White hat (computer security)

From Wikipedia, the free encyclopedia

The term "**white hat**" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems.[1] Ethical hacking is a term coined by IBM meant to imply a broader category than just penetration testing.[2] Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively.[3]

White-hat hackers may also work in teams called "sneakers",[4] red teams, or tiger teams.[5]

Contents

History

One of the first instances of an ethical hack being used was a "security evaluation" conducted by the United States Air Force of the Multics operating systems for "potential use as a two-level (secret/top secret) system." Their evaluation found that while Multics was "significantly better than other conventional systems," it also had "... vulnerabilities in hardware security, software security and procedural security" could be uncovered with "a relatively low level of effort." The authors performed their tests under a guideline of realism, so their results would accurately represent the kinds of access an intruder could potentially achieve. They performed tests involving simple information-gathering exercises, as well as outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassified reports describing ethical hacking activities within the U.S. military.[5]

By 1981 *The New York Times* described white hat activities as part of a "mischievous but perversely positive 'hacker' tradition". When a National CSS employee revealed the existence of his password cracker, which he had used

on customer accounts, the company chastised him not for writing the software but for not disclosing it sooner. The letter of reprimand stated "The Company realizes the benefit to NCSS and in fact encourages the efforts of employees to identify security weaknesses to the VP, the directory, and other sensitive software in files".[6]

The idea to bring this tactic of ethical hacking to assess security of systems was formulated by Dan Farmer and Wietse Venema. With the goal of raising the overall level of security on the Internet and intranets, they proceeded to describe how they were able to gather enough information about their targets to have been able to compromise security if they had chosen to do so. They provided several specific examples of how this information could be gathered and exploited to gain control of the target, and how such an attack could be prevented. They gathered up all the tools they had used during their work, packaged them in a single, easy-to-use application, and gave it away to anyone who chose to download it. Their program, called Security Administrator Tool for Analyzing Networks, or SATAN, was met with a great amount of media attention around the world in 1992.[5]

Tactics

While penetration testing concentrates on attacking software and computer systems from the start – scanning ports, examining known defects and patch installations, for example – ethical hacking may include other things. A full blown ethical hack might include emailing staff to ask for password details, rummaging through executive's dustbins and usually breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a security review of this magnitude are aware. To try to replicate some of the destructive techniques a real attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late at night while systems are less critical.[2] In most recent cases these hacks perpetuate for the long term con (days, if not weeks, of long term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software in a public area, as if someone lost the small drive and an unsuspecting employee found it and took it.

Some other methods of carrying out these include:

- DoS attacks
- Social engineering tactics
- Security scanners such as:
  - W3af
  - Nessus
  - Nexpose
- Frameworks such as:
  - Metasploit

Such methods identify and exploit known vulnerabilities, and attempt to evade security to gain entry into secured areas. They are able to do this by hiding software and system 'back-doors' that could be used as a link to the information or access the non-ethical hacker, also known as 'black-hat' or 'grey-hat', may want to reach.

Legality in the UK

Struan Robertson, legal director at Pinsent Masons LLP, and editor of OUT-LAW.com, says "Broadly speaking, if the access to a system is authorized, the hacking is ethical and legal. If it isn't, there's an offence under the Computer Misuse Act. The unauthorized access offence covers everything from guessing the password, to accessing someone's webmail account, to cracking the security of a bank. The maximum penalty for unauthorized access to a computer is two years in prison and a fine. There are higher penalties – up to 10 years in prison – when the hacker also modifies data". Unauthorized access even to expose vulnerabilities for the benefit of many is not legal, says Robertson. "There's no defense in our hacking laws that your behavior is for the greater good. Even if it's what you believe."[2]

Employment

The United States National Security Agency offers certifications such as the CNSS 4011. Such a certification covers orderly, ethical hacking techniques and team-management. Aggressor teams are called "red" teams. Defender teams are called "blue" teams.[4]

List of prominent white hat hackers

- Eric Corley
- Przemysław Frasunek
- Raphael Gray
- Barnaby Jack
- Michael Mansfield
- Kevin Mitnick
- Robert Tappan Morris
- Shahmeer Amir
- Kevin Poulsen

See also

- Certified Ethical Hacker
- IT risk
- Wireless identity theft

References

1. "What is white hat? - a definition from Whatis.com" . Searchsecurity.techtarget.com. Retrieved 2012-06-06.
2. Knight, William (16 October 2009). "License to Hack" . *InfoSecurity*. **6** (6): 38–41. doi:10.1016/s1742-6847(09)70019-9 .
3. Wilhelm, Thomas; Andress, Jason (2010). *Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques* . Elsevier. pp. 26–7.
4. "What is a White Hat?" . Secpoint.com. 2012-03-20. Retrieved 2012-06-06.
5. Palmer, C.C. (2001). "Ethical Hacking" (PDF). *IBM Systems Journal*. **40** (3): 769. doi:10.1147/sj.403.0769 .
6. McLellan, Vin (1981-07-26). "Case of the Purloined Password" . *The New York Times*. Retrieved 11 August 2015.