Computer Security and Penetration Testing

Chapter 1
Ethics of Hacking and Cracking
Objectives

- Understand how the act of unethical computer hacking is a crime
- Classify and identify groups and classes of hackers
- Distinguish the rationale for various types of hackers
Objectives (continued)

- Understand and determine differences in information warfare
- Understand how computer hacking originated and its evolution
- Recognize the importance of ethical hacking and the issues involved in hacker ethics
The Impact of Unethical Hacking

- **Computer cracking**
  - Term for illegally hacking into a computer system without the permission of the system’s owner

- Despite the motivations of computer **crackers**
  - Cracking a system is a crime
Hacker Communities

• Two ways commonly used to categorize hackers
  • White Hat good hackers vs. Black Hat bad hackers
  • Based loosely on psychological profiling
Hat Categories

- White Hat/Black Hat model
  - White hats represent the “good guys”
  - Black hats represent the “bad guys”
- Everything the good guys do is right, legal, and justified
- “Gray Hat” hackers
  - Evidence that the dichotomy of good and evil is NOT a very good fit to the real world
Hat Categories (continued)

<table>
<thead>
<tr>
<th>Motivations and Goals</th>
<th>White Hat Hackers</th>
<th>Grey Hat Hackers</th>
<th>Black Hat Hackers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Learning new things, protecting the network in their charge from intrusion or damage, maintaining status quo. Work with official sanction from official organizations.</td>
<td>Fame, credit for solving challenging network puzzles. More interested in damage than pillage. Hacktivists who deface Web sites and networks of target &quot;evil-doers&quot; (e.g., corporations involved in fur trade, tobacco sales, abortion, etc.) are part of this group.</td>
<td>Cash payments, injury to others. May steal trade secrets, credit card numbers, customer lists, employee lists. They want whatever information they can find that will generate a profit. They work with unofficial sanction from official and unofficial organizations.</td>
</tr>
</tbody>
</table>

Figure 1-1  Black Hat/White Hat model
Hacker Profiling

- Hacking requires that the practitioner be intimately familiar with the techniques of the perpetrator
  - Or opponent
- Reading and techniques used by both ethical and malicious hackers are identical
- Profile of a hacker is multifaceted
- Black Hat Briefings convention
  - Highlights breaking security research submitted by leading corporate professionals, government experts, and members of the underground hacking community
<table>
<thead>
<tr>
<th>Hacker Profile</th>
<th>Description</th>
</tr>
</thead>
</table>
| Novices                     | Limited computer and programming skills.  
Rely on toolkits to conduct their attacks.  
Can cause extensive damage to systems because they often don’t understand how attacks work.  
Looking for media attention. |
| Cyber-punks                 | Capable of writing their own software.  
Have an understanding of the systems they are attacking.  
Many are engaged in credit card number theft and telecommunications fraud.  
Have a tendency to brag about their exploits. |
| Internals                   | a) Disgruntled employees or ex-employees  
May be involved in technology-related jobs.  
Aided by privileges they have or were assigned as part of their job function.  
These hackers pose the greatest security threat.  

b) Petty thieves  
Include employees, contractors, consultants.  
Motivated by greed, or need to pay off habits, such as drugs or gambling.  
Opportunistic; take advantage of poor internal security,  
Computer literate. |
| Old guard hackers           | Appear to have no criminal intent.  
Alarming disrespect for personal property.  
Appear to be interested in the intellectual endeavor. |
| Coders                      | Act as mentors to newbies.  
Write scripts and tools that others use.  
Motivated by a sense of power and prestige.  
Dangerous; have hidden agendas, use Trojan horses. |
| Professional criminals      | Specialize in corporate espionage.  
Guns for hire.  
Highly motivated, highly trained, have access to state-of-the-art equipment. |
| Information warriors/      | Increase in activity since the fall of many Eastern Bloc intelligence agencies.  
Well funded.  
Mix political rhetoric with criminal activity. Political activists,  

cyber-terrorists           |                                                                                                                                 |
| Hacktivists                 | Work to eradicate or damage entities or causes they perceive to be evil.  
Mix political rhetoric with criminal activity. Political activists,  
Engage in hacktivism.        |

