Ethical Hacking

Joshua Punch

4/14/2026

Most people do not consider a job in the cybersecurity field until they have an actual security issue. This field operates as a very important aspect in day to day life. The field of ethical hacking relies on people who protect computers from criminal activities. Ethical hackers essentially are paid security testers. What this means is that they are paid to attempt to hack into systems for businesses so they can repair vulnerabilities before actual hackers can get into them.

What they actually do

This job sounds very technical, and while there are a lot of technical aspects involved, it also requires social skills so that positive working relationships can be made with people. Cyber criminals who are effective in their field do so because they can exploit common human errors or social engineering tactics. Social science studies human behavior because it is the study of how people make choices as well as how they interact with others.

Ethical hackers (also known as penetration testers) are hired to test the secureness levels of systems for businesses. Security professionals day to day will verify these security systems through testing which will tell them how secure these systems actually are against potential threats. These testers must have proper permission to test these systems by using legal methods which will say if they are able to test or not.

These projects determine if certain tasks will perform well daily. This team of testers will use scanning systems to determine and identify certain security flaws in current systems. Another

important part of this job is writing reports. This is done so that companies can understand which systems were not working for them.

Social science connection

The study of human behavior forms the primary link between ethical hacking and social science research. People make mistakes which lead to cyberattacks because systems have weaknesses. For example, phishing emails only work if someone clicks a bad link or enters their password. Ethical hackers use controlled environments to send fake emails which help them observe how people choose to react.

This is where psychology comes in. Ethical hackers need to understand what makes people trust messages. Things like urgency, authority, or fear are used a lot. The email informs users that their account will be locked immediately, which causes users to panic and make hasty decisions. These methods use emotional manipulation to achieve their goals.

Social engineering stands as another important concept. This term refers to people who use social techniques to achieve their objectives without needing to use technical methods. Ethical hackers study how attackers use persuasion and pressure to get information. The method demonstrates a surprising success rate, which proves to be effective.

Decision-making becomes vital to execute this role. Ethical hackers face a challenge to determine their appropriate penetration level during security assessments. Security specialists need to maintain system functionality while they conduct their testing activities. The process needs to maintain security testing with operational viability for the system.

The process also encompasses communication as a significant component. Ethical hackers need to present their findings to both technical and non-technical stakeholders. They need to present the information in a simplified way which preserves its original meaning. The

problem will remain unresolved because his explanation of the situation will not help him find a solution.

Real world examples

The employees in the workplace use human resources management principles to conduct their daily operations. The employees need to develop their skills which enable them to handle phishing tests by understanding the messaging system which employees will consider trustworthy. People need to understand real human behavior to create effective systems which will protect their organizations from unauthorized access.

These researchers study how people will make decisions while experiencing different periods of stress while experimenting. The researchers found that people can only focus on their current task, not allowing them to work on other things (multitasking.) The design of ethical hacking tests depends on behavior patterns of humans, which will act as the center of the professional domain.

Teamwork is a very important part of this field. The majority of work for these professionals will require them to interact with one another. They will work with IT teams as well as security personnel and even with staff in management. The process will require them to explain many technical problems through non-advanced language which will help people not in the field understand. This process of explaining these technical issues to those who have no understanding requires advanced levels of understanding as it presents multiple challenges.

Impact on society

Ethical hacking benefits society through its ability to protect computer systems from cyber threats which affect business operations. Some groups are more vulnerable to cyberattacks

than others. Older adults frequently become victims of age-related cyber threats because they lack technical knowledge to safeguard themselves against online threats. People who have limited digital expertise face higher vulnerability risks to online threats.

Ethical hackers protect systems from threats through their identification of security flaws which enemies intend to exploit. Security professionals must assess how users will interact with various system features. Complex security systems create challenges for users because they experience difficulties which lead to their unintentional creation of security gaps which leave them less protected.

Ethical hackers secure various vital systems which include hospitals and banks and educational institutions. The attack on these systems will create extreme repercussions for people who depend on specific companies to deliver essential services. The significance of this job extends beyond its relationships with computers.

Conclusion

The work of penetration testers (ethical hackers) required high level technical skill while also needing professionals to have knowledge about common human behavior. Social science concepts such as decision making, communication, and behavior habits will show up in this career quite frequently. The penetration testing role will require human interaction through not only testing these systems, but also conducting multiple simulations of phishing. They also will have to present these findings to others as well.

The world needs these professionals as they protect vulnerable companies from cyber attacks. This field will gain a lot more importance as technology continues to become more advanced. Penetration testers work not only in technology, but also in human behavior, which makes them vital for the field of cybersecurity.

Works cited:

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking-p-9781119433385

National Institute of Standards and Technology (NIST). (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Verizon. (2023). *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/