UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL TEST
MARCH 2026 SEMESTER

COURSE CODE	:	IKB 31603
COURSE NAME	:	ETHICAL HACKING
PROGRAMME NAME	:	BIT (HONS) IN COMPUTER SYSTEM SECURITY
DATE	:	25 JUNE 2026
TIME	:	2.00 pm – 4.00 pm
DURATION	:	2 HOURS

INSTRUCTIONS TO CANDIDATES

1. This question paper consists of TWO (2); Section A and Section B.
2. Answer ALL questions in Section A and Section B.
3. Please write your answers on the answer sheet provided to you.
4. Answer all questions in English language ONLY.

THERE ARE 7 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 20 marks)

INSTRUCTION: Answer ALL questions.

Choose the best answer for each question. Write the answer in the answer booklet.

1. A penetration tester deploys ARP spoofing in a switched network and observes intermittent traffic capture failures. What mitigation **MOST** likely explains the inconsistency?
   A. DHCP snooping with trusted uplinks
   B. Dynamic ARP Inspection enforcing binding validations
   C. Port mirroring with VLAN isolation policies
   D. STP guard preventing topology changes

2. During a web test, a tester captures a session cookie lacking the Secure flag but marked HttpOnly. Which attack vector remains **MOST** feasible?
   A. XSS-based session theft via DOM access
   B. Network sniffing over HTTP downgrade leading to session reuse
   C. CSRF requiring cookie read access in client scripts
   D. Clickjacking to extract cookie value via iframe overlay

3. A honeypot is configured with high-interaction services and realistic vulnerabilities. What is the **PRIMARY** risk compared to low-interaction honeypots?
   A. Increased likelihood of lateral movement into production systems
   B. Reduced visibility into attacker tactics
   C. Inability to collect full packet captures
   D. Lower attractiveness to attackers

4. A mobile app stores API keys in plaintext within its APK. What is the **MOST** appropriate mitigation?
   A. Hardcoding keys in native libraries to avoid decompilation
   B. Encrypting strings with static keys inside the app
   C. Code obfuscation combined with secure key storage and server-side controls
   D. Using HTTP instead of HTTPS to reduce interception complexity

5. A wireless network uses WPA2-PSK with a weak passphrase. Which attack is **MOST** practical for compromise?
   A. Real-time brute-force via deauthentication flooding
   B. Offline dictionary attack after capturing a 4-way handshake
   C. WEP IV collision exploitation
   D. TKIP Michael MIC failure exploitation

6. A SOC detects high volumes of SYN packets without ACK responses targeting a web server. What is the **MOST** likely impact?
   A. Data exfiltration via covert channels
   B. Resource exhaustion due to half-open connections
   C. Credential harvesting through phishing
   D. Cache poisoning in upstream resolvers

7. An Android app dynamically loads code at runtime from remote sources. What is the **PRIMARY** risk?
   A. Increased app performance overhead
   B. Remote code execution without app store validation
   C. Reduced attack surface due to modularization
   D. Improved patch management for vulnerabilities

8. An OT environment uses legacy protocols without authentication. Which attack is **MOST** concerning?
   A. Unauthorized command injection to critical control systems
   B. Web-based XSS attacks on operator dashboards
   C. SQL injection in historian databases
   D. Email phishing targeting operators

9. A wireless attacker performs deauthentication attacks before capturing handshakes. Why?
   A. To disable encryption temporarily
   B. To reset AP firmware to default settings
   C. To increase signal strength for capture
   D. To force clients to reconnect and generate a 4-way handshake

10. An organization faces a volumetric DDoS attack exceeding bandwidth capacity. Which mitigation is **MOST** effective?
    A. Increasing server CPU resources locally
    B. Blocking all inbound traffic at the firewall
    C. Upstream traffic scrubbing via cloud-based mitigation provider
    D. Deploying host-based antivirus

11. A low-interaction honeypot is deployed. What is its **PRIMARY** advantage?
    A. High fidelity attacker interaction data
    B. Ability to simulate full operating systems
    C. Detailed exploit chain reconstruction
    D. Reduced risk of compromise and easier maintenance

12. A mobile application fails to validate SSL certificates. What attack is **MOST** feasible?
    A. Man-in-the-middle interception with forged certificates
    B. SQL injection into backend databases
    C. Buffer overflow in native libraries
    D. Privilege escalation within OS kernel

13. An IoT botnet uses centralized command servers. What is a key weakness?
    A. Single point of failure for takedown operations
    B. Difficulty in scaling across devices
    C. Increased encryption overhead
    D. Limited device diversity support

14. A WPA3 network is targeted. Which attack is **MOST** relevant compared to WPA2?
    A. IV replay attacks in RC4 streams
    B. Dragonblood side-channel attacks exploiting SAE
    C. TKIP MIC failure exploitation
    D. WEP fragmentation attacks

