Ethical Hacker

Introduction:

An ethical writer, also known as a “white hat” hacker, is a cybersecurity professional that uses their hacking skills to find different vulnerabilities and problems in computer systems and networks. The term "ethical hacking" was introduced in 1995 by IBM Vice President John Patrick, but the practice itself has roots that stretch back much further. (Allicance, 2024) By the 1980s and 90s, the image of hackers changed dramatically. During that time, the rise of personal computers meant that critical data was all stored digitally. Malicious hackers, also known as “black hat hackers”, started noticing the value of the information that can steal or manipulate for money. Essentially, ethical hackers were made to stop black hat hackers. Ethical hackers are very important to our society. They serve a great purpose to multiple companies and businesses. Becoming one can be a hard process but you can have good opportunities for impact and salary potential.

Body:

Ethical hackers fill a vital role in security and society in various ways. For example, they search for vulnerabilities in different systems. Ethical hacks have greatly impacted social media, the software industry, etc. For instance, during 2018, ethical hackers [found software vulnerabilities](https://hub.packtpub.com/10-times-ethical-hackers-spotted-a-software-vulnerability-and-averted-a-crisis/) that averted crises in ten major companies. (Engineer, 2019) The career of an ethical hacker gained more popularity over the years. It also is a great career for individuals that are very good with computers and that want to make an impact. The demand for ethical hackers is expected to continue to grow due to the rising threat of cybercrime.

An ethical hacker’s primary purpose is to view security from the adversary’s perspective to find vulnerabilities that bad hackers could exploit. (Bowcut, 2025) White Hat hackers use the same techniques as malicious hacks within legal and moral boundaries. Ethical hacking can help benefit multiple companies to understand network flaws and vulnerabilities. By hacking networks with permission, ethical hackers can show how malicious hackers exploit various vulnerabilities and help the company discover and close the most critical ones. (IBM, 2023) Their perspective may find things that some internal analysts can miss.

The most important requirement for becoming a successful ethical hacker today is having high ethical standards, as is found in the name. (Bowcut, 2025) Ethics is the main thing that separates white hat hackers from black hat hackers. There are plenty of black hat hackers that have the skills to become an ethical hacker, but they choose to do the wrong thing. To become an ethical hacker, a person must understand networks, wired and wireless. They must be proficient with operating systems, especially Windows and Linux. They need to understand firewalls and file systems. (Bowcut, 2025)

The average [ethical hacker](https://www.coursera.org/articles/what-is-ethical-hacking) salary in the United States is $147,108, according to Glassdoor. The wide pay range for an ethical hacker suggests there may be many opportunities for advancement and increased pay based on certifications, skill level, education, location, experience, and expertise. (Staff, 2025) If an individual doesn’t have that much experience, the starting pay could be about $90,000. The more experience, the more that the starting pay is.

Conclusion:

In conclusion, an ethical hacker career is a good option. Ethical hackers fill a vital role in security and society in various ways. An ethical hacker’s primary purpose is to view security from the adversary’s perspective to find vulnerabilities that bad hackers could exploit. Also, they can help benefit multiple companies to understand network flaws and vulnerabilities. The most important requirement for becoming a successful ethical hacker today is having high ethical standards. Ethics is the main thing that separates white hat hackers from black hat hackers. The wide pay range for an ethical hacker suggests there may be many opportunities for advancement and increased pay based on certifications, skill level, education, location, experience, and expertise.

# References

Allicance, N. C. (2024, August 15). *The Evolution of Ethical Hacking: From Curiosity to Cybersecurity*. Retrieved from Careers and Education: https://www.staysafeonline.org/articles/the-evolution-of-ethical-hacking-from-curiosity-to-cybersecurity

Bowcut, S. (2025, April 3). *How to Become an Ethical Hacker: A Blueprint*. Retrieved from https://cybersecurityguide.org/resources/ethical-hacker/

Engineer, S. (2019, November 1). *Ethical Hackers: Filling a Vital Role in Society*. Retrieved from Security Through Education: https://www.social-engineer.org/newsletter/ethical-hackers-filling-a-vital-role-in-society/

IBM. (2023, October 20). *What is ethical hacking?* Retrieved from https://www.ibm.com/think/topics/ethical-hacking

Staff, C. (2025, March 13). *Ethical Hacker Salary: What You'll Make and Why*. Retrieved from https://www.coursera.org/articles/ethical-hacker-salary