الجامعة اللبنانية
كلية الإعلام
الفرع الأول

الجامعة اللبنانية
كلية الإعلام

Third Year

Semester VI

Advanced Data Security

Date:

Duration:

Final Exam
2023 / 2024

Instructor : Dr. K. Danach

Part I: Multiple Choice Challenge

1. This term describes a piece of data that a website stores on a user's machine and is designed to remember something about the user later.

   a. Cookie

   b. Cache

   c. Token

   d. Session

2. Which of the following is not considered a type of malware?

   a. Adware

   b. Freeware

   c. Spyware

   d. Ransomware

3. Engaging in the practice of spying on the user of an ATM machine to obtain their PIN is known as:

   a. Pharming

b. Phishing

c. Skimming

d. Shoulder surfing

4. This type of software is designed to infiltrate or damage a computer system without the owner's informed consent.

a. Spyware

b. Adware

c. Malware

d. Software bugs

5. Which encryption technology provides a secure channel over an insecure network in a client-server architecture?

a. Digital signature encryption

b. Symmetric key encryption

c. SSL/TLS encryption

d. Hashing algorithm encryption

6. What is the primary objective of confidentiality in communication?
   a. To ensure the message is encrypted
   b. To restrict access to only the sender and intended receiver
   c. To confirm the identity of each party involved
   d. To ensure the message is not altered without detection
7. How is confidentiality achieved in communication?
   a. By encrypting the message
   b. By confirming the identity of each party
   c. By ensuring message integrity
   d. By making services accessible and available
8. Why is authentication important in communication?

a. To encrypt the message contents
b. restrict access to only the sender and intended receiver
c. To confirm the identity of each party involved
d. To ensure the message is not altered without detection

9. What is the purpose of message integrity in communication?
   a. To encrypt the message contents
   b. To restrict access to only the sender and intended receiver
   c. To confirm the identity of each party involved
   d. To ensure the message is not altered without detection
10. What does the concept of access and availability refer to in communication?
   a. Encrypting the message contents
   b. Restricting access to only the sender and intended receiver
   c. Confirming the identity of each party involved
   d. Ensuring services are accessible and available to users
11. The use of computer and network resources to get unauthorized access to information.
   a. Hacking
   b. Cracking
   c. Cybercrime
   d. Ethical hacking
12. People that may not be trusted and have authorized access to some of a company's information.
   a. External Insiders Individuals
   b. Employees
   c. Eavesdroppers
   d. Financial Information
13. Which of the following is not an insider threat?
   a. Employees
   b. Distributors
   c. Service providers
   d. External internal individuals

14. Stealing personal information, and using it without one's permission in order to commit fraud.

a. Personal information
b. Fraud
c. Identity theft
d. Social engineering

15. Which of the following is considered a precaution to keep personal information safe?

a. Only carry essential documents.
b. Your trash is a treasure.
c. Use different PIN numbers for different cards.
d. All of the above

16. A unique name used to identify who is attempting to log onto a computer or network.

a. Second identification
b. Password
c. Username
d. User requesting access

17. A sequence of characters used to determine that a user requesting access to a system is really that particular user.

a. First identification
b. Password
c. Username
d. Access

18. Which of the following is not a method of social engineering?

a. Vishing
b. Skimming
c. Phishing
d. Shoulder surfing

19. Calling someone with the intent to gather information for criminal intent.

a. Vishing

b. Phishing

c. Skimming

d. Surfing

20. Malicious software that usually run silently and secretly every time the computer starts and can create a backdoor for criminals to access the system.

a. Trojan horse

b. Botnets

c. Dialers

d. Backdoors

21. What encryption method does the Secure Socket Layer (SSL) protocol use to secure the channel over the public Internet?

e. Private key encryption

f. Symmetric key encryption

g. Public key encryption

h. Hashing algorithm encryption

22. A method of verifying the identity of a device or person connecting to a service online, which involves multiple methods of proving identity:

a. Single-factor authentication

b. Two-factor authentication

c. Continuous authentication

d. Biometric authentication

23. Which of the following is a legitimate cybersecurity defense mechanism?

a. Social engineering

b. Phishing

c. Firewall

d. Spoofing

24. This attack involves a malicious individual entering a place of business to physically steal data or introduce a security threat:

    a. Tailgating

    b. Dumpster diving

    c. Spear phishing

    d. Piggybacking

25. Software specifically designed to detect and eliminate viruses and other malware from a computer is known as:

    a. Debugger

    b. Antivirus

    c. Defragmenter

    d. Compiler

Part II: Very Short Questions:

Question 1-What is confidentiality? Why is confidentiality important? How can confidentiality be achieved?

