Using the website(s) assigned to you in Unit 1, carry out the following exercise and answer the questions listed below.

Instructions

Carry out a literature search/audit on software sites and the national vulnerabilities database to create a baseline audit on potential vulnerabilities with websites.

Learning Outcomes

* Identify and analyse security threats and vulnerabilities in network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.
* Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.
* Gather and synthesise information from multiple sources (including internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues.

Record all reflections in your e-portfolio. Find guidance on creating a GitHub accout and e-Portfolio in the Module Resources tab.

|  |  |  |  |
| --- | --- | --- | --- |
| Cyber Kill Chain Phase | Identified in SolarWinds Exploit | Possible Mitigations | Tools to Utilize |
|  |  |  |  |
| Reconnaissance | Investigation in September 2019 | Create separate production and development server | VM, Docker, Firewall |
| Weaponization | Malicious code though backdoor | Conduct regular security audits and vulnerability scans. | VScan |
| Delivery | Attack using software delivery | Source code audit and scanning tools | SAST |
| Exploitation | Taking advantage of company trust | Regular software audits | Security team |
| Installation | Backdoor | Scan traffic and create source code review policy | VScan |
| Command and Control (C2) | Copy Orion traffic | Create an automated monitoring for packets and traffic | Tarpit |
| Actions on Objectives | Data theft | Implement continuous monitoring using logging | Logging tools and email notifications |

References:

(PDF) technical aspects of cyber kill chain - researchgate (no date). Available at: https://www.researchgate.net/publication/281148852\_Technical\_Aspects\_of\_Cyber\_Kill\_Chain (Accessed: February 25, 2023).