Mr. Azfar was tasked with identifying security vulnerabilities in the systems and software running in the company he worked for. Based on industry guidelines, there are two methods that can be used, namely Vulnerability Scanning and Penetration Testing. Discuss the advantages and disadvantages of both methods so that he can explain to the management the strategy to be used. (10 Marks)

A screenshot of a computer

Description automatically generatedA black and white chart with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A diagram of a black box test

Description automatically generatedA close-up of a test

Description automatically generated

A close-up of a document

Description automatically generated

Q1

1. HTTPS Support : encrypts data exchanged between the browser and websites,

ensuring confidentiality and integrity. It works by using SSL/TLS protocols to establish a

secure connection

2. Pop-up Blocker : Analyzing the code of web pages and blocking any attempts to

open new browser windows or tabs without user interaction.

3. Phishing and Malware Protection : When a user attempts to access a suspicious

website, the browser compares the site's URL against these databases and warns the

user

4. Cookie Management : Cookies are small pieces of data stored by websites on a

user's computer. Browser security features offer options for managing cookies, including

blocking third-party cookies, deleting cookies after a browsing session, or allowing only

trusted sites to set cookies.

5. Content Security Policy : CSP allows website administrators to define the trusted

sources of content that browsers should execute the pages. It helps prevent cross-site

scripting (XSS) attacks by restricting the types of content that can be loaded and

executed, reducing the risk of unauthorized code execution.

Q3

Risk Response strategies and briefly clarify how each strategy works

1. Avoidance- eliminate the risk all together by eliminating the cause

2. Transference- allocate the responsibility of risk to another agency or third

party

3. Acceptance- recognizing that the risk involved is nor entirely avoidable

4. Mitigation- protect against possible attacks and are implemented when the

impact of potential risk is substantial.

5. Deterrence- include physical security like a checkpoint inside or outside the

Buildings

Sem 21/22

1. **Technical Controls:**
   * **Definition:** Technical controls involve the use of technology to manage and control access to sensitive information and systems. These controls focus on the security of hardware, software, networks, and data.
   * **Examples:**
     + **Firewalls:** Hardware or software devices that monitor and control incoming and outgoing network traffic.
2. **Management Controls:**
   * **Definition:** Management controls are policies, procedures, and guidelines put in place by an organization's management to ensure the proper functioning of security measures and compliance with security policies.
   * **Examples:**
     + **Security Policies and Procedures:** Documented guidelines on how to handle security incidents, password management, data classification, etc.
3. **Operational Controls:**
   * **Definition:** Operational controls are daily practices and procedures that focus on the day-to-day tasks necessary to ensure the security of information systems.
   * **Examples:**
     + **Change Management:** Controlling changes to hardware, software, configurations, and procedures to minimize the impact on security and reliability.