National University of Computer and Emerging Sciences

Ms. Nosheen Manzoor

Cyber Security Tools and Technologies (CS3016)

Date: May 22nd 2025

Course Instructor(s)

Dr. Arshad Ali

Final Exam

Total Time: 3 Hours
Total Marks: 80
Total Questions: 08

Semester: SP-2025
Campus: Lahore
Dept: Computer Science

Student Name	Roll No	Section	Student Signature

CLO # 1: 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.
CLO # 3: 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.
CLO # 4: Identify security tools and hardening techniques.

Q1: Identify and write the correct option(s) on the provided answer sheet. [10]

I. Which type of cybercriminal (hacker) is the most likely to create malware to compromise an organization by stealing credit card information?
a. white hat b. gray hat c. black hat d. All of these

II. ---------- framework should be recommended for establishing a comprehensive information security management system in an organization.
a. ISO/IEC 27000 b. ISO OSI model c. CAI triad d. NIST NICE

III. W Alice and Bob use a pre-shared key to exchange a confidential message. If Bob wants to send a confidential message to Carol, what key should he use?
a. the same pre-shared key he used with Alice b. the private key of Carol
c. a new pre-shared key d. the public key of Bob

IV. ----------access control strategy allows an object owner to determine whether to allow access to the object.
a. RBAC b. DAC c. MAC d. ACL

V. ---------- hashing algorithm is recommended for the protection of sensitive, unclassified information.
a. MD5 b. AES-256 c. 3-DES d. SHA-256

VI. Primary purpose(s) of security frameworks?
a. Identifying security weaknesses b. Managing organizational risks
c. Protecting PII data d. All of these

VII. A security professional has been tasked with implementing strict password policies on workstations to reduce the risk of password theft. This is an example of security _____.
a. controls b. teams c. policies d. weaknesses

VIII. You are helping your security team consider risks when setting up a new software system. Using the CIA triad, you focus on confidentiality, availability, and what else?
a. Information b. integrity c. intelligence d. inconsistencies

IX. ----------is a common technique used to evade intrusion detection systems (IDS)
a. Increasing firewall logging b. VPN tunneling for authorized access
c. Packet fragmentation d. Using strong encryption algorithms

X. ---------- technology should be implemented to verify the identity of an organization, to authenticate its website, and to provide an encrypted connection between a client and the website.
a. Digital certificate b. Digital signature c. Salting d. Asymmetric encryption

Q2: Answer the following questions with reference to Nmap tool. **[3+1*9= 12 Marks]**

(A) Write the Nmap commands considering the following scenarios:
(I) Which command would you use to perform an ARP scan on a local subnet (i.e.192.168.1.0/24) without port scanning?
(II) Which Nmap command scans all 65535 ports on a target host i.e., 10.10.10.1?
(III) You want to scan ports 22, 80, and 443 only on a target host i.e., 10.10.10.1. What command should you use?
(B) What does nmap -sS 10.10.10.1 perform?
(C) What does nmap -sU 10.10.10.1 do?
(D) What is the difference between -sT and -sS in Nmap?
(E) What is the purpose of using -f or –mtu in Nmap?
(F) Which scan types are effective against stateless firewalls?
(G) What are the six port states identified by Nmap?
(H) What does the -n option do in Nmap?
(I) Which scan type is also known as a stealth scan and doesn't complete the TCP handshake?
(J) What does Nmap's -sn option do?
(K) How to fragment packets into 16-byte chunks?
(L) Which scan sets FIN, PSH, and URG flags?
(M) You suspect a server (IP: 172.16.5.5) is running a web application, and you want to identify open TCP ports. You're a root user and prefer stealth. Which scan will provide fast, stealthy results? Write the Nmap command as well.

