Certified Ethical Hacking

Ron Woerner, CISSP, CEH

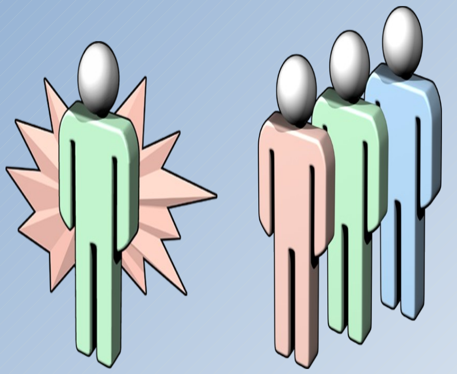
Agenda

- Is computer hacking necessary?
- What is a Certified Ethical Hacker?
- Is that an oxymoron?
- What I learned
- Cool stuff from the class
- The Exam
- Importance of certifications

Two Questions

- Why are you here?
- Why am I here?

Why you need to know



Defenders vs. Attackers

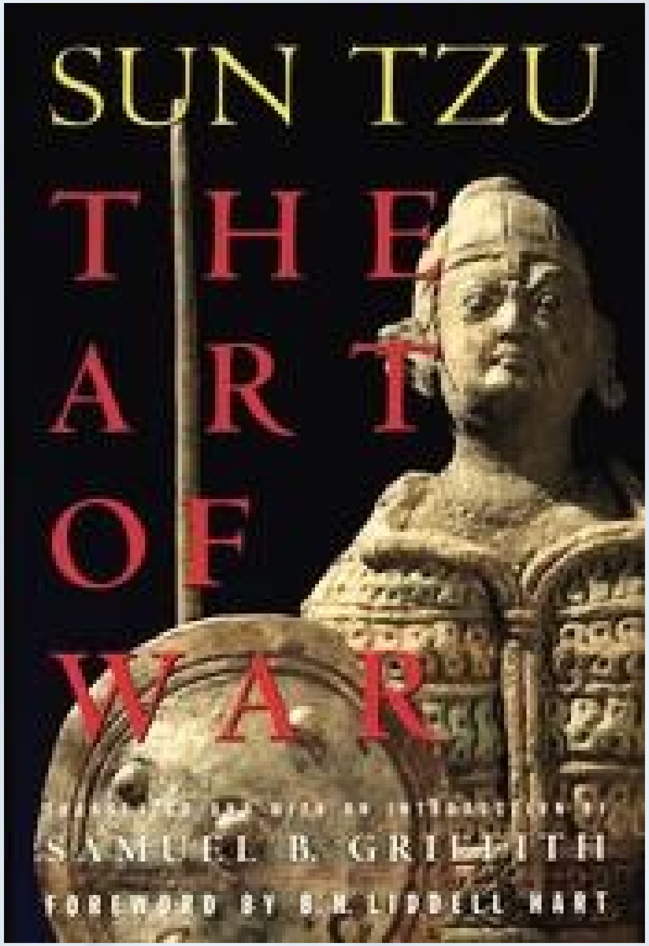
- Attacker needs to understand only one security issue
- Defender needs to secure all entry points
- Attacker has unlimited time
- Defender works with time and cost constraints

