Unit 2: Real-World Issues and Implications of Information Security Threats and Vulnerabilities

Objectives:

- Review the vulnerabilities of modern electronic medical devices.
- Discuss the use of exploitation software to create threats.
- Classify and evaluate the combination of threats and associated vulnerabilities and the impact on real-world devices.

Outcomes:

- Describe a number of typical vulnerabilities of modern electronic devices.
- Explain how common vulnerabilities can be exploited using software toolkits.
- Use industry-standard toolkits to classify and evaluate threats and vulnerabilities.

Reflection:

Nowadays, we have seen different security threats and vulnerabilities, leading to the CIA Triads' breach. Threats to security, security events, and security incidents are interwoven, but when applied to the field of cybersecurity, their definitions are distinct from one another (Rosencrance, L. 2021). We discussed some of the points regarding information security threats given below.

- Connected medical electronics equipment is vulnerable to additional risks, including denial-of-service attacks and patient data theft, from the perspective of information technology and modern electronic systems (Alguliyev, Imamverdiyev, and Sukhostat, 2018). On computer networks, viruses and other malicious software, known as malware, pose a significant threat to the care and privacy of patients.
- An attack on a computer system (software) that takes advantage of a particular vulnerability the system provides to attackers, such as flaws, is called a computer or software exploit. Revealing private information, Security issues, such as Buffer overflows, injections, and misconfigurations, Broken security measures, Deserialization that is not secure Authentication Errors.

As the threat increases day by day, information security researchers are also contributing and proposing new methods and schemes to overcome the impact of these threats, like vulnerability assessment tools. Basically, An evaluation of a system's or network's susceptibility to attack is called a vulnerability assessment, and its primary purpose is to locate and catalog potential vulnerabilities.

Finding out what sorts of threats are hiding around every corner is the purpose of doing a vulnerability assessment (also known as risk analysis). When conducting vulnerability assessments, the practice of using automated testing tools such as network security scanners is becoming more common.The results of these tests are compiled into an assessment report, which provides an overview of the findings. The purpose of vulnerability assessment tools is to carry out an automated search for new and existing threats that may attempt to compromise your application. Web application scanners, for

instance, may be used to test for and simulate attacks that have already been launched. Scanners look for protocols, ports, and network services that might be vulnerable to being compromised.

Reference:

Alguliyev, R., Imamverdiyev, Y. and Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, 100, pp.212–223. doi: 10.1016/j.compind.2018.04.017.

Alsuwaidi, A., Hassan, A., Alkhatri, F., Ali, H., QbeaaH, M. and Alrabaee, S. (2020). Security Vulnerabilities Detected in Medical Devices. *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*. doi:10.1109/urc49805.2020.9099192.

Pallavi, C., Girija, R. and Jayalakshmi, S.L. (2021). *An Analysis on Network Security Tools and Systems*. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3833455 [Accessed 10 May 2022].

Rosencrance, L. (2021)., *Top 10 types of information security threats for IT teams*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams. [Accessed 10 May 2022].