Answer:

(A)
(I) sudo nmap -PR -sn 192.168.1.0/24
(II) nmap -p- 10.10.10.1
(III) nmap -p22,80,443 10.10.10.1

(A) A TCP SYN scan (stealth scan) on the target IP.
(B) Performs a UDP port scan on the target.
(C) -sT completes the full TCP handshake (connect scan), while -sS does not (stealth SYN scan).
(D) Fragment packets to evade firewalls and IDS systems.
(E) Null (-sN), FIN (-sF), and Xmas (-sX) scans.

(F) Open, Closed, Filtered, Unfiltered, Open|Filtered, Closed|Filtered.
(G) Disables DNS resolution.
(H) TCP SYN scan (-sS)
(I) Performs host discovery without port scanning.
(J) Use -ff or -f -f.
(K) Xmas Scan (-sX).
(L) TCP SYN scan: sudo nmap -sS 172.16.5.5

Q3: Answer the following questions: **[6 x 2 = 12] (CLO #2)**

(A) In the context of virus scanners, differentiate between false positives and false negatives.

Answer: A false positive occurs when the virus scanner detects a given file as a virus when in fact it is not. For example, a legitimate program may edit a Registry key or interact with your email address book. A false negative occurs when a virus is falsely believed to be a legitimate program.

(B) The chmod command manioulates standard permissions. The syntax depends on whether you are using absolute or symbolic mode. You are required to write chmod command as required for the following scenarios: (I) write the command in absolute mode for the case where you want to grant the user read and write, the group read, and others execute to the example.txt file., (II) for the file in scenario I, your task is to write the command in symbolic mode which revokes the execute rights from others.

Answer: (I) chmod 641 example.txt; (II) chmod o-x example.txt

(C)In the context of firewall, describe the following concept: (i) stateful packet inspection (ii) screened host.

Answer: (i) Any **stateful packet inspection** (SPI) firewall will examine each packet and deny or permit access based not only on the examination of the current packet but also on data derived from previous packets in the conversation firewall is therefore aware of the context in which a specific packet was sent. This makes such a firewall far less susceptible to ping floods and SYN floods, as well as less susceptible to spoofing.

(ii) A ***screened host*** is really a combination of firewalls. In this configuration, you use a combination of a bastion host and a screening router. The screening router adds security by allowing you to deny or permit certain traffic from the bastion host. It is the first stop for traffic, which can continue only if the screening router lets it through.

(D) Describe how you would identify and exploit a SQL injection vulnerability in a web application. What would be your approach to mitigate this vulnerability?

Answer: To identify and exploit a SQL injection vulnerability, I would start by inputting malicious SQL code into the application's input fields. If the application is vulnerable, it might display database-related errors or behave unexpectedly. To mitigate this vulnerability, I would recommend using prepared statements or parameterized queries to validate and sanitize user input, ensuring that the SQL code cannot be injected into the application's database queries.

(E) You've been tasked with assessing the security of a corporate network. How would you conduct a network penetration test, and what tools would you use? Provide examples of potential vulnerabilities you might encounter.

Answer: For a network penetration test, I would use tools like Nmap and Wireshark to scan the network and analyze network traffic. I would look for open ports, services, and vulnerabilities in the network devices. Common vulnerabilities include weak passwords, outdated software, and

misconfigured firewall rules. Documenting these vulnerabilities and providing recommendations for mitigation, such as regular security patching and implementing strong access controls, would be part of the solution.

(F) You discover a security breach in a company's network during a penetration test. What immediate steps would you take to contain the breach, investigate the incident, and prevent future occurrences?
Answer: Upon discovering a security breach, the first step is to contain the breach by isolating affected systems. Simultaneously, I would start an investigation to identify the source and extent of the breach. This involves analyzing logs, network traffic, and other relevant data. After understanding the incident, I would develop a remediation plan, which might include patching vulnerabilities, resetting compromised credentials, and enhancing security measures. Finally, a post-incident report outlining lessons learned and recommendations for preventing future incidents should be prepared.

