**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. What cybersecurity frameworks are satisfied by the use of penetration testing and the tools?
5. Methodology

**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.
   * Penetration testing, also known as pen testing or ethical hacking, is a simulated attack on a computer system or network to identify vulnerabilities and weaknesses that could be exploited by malicious actors. The goal of penetration testing is to simulate a real-world attack to uncover security vulnerabilities before they can be exploited by actual attackers.
   * Penetration testing typically involves using a combination of automated and manual techniques to identify vulnerabilities, such as insecure software configurations, weak passwords, and unpatched software. The results of a penetration test are typically reported to the organization that commissioned the test, along with recommendations for addressing any identified vulnerabilities.
   * Penetration testing is an important component of an organization's overall security strategy, as it can help identify and remediate vulnerabilities before they are exploited by attackers and can help ensure compliance with regulatory requirements.

**Different types:**

* **White Box Testing**
  + Provides testers with all the details about an organization's system or target network and checks the code and internal structure of the product being tested. White box testing is also known as open glass, clear box, transparent or code-based testing. (Yasar & Mehta, 2022)
* **Black Box Testing**
  + Is a type of behavioral and functional testing where testers aren't given any knowledge of the system. Organizations typically hire ethical hackers for black box testing, where a real-world attack is carried out to get an idea of the system's vulnerabilities.(Yasar & Mehta, 2022)
* **Gray Box Testing**
  + Is a combination of white box and black box testing techniques. It provides testers with partial knowledge of the system, such as low-level credentials, logical flow charts and network maps. The main idea behind gray box testing is to find potential code and functionality issues. (Yasar & Mehta, 2022)

**Different Stages:**

* Reconnaissance and planning
* Scanning
* Obtaining Entry
* Maintaining Access
* Analysis (Yasar & Mehta, 2022)
  + the vulnerabilities the testers exploited;
  + the type of sensitive data the testers accessed; and
  + the amount of time the testers stayed connected to the target.
* Cleanup and Remediation (Yasar & Mehta, 2022)

**History:**

* One of the early pioneers in penetration testing development was James P. Anderson. In his 1972 report, Anderson outlined a series of definitive steps that tiger teams could take to test systems for their ability to be penetrated and compromised. Anderson’s approach included first identifying vulnerability and designing an attack on it, and then finding the weakness in the attack itself and ways to neutralize its threat. ( Infosec, 2021)
* In the 1970s and 1980s, research into how to create a secure system was still novel. Anderson’s 1980 publication that showed how to design a program to monitor the use of a computer system to identify unusual use that might signal hacker activity is so simple that any savvy computer user today would readily understand how it works and be able to point to any number of ways to get around it.
* Another system that was developed and used by a broad range of government, military and corporate entities was Multics (Multiplexed Information and Computing Service). It may be the granddaddy of computer systems, operating in some form or other from 1965 to 2000 and arguably still operating today. Honeywell eventually purchased it and service education, government, and industry. The key development that came from Multics was that it delivered secure computing service to users in remote locations, a radical development for the period. Fundamental designs from Multics are still in use even today in other operating systems such as UNIX.
* The Multics security system was so good it became the first and for many years the only operating system awarded a B2 rating by the US government. Still, in 1974, the US Air Force conducted an ethical hack on its Multics system, one of the earliest known white hat attacks in the USA, and plenty of vulnerabilities were revealed. Regardless, Multics is still considered to be one of the most secure systems in the world, in part because all of its security features are part of the standard product, rather than supplementary or add on features. As a result, application designers had to ensure that their product met the access design security clearances if they wanted their products to work with the Multics system. Today, though, when security features can be optional, and often are, applications may not be able to meet such requirements, leaving individual computer users vulnerable to hacking.( Infosec, 2021)
* In the 1990s, a security administrator tool for analyzing networks (SATAN) became available. The name scandalized, and developers added a feature allowing it to be reconfigured to SANTA, a testament to the perhaps natural mischievous nature of penetration testers and hackers. The tool allowed administrators to run a series of tests on their own networks to help identify areas of possible vulnerability and created a report along with a tutorial explaining what issues might arise. SATAN is no longer in development and has been replaced by other tools such as nmap and Nessus, to name a few.( Infosec, 2021)

