Cyber career in Penetration Testing

Daniel BrzezinskiRockwell

CYSE 201S

Introduction

The current connectivity that envelops the whole world and allows the majority of the human population to communicate has permanently altered humanity for the foreseeable future. The median that allowed this was the invention of the internet and the alternate reality that is cyberspace. Vast networks of wires and circuits are all interconnected, so nearly every person can utilize them for those who can access them. This also allowed businesses to grow and expand beyond what they could have in their physical location. However, not everyone on the internet or in cyberspace uses it for just means; like with everything that involves the potential for personal gain or return on investment, there will always be bad actors.

Anyone or anything can act maliciously on a single target or on a whole group of easy targets. This can be a government trying to inject propaganda to curry favor or to disrupt an opposition party. These attackers can also be individuals or small rouge groups that work independently for their own gain, that be, the thrill of the hunt, payout at the end of a ransom, or to get back those who slighted them. There are those who do these actions to help said target, like a vaccine to prevent an infection; a penetration tester could reveal weaknesses, test implementations of new securities, and advise on better practices to prevent an intrusion.

What Penetration Testers Do

Implementing tools and techniques that real-world hackers use, penetration testers attempt to gain access to information from active systems by exploiting weaknesses in the security infrastructure. This increase can occur due to a poorly made system or personnel not practicing proper cybersecurity practices. During these simulated attacks, the testers document in detail the actions they performed for the organization being tested to review how they could improve their performance. With their help, organizations can better prepare for when a bad actor tries to compromise their system, saving them money from fines and trust from their customers. Many companies in entire industries come victim to hacking attacks from individuals or rival groups to steal what they can from the company's system. As stated in an article from *the cybersecurity guide*, "One of the basic truths of human nature generally... is that bad actors will attempt to seize opportunities to take advantage of vulnerabilities." (*How to Become a Penetration Tester (Updated for 2020)*, 2021) Penetration testers fall under the category of ethical hackers, or hackers that provide their skills to companies so that they can be better prepared for other malicious hackers (Staff Writers, 2019). Since the purpose of penetration testers is to hack their employer's system, they would use techniques used in the real world, one of which is field research. Looking over the employee roster, they can target individuals that could get them access by observing their online presence and seeing if they could've devolved too much info for malicious intent to occur quicker.

Penetration tester: Not just for corporations

Most of the time, someone in the discipline of penetration testing will be for large corporations, but that has a rippling effect that can help a large majority of people. An example of how this can work is when they're testing a banking or medical archival firm and notice a fault in the code/firewall that could compromise millions of people's personal information. The tester takes note and passes it up the chain for a patch to be released, preventing such an action from occurring. (IBM, 2023) Now those people have their information secured under better conditions. Possibly saving thousands of dollars and the corporation millions of dollars in fees and court costs.

Conclusion

Though being a penetration tester is only a small part of the whole of cyber security, I consider it a key aspect of maintaining a safe online environment from those who attempt to exploit it. Like in the real world, no defense is unventilatable. There is always going to be a weakness to exploit or a hole someone forgot to cover up because they were made by imperfect beings, programmers and developers. I would go as far as to say that penetration testers are vital for a continued presence online; without them, even more significant and more detrimental security breaches would occur.

References:

Staff Writers. (2019, September 30). *How to Become a Penetration Tester | Requirements for Penetration Tester Jobs*. CyberDegrees.org; CyberDegrees.org. https://www.cyberdegrees.org/jobs/penetration-tester/

How to Become a Penetration Tester (Updated for 2020). (2021, May 4). Cybersecurity Guide. https://cybersecurityguide.org/careers/penetration-tester/

IBM. (2023, January 24). *Penetration testing*. Ibm.com. https://www.ibm.com/think/topics/penetration-testing