Vulnerability Analysis – Literature Review Activity

In our modern world of globalisation and technology, cybercrime is becoming more prevalent and poses a significant challenge to research, risk management, and cybersecurity. Unfortunately, limited data on cyber risks is available, exacerbating the problem. However, open datasets can provide invaluable assistance to cyber insurers, companies, and cybersecurity stakeholders to develop sustainable products and benchmark their internal postures. The most common cyber risk events are cyberattacking and data breaches, which have increased frequently in recent years (Cremer et al., 2022).

Li et al. (2023) state that software vulnerabilities can lead to severe consequences, such as data tampering and loss. To address this issue, researchers have suggested using empirical studies and automated techniques to identify and eliminate vulnerabilities in source code. However, the accuracy and applicability of these approaches depend heavily on the quality of the information extracted from publicly available datasets of vulnerabilities.

The National Vulnerabilities Database (NVD) assigns a Common Vulnerabilities and Exposures (CVE) identifier to every vulnerability. These identifiers define vulnerabilities as weaknesses in the computational logic of software or hardware components that negatively impact confidentiality, integrity, or availability. Coding changes, specification changes, or specification deprecations may be necessary to mitigate these vulnerabilities (NIST, 2019).

The severity of a vulnerability is measured using the Common Vulnerability Scoring System (CVSS), which industries, organisations, and governments widely use. It consists of three metric groups: Base, Temporal, and Environmental. The Base metrics generate a score between 0 and 10, which can be adjusted by scoring the Temporal and Environmental metrics. CVSS has become a standard measurement system by providing reliable and consistent vulnerability scores. NVD offers CVSS assessments for all published CVE records (NIST, 2019).

To ensure the security of websites, I conducted a thorough literature search and audit on various software sites and the national vulnerabilities database. This activity aimed to create a baseline audit of potential vulnerabilities that could pose a website risk. To achieve this, I carried out a systematic mapping study that delved into the structure and features of several vulnerability databases. I also examined their popularity, intended uses, methodologies and suggested tools. This detailed analysis enabled me to understand the potential risks that websites may face and develop effective strategies to mitigate them.

Effective cybersecurity is not just the absence of attacks. Cybercrime continues to cost billions every year. SecurityScorecard (N.D.) provides valuable information on network security threats, their various forms, and how to detect them. Protecting the network from these threats is crucial to safeguarding your valuable data. Network security threats can be categorised into four types: external, internal, structured, and unstructured. Understanding these categories is essential to securing your network.

SecurityScorecard (N.D.) also explains that vulnerabilities are flaws that attackers can exploit. They can be errors or oversights, such as misconfigured cloud storage services or lack of phishing training. Cyber threats are ever-evolving, including phishing attacks, ransomware attacks, malware, DDoS attacks, Advanced Persistent Threats (APTs), and SQL Injection.

To identify cybersecurity threats and vulnerabilities, SecurityScorecard (N.D.) recommends the following steps:

1. Monitor your network as an attacker to identify potential weaknesses.
2. Use threat intelligence to stay ahead of potential attacks.
3. Perform penetration testing to identify where defences may fail.
4. Manage permissions to control access to sensitive data.
5. Use firewalls to prevent unauthorised access to your network.
6. Continuously monitor and update your security controls to catch new threats.

To prepare for network security threats, consider the following tips from SecurityScorecard (N.D.):

1. Segregate your network into zones to limit the impact of an attack and mitigate threats.
2. Use a proxy server to monitor user behaviour and control site access.
3. Implement Network Address Translation to hide the internal network from the outside world and prevent unwanted website access and targeted attacks.
4. Consider using SecurityScorecard to monitor your networks, where our security ratings, based on an A scale, make it easy to prove governance over your vendor risk management program.

In the realm of cybersecurity, Gonzalez (2020) emphasises the vital role that threat modeling plays. This entails identifying potential threats, implementing procedures for detection and response, and deploying appropriate countermeasures. The process typically involves five steps: threat intelligence, asset identification, mitigation capabilities, risk assessment, and threat mapping. Eight primary methodologies are available for threat modeling, each offering a distinct approach to evaluating IT asset threats.