**Figure 1-2** Hacker profiles
Hacker Motivations

- Curiosity
- Love of puzzles
- Desire for recognition or fame
- Revenge
- Financial gain
- Patriotism or politics
Ethical Hacking

- Ethics are the principles of conduct that govern individuals, groups, and professions.
- Without a published code of ethics, it is difficult to gain public trust for a profession.
- **Network security** is emerging from a chaotic set of conflicting ethics.
- Separating the ethical hacker from the unethical cracker:
  - Will allow security professionals to present the benefits of their profession.
Evolution of Hacking

- The modern concept of hacking began in the late 1950s
  - Students at the Massachusetts Institute of Technology started using their access to the MIT mainframe
    - To work on new languages
- First password hacks were a response to the Compatible Time Sharing System (CTSS)
  - Developed in the early 1960s
Evolution of Hacking (continued)

- In the 1970s phone phreaks used **phreaking** to access telephone networks
  - To make free calls from payphones
- In the 1980s
  - **War dialers** were developed to search for open modems
  - Personal computer prices dropped and users became more common
  - Hacker communities also grew
  - Viruses, worms, and Trojans started appearing in 1988
Evolution of Hacking (continued)

- Antisocial actions of crackers and script kiddies made it difficult to defend the original concept of hacking
  - “Computer hacker” describes computer experts with malicious intent
Vendor-Neutral Security Certifications

- Security certificates and issuing bodies
  - CompTIA Security+™ Certification
  - Global Information Assurance Certification (GIAC), Security Administration Certifications
  - ISC² Certifications
  - Associate of (ISC)²
  - SSCP Examination
Vendor-Neutral Security Certifications (continued)

- Security certificates and issuing bodies (continued)
  - CAP Examination
  - CISSP Examination
  - CISSP Concentrations
  - EC-Council Certifications
Vendor-Specific Security Certificates

- There are almost as many vendor-specific certificates as there are network vendors
- Cisco’s CCNA, and Microsoft’s MSCE
  - Useful to newcomers to the network security industry
What Needs to Be Secured

- Protection of data provided to organizations or stored on personal computers is a high priority.
- Some crackers break into systems to utilize what they consider wasted computer energy.
- Using bandwidth without permission may seem harmless.
  - But it is a crime, in addition to being unethical.
- Many hackers find it tempting to copy, download, and use proprietary software and other copyrighted works.
What Needs to Be Secured (continued)

- Ethical Issues of Hacking
  - Professional hackers have a responsibility to society
    - Their activities should help to build and improve upon existing technology
    - They should use their skills and interests as opportunities to learn and to teach
  - Ethical hacker
    - A security professional who applies his or her hacking skills for defensive purposes
What Needs to Be Secured (continued)

- Ethical Hacking and System Security
  - Some companies prefer to pay an ethical hacker to discover their systems’ weaknesses and security gaps
  - Ethical hackers work to protect all areas of information technology
  - Hackers must have experience in software engineering, network engineering, and system security
Summary

- Computer cracking is illegally hacking into a computer system without the permission of the system’s owner
- Hackers are commonly thought of in two groups: White Hat and Black Hat
- Nine major profiles of hackers
- The techniques used by ethical and malicious hackers are similar
- Hackers may be motivated by curiosity, puzzles, fame, revenge, money, or patriotism
The modern concept of hacking began in the late 1950s.

While there are several vendor-neutral and vendor-specific certifications available to computer security professionals, there is no national certification standard.

Professional security experts, technologists, and hackers must develop a public code of ethics.

An ethical hacker is a security professional who applies hacking skills for defensive purposes.