An Introduction to Ethical Hacking

Matt Danda

Webster University

Abstract

This paper provides an overview of the ethical hacking field. It begins by reviewing two academic articles that cover the education of ethical hackers, which both stress the importance of teaching ethics and morals as part of the curriculum. Educational institutions are obligated to teach some hacking skills in order to successfully prepare future security professionals, however, they must also ensure that students do not become tempted to use those skills for illicit or criminal purposes. The remaining three articles reviewed in this paper provide insight into the freely available resources available to hackers of all types and levels. These articles provide a prospective ethical hacker with a list of forums, tools, and processes that they can incorporate into their studies.

Introduction

This research paper presents a series of academic papers that provide insight into the ethical hacking field. The first paper introduces ethical hacking and the pedagogical ethics of teaching students how to hack (Hartley, R., 2015). It suggests best practices for the instruction of ethical hacking to prevent students from using their skills in destructive ways. Why would a student turn to hacking? Xu, Z., Hu, Q., & Zhang, C. (2013) discuss this phenomenon in their paper, *Why Computer Talents Become Computer Hackers*. They argue that moral values and judgement appear to be the only differentiators between grey-hat and black-hat hackers. The remaining three papers in this series describe some of the powerful and free resources available to hackers. While presenting a novel method for gathering proactive cyber threat intelligence, Samtani, S., Chinn, R., Chen, H., & Nunamaker, J., (2017) provide interesting details on hacker communities and the forums that hackers use to share information and (often malicious) hacking tools. The final two papers discuss the variety of hacking tools available within Kali Linux, which is a freely available Linux-based operating system geared specifically for penetration testing. Babincev, I., & Vuletić, D. (2016) cover tools in Kali that can be used to analyze web application security, and Čisar, P., & Čisar, S. (2018) discuss tools and methods for penetrating wireless networks.

Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack

The article, *Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack*, introduces the field of ethical hacking and its importance in the cyber security industry. The ethical hacker performs penetration testing on networks using the same tools and techniques as criminals, with the same intent to find network vulnerabilities. By thinking and acting like a criminal hacker—but not actually doing damage or stealing information—the ethical hacker uses

an offensive approach to acquire valuable insight into the security of a network. This offensive approach produces better security than taking a defensive-only approach.

The author stresses that, in order to produce highly skilled computer security professionals, educational institutions should teach their students computer hacking skills. Otherwise, security professionals may not be adequately prepared for their careers. Educators should avoid watering-down content, and they should employ the same tools and techniques as black-hat hackers.

Because hacking skills can also be used for nefarious purposes, educational institutions face an ethical dilemma—how do you teach hacking skills without creating new cyber criminals? The author recommends several best practices for educational institutions, beginning with implementing a computer ethics policy that helps regulate a sense of ethics and permitted behavior. While a hands-on approach is required to learn hacking skills, educators should stress ethics at all times during instruction. One curious suggestion by the author is to use "Google hacking" as a tool for teaching web security.

Hartley argues convincingly that educational programs designed to produce cyber security professionals should teach ethical hacking skills. The author also describes the great ethical dilemma that educational institutions face by teaching skills that can be easily redirected toward criminal activities. The recommended solution is for educational institutions to tightly integrate the teaching of ethics into the curriculum. Sound advice, indeed.

Why Computer Talents Become Hackers

Now that we've discussed the importance of teaching ethical hacking skills to future security professionals, let's turn our discussion to the student. The second article in my research,

Why Computer Talents Become Computer Hackers, discusses why a skilled student would turn to criminal behavior. The authors admit that an "interesting but troubling aspect of the (cyber crime) epidemic is that so much of it is committed by college-age young people." (Xu et. al, 2013, p64) The article also admits that there are no consistent, widely acceptable theories as to why hackers evolve, nor effective guidance for preventing young people from becoming cyber criminals. However, through their research, they do provide some valuable insights into the mindset of the computer-savvy college-student who engages in illegal hacking activities.

Research indicates that hackers tend to be young males and school drop-outs in their mid-20s, and that they have some sort of "ethical deficit" that disposes them toward law-breaking behavior. Juveniles have not reached emotional maturity and are more likely to act on hedonistic impulses. However, this is not a complete picture.

The authors of this study researched six young hackers in China and summarized their findings. None of them were delinquent in adolescence nor did they appear to struggle with moral confusion. All of the students in the study were exceptionally bright, had an interest in computers, and appeared to be *uninterested* in being A-students—preferring hacking activities to schoolwork. They typically started hacking for innocent reasons and found early success due to porous security and a high tolerance from school administrators for the behavior. At some point, they started associating with like-minded individuals in hacking groups and college clubs. Such groups have a significant influence on how a student views the world and hacking activities.

