White hat (computer security)

A **white hat** (or a **white-hat hacker**, **a whitehat**) is an ethical security hacker.[1][2] Ethical hacking is a term meant to imply a broader category than just penetration testing.[3][4] Under the owner's consent, white-hat hackers aim to identify any vulnerabilities or security issues the current system has.[5] The white hat is contrasted with the black hat, a malicious hacker; this definitional dichotomy comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat, respectively.[6] There is a third kind of hacker known as a grey hat who hacks with good intentions but at times without permission.[7]

White-hat hackers may also work in teams called "sneakers and/or hacker clubs",[8] red teams, or tiger teams.[9]

History

One of the first instances of an ethical hack being used was a "security evaluation" conducted by the United States Air Force in 1972 - 1973, in which the Multics operating systems were tested for "potential use as a two-level (secret/top secret) system." The evaluation determined that while Multics was "significantly better than other conventional systems," it also had "... vulnerabilities in hardware security, software security and procedural security" that could be uncovered with "a relatively low level of effort."[10] 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; both results were of interest to the target audience. There are several other now unclassified reports describing ethical hacking activities within the US military.

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 encourages the efforts of employees to identify security weaknesses to the VP, the directory, and other sensitive software in files".[11]

On October 20, 2016, the Department of Defense (DOD) announced "Hack The Pentagon."[12][13]

The idea to bring this tactic of ethical hacking to assess the security of systems and point out vulnerabilities was formulated by Dan Farmer and Wietse Venema. To raise 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.[9]

Tactics

While penetration testing concentrates on attacking software and computer systems from the start – scanning ports, examining known defects in protocols and applications running on the system, and patch installations, for example – ethical hacking may include other things. A full-scale ethical hack might include emailing staff to ask for password details and rummaging through executive dustbins,[4] usually without the knowledge and consent of the targets. Only the owners, CEOs, and Board Members (stakeholders) who asked for such a security review of this magnitude are aware. To try and 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.[14] 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:

- Disk and memory forensics
- DoS attacks
- Frameworks such as:
  - Metasploit
- Network Security
- Reverse engineering
- Security scanners such as:
  - Burp Suite
  - Nessus
  - W3af
- Social engineering tactics such as:
  - Phishing
  - Pretexting
- Training Platforms
- Vulnerability research

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

Legality

Belgium

Belgium legalized white hat hacking in February 2023.[15]

China

In July 2021, the Chinese government moved from a system of voluntary reporting to one of legally mandating that all white hat hackers first report any vulnerabilities to the government before taking any further steps to address the vulnerability or make it known to the public.[16] Commentators described the change as creating a "dual purpose" in which white hat activity also serves the country's intelligence agencies.[16]

United Kingdom

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 offense under the Computer Misuse Act. The unauthorized access offense 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."[4]

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.[8] When the agency recruited at DEF CON in 2020, it promised applicants that "If you have a few, shall we say, *indiscretions* in your past, don't be alarmed. You shouldn't automatically assume you won't be hired".[17]

A good "white hat" is a competitive skillful employee for an enterprise since they can be a countermeasure to find the bugs to protect the enterprise network environment. Therefore, a good "white hat" could bring unexpected benefits in reducing the risk across systems, applications, and endpoints for an enterprise.[18]

Recent research has indicated that white-hat hackers are increasingly becoming an important aspect of a company's network security protection. Moving beyond just penetration testing, white hat hackers are building and changing their skill sets, since the threats are also changing. Their skills now involve social engineering, mobile tech, and social networking.[19]

Notable people

- Jim Browning, alias of a Northern Ireland white hat hacker, scam baiter, and journalist, with investigations published on YouTube and on BBC programmes such as *Panorama* and *Scam Interceptors*
- Charlie Miller, an American white hat hacker previously employed by the National Security Agency and Uber who has, amongst other exploits, published successful hacks into the vulnerabilities of the computer on a 2014 Jeep Cherokee along with Chris Valasek, being able to take control of acceleration, braking, and steering
- Jennifer Arcuri, an American technology entrepreneur founded the white hat consultancy Hacker House in 2016.

