنند. آموزش مهارت‌های هک و بدافزارنویسی ممکن است به دلیل ماهیت خطرناکی که این مهارت‌ها دارند، موجب به وجود آمدن مسائل اخلاقی و قانونی در جامعه شود، اما با این استدلال که این مهارت‌ها بالقوه خطرناک هستند و ممکن است موجب افزایش جرائم سایبری شوند، نمی‌توان لزوم برگزاری این برنامه‌های آموزشی را به‌طورکلی نفی کرد و از برگزاری آن‌ها جلوگیری کرد. به دلیل افزایش چشم‌گیر جرائم و حملات سایبری در سال‌های اخیر لزوم تربیت متخصصان امنیت فناوری اطلاعات اهمیت ویژه‌ای پیدا کرده است. برای مقابله با مسائل اخلاقی و قانونی آموزش مهارت هک و بدافزارنویسی دانشگاه‌ها و مؤسسات با انجام یک سری اقدامات می‌توانند خطرات و مشکلات این‌گونه آموزش‌ها را تا حد زیادی کاهش دهند. این اقدامات شامل آموزش مهارت‌های هک و بدافزارنویسی در محیط‌های دانشگاهی، تدریس مسائل اخلاقی و قانونی در کنار مسائل فنی و تخصصی، غربال کردن دانشجویان، تهیه و ارائه منشور اخلاقی، صدور پروانه یا گواهی‌نامه حرفه‌ای و تربیت مربیان خبره و با اخلاق برای به حداقل رساندن فرصت سوء استفاده‌های تصادفی یا عمدی است. اگرچه این راه‌کارها امکان سوء استفاده از این مهارت‌ها را به صفر نمی‌رسانند، اما رعایت آن‌ها تا حد زیادی می‌تواند تأثیرگذار باشد.

1. Ruhr-University Bochum

فهرست منابع

- آل‌بویه، علیرضا؛ آل‌بویه، زینب. (۱۳۹۴). هک کردن و نفوذ به سیستم‌های رایانه‌ای از منظر اخلاقی، فصلنامه علمی- پژوهشی نقد و نظر. ۲(۲۰)، ۱۲۸-۱۰۴.

References

- Applegate, S. D. (2013). The Dawn of Kinetic Cyber. *5th International Conference on Cyber Conflict*.
- Aycock, J. ;Barker, K. (2005). Viruses 101. In *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*, 152–156.
- Aycock, J. (2006). Teaching spam and spyware at the University of Ca1gery. *Third Conference on Email and Anti- Spam (CEAS)*, 137-141.
- Clarke, zuley; clawson, james; cordell, maria. (2003). A brief history of hacking. *http://steel. lcc. gatech. edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL. pdf*. 2016/10/5.
- Cook, T.; Conti, G. & Raymond, D. (2012), When Good Ninjas Turn Bad: Preventing Your Students from Becoming the Threat. *Proceedings of the 16th Colloquium for Information Systems Security Education Orlando*, 11-13.
- Curbelo, A. M. ; Cruz, A. (2013). Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems Undergraduates Students. *Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology*.
- Denning, D. E. . (2012). Stuxnet: What Has Changed?. *future internet* , 4, 672-687.
- Faily, S. (2014). Ethical Hacking Assessment as a Vehicle for Undergraduate Cyber-Security Education. *Processing of the BCS 19th Annual INSPIRE Conference*.
- Farwell, J. P. & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53*(1)*, 23-40.
- Grobert, F.; Kornau, T. & Pimenidis, L. (2008). Is Teaching Hacking in Academia Ethical?. *https://events. ccc. de/sigint/2009/Fahrplan/attachments/1275_main. pdf. 2016/9/20*.
- Kaspersky Security Bulletin (2015), https://securelist. com/files/2015/. . . /Kaspersky-Security-Bulletin-2015_FINAL_EN. pdf. 2016/7/2.
- Ledin, G. . (2005). Not teaching viruses and worms is harmful. *Communications of the ACM*, 48 *(1)*, 144.
- Ledin, G. . (2011). The growing harm of not teaching malware. *Communications of the ACM*, 54 *(2)*, 32-34.
- Livermore. (2007). What are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?. *Procedings of the 11th Colloquim for Information System Security Education*, Boston, MA.
- Logan, P. & Clarkson, A. . (2005). Teaching students to hack: Curriculum issues in information security. *Proceedings of the 36th SIGSE Technical Symposium on Computer Science Education*. 157-161.
- Mariotti, J. (2014). An introduction to malware. *https://www. ncsc. gov. uk/content/files/protected_files/guidance_files/An-introduction-to-malware. pdf*.

2016/7/14.
- Milošević, N. (2013). History of malware. *Digital forensics magazine*, 16*(1)*, 58-66.
- Pashel, B. A. . (2006). Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level. *InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development*, 197-200.
- Pike, R. E. . (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management*, 22, 67-76.
- Sullins, J. P. . (2014). A Case Study in Malware Research Ethics Education, When teaching bad is good. 2014 IEEE Security and Privacy Workshops,*www. ieee-security. org/TC/SPW2014/papers/5103a001. PDF*. 2016/8/6.
- Trabelsi, Z. & Ibrahim, W. (2013). Teaching ethical hacking in information security curriculum: A case study. 2013 IEEE Global Engineering Education Conference. *ieeexplore. ieee. org/iel7/6522574/6530074/06530097. pdf*. 2016/7/23.
- Zeltser, L. (2014). What is malware. *https://securingthehuman. sans. org/newsletters/ouch/issues/OUCH-201402_en. pdf*. 2016/5/1.
- Lachow, I. (2011). The Stuxnet Enigma Implications for the Future of Cybersecurity. *Georgetown Journal of International Affairs*. 118-126.

- http://panmore. com/ethical-hacking-code-of-ethics-security-risk-issues.
- http://www. mashreghnews. ir/fa/news/36007, 1395/6/15
- https://cert. eccouncil. org/images/doc/Ethics-Violation-Report-Form-v1. 1-03012012. pdf, 2016/9/14.
- https://www. eccouncil. org/code-of-ethics/,2016/9/14.
- https://www. helpnetsecurity. com/2002/04/08/the-history-of-hacking,2016/7/2.
- www. isna. ir/news/92102514875, 1395/6/19.
- www. tabnak. ir/fa/news/594370, 1395/6/19.
- www. yjc. ir/fa/news/5621944, 1395/6/19.

Resources written in Arabic / Persian

- Alebouyeh, A.; Alebouyeh, Zeinab. (2015). «Hacking and Intrusion into Computers Systems of Moral Perspective». *The Quarterly Journal of Philosophy & Theology*. Vol. 20, Issue 78, p. 104-128.