* certified ethical hacking
* Competitions or conferences related
  + Security
  + Techniques
  + Certification
  + Pwn2Own
* Career
  + Employment
  + Certifications
  + What it means for the quality of work done
* Tools
  + Traditional methods and applications (old)
    - Rootkits, root-access
    - Stack overflow
  + Newer methods and devices (new)
    - Exploits in mobile devices (http://mobile.slashdot.org/article.pl?sid=09/03/25/1238246)
    - Wifi capabilities and repercussions (handwritten apps, wardriving)
    - Browser exploits (ASP)
  + Social-related techniques
    - Social engineering
    - Gaining physical access

PowerPoint outline:

1. Introduction
   1. Purpose of this presentation
      1. Growing interest in topic as graduation approaches and graduate school / career choices grow
   2. What not to expect
      1. Technical details about hacking techniques
   3. What to expect
      1. Exploration of hacking: motivations, evolutions
2. Hacking
   1. Definition
      1. Origin of term (hack) refers to description of quick, unrefined, and unsupported solutions to technical problems. M-W: a usually creative solution to a computer hardware or programming problem or limitation
      2. M-W: to write computer programs for enjoyment
      3. M-W: to gain access to a computer illegally
      4. Both definitions describe the general attitude of the hacker, but the second one is what draws attention and hostility
   2. Motivations
      1. Material gain
         1. Stealing personal information via scam, fraud, phishing
         2. Selling information
         3. Prestige and accomplishment for a job well done
      2. Vendetta
         1. Response to personal loss or defacement
      3. Moral objection or statement
         1. Vandalism in response to trials for The Pirate Bay
            1. International Federation of the Phonographic Industry
         2. (http://blog.wired.com/27bstroke6/2009/02/ifpi-site-hacke.html)
      4. Improvement in security standards
         1. The only motivation that has legal backing, and only when carried out by certified hackers
3. Hackers
   1. Definition
      1. one that hacks
      2. an expert at programming and solving problems with a computer
      3. a person who illegally gains access to and sometimes tampers with information in a computer system
      4. Given these definitions and the ones for hacking, we can understand the following classifications of hackers.
      5. Expanded as a social term: a member of the subculture associated with the act of hacking
   2. Classifications
      1. Black hat
         1. "Villain" in contrast to "Hero" (white hat)
         2. Penetration testing refers to unauthorized access
            1. Due to exploiting known security flaw, rootkit implementation, packet sniffing, etc
         3. Performs unauthorized hack for reasons previously mentioned
         4. Group given responsibility for majority of malicious software (viruses, worms, spam)
         5. AKA crackers (as in software or password crackers)
            1. Breaking DRM or copy protection software (is this still truly bad?)
      2. Grey hat
         1. "True neutral" in D&D alignment
         2. Faces ethical dilemma upon discovery of security flaw
            1. Report and face possible charges for illegal action
            2. Fix flaw quietly if possible
            3. Leave unattended at the risk of the flaw's exploitation by a more malicious person
         3. Motivations are not necessarily clear cut (personal gain, but in the form of prestige and accomplishment rather than material)
      3. White hat
         1. "Hero" in contrast to "Villain" (black hat)
         2. Usually legally supported when performing typical actions of a hacker
            1. Explicit permission or acquired credentials
         3. AKA sneakers when professionally organized
         4. Safest and most ethical way to maintain a career based on hacking
         5. Generally avoids illegal action
   3. Abilities
      1. Assume for the purpose of this presentation that these three groups share the same capabilities and capacities to learn and acquire information for any particular hack.
      2. The key differences between them can then be derived to the limitations that each of them possess for using these abilities or knowledge.
         1. The justification for the limitations then characterizes the hacker
      3. Examples of justifications
         1. Black hat: "It's their own fault for leaving such a blatant hole in their security infrastructure. Their loss, my gain."
         2. Grey hat: "I'd like to help, but I want to do it my way." OR "They should be taught a lesson for such a stupid mistake, but they shouldn't suffer too much."
         3. White hat: "An uncertified consultant cannot be completely trusted or held liable. Nobody should ever hope to rely on the benevolent grey hat hacker."
   4. Distinction
      1. The boundaries between these groups are fuzzy at best and flexible
         1. It is not unheard of for criminal hackers to become security consultants after regaining their freedom.
      2. However, the underlying philosophies that represent each group are distinct enough to identify and appreciate the purpose of this presentation: the ethical hacker
4. The ethics involved
   1. In contrast: Software engineering's code of ethics
      1. Given a code of ethics from the Association for Computing Machinery
      2. Focused more specifically on proper management, development, and teamwork
   2. Hacker ethic
      1. Sharing
      2. Openness
      3. Decentralization
      4. Free access to computers
      5. World Improvement
      6. Refers more to the statement made by the original hacking community at MIT
      7. Principles behind these ethics help create strong, unchanging foundation despite the evolution of technology and the law that governs it
   3. Distinctions
      1. This code of ethics generally sounds wholesome and just, but hackers themselves are associated with illegal activities (see previous definitions)
      2. However, when one considers the results of some of these activities, they can be seen in a way that matches them to a tenet.
         1. Distributing content over P2P: sharing
         2. Creating and managing open-source software or eliminating obfuscation in a closed-source rival: openness
         3. Protesting laws that hurt net neutrality: decentralization and free access to computers (since all servers are computers, and all websites are files!)
         4. World improvement: free software on cheap and readily available hardware. Also, see VIM screenshot
   4. What went wrong? (a simple summary)
      1. All of these actions sound great, so why do hackers get a bad reputation?
      2. Hackers often utilize methods and utilities that go outside the normal realm of the average user.
      3. In the pursuit of (free) knowledge, security exploits are identified and distributed to raise awareness when exploring these methods.
      4. The opportunity for personal gain or malicious attacks arises.
      5. Not everyone follows the hacker ethic (or obeys the law).
      6. Thanks to the progress that hackers made in discovering security flaws, other, less benevolent individuals have now acquired root access to your machine.
      7. There are a number of reasons to blame one group over the other (the true hacker vs. the cracker/black hat), but the point is that both groups rightfully have some blame.
      8. Even white hat hackers can be met with criticism and scorn. Hey, nobody likes being compromised, right?
   5. What went right? (a simple response)
      1. To continue benefitting from the discoveries and good intentions of the white hat hacker while differentiating them from the black hat (and offering legal protection), the technology industry turned to its de facto solution: certification!
      2. An individual possessing the title of a Certified Ethical Hacker can be safely contracted to test the security of a given system without fear of legal action. Moreover, the contractor now has someone to hold responsible should anything go wrong.
   6. What REALLY happened
      1. The use of a CEH in a particular business is almost always beneficial for the health and safety of both its employees and its customers
      2. However, this course of action has led to the creation of the controlled black hat hacker, not the preservation of the white hat hacker in a corporate environment. The CEH still performs the same malicious attacks, but acquires personal gain through a salary rather than unhindered access to lucrative information.
      3. Still, while the motivation and use of a CEH does not adhere to the hacker ethic, it does not necessarily violate the tenets to a large degree.
5. The community
   1. The 2400
   2. Pwn2Own
   3. HOPE
6. Get involved!
   1. Contribute to open-sourced projects :)
7. More info