Gonzalez (2020) also highlights that organisations can employ various threat modeling methodologies based on their specific needs and the threats they aim to model. Some of the commonly used methods include:

- STRIDE: This Microsoft-developed model helps identify system threats by evaluating and prioritising systems against Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege.

- PASTA: This 7-step attacker-centric methodology correlates business objectives with technical requirements to identify, count, and prioritise threats. It involves defining business objectives, technical scope, application controls, threat analysis, vulnerability detection, attack enumeration, and risk analysis.
- CVSS: This standardised threat scoring system is used for known vulnerabilities. It helps security teams assess threats, determine patching priorities, and identify existing countermeasures by applying security scores to vulnerabilities as they are released. The system also allows teams to modify risk scores based on individual configurations.

- VAST: This automated threat modeling method generates reliable, actionable results and maintains scalability for large enterprises. It integrates into the DevOps lifecycle to identify various infrastructural and operational concerns by creating two threat models: application and functional.

- Trike: This security audit framework uses threat modeling techniques to manage risk and defence. It generates a step matrix to match possible actions and uses a data-flow diagram to identify threats. It assesses attack risks using a five-point probability scale and evaluates actors based on their permission level for each step.

- Attack trees: These are visual representations of potential attack paths in a system. They are commonly used in threat modeling, particularly during internal reviews of data flow, vendor risk, and system interoperability. Attack trees are often combined with other methodologies like PASTA, CVSS, and STRIDE to make threat modeling more effective.
- Security Cards methodology: This is a creative way to account for uncommon or novel threats and increase knowledge about threats and modeling practices. It uses 42 cards to help analysts answer questions about future attacks and simulate possible attacks.

- Hybrid Threat Modeling Method (hTMM): This methodology developed by SEI combines SQUARE and PnG to enable threat modeling. It eliminates unlikely PnGs, applies Security Cards, summarises results, and assesses risk using SQUARE for consistent and cost-effective results.

Therefore, Gonzalez (2020) states that security teams should clearly understand the system architecture to perform threat modelling effectively, use an ecosystem of tools, document and communicate findings, and foster collaboration and knowledge sharing among stakeholders. By following these best practices, security teams can identify potential attack points, vulnerabilities, and risks and prioritise which threats to address first.

As per Daniels' (2019) definition, network security encompasses protecting digital assets against unauthorised intrusion while safeguarding against cybercrime damages predicted to cost $6 trillion by 2021. To combat these threats, it is crucial to have adequate network security and visibility. Access control, anti-malware software, anomaly detection, and application security tools are utilised to achieve this goal.

Daniels (2019) highlights that network security has three key focuses: protection, detection, and response. Protection involves tools and policies to prevent intrusion, detection is for analysing network traffic, and the answer is for reacting to threats and resolving them quickly. Unfortunately, most businesses lack proper cybersecurity strategies, which is a growing threat as network breaches can compromise sensitive data.

Practical network security tools and devices help protect sensitive information business reputation and ensure continued operational ability. Cyberattacks can impede an organisation's ability to conduct business, leading to loss of revenue and reputational damage. Network security can minimise the impact of cyberattacks, and reliable tools and strategies can help ensure business continuity (Daniels, 2019).

Adequate network security is paramount to safeguarding the business and customers. There are various tools available that can enhance your existing cybersecurity measures by providing comprehensive visibility into network traffic. This increased visibility enables threat responders to identify and expose encrypted attacks, leaving cybercriminals nowhere to hide. By implementing this robust network security solution, you can rest assured that your data, business, and customers are protected (Daniels, 2019).

An IT audit evaluates an organisation's infrastructure, policies, and procedures to guarantee proper and secure operation. It also serves to pinpoint potential vulnerabilities, ensure compliance with privacy and security measures, and identify areas of inefficiency in IT processes. Several types of IT audits include cybersecurity audits, enterprise-level IT structure audits and physical IT facility audits. IT audits generally cover five essential areas: system security, standards and procedures, performance monitoring, documentation and reporting, and systems development (Emley, 2023).