Why you need to know

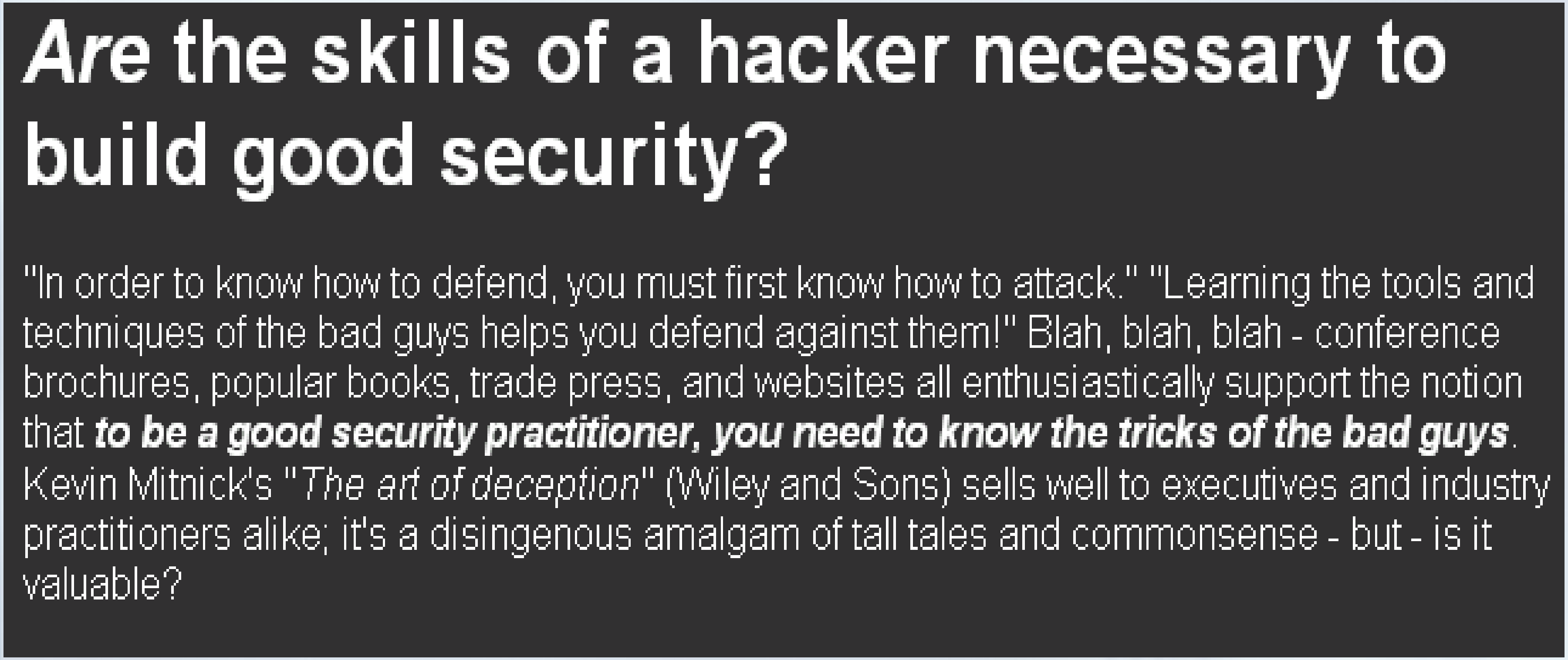
"*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*"

—Sun Tzu,

Art of War



From Marcus Ranum



Are the skills of a hacker necessary to build good security?

"In order to know how to defend, you must first know how to attack." "Learning the tools and techniques of the bad guys helps you defend against them!" Blah, blah, blah - conference brochures, popular books, trade press, and websites all enthusiastically support the notion that ***to be a good security practitioner, you need to know the tricks of the bad guys***. Kevin Mitnick's "*The art of deception*" (Wiley and Sons) sells well to executives and industry practitioners alike; it's a disingenous amalgam of tall tales and commonsense - but - is it valuable?

http://www.ranum.com/security/computer_security/index.html

Understand this (1):

- Hacking skills are good for the here and now;
- Knowledge of Security Principles are needed for the hereafter;
- Both are required to be an information security professional.

Understand this (2):

- "In a nutshell, security is now about risk management."
- Penetration / vulnerability testing is an element of the risk assessment.
- It is critical to balance the risks based on business decisions
- Degrees of separation
- The building of multiple layers

Understand this (3):

- CEH Helps you
  - Identify risks, vulnerabilities, threats and weaknesses;
  - Determine monitoring needs and incident response;
  - Sell Security

Certified Ethical Hacker

Defend your Network Against Hackers.

Master the Hacking Technologies.

Become a Certified Ethical Hacker.