**Today’s Tools:**

* Kali Linux, used in digital forensics and penetration testing. It contains eight standard security tools including Nmap, Aircrack-ng, Kismet, Wireshark, Metasploit Framework, Burp Suite and John the Ripper. That a single system would contain so many penetration testing tools demonstrates how much more sophisticated today’s technology has become and how many ways ingenious hackers are discovering to create mischief in shared computing environments, especially the Internet. Pentoo is a similar penetration testing focused system.
* The statistics on threats posed by hackers are sobering. A recent RAND report suggests that in one year as many as 65 million people in the USA alone have had their personal data breached in some way or other, and that cyber-crime generates billions of dollars in revenue each year. As well, the very tools created by those who work to secure cyber information can also be used to exploit it.( Infosec, 2021)

1. **Include statistics on penetration testing in general**
   * According to a recent study, 71% of businesses consider cybersecurity as their top priority.(Abdalslam, 2023)
   * 77% of companies use penetration testing to evaluate their security measures.(Abdalslam, 2023)
   * The global penetration testing market size is expected to reach USD 4.5 billion by 2025.(Abdalslam, 2023)
   * 57% of organizations have experienced a cybersecurity attack in the last year.(Abdalslam, 2023)
   * 68% of businesses believe that a cyber-attack is inevitable.(Abdalslam, 2023)
   * The average cost of a data breach in the US is $8.19 million.(Abdalslam, 2023)
   * 90% of cyber attacks start with a phishing email.(Abdalslam, 2023)
   * 69% of organizations do not have a formal incident response plan.
   * 43% of cyber attacks target small businesses.(Abdalslam, 2023)
   * [60% of small businesses](https://abdalslam.com/small-business-statistics) go out of business within six months of a cyber attack. (Abdalslam, 2023)

**Pen Testing Overview:**

* + The global penetration testing market is expected to reach $4.5 billion by 2025.(Abdalslam, 2023)
  + Penetration testing is now a requirement for compliance with many industry regulations, including PCI DSS, HIPAA, and ISO 27001.(Abdalslam, 2023)
  + According to a report by Cybersecurity Ventures, the global cost of cybercrime is projected to reach $10.5 trillion by 2025.(Abdalslam, 2023)
  + Penetration testing is a proactive approach to identifying and addressing security vulnerabilities rather than a reactive approach after a breach has occurred. (Abdalslam, 2023)

**Resources:**

* Abdalslam. (2023, April 13). *Penetration testing statistics, trends and facts 2023*. Abdalslam. Retrieved May 1, 2023, from <https://abdalslam.com/penetration-testing-statistics#:~:text=77%25%20of%20companies%20use%20penetration,a%20cyber%20attack%20is%20inevitable>.
* Infosec. (2021, September 4). *The history of penetration testing*. Infosec Resources. Retrieved May 1, 2023, from <https://resources.infosecinstitute.com/topic/the-history-of-penetration-testing/>
* Yasar, K., & Mehta, P. (2022, November 18). *What is penetration testing?: Definition from TechTarget*. Security. Retrieved May 1, 2023, from <https://www.techtarget.com/searchsecurity/definition/penetration-testing>

**3.Explain why penetration testing is vital in a secure program**

* Penetration testing, also known as pen testing, is an essential part of a secure program because it helps identify vulnerabilities and weaknesses in an organization's systems, applications, and network infrastructure.
* Penetration testing involves simulating an attack on the organization's IT infrastructure to identify weaknesses that attackers could exploit to gain unauthorized access or steal sensitive information. The goal is to identify vulnerabilities before an attacker does, so they can be fixed or mitigated to prevent a potential breach.
* By conducting penetration testing, an organization can proactively identify and address vulnerabilities, reduce the risk of a successful cyber attack, and ensure that its security measures are effective. It can also help organizations comply with regulations and industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), which requires regular penetration testing for organizations that process credit card payments.

Overall, penetration testing is an essential tool for organizations to assess and improve their security posture, identify and address vulnerabilities before they can be exploited by attackers, and ensure that their systems and data are adequately protected. Pen testing is an essential aspect of any secure program. It involves simulating a real world cyber attack on a system, network or application in order to identify where there are vulnerabilities and weaknesses that can potentially be exploited by attackers.

