Unit 5: An Introduction to Testing

1. Describe the key terms associated with testing software for security.

Security testing ensures software is secure and dependable by assessing vulnerability to cyber-attacks and the impact of malicious inputs. It falls under non-functional testing, which examines if the application is designed and configured correctly (Moradov, 2021). Takanen (2012) describes that security testing aims to check if the system meets its security requirements and objectives. This type of testing is conducted at different stages of the product lifecycle, from requirements analysis and design to implementation, verification and maintenance.

Application security is crucial for protecting data and code from theft or hijacking. However, complex programs and cloud-based technologies make it hard to keep up with threats. To overcome these challenges, a comprehensive security program should be incorporated into the software development life cycle, and automated tools should be used to detect and remediate vulnerabilities. Secure code review, source-code analysis, and regular penetration testing should also be implemented to ensure protection against the latest threats and vulnerabilities and to scale the program as the business grows (Cipollone, 2023).

However, SISA (2022) suggested that various forms of security testing aim to safeguard software programs from internal and external risks. With prolonged use, any program, application, or network may become susceptible to security threats. Consequently, several security testing techniques offer organisations a reliable means of enhancing their cybersecurity stance. The Open-Source Security Testing Methodology has categorised these techniques into several groups, as outlined below:

1. **Vulnerability test**: Performing a vulnerability test is a crucial first step in network security. It looks for missing security patches, weak passwords, and malware. This type of testing is automated and can be scheduled regularly.

2. **Security testing:** Network security testing is a method to find vulnerabilities in networks, computers, and applications. It analyses operating systems, applications, and web servers. The goal is to eliminate risks through both manual and automated scanning. To ensure accuracy, live and test data should be used, and scans should be conducted regularly based on the level of risk involved.

3. **Penetration testing:** Penetration testing is a crucial security measure that involves a thorough search for potential vulnerabilities within a system to determine the level of risk involved. This testing is mandatory for compliance with the Payment Card Industry Data Security Standard (PCI-DSS). It should be performed by a skilled professional who can identify potential risks and offer effective mitigation strategies. The highest industry standards include requirement analysis, threat identification, vulnerability evaluation, exploitation, post-exploitation, and comprehensive reporting.

4. **Risk Assessment:** Risk assessment helps identify and prioritise potential risks to a project or organisation. By evaluating threats and their capabilities, measures can be taken to prevent or mitigate them. This involves identifying, prioritising, and analysing risks qualitatively and quantitatively. Regular risk assessments are necessary to avoid emerging threats and protect against vulnerabilities. Many service-based companies perform monthly or quarterly evaluations for improved security.

5. **Security Audit:** A security audit thoroughly evaluates an organisation's information security defences. Regular audits can help identify and eliminate security flaws. Methods include code review, fuzz testing, and penetration testing. Cybersecurity audits validate a company's security policies and procedures. To prepare for an audit, companies should review compliance standards, detail network structure, create access policies, and review data for discrepancies.

6. **Ethical Hacking:** Conducting ethical hacking is essential for security testing. Through this process, vulnerabilities that may not be detected through technical or manual testing can be identified by skilled hackers. It is important to note that ethical hacking is vastly different from malicious hacking, as the former does not result in any data theft or damage. The three types of scanning involved in ethical hacking are port scanning, network scanning, and vulnerability scanning.

7. **Assessment of Posture:** A security posture assessment evaluates an organisation's security controls, identifies gaps, and recommends corrective measures to enhance its security strategy. External professionals typically perform this assessment, ranging from a few hundred to several thousand

dollars. The process involves analysing current controls and conducting a thorough penetration test. The results are presented in a comprehensive report that proposes actionable recommendations for improvement.

8. **API Security Testing:** API security testing is crucial as using APIs targeting the cloud brings new risks for organisations, including misconfiguration and API misuse to launch attacks. It helps identify any irregularities in an API and covers network security services to find vulnerabilities and resolve loopholes. Regular use of API security testing tools is necessary to fight unauthorised access, including Man-in-the-Middle attacks where hackers can steal sensitive data by eavesdropping on communications.