Question 4: Answer the following questions: **[2+2+2+2 = 8]**
(A) An attacker sends packets that are deliberately fragmented and ordered out of sequence to avoid detection. What is this technique called, and which device can be easily bypassed by it?
Answer: This is called **evasion via packet fragmentation** or **session splicing**. It can **bypass IDS** that **do not properly reassemble** fragmented packets before inspection.
(B) An attacker is using polymorphic malware that changes its code on each infection. What limitations do a signature-based IDS have in this scenario?
Answer: Signature-based IDS **fails to detect polymorphic malware** because it relies on **static patterns**. The malware's **changing code evades detection**, unless **behavior-based or anomaly-based detection** is used
(C) Define Demilitarized Zone (DMZ). What is the basic characteristic of a firewall responsible for its creation.
Answer: It is network that serves as a buffer between the internal secure network and insecure internet.
It can be created using a firewall with three or more network interfaces assigned with specific roles as internal trusted network, DMZ network, and external un-trusted network.
(D) Which type of Honeypot is used (i) to simulate all services and applications, (ii) for collecting internal flaws and attackers within an organization?
Answer: (i) High Interaction Honeypots, (ii) production honeypots

Q5: 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 listed by OWASP Top 10 2021**.**
[1x 8 = 8] (CLO # 3)
Note: A cheat sheet at the end gives list of OWASP top 10 risks.
(A). An e-commerce platform allows users to update their account information using an endpoint like /user/edit/123. A malicious user changes the user ID in the URL to /user/edit/456 and successfully modifies another user's data.
(B) A banking app transmits user login details over HTTP instead of HTTPS. User credentials are intercepted during a public Wi-Fi session.

(C) A search bar in a web application allows users to input SQL statements, leading to unauthorized database access and data extraction using payloads like OR 1=1. Which OWASP Top 10 2021 category/risk is this vulnerability associated with?
(D) A cloud-hosted web application has an exposed admin panel (/admin) without access restrictions. Default credentials (admin/admin) are active.
(E) Tester discovers that an internal API exposes full user data (email, phone number, address) without authentication.
(F) A major airline had a data breach involving more than ten years' worth of personal data of millions of passengers, including passport and credit card data. The data breach occurred at a third-party cloud hosting provider, who notified the airline of the breach after some time.
(G) A cloud service provider (CSP) has default sharing permissions open to the Internet by other CSP users. This allows sensitive data stored within cloud storage to be accessed.
(H) A user reports that when visiting a company web app, their session was hijacked.

Answer:

(A) - A01:2021- Broken Access Control
(B) - A02:2021- Cryptographic Failures
(C)-A03:2021 - Injection
(D) A05:2021 - Security Misconfiguration
(E) A01:2021 – Broken Access Control
(F) A09:2021 – Security Logging and Monitoring
(G) A05:2021 – Security Misconfiguration
(H) A05:2021 – Security Misconfiguration & A01:2021 – Broken Access Control.

Question 6: Read each of the following scenarios carefully. For each one, identify the function (e.g., Govern , Identify, Protect, Detect, Respond, Recover), and the exact name of category it belongs to.
[1 x 10 = 10 Marks]

(A) Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes.
(B) Follow the organization's breach notification procedures for recovering from a data breach incident
(C) Review strategy in light of cybersecurity incidents
(D) Periodically assess or test users on their understanding of basic cybersecurity practices
(E) Apply criteria to estimate the severity of an incident
(F) Implement zero trust architectures to restrict network access to each resource to the minimum necessary
(G) Assess network and system architectures for design and implementation weaknesses that affect cybersecurity
(H) Select recovery actions based on the criteria defined in the incident response plan and available resources
(I) Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation
(J) Use full disk encryption to protect data stored on user endpoints

Answer:

(A) Identity: Asset Management (ID.AM)
(B) Recover: Incident Recovery Communication (RC.CO)
(C) Govern: Oversight (GV.OV)

