

Pros of an Ethical Hacking Course

Thorna Humphries
January 22, 2009

Information Assurance Symposium
Hampton University

Quote by John Viega and Gary McGraw
Building Secure Software

“Do we call locksmiths burglars just because they could break into our house if they wanted to do so? Of course not. But that’s not to say that locksmiths can’t be burglars. ...”

Term--Hacker

- Originally had a positive connotation
 - ▣ Sprang up in computer science community at MIT in late 1960s
 - ▣ Referred to people who were exceptional programmers
 - ▣ McGraw compares a hacker to MacGyver (star of television show in 80's)
 - Solves tricky or hard problems through programming like MacGyver got out of tight spots as an agent using his mind and everyday tools such as fishing lines, a match book, etc.



Hacker – The Negative Connotations

- Software Engineering
 - ▣ Programmer who solved programming problems in an ad hoc fashion
- Common definition
 - ▣ A person that maliciously tries to break software



Reality, Now

- White hat hackers
 - ▣ Penetrate systems to understand vulnerabilities in systems on behalf of clients within ethical standards

Definition of Ethical Hacking

- According to Security Search,

Ethical hacking is penetration testing, intrusion testing and red teaming to detect vulnerabilities in a system.

Pros for the Development of an Ethical Hacking Course

- The need for companies to protect their information and that of their customers
- A proven approach in other industries
 - ▣ The same premise as the automobile industry (e.g. crash testing) and the military branches
- More experts needed as security professionals (e.g., system and network administrators)
- Knowledge gained will enable individuals to protect and guard their systems and networks from common attacks

Pros (Continued)

- Technical knowledge is available for creating viruses, students need to understand the attacks and how to prevent them in an ethical and organized manner.
- Knowledge of hacking skills and practices improves security

Course Content

- An approach or process to ethical hacking
 - ▣ Design exercises that teach information on the development of security audits that can provide constant assessment of system vulnerabilities
- Risk management analysis
 - ▣ The incorporation of known vulnerabilities of the system compared with IT governance policies and procedures and best practices
- Ethical obligations
 - ▣ Class policies to dissuade improper forms of hacking
- The consequence of malicious hacking from a legal perspective
- Identification of threats and countermeasures with lab exercises
 - ▣ Include exercises that are similar to attacks that security administrators must identify and rectify

Laboratory Design

- A closed laboratory that simulates a corporate system (best case scenario) and allows
 - Simulating a broad range of real-world vulnerabilities
 - Assessments of vulnerability
 - Testing defenses against attacks
 - Implementing tool sets
- A controlled environment that has been designed in consultation with IT security specialist on university campus

References

- Patricia Logan and Allen Clarkson, “Teaching Students to Hack: Curriculum Issues in Information Security” *SIGCSE’05*, February 2005, St. Louis, Missouri
- Syed Saleem, “Ethical Hacking as a risk management technique”, *InfoSecCD Conference’06*, September 2006, Kennesaw,GA.
- John Viega and Gary McGraw, *Building Secure Software: How to avoid the Security Problems the Right Way*, Addison-Wesley, 2002.

Questions