15. A slowloris attack targets a web server. What is its impact?
    A. Flooding bandwidth with large volumes of data
    B. Exploiting SQL queries for data extraction
    C. Injecting scripts into user sessions
    D. Exhausting connection slots with partial HTTP requests

16. A firewall implements stateful inspection. Which behavior defines it?
    A. Filtering only based on IP and port
    B. Blocking all unsolicited inbound traffic without context
    C. Tracking connection states and allowing related packets
    D. Allowing all outbound traffic without logging

17. A web application is vulnerable to SSRF. What internal risk arises?
    A. Direct SQL database compromise
    B. Access to internal services and metadata endpoints
    C. Client-side script execution
    D. Browser cache poisoning

18. An OT network implements network segmentation. What is the **PRIMARY** benefit?
    A. Increasing bandwidth for control systems
    B. Simplifying device configuration
    C. Limiting propagation of attacks between zones
    D. Eliminating need for monitoring tools

19. Malware uses sandbox detection techniques. Which method is **MOST** indicative?
    A. Checking for virtualized environments and analysis artifacts
    B. Increasing network traffic to trigger alerts
    C. Using static payloads for execution
    D. Avoiding encryption altogether

20. A penetration tester attempts to bypass IPS using packet fragmentation. What is the risk if improperly reassembled?
    A. IPS may fail to detect malicious signatures across fragments
    B. Network latency increases beyond detection thresholds
    C. Packets are dropped by all routers
    D. Payload size becomes too small to execute

SECTION B (Total: 60 marks)

INSTRUCTION: Answer ALL questions.
Choose the best answer for each question.

Question 1 **(30 marks)**

Extract from news article (*https://thehackernews.com/2026/06/hackers-exploit-critical-everest-forms.html*) :

The article reports a critical Remote Code Execution (RCE) vulnerability (CVE-2026-3300) in the Everest Forms Pro WordPress plugin that is actively exploited by attackers to fully compromise websites. The flaw affects versions up to 1.9.12 and has a high severity score (CVSS 9.8).

The root cause of the vulnerability lies in insecure coding practices. Specifically, the plugin's "Complex Calculation" feature constructs PHP code dynamically by concatenating user-supplied input and executing it using the dangerous *eval()* function. Although input is processed with *sanitize_text_field()*, it fails to properly escape special characters such as single quotes. This allows attackers to break out of the intended string context and inject arbitrary PHP code, resulting in PHP code injection (RCE).

Attackers exploit this flaw without authentication by submitting crafted values into common form fields such as text, email, or URL inputs. The injected payload is then executed on the server, enabling attackers to perform malicious actions. One commonly observed attack involves creating rogue administrator accounts, which grants full control over the compromised WordPress site.

The impact of successful exploitation is severe. Attackers can take over entire websites, deploy web shells, install backdoors, modify content, exfiltrate of sensitive data, and maintain persistent access. This vulnerability has already been widely targeted, with more than 29,000 exploitation attempts recorded, highlighting the scale and automation of such attacks. Overall, the incident emphasizes the importance of secure coding, timely patching, and proactive monitoring in defending web applications against real-world exploitation.

a) Explain the root cause of the vulnerability in Everest Forms Pro. State **THREE** main causes.

(6 marks)

b) Describe the **SIX** steps in the attack chain used by attackers to exploit this vulnerability.

(6 marks)

c) Propose **THREE** mitigation strategies suitable for this case study and justify each strategy.

(9 marks)

d) Discuss **FOUR** impacts of successful exploitation of this attack.

(8 marks)

e) Which general type of software vulnerability category does this attack belong to? Name the vulnerability.

(1 mark)

Question 2

Scenario. You are the lead penetration tester engaged by **Acme Corp**. Under the agreed RoE you are authorised to assess the internal host 10.10.10.15. You begin reconnaissance with a full TCP service/version scan. The (abridged) result is shown below.

Figure — output of nmap -sV -sC -oA -T4 10.10.10.15

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-10 14:32 +08
Nmap scan report for 10.10.10.15
Host is up (0.018s latency).
Not shown: 65515 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
6667/tcp open  irc         UnrealIRCd
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:A5:12:9F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Nmap done: 1 IP scanned in 24.13s
```

a) From the scan output, identify **FOUR (4)** services that represent the most promising initial attack surface. For each, state the port, the service/version, and give a one-line justification.

(12 marks)

b) The FTP banner reads vsftpd 2.3.4. Explain the specific vulnerability tied to this exact version: state the trigger mechanism, the result of successful exploitation and tool suitable to be used for this exploitation.

(5 marks)

c) Explain **THREE (3)** exploitations that attacker would typically performed (conceptually, not commands) on the vsftpd 2.3.4 vulnerability.

(6 marks)

d) State what level of access an attacker would gain.

(1 mark)

e) Recommend **THREE (3)** mitigation strategies Acme Corp should implement to prevent such attacks in the future.

(6 marks)

END OF QUESTION PAPER