IT221 Exam

Section 1: True / False [5 marks]

1. Availability ensures that information is not altered or modified.	
2. An IOC is evidence of an ongoing attack that has already fully completed.	
3. A memory safety vulnerability is never related to buffer overflows.	
4. Threat actors can use social engineering to manipulate individuals rather than exploiting technical vulnerabilities.	
5. A code review is an example of static code analysis.	
6. CSRF exploits a website's authentication token to force an authenticated user to perform actions.	
7. Rationale for risk indicators (KRIs) exceeding normal bounds could be an indicator of compromise (IOC).	
8. A fileless virus attaches malicious code to a file on disk to spread.	
9. A penetration test is typically a continuous, ongoing process rather than a single event.	
10. Threat hunting is only performed after a breach has been confirmed.	

Section 2: Choose the suitable answer [5 marks]

1. Which attack targets vulnerabilities in an API, DLL, or driver used by an application?
a) Attacks on external software components
b) CSRF
c) SQL injection
d) XSS

2. Which term is used for a software testing approach that uses random inputs to trigger unexpected behavior and potential crashes? a) Penetration testing
b) Fuzzing
c) Dynamic code analysis
d) Static code analysis

3. Which vulnerability type involves exploiting a web application's handling of input data to manipulate a database? a) SQL injection
b) XML External Entity (XXE)
c) XSS
d) Buffer overflow

4. Which endpoint security technology can aggregate data from multiple endpoint computers and use sophisticated analytics that identify patterns and detect anomalies? a) HIDS
b) SIEM
c) HIPS
d) Endpoint Detection and Response (EDR)
5. What hardware/firmware mechanism provides a secure starting point that cannot be altered by software?
a) Secure Boot key
b) Hardware root of trust
c) Trusted Platform Module (TPM)
d) Software root of trust

6. A program that secretly records keystrokes on a user's keyboard is commonly known as a:
a) Rootkit
b) Spyware
c) RAT
d) Keylogger

7. Which term describes a vulnerability that exists in third-party components, such as APIs or libraries, rather than in your own code?
a) External software component vulnerability
b) Zero-day vulnerability
c) Privilege escalation vulnerability
d) SQL injection vulnerability

8. Which technique is used by some memory-related attacks to cause a program to overwrite adjacent memory areas? a) Buffer overflow
b) Stack overflow (non-malicious)
c) Heap fragmentation
d) Integer overflow

9. Which of the following best describes a vulnerability assessment that is performed with credentials to mimic an attacker with access rights? a) Non-credentialed vulnerability scan
b) Passive OSINT scan
c) Intrusive penetration test
d) Credentialed vulnerability scan

10. Which measure involves allowing only known-good applications to run on a device?
a) Sandboxing
b) Antivirus scanning
c) Application whitelisting
d) Blacklist enforcement

Question 3: Attempt all the following questions [5 marks]

a. What is the purpose of a sandbox in endpoint hardening?

_____
_____
_____
_____

b. What is the primary difference between a file-based virus and a fileless virus?

_____
_____
_____
_____

Question 4: Answer the following two questions [5 marks]

a. A small business has a limited budget. They must choose between hiring an external penetrationtesting consultant and purchasing a continuous vulnerability scanner. Which choice is more appropriate if their primary concern is identifying deep, manual vulnerabilities that an automated scan might miss? Justify your answer.

_____
_____
_____
_____
_____
_____
_____

b. An employee receives an email claiming to be from the IT department, warning of a "deadlyvirus" and instructing the user to delete a specific system file. What type of social engineering attack is this, and why is it particularly dangerous?

_____
_____
_____
_____
_____
_____
_____

Answer Key

True/False:

1. False
2. False
3. False
4. True
5. True
6. True
7. True
8. False
9. False
10. False

MCQ:

1. a
2. b
3. a
4. d
5. b
6. d
7. a
8. a
9. d
10. c

Short Answers:

Q3(a): A sandbox isolates applications in a controlled environment to safely test suspicious behavior.

Q3(b): File-based viruses use files on disk, while fileless viruses run in memory without files.

Q4(a): Penetration testing is better because it finds deeper vulnerabilities that scanners may miss.

Q4(b): This is a Hoaxes. It tricks users into harmful actions using false information.