**Topics in Penetration Testing**

**Penetration Testing (in General):**

Your research (notes) and write up should be able to:

1. Define what penetration testing is and give a brief history of penetration testing.
2. Include statistics on penetration testing in general
3. Explain why penetration testing is vital in a secure program
4. Answer: What cybersecurity frameworks are satisfied by the use of penetration testing and its tools?
5. Explain why non-profits want to utilize penetration testing
6. Optional: Explain the difference between penetration testing through virtual machines vs. AWS vs. cybersecurity labs

**Group Members:** Mishelly Sandoval / Lucas Higgs

**Password Cracking:**

Your research (notes) and write up should be able to:

1. Define what password cracking is as a method of penetration testing
2. Explain how password cracking works and why it is used by cyber criminals
3. Include statistics on password cracking as a form of penetration testing
4. Discuss what John-the-Ripper is and how it is used (Or discuss another password cracking tool used in pentesting). You can explain how it is used within AWS (because TKH utilizes AWS) and outside of AWS.
5. Technical documentation - steps that clearly show how to download, install and use a password cracking tool

**Group Member:** Jane Pierre

**Social Engineering:**

Your research (notes) and write up should be able to:

1. Define what social engineering is as a method of penetration testing
2. Explain how social engineering works and why it is used by cyber criminals
3. Include statistics on social engineering as a form of penetration testing
4. Discuss what Social Engineer Toolkit (SET - can be used in AWS) is and how it is used (Or discuss another social engineering tool used in pentesting). You can explain how it is used within AWS (because TKH utilizes AWS) and outside of AWS.
5. Technical documentation - steps that clearly show how to download, install and use a social engineering tool

**Group Member:** Elizabeth Bond

**Web Application Testing:**

Your research (notes) and write up should be able to:

1. Define what network scanning is as a method of penetration testing
2. Explain how network scanning works and why it is used by cyber criminals
3. Include statistics on web application testing as a form of penetration testing
4. Discuss what BurpSuite is and how it is used (Or discuss another web application tool used in pentesting like OWASP ZAP). You can explain how it is used within AWS (because TKH utilizes AWS) and outside of AWS.
5. Technical documentation - steps that clearly show how to download, install and use a web application testing tool.

**Group Member:** Frederick Asante

**Exploitation**:

Your research (notes) and write up should be able to:

1. Define what exploitation is as a method of penetration testing
2. Explain how exploitation works and why it is used by cyber criminals
3. Include statistics on exploitation as a form of penetration testing
4. Discuss what John the ripper & Metasploit are and how they are used (Or discuss another exploitation tool used in pentesting). You can explain how they are used within AWS (because TKH utilizes AWS) and outside of AWS.
5. Technical documentation - steps that clearly show how to download, install and use an exploitation tool

**Group Member:** Tianna Green/Shamar

**Network Scanning:**

Your research (notes) and write up should be able to:

1. Define what network scanning is as a method of penetration testing
2. Explain how network scanning works and why it is used by cyber criminals
3. Include statistics on network scanning as a form of penetration testing
4. Discuss what nmap is and how it is used (Or discuss another network scanning tool used in pentesting like Masscan). You can explain how it is used within AWS (because TKH utilizes AWS) and outside of AWS.
5. Technical documentation - steps that clearly show how to download, install and use a network scanning tool.

**Group Member:** Shamar Brown/ Aaron Kaah

**Sprint Three Deliverables**

**Group:**

1. Sprint Three Summary
2. Sprint Three PPT Presentation
3. Technical Documentation on the tools used in this sprint
4. Updated group GitHub repository

**Individual Roles:**

1. ***If you are working with a penetration testing category/tool:***
   1. A written paragraph describing your penetration testing category (for example a discussion on password cracking in general) and the specific tool used (for example a discussion on john-the-ripper as a password cracking tool) with APA citation. If writing isn’t your strong suite, provide clear bulleted notes and the website where you found your information. Make it easy for your work to be streamlined into this Sprint without having to reach out to you too much. 🙂
   2. Technical documentation - steps that clearly show how to download, install and use the pentesting tool
2. ***Documentation -* Jane Pierre and Elizabeth Bond**
   1. Responsible for writing and editing the summary for this sprint
   2. Responsible for compiling technical documentation into one large document
   3. Responsible for updating the GitHub group repository
3. ***PowerPoint Presentation- Tianna Green***
   1. Responsible for developing, designing and inputting content for the PPT presentation