See also

- Bug bounty program
- IT risk
- Locksmith
- MalwareMustDie
- Wireless identity theft

References

1. "What is white hat? - a definition from Whatis.com" (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550882,00.html). Searchsecurity.techtarget.com. Archived (https://web.archive.org/web/20110201231325/http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550882,00.html) from the original on 2011-02-01. Retrieved 2012-06-06.
2. Okpa, John Thompson; Ugwuoke, Christopher Uchechukwu; Ajah, Benjamin Okorie; Eshioste, Emmanuel; Igbe, Joseph Egidi; Ajor, Ogar James; Okoi, Ofem, Nnana; Eteng, Mary Juachi; Nnamani, Rebecca Ginikanwa (2022-09-05). "Cyberspace, Black-Hat Hacking and Economic Sustainability of Corporate Organizations in Cross-River State, Nigeria" (https://doi.org/10.1177%2F21582440221122739). *SAGE Open*. **12** (3): 215824402211227. doi:10.1177/21582440221122739 (https://doi.org/10.1177%2F21582440221122739). ISSN 2158-2440 (https://search.worldcat.org/issn/2158-2440). S2CID 252096635 (https://api.semanticscholar.org/CorpusID:252096635).
3. Ward, Mark (14 September 1996). "Sabotage in cyberspace" (https://www.newscientist.com/article/mg15120471-700-sabotage-in-cyberspace-the-threat-to-national-security-from-computer-terrorists-is-vastly-overblown-most-hackers-are-after-nothing-more-than-an-intellectual-thrill/). *New Scientist*. **151** (2047). Archived (https://web.archive.org/web/20220113120127/https://www.newscientist.com/article/mg15120471-700-sabotage-in-cyberspace-the-threat-to-national-security-from-computer-terrorists-is-vastly-overblown-most-hackers-are-after-nothing-more-than-an-intellectual-thrill/) from the original on 13 January 2022. Retrieved 28 March 2018.
4. Knight, William (16 October 2009). "License to Hack" (http://www.infosecurity-magazine.com/view/4611/license-to-hack-ethical-hacking/). *InfoSecurity*. **6** (6): 38–41. doi:10.1016/s1742-6847(09)70019-9 (https://doi.org/10.1016%2Fs1742-6847%2809%2970019-9). Archived (https://web.archive.org/web/20140109211618/http://www.infosecurity-magazine.com/view/4611/license-to-hack-ethical-hacking/) from the original on 9 January 2014. Retrieved 19 July 2014.

