**Nancy, Jane, Ella, Gyan, Neiman, Anna, Emilie, Francisco, Victor, Ameha, Jared, Volha, Tyesha, Alena, Mayra, Diego**

**Cyber Range Team Capstone Project Summary**

**Sprint One**

**The Knowledge House**

**Professor George Robbins**

**04/09/23**

There is an average of 2,200 cyberattacks per day with the United States remaining the most highly targeted country with 46% of global cyber incidences, according to research updated in January 2023 by CompTIA (CompTIA, 2023). Cybersecurity has developed to be one of the most in-demand industries in response to the growing threats. Organizations need proper security assessments to ensure that they are operating in compliance and are effective at defending the organization from unknown or “zero-day threats”. Red teaming is a proactive approach to cybersecurity that simulates real-world attacks to identify vulnerabilities and improve defenses.

In a move towards launching a full-scale cloud native cybersecurity training range environment in AWS, we are implementing several offensive security measures that consider social engineering, password cracking, network scanning, web application testing, and, exploitation, and penetration testing.

Social engineering is cyberattacks where attackers trick people into divulging sensitive information or performing actions they wouldn't normally do. The success of a social engineering attack depends on the attacker's ability to manipulate the victim's trust and emotions and can have serious consequences such as data breaches, identity theft, and financial loss. We are deploying Social-Engineer Toolkit (SET), an open-source tool that provides a range of social engineering attacks, including phishing, spear-phishing, and credential harvesting, to provide real-life scenarios of how attackers operate so clients and organizations can identify behaviors to look out for to mitigate risks.

Password cracking tools are software applications designed to reveal or recover passwords for digital authentication mechanisms. These tools use various techniques, such as brute force, dictionary attack, and hybrid attack, to guess or crack passwords. John the Ripper is a popular password-cracking tool that can crack passwords from various operating systems, including Linux, macOS, and Windows (J. the Ripper, n.d.). This tool can also use different hashing algorithms, including MD5, SHA-1, and bcrypt. To use John the Ripper, the program needs to be provided with a password file, which contains hashed passwords. A hashed password is a one-way cryptographic function that transforms a password into a fixed-length string of characters representing the original password. The program then uses the selected cracking method to try and crack the passwords. John the Ripper can also use wordlists and rulesets to modify dictionary words and increase the likelihood of cracking passwords.

Network scanning in AWS is a process of analyzing the network infrastructure of an Amazon Web Services (AWS) environment to identify potential security issues, misconfigurations, and vulnerabilities. AWS Inspector is an automated and continual vulnerability scanning service that assesses applications deployed on AWS. Inspector uses a set of predefined rules to assess the security of your applications, including network configuration, operating system vulnerabilities, and application security. Inspector generates a report with a list of security issues and recommendations for remediation. Nmap is an open-source tool used for network exploration and security auditing. Nmap can be used to do different scans, including host discovery, port scanning, and OS detection. It can also detect vulnerabilities such as misconfigured services or outdated software. OpenVAS is a powerful vulnerability scanner that can be used in conjunction with Nmap to identify potential security weaknesses in a network (Lansweeper Community, 2023).

Web application testing is the process of testing web-based software applications to ensure they function properly and meet the desired requirements. Ghostbuster is a web application vulnerability scanner that can help identify security weaknesses in a website or web application. It is designed to automate the process of detecting vulnerabilities such as SQL injection, XSS, CSRF, and other common web application security issues. Ghostbuster can be particularly useful when it comes to web application testing using Vulhub, a vulnerable web application environment designed for practicing penetration testing. By running Ghostbuster against Vulhub, testers can identify potential vulnerabilities and weaknesses in the system, allowing them to better understand the risks associated with the application and take appropriate measures to mitigate those risks.

Exploits are a common type of cyber attack that exploits vulnerabilities or weaknesses in computer systems, software applications, or networks to gain unauthorized access, escalate privileges, or execute malicious code. Mitre ATT&CK framework was chosen to simulate an exploit on S3 bucket and identify weaknesses in security defense. For a demonstration, a common attack vector for cloud exploitation is misconfigured in S3 buckets. Attackers can exploit misconfigured S3 buckets to gain unauthorized access to sensitive data stored in the cloud.

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack by a malicious actor. The NIST pen-testing methodology better serves the immediate demands of our use case. To accommodate the large variety of utilities that pen-testing can include the training range will mainly use Kali Linux along with the surplus of tools and programs that come with it (Metasploit, Nmap, etc.) to best illustrate the processes involved in different types of penetration testing. Vulnerable machines from Vulnhub will be imported, uploaded to AWS S3, and run as EC2 instances in a private subnet with the intention to be exploited with Kali Linux by students using the training range. The vulnerable machines chosen will have supplementary walkthrough documentation and instructional videos provided by Hackersploit to better elaborate upon the concepts while guiding students step-by-step through the material.

Ultimately, the goal of our cyber range is to provide a safe and realistic environment for training and testing cybersecurity skills. While Red teaming is a crucial aspect of this training as it allows participants to simulate real-world attacks and identify vulnerabilities in a system, it is essential to be mindful of policies when red teaming to ensure that the simulated attacks do not violate any legal or ethical boundaries. Staying in compliance with policies and regulations helps to avoid any potential legal or reputational consequences that could arise from unauthorized actions. By utilizing red team tactics, organizations can better understand their security strengths and weaknesses and improve their overall cybersecurity posture.

**References**

How *to scan an AWS cloud environment*. Lansweeper Community. (2023, January 12). Retrieved April 9, 2023, from https://community.lansweeper.com/t5/scanning-your-network/how-to-scan-an-aws-cloud-environment/ta-p/64485

J. the Ripper. (n.d.). Retrieved April 7, 2023, from<https://www.openwall.com/john/>

Lainhart, J. (2020).

Watters, A. (2023, January 27). *Top 50 cybersecurity statistics, figures and facts*. Top 50 Cybersecurity Statistics, Figures and Facts. Retrieved April 7, 2023, from https://connect.comptia.org/blog/cyber-security-stats-facts