**4. What cybersecurity frameworks are satisfied by the use of penetration testing and the tools?**

Several cybersecurity frameworks require or recommend the use of penetration testing as part of a comprehensive security program. Some examples are listed below.

**Frameworks:**

* NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) Cybersecurity Framework recommends the use of penetration testing to identify vulnerabilities and assess the effectiveness of security controls. It is part of the "Detect" and "Respond" functions of the framework.
* ISO/IEC 27001: This standard for information security management systems (ISMS) requires organizations to conduct periodic risk assessments and take appropriate measures to manage those risks, which can include penetration testing. It is part of the "Assess" and "Evaluate" phases of the ISMS.
* PCI DSS: The Payment Card Industry Data Security Standard requires organizations that process credit card payments to conduct regular penetration testing to identify vulnerabilities and assess the effectiveness of security controls. It is part of Requirement 11.3 of the standard.
* OWASP: The Open Web Application Security Project (OWASP) provides a range of resources and tools for identifying and mitigating security vulnerabilities in web applications, including a testing guide that covers penetration testing techniques.

There are various tools that can be used in penetration testing, depending on the specific needs and goals of the testing. Listed below are some of the tools used for penetration testing.

**Tools:**

1. **Nmap:** A network mapping tool used to discover hosts and services on a network, as well as identify vulnerabilities and potential attack vectors.
2. **Metasploit:** An exploitation framework used to test and demonstrate various attack scenarios, including vulnerabilities in web applications, databases, and operating systems.
3. **Burp Suite:** A web application testing tool used to identify vulnerabilities in web applications, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
4. **Wireshark:** A network protocol analyzer used to capture and analyze network traffic, including packets, headers, and payloads.
5. **John the Ripper:** A password cracking tool used to test the strength of passwords by attempting to crack them through brute force or dictionary attacks.
6. **Nessus:** A vulnerability scanner used to identify security vulnerabilities in systems, applications, and network infrastructure.
7. **Aircrack-ng:** A suite of tools used to test and exploit weaknesses in wireless networks, including cracking Wi-Fi passwords and conducting man-in-the-middle attacks.

Penetration testing is a valuable tool for any organization looking to improve its security posture and comply with various cybersecurity frameworks and standards. By identifying vulnerabilities and assessing the effectiveness of security controls, organizations can proactively manage risk and protect their critical assets from cyber threats. t's important to choose the right tool or combination of tools based on the specific needs and goals of the testing, as well as the systems and applications being tested. It's also essential to ensure that the testing is conducted in a safe and ethical manner to avoid causing any harm or damage to the organization being tested.

**5. Methodology**

Penetration testing methodology is a structured approach used to plan, execute, and report on a penetration testing engagement. It involves a series of steps or phases that help ensure the testing is thorough, systematic, and consistent. While specific methodologies may vary depending on the testing goals, scope, and environment, here are the general steps involved in a typical penetration testing methodology:

1. **Planning**: This involves defining the scope of the testing, identifying the goals and objectives, and developing a testing plan that outlines the testing methodology, tools, and techniques that will be used.
2. **Reconnaissance:** This involves gathering information about the target systems, applications, and network infrastructure using various techniques, such as network scanning, OSINT (Open Source Intelligence) gathering, social engineering, and dumpster diving.
3. **Enumeration:** This involves identifying the specific systems, services, and applications that will be targeted for testing, and gathering more detailed information about them, such as versions, configurations, and vulnerabilities.
4. **Vulnerability analysis:** This involves identifying and exploiting vulnerabilities in the target systems, applications, and network infrastructure, using various techniques, such as manual testing, automated scanning, and exploitation frameworks.
5. **Reporting:** This involves documenting the findings of the testing, including any vulnerabilities identified, their severity, and recommendations for remediation. The report should be detailed, concise, and provide actionable recommendations for improving the security posture of the organization.
6. **Remediation:** This involves addressing the vulnerabilities identified in the testing and implementing measures to prevent similar vulnerabilities from occurring in the future.
7. **Verification:** This involves re-testing to verify that the vulnerabilities have been properly remediated and that the organization's security posture has improved.

following a structured methodology for penetration testing can help ensure that the testing is thorough, systematic, and consistent, and that the organization receives a comprehensive report that helps them improve their security posture.

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