

The Human Element of Security: Social Science in Penetration Testing

Nicholas Duggins

08/09/2026

The Human Element of Security: Social Science in Penetration Testing

Cybersecurity is often seen as a field focused on computers, firewalls, coding, and networks. While those things are important, cybersecurity professionals also must understand people. This is especially true for penetration testers. A penetration tester, or ethical hacker, is hired to find weaknesses in an organization's security before a real attacker can exploit them. These weaknesses are not always found in computer systems. Many times, the weakest part of security is the person using the system. Because of this, penetration testers depend on social science principles such as psychology, social exchange, criminology, and research methods.

Social Science Principles in Daily Penetration Testing Operations

One of the most important concepts used in penetration testing is behavioral psychology. Social engineering attacks are designed around the way people think and make decisions. For example, during a phishing simulation, a penetration tester might send an email that appears to come from an IT manager and tells an employee that they need to reset their password immediately. The tester is looking at whether the employee recognizes the warning signs or reacts to the pressure. Concepts such as authority, urgency, trust, and cognitive bias help explain why people sometimes respond without questioning the request.

Social Exchange Theory is another concept that applies to penetration testing. This theory suggests that people often make decisions by considering the costs and benefits of interaction. Penetration testers can use this idea during social engineering, physical security testing, and open-source intelligence (OSINT) gathering. By building rapport, being friendly, or using familiar company terminology, a tester may make an employee feel comfortable enough to provide information. This can reveal weaknesses that technical security tools cannot find. Hatfield (2019) explains that social engineering creates important ethical questions because penetration testers intentionally use human behavior as part of their assessments.

Criminological theories can also help penetration testers understand how attackers think. Routine Activity Theory states that crime becomes more likely when a motivated offender, a suitable target, and a lack of capable guardianship come together. A penetration tester can use this theory to identify situations where these factors overlap. For example, an employee with access to sensitive information and weak security habits could become an attractive target. Rational Choice Theory can also be applied because attackers often consider the potential rewards and risks of targeting an organization. Penetration testers use this thinking to determine what makes an organization attractive to an attacker and how those risks can be reduced.

Qualitative Research and Ethical Leadership

Another important connection is qualitative research. Before testing a system, penetration testers gather information about the organization, its employees, technology, and normal routines. This reconnaissance can involve company websites, social media, public records, and other sources. Testers use this information to identify patterns and develop ideas about possible weaknesses before conducting controlled tests. Hemalatha et al. (2026) explains that modern ethical hacking increasingly combines artificial intelligence with human decision-making. AI can collect and analyze information quickly, but human judgment is still necessary to understand the results and decide what actions should be taken.

Ethics are also a major part of penetration testing. Testers may send deceptive emails, attempt to access restricted areas, or interact with employees using false identities. The difference between an ethical hacker and a criminal is that the penetration tester has permission and is working to improve security. Hatfield (2019) discusses how virtue ethics can help testers balance realistic testing with the responsibility to avoid unnecessary harm or embarrassment. Charalambous et al. (2026) similarly emphasize the importance of ethical leadership in cybersecurity education. A penetration tester needs

more than technical skills because they may have access to sensitive information and systems. They must understand privacy, legal requirements, and the consequences of their decisions.

Career Connections to Society and Marginalized Groups

Penetration testing also has a major connection to society and marginalized groups. Cybersecurity professionals help protect hospitals, banks, schools, government agencies, and other organizations that people depend on. When these systems are attacked, the effects can reach thousands or even millions of people. Some groups may be more vulnerable to social engineering, including people with lower digital literacy, older adults, or individuals facing language barriers. A successful attack can cause financial loss or identity theft, and people with fewer resources may have a harder time recovering.

Penetration testers must also be careful not to create bias during reconnaissance. Modern OSINT and AI tools can collect large amounts of information about individuals. If testers make assumptions based on someone's age, language, background, or other characteristics, their testing can become unfair. Human oversight is important to make sure technology is being used responsibly.

Conclusion

Overall, penetration testing shows why cybersecurity cannot be separated from social science. Psychology, Social Exchange Theory, criminology, and qualitative research all help penetration testers understand how people and organizations behave. At the same time, ethics and social responsibility help professionals make sure their work does not create unnecessary harm. The research from Hatfield (2019), Hemalatha et al. (2026), and Charalambous et al. (2026) demonstrates that cybersecurity is not just about technology. It is also about people. A strong penetration tester needs to understand both the computer system and the human being behind it.

Reference:

Charalambous, A., Peratikou, A., Piki, A., Stavrou, S., & Stavrou, E. (2026). Embedding ethical leadership in cybersecurity education: The case of the penetration tester role. 2026 IEEE Global Engineering Education Conference (EDUCON), 1–10.

<https://doi.org/10.1109/EDUCON67543.2026.11574277>

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration testing. *Computers & Security*, 83, 70–82. <https://doi.org/10.1016/j.cose.2019.02.012>

Hemalatha, S., Jency, A., Gnanasekar, A., Krishna, R. V. V., Satyanarayana, S. K., & Singh, C. (2026). A comprehensive survey on ethical hacking, foot printing, and AI-driven penetration testing in modern cybersecurity. *International Journal of Safety & Security Engineering*, 16(4), 837.

<https://doi.org/10.18280/ijssse.160411>