Slide 1: Introduction

Good morning, good afternoon, good evening, wherever you are, thank you for joining us today. I’m pleased to be giving this talk on Penetration Testing, as I personally find the topic quite fascinating. Given how big the Cyber Security industry is, it's another perspective on how to strengthen the security posture of a system and improve its resilience to external threats. So let's get started.

Slide 2: About me

My name is Joseph Doba, and I’m a Cyber Security Specialist located in Victoria, BC. I also have a background in Audio Engineering, Web Development, Music, and eCommerce. I've been fascinated by computers for over 20 years, and I always loved tinkering with technology, whether it's with synthesizers, modding video games, computer programming, or other endeavors that capture my curiosity.

Slide 3: Overview

We will start with a brief overview of what Red Team and Blue Team dynamics are, How Penetration testing is defined, common methodologies, a use case scenario using the Premium House Lights Inc case study, some common tools of the trade, and the conclusion.

Slide 4: Blue Team Red Team

So, What are the blue and red teams? In cybersecurity, they represent a domain of security from either defending or attacking. Both teams work together to strengthen the other.

Blue Team: The Blue Team are the 'defenders'. They protect the organization’s systems and data by setting up security measures, monitoring for suspicious activity, and conducting incident response to live attacks.

Red Team: On the other side, the Red Team are the 'attackers'. They simulate real-world cyberattacks to find vulnerabilities and weaknesses, as per the rules of engagement set beforehand. They think and act like hackers, therefore using similar tools and techniques as real threat actors to infiltrate systems.

The key difference between Red Team and Penetration Tester, while they are both in Offensive Security, is that a Penetration Tester is limited by scope, such as specific targets, testing methods, depth of testing, exclusions, and timeframes agreed upon with the client—whereas a general Red Team operates with broader objectives, including social engineering, phishing, and ethical hacking, often without boundaries or limitations on scope.

Slide 5: Penetration Testing Concepts

https://csrc.nist.gov/glossary/term/penetration_testing
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

The National Institute of Standards & Technology (aka NIST), has quite a lengthy definition, yet it does capture it quite well.

"Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers."

However, for sake of time, a Penetration test is simply a simulated real-world attack scenario of a systems security effectiveness, with the goal to see how many vulnerabilities they can exploit at once and how deep within a network an attacker could go, then report those findings to the blue team for remediation. It's better that we find them first, rather than a malicious actor since they're not going to be as nice about letting us know they found a vulnerability.

Slide 6: Methodology

https://igspectrum.com/network-penetration-testing/
https://igspectrum.com/wp-content/uploads/2021/08/Network.png

Pen testers have permission to infiltrate a system. Once they have permission, their method is broken down into steps to assess the system defenses, and how to best improve upon them.

In the initial scoping and Objectives agreement, terms of engagement are used to determine rules of what's allowed during a test. These attacks are suppose to be as close to a real attack as possible. These rules are in place to allow Pen testers to work, without destroying or disrupting services entirely.

Once it starts, Reconnaissance, Scanning, and Exploitation follow Lochheed Martin's Cyber Kill Chain framework, which provides a useful model for understanding the typical flow of many cyber attacks.

Once complete, and the attack is concluded, reports and methods on how to remediate and patch said vulnerabilities are shared with the Blue Team, they improve their defenses, which in turn forces Red Team to come up with more sophisticated attacks, ad nauseum.

Slide 7: Case Study

Since Pen Testers are using the same tools and are thinking like adversaries, many of the tactics outlined in the Premium House Lights study would be in the Pen Tester toolkit as well. Imagine if we found these vulnerabilities first? It would be easy to make recommendations such as encrypting the data flow, and other practices such as sanitizing inputs so they're not exploited to SQL injection attacks, and so forth.

Slide 8: Tools

Some of the tools Pen testers use are similar to Blue Team, however the crucial difference is for offensive security. Tools such as metasploit, burp suite, and Nessus are designed to find openings to exploit in systems, even offensive security distributions such as Kali Linux come with a suite of tools out of the box to aid this objective. Since technology changes at a rapid pace, there's always something new to learn and exploit, before malicious actors do.

Slide 8: Conclusion

"In conclusion, penetration testing involves simulating attacks on predefined attack surfaces to find and fix vulnerabilities. This practice ultimately helps organizations improve their security posture and protect their valuable assets. By identifying and addressing weaknesses before malicious actors can exploit them, penetration testing plays a crucial role in maintaining robust defenses and ensuring the overall safety of systems and data.