National University of Computer and Emerging Sciences

Cyber Security Tools and Technologies (CS3016)

Date: 12,April 2025

Course Instructor(s)

Dr. Arshad Ali

Ms. Nosheen Manzoor

Sessional-II Exam

Total Time: 1 Hour

Total Marks: 30

Total Questions: 04

Semester: SP-2025

Dept: Computer Science

Student Name	Roll No	Section	Student Signature

Instruction/Notes:

- Attempt all questions on the provided separate answer sheet.
- You are required to attempt all questions and parts thereof in a sequence. This implies that first attempt all parts of Question 1, then the same for Question 2 and so on.
- If you find any ambiguity in a question, you can make your own assumption and answer the question accordingly by stating the same.
- The paper is open book/notes/articles. Students are allowed to bring the same in printed or handwritten form. Sharing of material with fellow students is not allowed.

CLO # 1 (Questions 1 to 2): Understand the flow of information in the modern world and be able to recognize and mitigate threats at every stage, e.g. network, coding and software layers; to this end, setting up and running appropriate tools and environments.

Q # 1: Read the given scenario carefully and identify the appropriate web application security risk from the OWASP Top 10 (2021). Write the exact name of the risk as listed by OWASP.**[1x8=8 Marks]**

A. A web application uses weak passwords, and a user's account is compromised. What are the potential risks, and how can this vulnerability be addressed?

Vulnerability: Identification and Authentication Failures

B. A web server's default configuration includes a directory that contains sensitive configuration files. What are the potential risks, and how can this vulnerability be addressed?

Vulnerability: Security Misconfiguration

C. A web application allows users to enter product names and descriptions in a search box. An attacker enters a malicious script in the search box, and when another user uses the search box, the malicious script executes in their browser. What type of vulnerability is this, and how can it be prevented?

Vulnerability: Cross-Site Scripting (XSS)

D. A web application allows users to view their own orders and edit their profile information. However, an attacker discovers that by manipulating the URL, they can access other users' order details and modify their profiles. What type of vulnerability is this, and how can it be mitigated?

Vulnerability: Broken Access Control (IDOR - Insecure Direct Object References)

E. A web application uses an outdated encryption algorithm to protect sensitive data. What are the potential risks, and how can this vulnerability be addressed?

Vulnerability: Cryptographic Failures

F. A banking application uses session tokens to track logged-in users. These tokens are stored in the URL and can be intercepted or guessed easily. The application also does not expire sessions promptly after logout or timeout.
Vulnerability: Identification and Authentication Failures

G. An API endpoint used by a mobile app accepts JSON input and uses an insecure deserialization method to convert data into objects. An attacker manipulates the input to execute arbitrary code on the server.
Vulnerability: Software and Data Integrity Failures

H. The application integrates several third-party libraries, including one with a known vulnerability that hasn't been updated in two years. No dependency scanning is in place.
Vulnerability: Vulnerable and Outdated Components

Q#2 Provide precise and short answers to the following questions. [2 x 4 =8 Marks]

A. How do cryptographic protocols such as SSL/TLS use cryptographic techniques to secure online communications?

Answer: SSL/TLS uses asymmetric encryption to authenticate the server and establish a secure session key, then uses symmetric encryption to encrypt data. It also uses hashing for integrity and digital certificates for trust.

B. If Bob receives a message encrypted with his public key, can he be sure it came from Alice?

Answer: No! Anyone can encrypt with Bob's public key. To prove authenticity, Alice must **sign** the message with her private key (or encrypt a signature with Bob's public key).

C. If a message is encrypted using the recipient's public key, who can decrypt it and what does that guarantee about the message?

Answer: ***Only the recipient can decrypt it using their private key. This guarantees confidentiality, ensuring that only the intended recipient can read the message.***

D. Describe a real-world scenario where combining both symmetric and asymmetric encryption (i.e., hybrid encryption) would be necessary.

Answer: In HTTPS (secure web browsing), asymmetric encryption is used initially to securely exchange a symmetric session key. After that, all communication uses faster symmetric encryption. This combines the security of asymmetric with the speed of symmetric encryption.

CLO # 1 (Questions 3 to 4): Evaluate the computer and data security needs of an organization, and be able to assess the current security landscape, including the nature of threats, the status of common vulnerabilities, and the likely consequences of security failures..

Q#3. Read each of the following scenarios carefully. For each one, identify the function (e.g., Govern , Identify, Protect, Detect, Respond, Recover), the exact name of category it belongs to and the subcategory code from the NSIT CSF 2.0 framework. **[1 x 8 = 8 Marks]**

A. A startup conducts an internal review to document and classify all IT assets and their roles within the organization.
Answer:
Function: Identify
Category: Asset Management
Subcategory Code: ID.AM-01

B. An enterprise develops and enforces a policy requiring strong passwords, screen lockouts, and automatic logoff features.
Answer:
Function: Protect
Category: Identity Management, Authentication, and Access Control
Subcategory Code: PR.AA-02

C. An organization updates its supplier contracts to include specific cybersecurity requirements and right-to-audit clauses.
Answer:
Function: Govern
Category: Supply Chain Risk Management
Subcategory Code: GV.SC-03

D. A hospital maintains cloud backups and regularly tests restoration processes to ensure business continuity during disasters.
Answer:
Function: Recover

Category: Incident Recovery
Subcategory Code: RC.IR-01

E. An IT administrator configures access permissions, so employees only have access to systems relevant to their roles.
Answer:
Function: Protect
Category: Identity Management, Authentication, and Access Control
Subcategory Code: PR.AA-03

F. After detecting unusual system behavior, the IT team isolates the affected system and notifies stakeholders within 15 minutes.
Answer:
Function: Respond
Category: Detection and Analysis
Subcategory Code: RS.AN-01

G. An organization regularly evaluates its internal capabilities and resources to understand if it can meet emerging cybersecurity threats and operational demands.
Answer:
Function: Identify
Category: Organizational Context
Subcategory Code: ID.OC-02

H. A university's IT department has configured their systems to automatically flag unusual data transfer patterns, such as a sudden spike in outbound traffic late at night.
Answer:
Function: Detect
Category: Anomalies and Events
Subcategory Code: DE.AE-01

CLO # 4 (Question 5): *Identify security tools and hardening techniques.*

Q # 4: Answer the following questions with reference to Nmap tool. **[1x 6 = 6 Marks]**

A. How can you reduce the likelihood that a standard firewall/IDS would detect your Nmap activity?

It is not easy; however, depending on the type of firewall/IDS, breaking the packet into smaller packets may help.

B. Which command is used to tell Nmap explicitly which network interface to use and not to expect to receive a ping reply.
nmap -e NET_INTERFACE -Pn -S SPOOFED_IP MACHINE_IP

C. You're scanning a network where you don't have root privileges. Which TCP scan type should you use and why?
Answer: You should use **TCP connect scan (-sT)** as it does not require root privileges to craft raw packets. TCP connect relies on the OS to establish the connection using the full three-way handshake.

D. You use a NULL scan on a network and receive many "open|filtered" results. What does this tell you?
Answer:
It indicates that Nmap couldn't determine whether the port is open or filtered because there was no response. This typically means the target system is not RFC 793-compliant or a firewall is blocking the probes.

E. You're scanning a system that logs all connection attempts. Which scan should you avoid?
Answer:
Avoid **TCP connect scan (-sT)**, as it completes a full TCP handshake and is easily logged.

F. Which scan type is likely to go undetected by most IDS systems?
Answer: FIN, Xmas, and Null scans (T3-T5) are generally stealthier and may bypass firewalls and IDS systems that are not configured to detect non-standard TCP flags.