# Cybersecurity Professional Career Paper: Pen Testers: Full Overview

Student Name: Alessandro Arroyo

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: 13th November 2025

## Introduction

Today I will be speaking about Penetration Testers, which are also known as ethical hackers. As stated in ***It Takes a Pirate to Know One: Ethical Hackers for Healthcare Cybersecurity*** "Cybersecurity is a major concern in almost every context nowadays, and our reliance on interconnected technologies leaves companies and institutions extremely vulnerable to hackers' attacks" (Lorenzini et al., 2022). This very statement shows the need for an ethical hacker to discover weak points and malfunctions in security systems before the bad actors can. In this paper, I will be stating how Pen Testers use social science principles in their work, use key concepts in cybersecurity, and discuss their impact on marginalized groups and society as a whole.

## Social Science Principles

When it comes to social science principles, Pen testers use various principles in this discipline, and you can see them in their everyday work. As stated in ***A Qualitative Study of Penetration Testers and What They Can Tell Us About Information Security in Organizations*** "Social engineering also comprises testing stages. Mouton et al. (2016) described six: (1) attack formulation, (2) information gathering, (3) preparation, (4) develop relationship (5) exploit relationship, and (6) debrief" (De Paoli & Johnstone, 2025). Now social engineering and ethical hacking are both important aspects of Pen Testers' work and each of them deals with social science principles as you need to deal with people to achieve your goals. Understanding how people act to exploit relationships, using data to gather repeated actions, and preparation for encounters with potential targets are some of the many principles used that Pen Testers must master to become great at their craft. Looking at everything stated above, you can see that

cybersecurity and social science principles are very important to this job specifically as you will be dealing with technology and people constantly.

## Application of Key Concepts

Looking throughout all the principles and responsibilities of Pen Testers, you can see key concepts that correlate with cybersecurity and social science principles. When looking into the techniques of a Pen Tester "It is true that pen-testers often resort to the same techniques and tools as malicious hackers, which can sometimes be controversial (e.g. social engineering strategies, such as phishing and USB drops)" (Lorenzini et al., 2022). Phishing is a main technique that is discussed often in cybersecurity, and everything from email, spear, and vishing is used by Pen Testers to gain relations to be able to break into security systems. These techniques often use deception to gain access to people's accounts. However, anything is able to be used for ethical hackers as they imitate the real thing. This also includes social engineering (another key concept) which targets people's emotions rather than accounts and systems as a whole. Looking at both key concepts, we can see the development of both social and cybersecurity principles and ways Pen Testers exploit both.

## Marginalization

As stated in ***Generative AI for Pentesting: The Good, The Bad, The Ugly*** "Cyber threats, such as data breaches, ransomware attacks, and identity theft, have become more complex, posing significant risks to individuals, businesses, and governments alike" (Hilario et al., 2024). With the increase in breaches and attacks, the need for Pen Testers is at an all-time high, and there is a supply and demand for great ones. So how does cybersecurity society combat this need for Pen Testers? By using Generative AI, we can have more Pen Testers that aren't as

skilled to still do high level jobs as the new AI is balancing out the playing field. As we can see "By leveraging the capabilities of LLMs, security professionals can automate the generation of test scenarios, identify novel attack vectors, and adapt testing methodologies to specific environments" (Hilario et al., 2024). With the increase of attacks and breaches we have leaned into AI which is developing at a major rate to combat this and help us with strategies, mitigation, and training for Pen Testers. This trend is only going to continue, and we will have to rely on things such as AI and other programs to continue to help us cover more ground.

## Career Connection to Society

I believe this quote sums everything up "Cyber threats to healthcare are an unavoidable new reality. However, there are ways to strengthen healthcare cybersecurity. For this sector, cybersecurity is not only about protecting data: health data is particularly sensitive and protecting it equals maintaining patients' safety, privacy, and trust" (Hilario et al., 2024). Alot of people may think Pen Testers deal with just cybersecurity however this involves all essential services and it's important to keep essential data secure. Whether it's health data or public domain data, the help of Pen Testers trying to find holes in systems will lead to stronger programs and teams overall. This cannot be understated as the information and training overall will lead to better results in defense and a safer society overall.

## Scholarly Journal Articles

- **Source 1:** ***It Takes a Pirate to Know One: Ethical Hackers for Healthcare Cybersecurity***
- **Source 2:** ***A Qualitative Study of Penetration Testers and What They Can Tell Us About Information Security in Organizations***
- **Source 3:** ***Generative AI for Pentesting: The Good, The Bad, The Ugly***

## References

Hilario, E., Azam, S., Sundaram, J., Imran Mohammed, K., & Shanmugam, B. (2024). Generative AI for pentesting: the good, the bad, the ugly. *International Journal of Information Security*, *23*(3), 2075–2097. https://doi.org/10.1007/s10207-024-00835-

De Paoli, S., & Johnstone, J. (2025). A qualitative study of penetration testers and what they can tell us about information security in organizations. *Information Technology & People (West Linn, Or.)*, *38*(1), 380–398. https://doi.org/10.1108/ITP-11-2021-0864

Lorenzini, G., Shaw, D. M., & Elger, B. S. (2022). It takes a pirate to know one: ethical hackers for healthcare cybersecurity. *BMC Medical Ethics*, *23*(1), Article 131. https://doi.org/10.1186/s12910-022-00872-y