Unconventional Careers

Ethical Hacker

An Ethical Hacker, also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners and with their permission to find security vulnerabilities that a malicious hacker could potentially exploit.

The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

Ethical Hackers use their skills and many of the same methods and techniques to test and bypass organizations' IT security as their unethical counterparts, who are referred to as black hat hackers. However, rather than taking advantage of any vulnerabilities they find for personal gain, Ethical Hackers document them and provide advice about how to remediate them so organizations can strengthen their overall security.

Ethical Hackers generally find security exposures in insecure system configurations, known and unknown hardware or software vulnerabilities as well as operational weaknesses in process or technical countermeasures.

Any organization that has a network connected to the Internet or provides an online service should consider subjecting it to penetration testing conducted by Ethical Hackers.

Benefits of Ethical Hacking

There are a number of ways Ethical Hackers can help organizations, including:

- **Finding Vulnerabilities.** Ethical Hackers help companies determine which of their IT security measures are effective, which need to be updated and which contain vulnerabilities that can be exploited. When Ethical Hackers finish

evaluating organizations' systems, they report back to company leaders about those vulnerable areas, for instance, a lack of sufficient password encryption, insecure applications or exposed systems running unpatched software. Organizations can use the data from these tests to make informed decisions about where and how to improve their security posture to prevent cyberattacks.

- **Demonstrating Methods Used by Cybercriminals.** These demonstrations show executives the hacking techniques that malicious users apply to attack their systems and wreak havoc with their businesses. Companies that have in-depth knowledge of the methods the attackers use to break into their systems are better able to prevent them from doing so.
- **Helping Prepare for a Cyberattack.** Cyberattacks can cripple or destroy a business, especially a small business. However, most companies are completely unprepared for cyberattacks. Ethical Hackers understand how threat actors operate and they know how these bad actors will use new information and techniques to attack systems. Security professionals who work with Ethical Hackers are better able to prepare for future attacks because they can better react to the constantly changing nature of online threats.

How to Become an Ethical Hacker

There are no standard education criteria for an Ethical Hacker, so an organization can set its own requirements for that position. Those interested in pursuing a career as an Ethical Hacker should consider a **Bachelor's** or **Master's** degree in **Information Security, Cyber Security, Computer Science** or even **Mathematics** as a strong foundation.

Other technical subjects including Programming, Scripting, Networking and Hardware Engineering, can help those pursuing a career as Ethical Hackers by offering a fundamental understanding of the underlying technologies that form the systems that they will be working on. Other pertinent technical skills include system administration and software development.

Certified Ethical Hackers: International Certifications

There are a number of Ethical Hacking certifications as well as IT certifications related to security that can help individuals become Ethical Hackers, including:

Certified Ethical Hacker (CEH): This is a vendor-neutral certification from the EC-Council, one of the leading certification bodies. This security certification, which validates how much an individual knows about network security, is best suited for a penetration tester role. This certification covers more than 270 attacks technologies. Prerequisites for this certification include attending official training offered by the EC-Council or its affiliates and having at least two years of information security-related experience.

Certified Information Systems Auditor (CISA): This certification is offered by Information Systems Audit and Control Association ISACA, a non-profit, independent association that advocates for professionals involved in information security, assurance, risk management and governance. The exam certifies the knowledge and skills of security professionals. To qualify for this certification, candidates must have five years of professional work experience related to information systems auditing, control or security.

Certified Information Security Manager (CISM): CISM is an advanced certification offered by Information Systems Audit and Control Association ISACA that provides validation for individuals who have demonstrated the in-depth knowledge and experience required to develop and manage an enterprise information security program. The certification is aimed at information security managers, aspiring managers or IT consultants who support information security program management.

GIAC Security Essentials (GSEC): This certification created and administered by the Global Information Assurance Certification Organization (GSEC) is geared towards security professionals who want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate they understand information security beyond simple terminology and concepts.

Local and International Universities offering Courses in Information Security, Cyber Security and Computer Science

International Universities

- **Information Security**

https://www.hotcoursesabroad.com/study/training-degrees/international/undergraduate/slevel/2/subject/information+security/sin/ct/programs.html

- **Cyber Security**

https://www.hotcoursesabroad.com/study/training-degrees/international/undergraduate/slevel/2/subject/cyber+security/sin/ct/programs.html

- **Computer Science**

https://www.hotcoursesabroad.com/study/training-degrees/international/undergraduate/computer-science-courses/slevel/2/cgory/e1-3/sin/ct/programs.html

Pakistani Universities

- **Cyber Security**

https://www.eduvision.edu.pk/institutions-offering-cyber-security-with-field-computer-sciences-information-technology-at-bachelor-level-in-pakistan-page-1

- **Computer Science**

https://www.eduvision.edu.pk/institutions-offering-computer-science-with-field-computer-sciences-information-technology-at-bachelor-level-in-pakistan-page-1

Note:

The Information is shared in good faith. Any disagreeable content may be ignored, please.