9. **Mobile application security:** Mobile app security involves analysing the app's purpose and data handling. Testing includes decrypting encrypted data, static analysis to find weak spots, and penetration testing to assess attack response. Dynamic testing with manual and automatic reviews provides the best results.

10. **Network Security Testing:** Network security testing is crucial for identifying vulnerabilities and determining risks. It can include mapping the network infrastructure, evaluating technical security controls, and using administrative tools to protect confidential data. Safeguarding your network includes using a firewall, NAC, antivirus, and other devices. Antivirus software deals with viruses, while network security protects against phishing and spyware.

For instance, My-course (2020) highlights the following key terms in Software Testing:

Testability refers to a software's capacity to uncover flaws and defects through testing. To guarantee a system that is free of faults, it is crucial to have code that can be tested and capable of detecting and correcting errors before implementation.

Quality assurance testing is essential in software development to ensure the product meets customer needs and functions as intended. Identifying and addressing defects and issues before release improves performance, security, and functionality, ultimately leading to higher customer satisfaction.

A system's capacity to meet customer requirements and conform to the specified criteria is evaluated through **validation** and **verification**. Nonetheless, if the

customer's needs are not comprehensively grasped, conflicting scenarios may emerge, mandating modifications to the code.

There are two primary approaches in software testing: **Whitebox** and **Blackbox**. White box testing scrutinises internal operations, while **Blackbox** testing evaluates overall functionality. **Whitebox** tests include unit and branch testing, while **Blackbox** tests encompass equivalence and use case testing.

Automated testing boasts speed and efficiency advantages over manual testing, given that computers instead of humans execute it. Additionally, it offers broader test coverage.

When conducting **manual testing**, one must meticulously document their findings and assess multiple systems, which can prolong the testing process. On the other hand, automated testing necessitates the upkeep of test scripts. However, depending on the situation, both techniques can be advantageous.

Snyk (N.D.) states that in the world of application development, we may encounter various security acronyms that we are unfamiliar with. This is a common occurrence, especially in DevSecOps organisations. Snyk (N.D.) has launched SAST (Static Application Security Testing) capabilities, which left many individuals uncertain about its meaning. To address this, Snyk (N.D.) has developed a helpful cheat sheet featuring the top 10 most frequently used security acronyms shown below:

(Snyk, N.D.)

2. **Prepare a list of questions to ask when designing a test plan for secure software.**

Although security products and applications are helpful, they may not always provide foolproof protection against cyberattacks. To ensure the safety of applications, it's best to utilise QA testing and a comprehensive web security checklist. Additionally, cyber security penetration testing is an essential step that should be taken for all types of applications. When developing a test plan, ask the right questions to ensure security (Joseph, 2020).

Before testing a product in the security domain, create a cyber security checklist with defined answers. Here are some essential steps for your software security test plan, according to Joseph (2020):

1. **How is the application being tested?**

To create a thorough security testing checklist, identify the type of application (desktop, cloud, mobile, or web-based) and determine relevant cybersecurity tests. Efficiency is crucial, so define your application to prioritise tests. For a mobile app, include comprehensive mobile penetration testing in your plan.

2. **What Type of Product or Software Application is Being Tested?**

When creating a cyber security checklist, determine if your product falls under System Security, Security Risk Assessment, or Identity Security. Consult a testing company to help select the most relevant category for your product's testing.

3. **What Threats Is This Product or Software Protected Against?**

When creating a cyber security checklist, determine if your product falls under System Security, Security Risk Assessment, or Identity Security. Consult a testing company to help select the most relevant category for your product's testing.

4. **What Environments Can Your Software or Product Operate in?**

Identify which environments your product supports to create specific test cases for cyber security. Determine supported operating systems, browsers, and mobile devices. Plan thorough cyber security tests accordingly.

5. **Is the test strategy well-considered and meticulously prepared?**

Ensure your security testing checklist is prepared to prevent delays. Review test cases and consider additional testing for system security.

