Benefits of Ethical Hacking

Topic 1: Ethical Hacking

Discuss the main benefits and risks of ethical hacking. Provide examples and/or details to support your ideas. If you have seen examples of ethical hacking, please share these with the group.

Edward Jackson

3/28/2015 4:43:41 PM

A hacker is as a hacker does

I would like to start by saying, being a hacker---or hacking---does not have to be bad. From an academic/professional point of view, learning hacking can allow IT professionals to build safer, stronger computer network systems. From a software development point of view, understanding the mind of a criminal hacker can allow companies and development teams to design better, more secure software. Now, if we look at what the term “hacker” has come to mean, it conjures up teenagers drinking Jolt cola, breaking into computers and networks to plant viruses or steal private data. Paul Graham (2004) suggests to hack and to be a hacker has numerous meanings, and it really depends upon the context on whether the meaning is good or bad (Graham, 2004). I believe, like most things in life, this is a more practical way to look at hacking---hacking in general. To me, intent is everything. Intent is good enough to work for our judicial system; it should be good enough to address the many levels and aspects of hacking.

Something I would like to point out, “hacking” existed long before computers. I guess when people mention hackers today, what they really mean is a computer hacker, and more specifically, a black hat computer hacker. According to Hoffman (2013), there are three types of hackers: White hat, black hat, and gray hat (Hoffman). White hat hackers hack for good, and hack in defense of corporate/business computer networking systems. A gray hat hacker may do things questionable in nature, but not to intentionally hurt people or damage systems, unless there is an actual positive outcome. A black hat hacker will exploit computers and networks, without having a good reason, or caring about a positive outcome.

On one hand, I see how society could fear hackers, after all, when the nightly news covers a hacking story, 100% of the time it is bad. Thus, all hacking and hackers are getting a bad repetition. However, the reality of things, is that the world needs “ethical” hackers. Without those that really understand the mind of a hacker, business systems are at serious risk. By serious risk, I mean all computer security is hopelessly, laughably,

left in the hands of criminals. If you were to ask any business out there, would they willingly hand over their company passwords to criminal hackers, I am sure they would respond with an immediate NO. They would probably look at you like you are crazy. However, by not employing ethical hackers to properly test all computing and networking equipment, that is exactly what companies are doing. Try as they will, there is no way an average security officer is prepared for an outside attack (or internal one for that matter), if that attack is being launched by black hat hackers. If you think about it just for a minute, you should be scared. This all leads to this statement, without ethical hackers, the businesses of today (and tomorrow), are guaranteed to have compromised computer networking systems. Here is yet another frightening fact, according to Hoover (2012)---from InformationWeek DARKReading---cyber terrorism is on the rise, and pose one of the greatest threats to national security. This further supports my claim that the world, especially the United States, needs ethical hackers.

Now, time for some real world experience. The year was 2006, and I was working in Healthcare IT (I spent some 9 years in Healthcare IT). Of course, computer network security was our main concern. The problem was, our security knowledge was limited to reading best practices and off-the-shelf, professional training books. We implemented security mechanisms to computers and network based upon what we had read. The problem was, we had no idea whether or not if the security was working, if it could be easily broken into, or had holes in it. This led to me to seek “ethical” knowledge on testing security. One technology certification that was gaining in popularity at the time was from EC-Council, the Certified Ethical Hacker. The idea of an ethical hacker made me laugh at the time, at least from a training perspective. That was, until I started digging into the material, and learning all the things I did not know. Without explaining too much, let’s just say, I basically knew nothing about penetration testing, cracking passwords, how viruses worked, capturing data flying through the air over wireless, etc. The course was a real eye-opener. Before the CEH certification, I had taken the Security+, offered by CompTIA. After the Security+ certification, I thought I knew how to protect computer systems. I was wrong. The CEH offered knowledge that pretty much no one wanted to talk about, other than perhaps black hat hackers. I spent many years after that working on hardening hardware and software, performing pen testing, and testing the strength of security. To say the least, I fully support educating---those that have passed background checks---on what ethical hacking means. These days, I’m nowhere near a security officer, I work as a computer systems engineer. But, let me tell you, just having the CEH certification, and some kind of experience with security, has made all my technology-based solutions much better. I’m always thinking in the back of mind when I create something, how it could possibly be exploited. Thus, I believe the main advantages of ethical are preventing exploits (at all levels in a business), properly securing computers and networks, and learning how to test security, in the

same ways a black hat may use to compromise security.