Ethical Hacking and Countermeasures

http://www.eccouncil.org

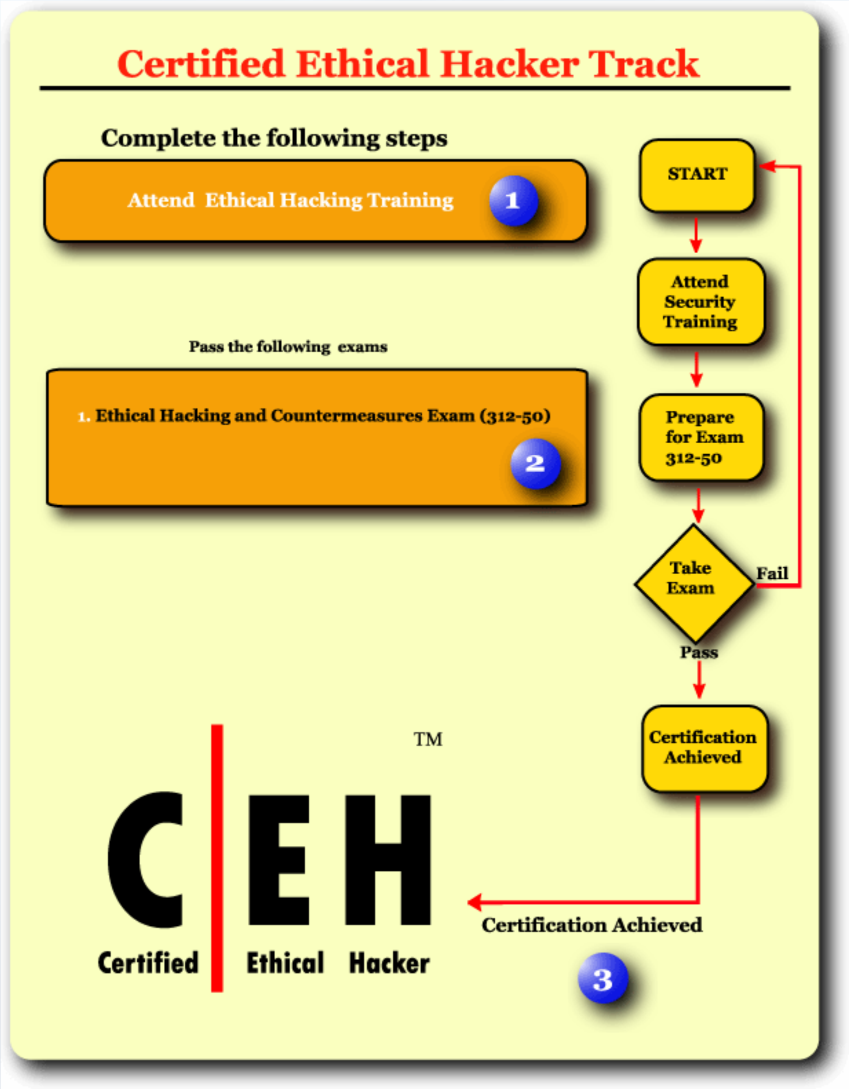
EC-Council

Certified Ethical Hacker

“If you want to stop hackers from invading your network, first you’ve got to invade their minds.”

- Ethical Hacking & Countermeasures course
- “Official” certification from EC-Council (http://www.eccouncil.org)

Certified Ethical Hacker



Certified Ethical Hacker Track

Complete the following steps

Attend Ethical Hacking Training 1

Pass the following exams

1. Ethical Hacking and Countermeasures Exam (312-50) 2

Certification Achieved 3

Can Hacking be Ethical (and can you really be certified in it)?

IT DEPENDS

Can Hacking be Ethical (and can you really be certified in it)?

- The noun '*hacker*' refers to a person who enjoys learning the details of computer systems and stretch their capabilities.
- The verb '*hacking*' describes the rapid development of new programs or the reverse engineering of already existing software to make the code better, and efficient (and more secure).
- The term '*cracker*' refers to a person who uses his hacking skills for offensive (malicious) purposes.
- The term '*ethical hacker*' refers to security professionals who apply their hacking skills for defensive purposes.

