Penetration Testing

Alex Brown

School of Cybersecurity: Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Diwakar Yalpi

4/14/2026

Penetration Testing

Cybersecurity is a rapidly growing field dedicated to protecting computer systems and networks. As technology advances, the need for robust security measures has become paramount. The cybersecurity profession encompasses a diverse range of roles dedicated to the protection of digital infrastructure, including networks, hardware, and sensitive information. Beyond simple data protection, the field is responsible for ensuring the confidentiality, integrity, and availability of information in an era where cyber threats are increasingly sophisticated. Professionals in this sector work to mitigate risks from various actors, including state-sponsored groups, organized crime, and individual hackers. Their work involves a mix of technical defense, risk management, and strategic planning to safeguard everything from personal privacy to national security. While the field includes specialized areas such as incident response, forensic analysis, and security architecture, one of its most critical proactive functions is identifying and addressing weaknesses before they can be weaponized. This is where penetration testing plays a vital role. Penetration testing, or pen testing, is a crucial aspect of this. It involves simulating cyberattacks to identify vulnerabilities. It helps organizations strengthen their defenses before malicious actors can exploit them. This proactive approach is essential for preventing data breaches, financial losses, and reputational damage. In this paper, we will delve into the specifics of penetration testing, exploring its methodologies, tools, and the critical role it plays in modern cybersecurity.

Social Sciences

Social science plays a huge role in the field of cybersecurity and penetration testing. This is the case because it helps professionals understand human behavior, which can be a very vulnerable part of a security system. Social science research with help from psychology and sociology help explain the motivations someone might have when hacking. Many of these motivations can range from financial gain to social recognition as well as an ethical consideration, as it can be considered that some hacking

can be responsible for ethical hacking practices. Therefore, in pen testing, principles such as psychology and sociology are very relevant as many attacks are targeted toward people rather than systems. So, concepts such as cognitive bias and social influence play crucial roles as they help explain why users may fall victim to phishing emails or why someone might ignore security warnings.

These social science ideas are integrated into cybersecurity practices through human interaction on human computers or HCI. Research and professionals take the data collected from watching the interaction of a user and a computer to understand how users interact, and how they respond to certain situations when prompted. With this pen testers apply the knowledge gained from social engineering techniques such as phishing sims or impression attempts to evaluate how employees react. Doing this by analyzing the user's response helps testers find and identify weaknesses both technically and physically. Then with the data and finding cybersecurity professionals create and develop stronger security awareness programs to help improve employee awareness and designing systems that help reduce the chances of user error, which therefore leads to more effective decision making.

Application of Key concepts

Penetration testing is based on several key principles of science, such as the scientific method and Empiricism. The scientific method involves observation, hypothesis, experimentation, and analysis, which pen testers use to systematically find and validate vulnerabilities. Empiricism means that findings must be proven through real-world testing, not just theory. Pen testers use tools like Nmap and Burp Suite to collect evidence and confirm vulnerabilities. In a journal Weir, D., Sasse, M. A., & Albrechtsen, E. (2017) they use their study to emphasize the main driving point that penetration testing is most effective when its structure is evidenced based with the processes being quite similar to the scientific method. As their research showed that systematic testing can improve the accuracy of security assessment, it was a major impact to ensure the organizations could reduce cyber risks. Therefore, making this source relevant because it provides evidence that penetration testing can be conducted like

a scientific process being able to be repeated. The principle of systems thinking is also vital, as pen testers view organizations as interconnected systems where a weakness in one area can impact the entire network. Risk analysis and probability are also key, helping testers assess the likelihood and impact of an attack. Tools like Metasploit Framework are used to simulate these attacks and measure real-world outcomes. This directly supports the scientific principle of empirical evidence, ensuring that findings are verifiable and actionable. As in another source, NIST (2012) explains how cybersecurity professionals are all about structure. As they use structured frameworks to protect critical infrastructures such as healthcare, banking, and government systems.

Marginalized groups

The term of marginalization in cybersecurity is in reference to how different groups may face unequal access to digital resources and increased exposure to cyber risk. With this having more direct implications for pen testing then one would think. These marginalized communities in many cases have limited access to up to day technology, leaving them with less knowledge and education on cybersecurity. Which leaves them more at-risk phishing attacks and account compromise. As from the sphere of pen testing, professionals can easily recognize and exploit the inequalities. Targeting these groups are easier, as they have less resources leading to weaker security. As a hacker is more likely to be able to get into the security system of a non-profit business rather than a large corporation. Wash, R. (2010) explored this further by understanding how human behavior and cognitive biases could factor into the influence of cybersecurity outcomes. Through the study, it presents that users often fall victim to phishing and social engineering tests, due to three major elements being trust, urgency bias, and knowledge on security. It then further highlights the fact that an individual that is part of a marginalized group faces higher risks of cybersecurity due to their limited access to training or technology and there less education of digital literacy. Furthermore, this article supports the analysis of social science

principles, as it shows that cybersecurity not only depends on technical systems, but psychology and social conditions as well.

It's also good to note that pen testers and cybersecurity professionals have to act in consideration of ethical and legal boundaries, especially when testing systems. They must ensure that there is no harm to users during their assessment process, or that they don't disrupt services beyond repair. Therefore, cybersecurity professionals must work around, so they use the data and results of pen testers to recommend the best security improvements that would be fit for the user. Additionally, the major efforts that have been put into diversifying the workforce of cybersecurity help ensure that pen testing has to consider a wide range of users. Ultimately, pen testing not only identifies technical vulnerabilities but also highlights how social inequality can influence security risk. Which leads to more inclusive and effective cybersecurity practices.

Career to society

Penetration testing plays an important role in cybersecurity by helping protect the systems that society depends on. From financial institutions to healthcare systems, government networks, and communication services. The proactive identification and remediation of vulnerabilities is crucial. To maintain the integrity and confidentiality of sensitive data. It also helps organizations comply with various regulations and standards. Pen testing simulates real attacks in the hopes to find vulnerabilities and weaknesses before major attacks occur. This prevents disruptions and is essential to a reliable and secure security system.

Penetration testing also supports public cybersecurity policies and regulations. For example, it helps organizations comply with data privacy laws like GDPR and CCPA. It also aids in meeting industry-specific standards such as HIPAA for healthcare. This compliance aspect is crucial for building trust with customers and partners. It also ensures that we are legally protected and avoid hefty fines. This is a key benefit to regular penetration testing. It demonstrates a commitment to security. Overall, penetration

testing contributes to societal stability by reducing cyber risks, protecting sensitive data, and ensuring that essential services remain safe and reliable for the public.

References

NIST. (2012). *Computer security incident handling guide (SP 800-61 Rev. 2).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*. https://doi.org/10.1145/1837110.1837113

Weir, D., Sasse, M. A., & Albrechtsen, E. (2017). Security testing and human factors in penetration testing. *Computers & Security, 70*, 345–356.

For additional information on APA Style formatting, please consult the APA Style Manual, 7th Edition.