Question 2- What is authentication? Why is authentication important? How can authentication be achieved? What is network access control?

Question 3- What is message integrity? Why is message integrity important? How can message integrity be achieved?

Question 4- What is access? What is availability? Why are access and availability important? How can access and availability be achieved?

Question 5- What are the six phases of penetration testing? What are the goals of each phase of penetration testing?

Part III: Case Study

Case Study Exercise: Social Engineering Attack on TechCo Inc.

Background: TechCo Inc., a mid-sized technology firm specializing in data analytics software, recently experienced a security breach. The breach was traced back to a social engineering attack. An attacker, pretending to be an IT support technician, contacted employees via email and phone, eventually convincing one of them to provide their login credentials. This case study explores how the breach occurred and aims to identify preventive measures.

Scenario: You are part of the cybersecurity team at TechCo Inc. tasked with analyzing the breach and developing strategies to prevent similar incidents in the future.

Exercise:

Part 1: Identification

- Task 1: Analyze how the attacker could identify and select their target within TechCo Inc. Consider the possible information sources the attacker might have used.
- Task 2: Identify the key vulnerabilities (technical and human) that were exploited in this attack.

Part 2: Attack Execution

- Task 3: Describe the steps taken by the attacker from initial contact to the successful acquisition of the credentials.
- Task 4: Discuss the role of social engineering techniques such as pretexting, phishing, and baiting in this scenario.

Part 3: Impact Assessment

- Task 5: Evaluate the immediate and long-term impacts of this breach on TechCo Inc. Consider both tangible and intangible effects.
- Task 6: Assess how the breach could have been detected earlier.

Part 4: Prevention and Response

- Task 7: Propose a comprehensive training program for employees to recognize and respond to social engineering attacks.
- Task 8: Recommend technical safeguards and policies that TechCo Inc. should implement to enhance its defense against social engineering attacks.
- Task 9: Develop a response plan for potential future incidents that includes both mitigation strategies and communication protocols.

Session 1

I)

1) a
2) b
3) d
4) c
5) c
6) b
7) b
8) c
9) d
10) d
11) a
12) a
13) b
14) c
15) d
16) c
17) b
18) c
19) a
20) a
21) c
22) b
23) c
24) a
25) b

II) 1- Def: Ensures information accessible only to authorized individuals

Confidentiality
- Importance: Protects sensitive data from unauthorized access
- Achievement: Encryption, access controls, password SSL

2- Def: Verifying identity of users/systems

Authentication
Importance: Prevent unauthorized access
Achievement: Passwords, biometrics, multi-factor authentication

Integrity
3- Def: Ensures data hasn't been altered during transmission
- Importance: Prevents tampering and corruption
- Achievement: Digital signatures, hash function

Availability

4- Def: Ability to access data
Importance: Essential for business operations
Achievement: Redundancy, backups

Penetration Test

5- 1) Penetration Preparation
. Define test goals and methods
. Create comprehensive test plans and timelines

2) Information Reconnaissance
. Gather as much info as possible about the target

3) Scanning (Vulnerability Identification)
. Discover network details, open ports, running services
. Identifying potential vulnerabilities
~~Vulnerability identification~~

4) Exploitation
. Attempt to get access to the target system and exploid vulnerabilities found
. The goal is to simulate how an actual attacker would gain control over systems

5) Post-Exploitation
. Understand the extent of the damage that could be caused once a vulnerability is exploited

6) Reporting
. Report all findings
. Provide security recommendations