In order for a crime to occur, the authors list three essential elements: a motivated offender, an appropriate target, and the absence of an able guardian. To avoid turning young students into criminal hackers, the authors provide the following recommendations: eliminate

tolerance in schools for hacking activities and strengthen the moral values of students. Society must work to channel their interest in computers in a positive direction.

This article provides valuable insight into the mind of a potential hacker and offers a framework for educators to follow to help prevent students from criminal activities. The two articles I've discussed thus far stress the importance of teaching ethics and moral values to computer-savvy students, i.e., "soft skills." At this point, I'd like to examine some of the technical, or "hard skills," employed by hackers. The following three papers discuss various resources, processes, and tools that are common among hackers—ethical and criminal alike.

Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence

Traditionally, threat intelligence is analyzed after an incident has occurred, which is a reactive approach. The article, *Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence*, proposes a framework for gathering threat intelligence for the purpose of taking a proactive approach to network defense. Network administrators could apply this framework to understand potential threats as taken directly from the hacker community. They could then take measures to guard against those threats before an incident occurs.

The framework is designed to gather intelligence from various hacking resources, and then apply state-of-the-art data mining and artificial intelligence techniques to gather and analyze the vast amounts of data available. Some challenges of gathering data include "robust anticrawling measures, foreign-language barriers, little-known hacking terms, and complex forum structures." (Samtani et al, 2017, p1025)

While the technical details of the framework are beyond the scope of this research paper, the article is interesting because it provides insight into the various resources hackers use to gather and share information. The authors performed an extensive literature review of hacker communities, cyber threat intelligence, source code analysis, and social network analysis. These resources provide a roadmap for further research into the hacker community and mindset.

For example, the authors selected seven hacker forums, one English and six Russian, that are well known to the hacker community for distributing malicious assets. The English forum is OpenSC and the Russian forums are Damagelab, ExploitIN, Prologic, Reverse4you, Xakepok, and Xeksec. The authors also cite technical skills important for hacking, such as the ability to analyze source code. Malware such as memory injections, shellcode exploits, and process injections are primarily written in Delphi or C/C++, Metasploit modules in Ruby, and SQL injections in SQL. PHP is used to exploit websites, and Python is commonly used for password cracking tools. Java is used for spam services, banking rootkits, and decryption tools. Additional technologies cited in the article are Remote Administration Tools (RATs) and keylogging tools. As part of their research, the authors were able to identify trends that linked the type of malware discussed on the forums with the most common security issues of the period, and they could identify which types of exploits were popular at which time.

Although the primary purpose of the article was to demonstrate how modern data mining techniques can be applied to cyber security, this article also provides a broad overview of the types of technical skills employed by modern hackers and some of the forums that hackers use to share information, code, and tools. The final two articles in this research paper go into further detail and present some of the freely available tools that are commonly used by ethical and criminal hackers alike.

Web Application Security Analysis Using the Kali Linux Operating System

The article, *Web Application Security Analysis Using the Kali Linux Operating System*, introduces a set of freely available hacking tools that can be used to find vulnerabilities in web applications. These tools are included with the Kali Linux operating system, which is a free Linux distribution intended for penetration testing. Kali organizes its tools into the following groups: information gathering, vulnerability analysis, web applications (the focus of the article), password attacks, wireless attacks, exploitation tools, sniffing and spoofing, maintaining access, reverse engineering, stress testing, hardware hacking, forensics, reporting tools, and system services. As you can see, Kali covers the gamut of the hacking domain.

After introducing Kali, the authors introduce a series of tools for detecting web application vulnerabilities, which includes a brief description of the types of exploits each tool is investigating. These tools are:

- **Burp Suite**: a platform with multiple tools for performing security testing of web applications. The article discusses only one of the tools in the Burp Suite, Intruder.
- **XSSer**: a tool that automates the process of detection and exploitation of cross-site scripting (XSS) vulnerabilities on web sites or applications.
- **Nessus**: oddly enough, this tool is not actually included in Kali, but it is free and used for scanning and finding vulnerabilities in computer systems. Nessus supports over 50,000 plug-ins for detecting various types of vulnerabilities.
- **Nikto**: another tool designed specifically for web application testing.
- **Vega**: a highly regarded tool used to check for vulnerabilities such as SQL injection, cross-site scripting, cross-site request forgery, and others.