EC-Council Code of Ethics

EC-Council Code of Ethics

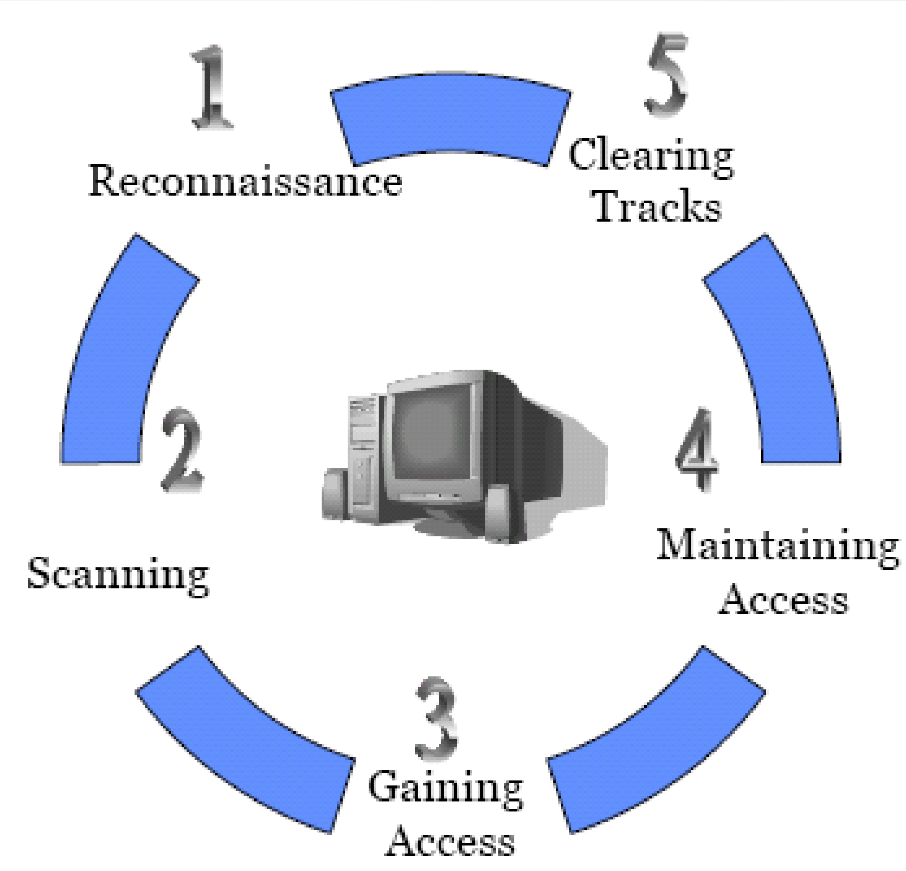
In other words, don’t be stupid.

Ethical Hacking

- Ethical hackers try to answer:
  - What can the intruder see on the target system? (Reconnaissance and Scanning phase of hacking)
  - What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
  - Does anyone at the target notice the intruders attempts or success? (Reconnaissance and Covering Tracks phases)
- If hired by any organization, an ethical hacker asks the organization *what* it is trying to protect, *against whom* and *what resources* it is willing to expend in order to gain protection.

Hacking 101

1. Reconnaissance (legal)
   1. Active / passive
2. Scanning (legal?)
3. Gaining access (illegal)
   1. Network level
   2. O.S. level
   3. Application level
4. Maintaining / Escalating access (illegal)
5. Covering Tracks (illegal)



Class Modules

1. Legality
2. Footprinting
3. Scanning
4. Enumeration
5. System Hacking
6. Trojans & Backdoors
7. Sniffers
8. Denial of Service
9. Social Engineering
10. Session Hacking
11. Hacking Web Servers

1. Web App Vulnerabilities
2. Web-based password cracking
3. SQL injection
4. Hacking Wireless Nets
5. Virus
6. Physical Security
7. Linux Hacking
8. Evading IDS, etc.
9. Buffer Overflows
10. Cryptography
11. Pen Test Methodologies

Footprinting

- Web tools
  - www.samspade.org
  - www.dnsstuff.com
  - www.netcraft.com
  - Web site archives: www.archive.org (wayback machine)
  - People Search: www.intellius.com
- Tools
  - Whois (www.networksolutions.com) (Free)
  - Nslookup (Free)
  - ARIN (http://www.arin.net/whois) (Free)
  - Traceroute (Free)
  - Visual Route (http://www.visualroute.com/) ($$)
  - SmartWhois (www.tamos.com) ($$)

Scanning – Port & Ping

- NMap / NMapWin (Free)
- HPing2 (UNIX) (http://www.hping.org/) (Free)
- Superscan (Free)
- Firewalk (UNIX) (http://www.packetfactory.net/firewalk/) (Free)
- WPSweep (http://ntsecurity.nu/toolbox/ipsecscan/) (Free)
- IPSec Scan (http://ntsecurity.nu/toolbox/ipsecscan/) (Free)
- Cheops (UNIX) (http://cheops-ng.sourceforge.net/) (Free)
- NetScan Tools Pro (www.netscantools.com) ($$)

Scanning – Vulnerability

- NESSUS (UNIX) (www.nessus.org) (Free)
- GFI LANGuard (www.gfi.com/downloads) ($$)
- Retina (http://www.eeye.com/retina) ($$)
- SAINT (UNIX) (www.saintcorporation.com/saint/) ($$)
- ISS Security Scanner (www.iss.net) ($$)
- SATAN (UNIX) (Free)
- Nikto web scanner (http://www.cirt.net/code/nikto.shtml) (Free)