3. **Design software tests by understanding how software security can be breached.**

In the realm of software development, the design of tests is paramount. This includes crafting test cases to authenticate functionality, pinpointing various scenarios and conditions, and uncovering glitches. It demands meticulous planning, a keen eye for detail, and an extensive comprehension of the product (Priya, 2023). However, Potter & McGraw (2004) mention that security testing has become vital in assessing system behaviour in today's digital landscape. Nevertheless, testing software security can often be misconstrued. To ensure software security is thoroughly evaluated, testers must implement risk-based methodologies that identify potential risks and develop tests based on those risks.

Singh (2019) demonstrates as a software developer, several steps can be taken to prepare and plan for security testing. Firstly, it's essential to assess whether the software meets the requirements through architecture study and analysis. Next, identify all potential threats and risk factors that require testing. Then, based on the identified threats, vulnerabilities, and security risks, execute the tests using relevant software security testing tools for web applications. Any issues discovered during the security test should be addressed manually or with suitable open-source code. Finally, create a detailed test report with a list of vulnerabilities, threats, and issues resolved and those that still need attention.

Software applications are developed for various purposes, from embedded systems and mobile devices to banking and transactional services. However, it's easy to overlook the importance of security measures in designing and operating these apps

and digital experiences. This can lead to significant risks that must be addressed with top priority (Saladino, 2023).

Developing secure software involves intentionally designing and executing software applications with security as a top priority. Tran (2023) explains that to ensure safety, it is essential to implement best practices such as threat modeling, secure coding, code review, testing, secure configuration management, access control, regular updates and patches, security training, incident response, and continuous monitoring.

References:

Moradov, O. (2021). *Security Testing: Types, Tools, and Best Practices*. [online] Bright Security. Available at: https://brightsec.com/blog/security-testing/.

Takanen, A. (2012). *Security Testing Terminology and Concepts*. Available at: https://docbox.etsi.org/mts/mts/05-contributions/2012/mts(12)sig013_security_testing_terminology_and_concepts.pdf.

Cipollone, F. (2023). *What is application security? top 10 popular terms*. [online] Phoenix Security. Available at: https://phoenix.security/what-is-application-security-top-10-popular-terms/ [Accessed 9 Sep. 2023].

SISA (2022). *10 Types of Security Testing Techniques | SISA Insights*. [online] SISA. Available at: https://www.sisainfosec.com/blogs/10-types-of-security-testing-techniques/.

My-course (2020). *Testing.* [online] Available at: https://www.my-course.co.uk/Computing/Computer%20Science/SSDCS/SSDCS%20Lecturecast%203/content/index.html#/lessons/Odi_VP_olGIok2zv7Dd0XDr9uuOlzkcA [Accessed 9 Sep. 2023].

Snyk (N.D.). *Top 10 application security acronyms*. [online] Available at: https://snyk.io/learn/application-security/glossary-acronyms/ [Accessed 9 Sep. 2023].

Joseph, T. (n.d.). *Cyber Security Testing Checklist: 9 Steps To Complete Before Testing a Product in the Security Domain*. [online] blog.qasource.com. Available at: https://blog.qasource.com/cyber-security-testing-checklist.

Priya, Y. (2023). *Test Design in Software Testing - A Comprehensive Guide*. [online] Available at: https://testsigma.com/blog/test-design/ [Accessed 9 Sep. 2023].

Potter, B. & McGraw, G. (2004). Software security testing. *IEEE Security & Privacy Magazine*, 2(5), pp.81–85. doi:https://doi.org/10.1109/msp.2004.84.

Singh, R. (2019). *Software Security Testing Approach, Types, and Tools*. [online] Insights - Web and Mobile Development Services and Solutions. Available at: https://www.netsolutions.com/insights/software-security-testing/.

Saladino, G. (2023). *What Is AppSec — Application Security Overview* | *Perforce*. [online] www.perforce.com. Available at: https://www.perforce.com/blog/kw/what-is-appsec [Accessed 10 Sep. 2023].

Tran, D. (2023). *Best Practices For Secure Software Development*. [online] Perforce Software. Available at: https://www.perforce.com/blog/sca/best-practices-secure-software-development.