In addition, the article introduces two applications designed for testing purposes, so that the user can play with the tools in a safe, controlled environment: Damn Vulnerable Web Application (DMVA) and Mutillidae.

The authors conclude their survey by providing some advice on conducting web application tests. Because testing for XSS, SQL injection, and other vulnerabilities is a time-consuming task, they recommend using multiple automated scanners simultaneously. They also stress that the reports and output of these tools may include many false positives, as a result, the reports need to be reviewed by a skilled analyst.

This article is interesting to prospective hackers because it provides guidance and recommended tools for conducting penetration testing on web applications. It does not provide step-by-step instruction, but it does introduce a framework that a prospective hacker can use as a starting point. It is also worth mentioning that all of the tools listed in the article are legal and that they (or versions of them) can be downloaded for free from the internet.

Ethical Hacking of Wireless Networks in Kali Linux Environment

The final article in this research paper provides an introduction to the process of hacking wireless networks using the tools available in Kali Linux. It begins with a general procedure that describes how to set up a computer for wireless hacking, followed by a step-by-step description of how to sniff a network and capture packets. This section introduces the reader to the concept of MAC addresses (and how to change them!) as well as using Linux tools such as ifconfig, iwconfig, airmon, Aircrack, and others.

Next, the article covers deauthentication attacks, in which the hacker attempts to disconnect a target device from a wireless network. The article then provides an interesting

lesson in how to set up a fake access point, as well as an informative section on wireless protocols such as WPA, WPA2, WEP, AES, and TKIP. It then explains the steps to crack WEP and WPA networks using various Linux tools including aircrack, wash, and crunch.

The article concludes by praising the look, features, tools, and workflow of Kali Linux. Kali "provides a means of ethical hacking and network analysis tools [sic] that may not only allow user [sic] to audit and save his environment but, besides, learn a whole lot about the network stack, attacks, vulnerabilities and command line utilization." (Čisar et al, 2018, p186) The authors also point out that the efficiency of the cracking process depends heavily on the cracking tool employed.

One striking omission from this article is any discussion of ethics, which I believe is a central concept to the ethical hacking field. Instead, the article provides a coherent, entry-level lesson on cracking wireless networks using the tools freely available in Kali. There is very little to distinguish this academic paper from an entry-level tutorial on black-hat hacking. Overall, in my opinion, the article effectively introduces the reader to the processes, technologies, and tools involved in cracking wireless networks using Kali Linux.

Conclusion

The articles presented in this research paper provide a glimpse into the ethical hacking field. Ethical hackers must have a thorough grounding in ethics and morals, otherwise, they may be tempted to use their skills in unethical ways. Hackers must possess strong technical skills, and educational institutions that train future security professionals should teach those skills. However, schools should also tightly integrate ethics into the curriculum. Finally, a hacker can find a tremendous amount of useful information and resources—including free tools—on the

internet. Many of these resources are documented in academic papers. One valuable technical resource is the Kali Linux distribution, which provides a plethora of penetration testing and network analysis tools.

References

Babincev, I. M., & Vuletić, D. V. (2016). Web Application Security Analysis Using the Kali Linux Operating System. *Military Technical Courier / Vojnotehnicki Glasnik*, *64*(2), 513–531. Retrieved from https://doi-org.library3.webster.edu/10.5937/vojtehg64-9231

ČISAR, P., & ČISAR, S. M. (2018). Ethical Hacking of Wireless Networks in Kali Linux Environment. *Annals of the Faculty of Engineering Hunedoara - International Journal of Engineering*, *16*(3), 181–186. Retrieved from https://library3.webster.edu/login?url=https://search-ebscohost-com.library3.webster.edu/login.aspx?direct=true&db=a9h&AN=131841584&site=ehost-live

Hartley, R. D. (2015). Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack. *Journal of International Technology & Information Management*, *24*(4), 95–104. Retrieved from https://library3.webster.edu/login?url=https://search-ebscohost-com.library3.webster.edu/login.aspx?direct=true&db=bth&AN=122400154&site=ehost-live

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. *Journal of Management*

Information Systems, *34*(4), 1023–1053. Retrieved from https://doi-org.library3.webster.edu/10.1080/07421222.2017.1394049

Xu, Z., Hu, Q., & Zhang, C. (2013). Why Computer Talents Become Computer Hackers. *Communications of the ACM*, *56*(4), 64–74. Retrieved from https://doi-org.library3.webster.edu/10.1145/2436256.2436272