5. Filiol, Eric; Mercaldo, Francesco; Santone, Antonella (2021). "A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach" (https://doi.org/10.1016%2Fj.procs.2021.08.210). *Procedia Computer Science*. **192**: 2039–2046. doi:10.1016/j.procs.2021.08.210 (https://doi.org/10.1016%2Fj.procs.2021.08.210). S2CID 244321685 (https://api.semanticscholar.org/CorpusID:244321685).
6. Wilhelm, Thomas; Andress, Jason (2010). *Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques* (https://books.google.com/books?id=aVnA8pQmS54C&pg=PA26). Elsevier. pp. 26–7. ISBN 978-1-59749-589-9.
7. "What is the difference between black, white, and grey hackers" (https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html). *Norton.com*. Norton Security. Archived (https://web.archive.org/web/20180115172110/https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html) from the original on 15 January 2018. Retrieved 2 October 2018.
8. "What is a White Hat?" (http://www.secpoint.com/What-is-a-White-Hat.html). Secpoint.com. 2012-03-20. Archived (https://web.archive.org/web/20190502061110/https://www.secpoint.com/what-is-a-white-hat.html) from the original on 2019-05-02. Retrieved 2012-06-06.
9. Palmer, C.C. (2001). "Ethical Hacking" (http://pdf.textfiles.com/security/palmer.pdf) (PDF). *IBM Systems Journal*. **40** (3): 769. doi:10.1147/sj.403.0769 (https://doi.org/10.1147%2Fsj.403.0769). Archived (https://web.archive.org/web/20190502061107/http://pdf.textfiles.com/security/palmer.pdf) (PDF) from the original on 2019-05-02. Retrieved 2014-07-19.
10. Paul A. Karger; Roger R. Scherr (June 1974). MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS (https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/karg74.pdf) (PDF) (Report). Archived (https://web.archive.org/web/20171113060242/https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/karg74.pdf) (PDF) from the original on 13 November 2017. Retrieved 12 Nov 2017.
11. McLellan, Vin (1981-07-26). "Case of the Purloined Password" (https://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html?pagewanted=3&pagewanted=all). *The New York Times*. Archived (https://web.archive.org/web/20160307215920/http://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html?pagewanted=3&pagewanted=all) from the original on 2016-03-07. Retrieved 11 August 2015.
12. "DoD Announces 'Hack the Pentagon' Follow-Up Initiative" (https://www.defense.gov/News/News-Stories/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative/platform/dod-announces-hack-the-pentagon-follow-up-initiative/https://www.defense.gov/News/News-Stories/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative/). *U.S. Department of Defense*. Retrieved 2023-12-15.
13. Perez, Natasha Bertrand, Zachary Cohen, Alex Marquardt, Evan (2023-04-13). "Pentagon leak leads to limits on who gets access to military's top secrets | CNN Politics" (https://www.cnn.com/2023/04/13/politics/pentagon-leaks-limit-access-military-secrets/index.html). *CNN*. Archived (https://web.archive.org/web/20231215184601/https://www.cnn.com/2023/04/13/politics/pentagon-leaks-limit-access-military-secrets/index.html) from the original on 2023-12-15. Retrieved 2023-12-15.
14. Justin Seitz, Tim Arnold (April 14, 2021). *Black Hat Python, 2nd Edition: Python Programming for Hackers and Pentesters* (https://python.engineering/black-hat-python/). No Starch Press. ISBN 978-1-7185-0112-6. Archived (https://web.archive.org/web/20210826111249/https://python.engineering/black-hat-python/) from the original on August 26, 2021. Retrieved August 30, 2021.

15. Drechsler, Charlotte Somers, Koen Vranckaert, Laura (3 May 2023). "Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?" (https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/). *CITIP blog*. Archived (https://web.archive.org/web/20230517194250/https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/) from the original on 17 May 2023. Retrieved 7 May 2023.
16. Brar, Aadil (18 January 2024). "China Raises Private Hacker Army To Probe Foreign Governments" (https://www.newsweek.com/china-hackers-probe-foreign-governments-computers-online-cybersecurity-1861721). *Newsweek*. Archived (https://web.archive.org/web/20240120053025/https://www.newsweek.com/china-hackers-probe-foreign-governments-computers-online-cybersecurity-1861721) from the original on 20 January 2024. Retrieved 20 January 2024.
17. "Attention DEF CON® 20 attendees" (https://web.archive.org/web/20120730224626/http://www.nsa.gov/careers/dc20). National Security Agency. 2012. Archived from the original (http://www.nsa.gov/careers/dc20) on 2012-07-30.
18. Caldwell, Tracey (2011). "Ethical hackers: putting on the white hat". *Network Security*. **2011** (7): 10–13. doi:10.1016/s1353-4858(11)70075-7 (https://doi.org/10.1016%2Fs1353-4858%2811%2970075-7). ISSN 1353-4858 (https://search.worldcat.org/issn/1353-4858).
19. Caldwell, Tracey (2011-07-01). "Ethical hackers: putting on the white hat" (https://www.sciencedirect.com/science/article/pii/S1353485811700757). *Network Security*. **2011** (7): 10–13. doi:10.1016/S1353-4858(11)70075-7 (https://doi.org/10.1016%2FS1353-4858%2811%2970075-7). ISSN 1353-4858 (https://search.worldcat.org/issn/1353-4858).