Conducting a cybersecurity audit is crucial to safeguard against data breaches (Cheq, 2023). For instance, this process enables pinpointing vulnerabilities and mitigating risks to prevent significant oversights. It is essential to determine the type of audit, whether internal or external and to understand the distinctions between risk assessment and penetration testing. Be aware of threats like zero-day exploits, password theft, social engineering, DDoS, SQL injections, and malware infections.

According to Cheq (2023), the following best practices should be followed to carry out a successful cybersecurity audit:

1. Assess the situation to determine which issues need attention. Identify categories of threats and get feedback from stakeholders on regulatory compliance. Perform a security gap analysis to identify areas that need improvement to meet security standards. Standardised templates such as ISO 27001 are useful for gap analysis.

2. Objectives should be SMART and include specifics on the best tools for the job. This section can be revisited after the strategy and tactics section is fully fleshed out. For example, if fraud is identified as a primary issue, the main goal might be to contact fraud protection services for assistance.

3. Use the right tools and strategies for specific threats. For example, for Zero-Day Exploitations, use Immunity Debugger, Metasploit, and Nessus; for Password Theft, use Hydra and John the Ripper. Each industry may face more specific threats.

4. Prioritize the most critical threats and counteract them first using a GANTT chart to allocate expected time frames. Consider using Vonage cloud phone systems to delegate tasks to remote teams. Involve your back-end team to ensure adequate technical implementation.
5. Regularly analyse results and stay vigilant against evolving threats to protect your business from ransomware. Identify areas that need improvement and adjust your cybersecurity strategy accordingly until threats are contained to a reasonable level.

A cybersecurity audit is simple and effective if we follow the best practices. Identify risks, use the right tools and strategies, and conduct quality checks to protect your organisation from cyber threats (Cheq, 2023).

Reflection:

In recapping this activity, I realised that the literature search on auditing software sites and reading about the concepts of the national vulnerability database were crucial steps in understanding the challenges developers face in maintaining the security of their applications and sites against cyber threats. Although I encountered some challenges during the research, such as the need for greater familiarity with technical terms and tools, I overcame them by conducting additional research.

The insights gained from this activity will significantly impact my final report as I better understand software vulnerabilities and how to address them. In particular, I am committed to exploring the tools available to test for vulnerabilities and understand their effectiveness in securing applications and websites. This knowledge will be invaluable if I become part of a team that needs to ensure an application or guarantee a website, as I will have a foundation to build on.

References:

- Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, [online] 47(3). doi:https://doi.org/10.1057/s41288-022-00266-6.
- Li, X., Moreschini, S., Zhang, Z., Palomba, F. & Taibi, D. (2023). The anatomy of a vulnerability database: A systematic mapping study. *Journal of Systems and Software*, 201, pp.111679–111679. doi:https://doi.org/10.1016/j.jss.2023.111679.
- NIST (2019). *NVD - Vulnerabilities*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln.
- NIST (2019). *NVD - Vulnerability Metrics*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln-metrics/cvss.
- SecurityScorecard. (N.D.). *How to Identify and Prepare for Network Security Threats and Vulnerabilities*. [online] Available at: https://securityscorecard.com/blog/identify-network-security-threats-and-vulnerabilities/.
- Gonzalez, C. (2020). *6 Threat Modeling Methodologies: Prioritize & Mitigate Threats*. [online] Exabeam. Available at: https://www.exabeam.com/information-security/threat-modeling/.
- Daniels, D. (2019). *14 Network Security Tools and Techniques to Know*. [online] Gigamon Blog. Available at: https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/.
- Emley, B. (2022). *The ultimate guide to conducting an IT audit (with checklist)* | *Zapier*. [online] zapier.com. Available at: https://zapier.com/blog/it-audit/.
- cheq.ai. (2023). *5 Best Practices When Conducting a Cybersecurity Audit*. [online] Available at: https://cheq.ai/blog/5-best-practices-cybersecurity-audit/ [Accessed 18 Nov. 2023].