(D) Protect: Awareness and Training (PR.AT)
(E) Detect: Incident Management (RS.MA)
(F) Protect: Technology Infrastructure Resilience (PR.IR)
(G) Identity: Risk Assessment (ID.RA)
(H) Recover: Incident Recovery Plan Execution (RC.RP)
(I) Detect: Adverse Event Analysis (DE.AE)
(J) Protect: Data Security (PR.DS)

Question 7: Give precise and short answers to the following questions: (8 x 1 +2 = 10)

(A) A database breach exposes unencrypted credit cards. Which CIA component is violated by this?

(B) Which threat involves long-term, stealthy access to steal data?
(C) What does Zero Trust architecture enforce by default?
(D) Why is AES preferred over DES in modern cryptography?
(E) What is the role of Machine Learning (ML) in malware detection?
(F) Why do we convert labels like 'spam' and 'ham' into numeric values (-1 and 1)?
(G) What role does the learning rate (eta0) play in the Perceptron learning algorithm?
(H) What are the challenges of using static rules in spam filtering?
(I) What is the difference between Discretionary and Mandatory Access Control?

Answer:
(A) Confidentiality
(B) Advanced Persistent Threat (APT)
(C) Verify every access request (never trust, always verify).
(D) AES has stronger encryption (e.g., 256-bit keys).
(E) Classifies files/behavior as malicious based on training data
(F) Many ML algorithms, like Perceptron and SVM, require numerical inputs for computations and classification tasks.
(G) It controls how much the model's weights are updated during training. A small value slows learning; a large value may cause instability.
(H) Static rules are rigid and easily bypassed by spammers using new formats or words. They don't adapt to new patterns.

(I) **Discretionary Access Control (DAC):** Access is controlled by the **owner** of the object, who can grant permissions to others. It's **flexible but less secure**. Common in general-purpose systems like Windows and Linux.

Mandatory Access Control (MAC): Access is controlled by a **central authority** based on **security labels and policies**. It's **strict and more secure**, used in military and classified environments.

Question 8: Answer the following questions: **(3x2 + 2 + 2 = 10)**
(A) Write the output of the following python code snippets. Assume that necessary libraries are imported by default.
(I)

```
1  def display_investigation_message():
2      print("investigate activity")
3  application_status = "potential concern"
4  email_status = "okay"
5  if application_status == "potential concern":
6      print("application_log:")
7      display_investigation_message()
8  if email_status == "potential concern":
9      print("email log:")
10     display_investigation_message()
```

II.

```
1  username_list = ["bmoreno", "wjaffrey", "tshah", "sgilmore", "btang"]
2  username_index = username_list.index("tshah")
3  print(username_index)
```

III.

```
import numpy as np
def predict(data, w):
    return data.dot(w)

w = np.array([0.1, 0.2, 0.3])
data = np.array([1.0, 2.0, 3.0])
print(predict(data, w))
```

(B) The execution of the following code throws an exception. You are required to write the line(s) number (s) which resulted in the exception. Moreover, how can you overcome the exception without deleting any line of code.

```
1  username = "elarson"
2  month = "March"
3  total_logins = 75
4  failed_logins = 18
5  print("Login report for", username, "in", month)
6  print("Total logins:", total_logins)
7  print("Failed logins:", failed_logins)
8  print("Unusual logins:", unusual_logins)
```

(C) Write code to split dataset into training and testing (70% and 30% respectively) using scikit-learn.

Answer:

(A)

I.

application_log:
investigate activity

II. 2

III. $0.1\times1 + 0.2\times2 + 0.3\times3 = 1.4$

(B) Line # 8 (as this includes a variable that hasn't been assigned)
Add the following code before line # 4: unusual_logins = 9 (value is assigned to the variable that was used in line # 8.
(C) Answer:

```
from sklearn.model_selection import train_test_split
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=0)
```