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

1. Define what exploitation is as a method of penetration testing
   1. Exploitation is the step after scanning, where the penetrator attempts to gain access to the target system so they can then exploit the identified vulnerabilities (this is where Metasploit is used). It is the most delicate of the steps within penetration testing because it requires bypassing security restrictions. Penetrators must be cautious that they don’t compromise or damage the system.
2. Explain how exploitation works and why it is used by cyber criminals
   1. Exploitation works by a cyber criminal using some tool to find vulnerabilities within a system. Methods: hacking of social media and email passwords, phishing- fake emails asking for security information and personal details, malicious software- including ransomware that allows criminals to hijack files and hold them ransom and distributed denial of service (ddos) attacks against websites. Cyber criminals exploit security and human vulnerabilities so they can steal passwords, data, or money.
3. Include statistics on exploitation as a form of penetration testing
   1. In 2022 the exploitation of vulnerabilities was down 15% since 2021, and there were 33% fewer vulnerabilities that were known to be exploited for ransomware attacks
   2. In 2020 30% of the vulnerabilities reported were exploited within a week of disclosure, in 2021 it went to 50% and in 2022 it rose to 56%
   3. Citrix remote access vulnerability attacks increased 2,066% in 2022 while Cisco vulnerability attacks increased by 41%, RDP vulnerability attacks increased by 85% and VPN vulnerability attacks increased by 610% (O’driscoll, 2023)
   4. 31% of companies detected attempts to exploit software vulnerabilities (O’driscoll, 2023)
   5. 80% of exploits are published before CVEs (common vulnerability exposures)are released (James, 2023)
   6. The presence of critical vulnerabilities increased to 8% when it comes to applications that process payment card data (James,2023)
   7. 57% of cyber attacks are attributed to phishing and social engineering (James,2023)
   8. Zero-day malware accounted for 66% of all threats in the last quarter of 2021 (James,2023)
   9. Companies with more than 10,000 employees have the most amount of critical severity vulnerabilities (James,2023)
4. Discuss what John the ripper is and how it is used (Or discuss another exploitation tool used in pentesting). You can explain how it is used within AWS (because TKH utilizes AWS) and outside of AWS.
   1. John the ripper is a password cracking tool that can be used to perform brute force attacks using different encryption technologies and helpful wordlists. Penetration testers and ethical hackers use this to find the “true passwords” behind hashes. It can help to show how easy it is to reveal weak passwords as well as sophisticated ones. (Maury, 2023)
   2. How to crack passwords with John the Ripper : “The “john” command has an extensive range of options and flags you can use to run accurate sessions and match the specific format and encryption of your targeted password. The tool has built-in wordlists that automatically apply by default, but you can specify your own with *–wordlist* and the path to your custom wordlist” (Maury, 2023)
   3. In AWS, John the Ripper supports recovering or auditing security of passwords to hundreds of different hash and cipher types
5. Technical documentation - steps that clearly show how to download, install and use an exploitation tool
   1. In AWS there is a prebuilt and precogfigured John the Ripper in the home directory. To run it you will just have to type “john”
   2. Download and install instructions for Ubuntu: <https://linuxhint.com/john_ripper_ubuntu/>
   3. Download and install instructions for Windows: <https://www.geeksforgeeks.org/how-to-install-john-the-ripper-on-windows/>
   4. Download and install ibstructiosn on Mac Osx: <https://www.youtube.com/watch?v=fzrgz6higj0>

Research:

<https://www.securityweek.com/vulnerabilities-being-exploited-faster-than-ever-analysis/#:~:text=To%20be%20precise%2C%2056%25%20of,an%2087%25%20increase%20over%202020>.

<https://resources.infosecinstitute.com/topic/top-18-tools-for-vulnerability-exploitation-in-kali-linux/>

<https://lodestone.com/insight/mastering-the-kill-chain-step-four-exploitation/>

<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime#:~:text=Cyber%20criminals%20seek%20to%20exploit,social%20media%20and%20email%20passwords>

<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/#:~:text=Exploitation,-Exploitation%20is%20the&text=In%20the%20exploitation%20step%20of,network%20to%20reach%20their%20targets>.

<https://www.rapid7.com/blog/post/2023/02/28/a-shifting-attack-landscape-rapid7s-2022-vulnerability-intelligence-report/>

<https://www.esecurityplanet.com/products/john-the-ripper/#:~:text=John%20the%20Ripper%20is%20a,the%20true%20passwords%20behind%20hashes>.

<https://linuxhint.com/john_ripper_ubuntu/>

<https://www.geeksforgeeks.org/how-to-install-john-the-ripper-on-windows/>