References

Graham, Paul. (2004). The word “hacker”. Retrieved from http://www.paulgraham.com/gba.html

Hoffman, Chris. (2013). Hacker hat colors explained: Black hats, white hats, and gray hats. Retrieved fromhttp://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Hoover, Nicholas. (2012). Cyber Attacks becoming top terror threat, FBI says. Retrieved fromhttp://www.darkreading.com/risk-management/cyber-attacks-becoming-top-terror-threat-fbi-says/d/d-id/1102582?

Edward Jackson
reply to student

3/25/2015 9:01:32 PM

RE: Ethical Hacking

Your points on who an ethical hacker is, and what are considered advantages and disadvantages of "ethical" hacking, are spot on for a modern definition. For as long as I can remember (I’m a little old school), hacker meant someone who deconstructs things, tears things apart to learn how they work, and a person who was interested in things that most people took for granted. I actually knew people who were electronic hackers, mechanical hackers, and even food hackers…all of which had nothing to do with criminal activity. However, these days, hacker definitely means something nefarious. I consider myself a computer systems engineer (my actual job title), but many of the software/hardware tasks that come my way have been deemed “impossible.” This usually means I have to “hack” until I arrive at a solution. It’s a wonderful job really. Anyway, I do believe there is a place in this world for ethical hackers. I’m excited to be taking this course.

Edward Jackson

3/26/2015 9:30:41 PM

reply to student

RE: Topic 1: Ethical Hacking

You made several good points about hackers and ethical hacking. I completely understand why a person would take up and learn ethical hacking, or hacking in a non-criminal way. Part of my job as a computer system engineer is to deconstruct technology, and figure out workarounds and fixes to current software and hardware problems. You could consider this a form of hacking. What I don't understand, is why people would damage computer and network systems, the very systems that allow society to function. What exactly does a person gain by hacking a healthcare system and putting someone's private medical information on the internet? I think our government needs to do a lot more to protect this country's computer and network systems. This means even from spam, all forms of malware, and spyware. I believe we need harsher penalties for computer-related crimes. Anyway, your write up was good. I look forward to corresponding further with you throughout the course.

Introduction to Ethical Hacking

An ethical hacker is a security expert who attacks a system on behalf of the system's owners. This course focuses on discovering network vulnerabilities that a malicious hacker can exploit. The course explores penetration testing; footprinting and social engineering; scanning and enumeration; operating system weaknesses; and the methods used to hack Web servers and wireless networks. Students perform hands-on projects using state-of-art hacking tools and techniques.

Outcomes

After completing this unit you should be able to:

- Discuss the concept of ethical hacking.
- Document an attack and penetration test plan.
- Compile preliminary reconnaissance information.

Course outcomes practiced in this unit:

IT542-1: Perform vulnerability tests using computer and network tools and utilities.

What do you have to do in this unit?

- Complete assigned Reading.

- Participate in Discussion.
- Complete unit Assignment.
- Participate in Seminar or Alternative Assignment.
- Complete the unit Quiz.
- Complete the optional Learning Activity.

Read the following chapters in your textbook:

Chapter 1: Hacking: “The Next Generation”

Chapter 2: “TCP/IP Review”

Chapter 3: “Cryptographic Concepts”

The Reading begins by introducing you to ethical hacking and explaining the role that ethical hackers play in securing information systems in the modern enterprise. There are similarities between ethical hacking and other forms of hacking, but also distinct differences. The Reading reviews networking concepts and technologies, with a focus on TCP/IP. The Reading on networking should be a review of knowledge you already gained in your previous courses. The Reading concludes with an introduction of key concepts from cryptography that are important to understand, since hacking often involves circumventing the security measures intended by cryptographic techniques.

Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allow you to come together in real time with your fellow classmates. You must either attend the live Seminar or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

Option 1: Attend the Seminar:

During the Seminar, the instructor will briefly review the course Syllabus. The instructor will also review the first lab, preview the upcoming lab, and lead a discussion on the virtual lab environment used for the lab activities.

Option 2: Alternative Assignment:

You will benefit most from attending the graded Seminar as an active participant. However, if you are unable to attend you have the opportunity to make up the points by completing the alternative assignment.

The alternative assignment consists of reviewing the recording from the live Seminar and then submitting a paper of at least three double-spaced pages that presents an overview of the topics covered during the Seminar. The paper must include at least one citation to a research paper relating to one of the topics from the Seminar. Your paper should be in APA format and cite all references used. Submit to the Seminar Dropbox.

Assignment 1

Outcomes addressed in this activity:

Unit Outcomes:

- Discuss the concept of ethical hacking
- Document an attack and penetration test plan
- Compile preliminary reconnaissance information

Course Outcome:

IT542-1: Perform vulnerability tests using computer and network tools and utilities.

Assignment 1

Outcomes addressed in this activity:

Unit Outcomes:

- Discuss the concept of ethical hacking
- Document an attack and penetration test plan
- Compile preliminary reconnaissance information

Course Outcome:

IT542-1: Perform vulnerability tests using computer and network tools and utilities.

Assignment Instructions:

This Assignment provides the hands-on element to your studies. It gives you the opportunity to gain practical experience using the tools and techniques associated with ethical hacking. Read and perform the lab entitled "**Lab 1: Assessing and Securing Systems on a Wide Area Network (WAN)**" found in Doc Sharing. Complete all five parts of Lab 1. Compile your lab report in a Word® document with a title page, labeling all screenshots you are required to capture, and including explanatory text where needed or required by the lab. Within your Word document, after your lab report, answer the Assessment Worksheet questions listed at the end of the lab. Conduct research and cite supporting sources in APA format where appropriate.

Directions for Submitting Your Assignment:

Save your Word document containing your lab report and Assessment questions using the following file name format: Username-IT542-Assignment -Unit#.docx (Example: **TAllen-IT542 Assignment-Unit1.docx**). Submit your file to the Unit 1 Assignment Dropbox by the end of Unit 1.

Assignment Requirements:

All lab steps are completed, including screenshots and explanations where required. Assessment question answers contain sufficient information to adequately address the questions. The lab report and answers are accurate and complete, as well as free from grammar and spelling errors.

For more information and an example of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable Assignments and Discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity.

Black-box testing: A kind of testing of a computer system in which the testing team must approach it like a “black box,” with no prior knowledge of it.

White-box testing: A kind of testing in which the testing team is given advance knowledge of the system to be tested; contrasts with “black-box testing.”

Exploit: A piece of software, data, or other similar item that can take advantage of a vulnerability or weakness inherent in a system.

Vulnerability: The absence or weakness of a safeguard in an asset.

Ethical hacker: Someone who knows how hacking works and understands the dangers it poses but uses those skills for good purposes: often known as a “white-hat hacker.”

Asymmetric encryption: An algorithm that uses a pair of cryptographic keys to perform encryption/decryption functions on information. These keys, and the algorithms that use them, have a unique property: If one key is used to perform an operation, its companion key is the only one that can reverse the operation.

Symmetric encryption: Encryption that uses the same key to encrypt and to decrypt information.

Hash (or hash value): The unique number produced by a hash algorithm when applied to a dataset. A hash value verifies the integrity of data.

Brute-force attack: An effort to break something such as a password by using all possible combinations of characters until a combination works.

Dictionary attack: An attack in which a predefined list of words is tried to see whether one of them is a user's password.