Enumeration

- DumpSec (www.systemtools.com/somarsoft) (Free)
- Winfo (http://ntsecurity.nu/toolbox/winfo/) (Free)
- Enum (http://www.bindview.com/services/razor/utilities/) (Free)
- GetAcct (www.securityfriday.com)
- SolarWinds (www.solarwinds.net/) ($$)
- Winfingerprint (winfingerprint.sourceforge.net/) (Free)
- NetBIOS Auditing Tool – NAT () (Free)

System Hacking

- Cracking Passwords
  - Smbbf – SMB Bruteforcer (Free)
  - L0phtcrack ($$)
  - RainbowCrack (http://www.rainbowcrack.com/) (Free)
  - KerbCrack (http://www.ntsecurity.nu/toolbox/kerbcrack/) (Free)
  - Legion (Free)
  - John the Ripper (http://www.openwall.com/john/) (Free)
  - Cain & Abel (www.oxid.it) (Free)
- Executing Applications
  - Psexec (http://www.sysinternals.com/Utilities/PsTools.html) (Free)
  - Netcat (http://netcat.sourceforge.net/) (Free) (video)

Web Hacking – Cracking Passwords

- Cracking Passwords
  - Authforce (kapheine.hypa.net/authforce/) (Free)
  - Brutus (www.hoobie.net/brutus/) (Free)
  - WebCracker (Free)
  - PassList (Free)
- SQL Injection
  - SQLScan (www.foundstone.com/resources/overview.htm) (Free) (video)
  - Manual techniques

Web Application Hacking

- Instant Source (www.blazingtool.com/) ($$)
- Gnu Wget (www.gnu.org/software/wget/wget.html) (Free)
- Websleuth (www.geocities.com/dzzie/sleuth/) ($$)
- Black Widow (softbytelabs.com) ($$)
- Burp Suite (portswigger.net/) (Free)
- WebGoat (www.owasp.org) (Free)
- WebScarab (www.owasp.org) (Free)

Class Modules

1. Legality
2. Footprinting
3. Scanning
4. Enumeration
5. System Hacking
6. Trojans & Backdoors
7. Sniffers
8. Denial of Service
9. Social Engineering
10. Session Hacking
11. Hacking Web Servers

1. Web App Vulnerabilities
2. Web-based password cracking
3. SQL injection
4. Hacking Wireless Nets
5. Virus
6. Physical Security
7. Linux Hacking
8. Evading IDS, etc.
9. Buffer Overflows
10. Cryptography
11. Pen Test Methodologies

Link to CEH Brochure

The CEH Exam

The examination tests you on security related concepts, hacking techniques and technology. You will be asked to decipher exploit codes, study log files, infer output and apply the knowledge acquired through the course.

- Exam length: 125 questions
- Time length: 3 hours
- Passing score: 70%
- Web-based
- Can be taken anytime
- No recertification necessary

The CEH Exam – Sample Questions

What is the essential difference between an “Ethical Hacker” and a “Cracker”?

A. The ethical hacker does not use the same techniques or skills as a cracker.

B. The ethical hacker does it strictly for financial motives unlike a cracker.

C. The ethical hacker has authorization from the owner of the target.

D. The ethical hacker is just a cracker who is getting paid.

Answer: C

The CEH Exam – Sample Questions

This tool is a a file and directory integrity checker. It aids system administrators in monitoring a designated set of files for any changes.

A. NMap
B. Integricheck
C. DSniff
D. Cybercop Scanner
E. Tripwire

Answer: E

The CEH Exam – Sample Questions

Netcat is a simple network utility which reads and writes data across network connections, using TCP or UDP protocol. Which of the following command scans for open ports between [1 - 140]?
(Select the Best Answer)

A. nc -xx -q -w2 my-attacker-IP-address [1-140]
B. nc -vv -z -w2 my-attacker-IP-address 1-140
C. nc my-attacker-IP-address (1,140)
D. nc 140 my-attacker-IP-address -vv

Answer: B

The CEH Exam – Sample Questions

Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by an IDS? (Select the Best Answer)

A. SYN scan
B. ACK scan
C. RST scan
D. Connect scan
E. FIN scan

Answer: D

What I got from it

- A great way to get out of work for a week and play with hacking tools
- A cool set of tools & toys
- Another free t-shirt
- A way to prove knowledge (& ability)
- Another TLA after my name

Final thoughts

- Overall, CEH is a good experience.
- It provides for a well-rounded information security background.
- There is no silver bullet for security.
- Penetration testing / Hacking is only part of the risk management cycle.
- “Security is about risk management”

What you really get

Ron Woerner, CISSP, CEH

ron.woerner@conagrafoods.com