Unit 6: An Evaluation of Commonly Utilized Network Scanning and Vulnerability Testing Tools

Objectives:

- Evaluate network scanning and intrusion tools.
- Submit part 1 of your course assessment – the proposal.

Outcomes:

- Select a toolset to use for scanning and vulnerability testing.
- Justify your selection.
- Submit the first part of your course assessment.

Reflection:

There are many different ways to detect vulnerabilities in applications by utilizing various vulnerability scanning tools (Coffey et al., 2018). Used the tools for code analysis and vulnerability testing, bugs in the code are investigated. The use of vulnerability auditing tools enables the detection of many common rootkits and trojans. There are already a growing number of vulnerability scanners available on the market. There are open-source, open-source-free, and premium solutions available. GitHub is a fantastic resource for discovering a large selection of free and open-source software in one convenient location. When choosing a security tool, you need to consider several different factors, such as the kind of vulnerability, the amount of money you have available, how often the security tool is updated, etc. Below we described some famous tools for vulnerability scanning.

- **Nikto2** is a scanner for vulnerabilities in web applications that are both free and open-source (Varghese and Kurian, 2021). Nikto2 can detect around 6700 files that might be harmful and report on server-based versions that are no longer up to date. You won't ever have to stress about the state of your servers again, thanks to Nikto2's notifications and web server inspections. Nikto2 does not provide any remedies or risk assessment tools if a vulnerability is detected. Nikto2, on the other hand, is a program that receives frequent updates and enables a more excellent coverage of vulnerabilities.
- **Nuclei** is an efficient and adaptable vulnerability scanner that utilizes a YAML-based basic DSL. In the past, it used a template to send requests to a large number of targets. It ensured that there were no false positives and that many servers could be scanned in a short amount of time. Nuclei is capable of scanning for a wide variety of protocols. These protocols include TCP, DNS, HTTP, SSL, File, Whois, Websocket, and Headless. The extensive and adaptable templating that Nuclei provides may be used to mimic any form of security check (GitHub., 2022).

An attack that starts with a modification to the networking configuration of the device will be detectable by the tools, and they will be able to stop it. They assist you in remaining following requirements by locating and repairing out-of-process alterations, auditing installations, and even settling violations. In order to successfully complete a vulnerability assessment, you will need to follow the steps outlined below.

1. Begin the process by making a list of everything that has to be accomplished, determining which tool or tools will be used, and obtaining authorization from the relevant stakeholders.
2. When doing vulnerability scanning, be sure you use the appropriate tools. Ensure that you save all of the information that these vulnerability tools provide you with.
3. Conduct an analysis of the findings and determine which of the flaws you discovered might potentially pose a risk. You may also devise a strategy to cope with the dangers after ranking them in order of severity.
4. Make sure that all of the findings are written down and that you create reports for the relevant individuals.
5. Fix the problems that have been found.

Advantages of Scanning for Vulnerabilities:
Scanning for vulnerabilities protects systems against intruders and external threats..
Other benefits include:

1. Affordable: Most vulnerability scanners are offered at no cost to their users.
2. Quick: the evaluation can be finished in a few hour's time.
3. Automate: it is feasible to conduct scans regularly without any human interaction.
4. Performance: A vulnerability scanner can carry out a wide variety of standard scans.
5. Cost/Benefit: minimizing potential dangers to increase economic returns while keeping expenses to a minimum.

Reference:

Coffey, K., Smith, R., Maglaras, L. and Janicke, H. (2018). *Vulnerability Analysis of Network Scanning on SCADA Systems*. [online] Security and Communication Networks. Available at: https://www.hindawi.com/journals/scn/2018/3794603/.

GitHub. (2022). *projectdiscovery/nuclei*. [online] Available at: https://github.com/projectdiscovery/nuclei [Accessed 22 May 2022].

Varghese, S. and Kurian, R. (2021). Identifying Vulnerabilities in a Website Using Uniscan and Comparing Uniscan, Grabber, Nikto. [online] 3(1). doi:10.5281/zenodo.5091326.