Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	SECURITY ASSESMENT AND TESTING
COURSE CODE	:	BIS 33703
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY/AUGUST 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK**. 3. STUDENT ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **EIGHT (8)** PAGES.

SECTION A

Choose the **BEST** answer for each of the following questions.

Q1 Open-source intelligence (OSINT) collection frameworks are used to effectively manage sources of collected information.

Which of the following best describes open-source intelligence?

A. Company documentation labeled "Confidential" on an internal company storage share requiring authentication.
B. Press release drafts found on an undocumented web page inside a company's intranet.
C. Any information or data obtained via publicly available sources that is used to aid or drive decision-making processes.
D. Information gained by source code analysis of free and open-source software (FOSS).

(2 marks)

Q2 Which static web page is focused on information gathering, providing web links and resources that can be used during the reconnaissance process, and can greatly aid penetration testers in the data-mining process?

A. Maltego.
B. OSINT Framework.
C. Shodan.
D. Censys.

(2 marks)

Q3 Which technique is used during passive reconnaissance to map a user-defined hostname to the IP address or addresses with which it is associated?

A. DNS zone transfer.
B. Reverse DNS lookup.
C. Investigation.
D. Forward DNS lookup.

(2 marks)

Q4 While footprinting an organization for a penetration test, you discover that a service it relies on using FTP port 14147 for data transfers.

How could you refine a Shodan search to only reveal FTP servers on that port?

A. `FTP port 14147`
B. `FTP:14147`
C. `FTP port:14147`
D. `FTP;port 14147`

(2 marks)

Q5 In a penetration test, it often occurs that a great deal of information pertinent to attacking target systems and goals is provided to the penetration tester.

Which of the following are often provided by the target organization? Choose **TWO (2)** answers.

A. IP addresses
B. Live usernames
C. Domain names
D. Administrator passwords for the Exchange and Active Directory servers

(2 marks)

Q6 What is the process of assessing a target to collect preliminary knowledge about systems, software, networks, or people without directly engaging the target or its assets?

A. Reconnaissance.
B. Passive information gathering.
C. Web searching.
D. Active information gathering.

(2 marks)

Q7 What is the primary purpose of penetration testing?

A. To identify and exploit vulnerabilities in a target system or network.
B. To improve the overall security posture of a target system or network.
C. To secure a target system or network against future attacks.
D. All of the above.

(2 marks)

Q8 Which of the following is **NOT** an ethical hacking tool?

A. Metasploit
B. Wireshark
C. Nmap
D. Backdoor

(2 marks)

Q9 Which of the following is a commonly used technique for discovering vulnerabilities in a target system or network?

A. Vulnerability scanning.
B. Port scanning.
C. Traffic analysis.
D. All of the above.

(2 marks)

Q10 Which of the accompanying should a penetration tester do next in the wake of recognizing that an application being tried has proactively been compromised with malware?

A. Analyzing the malware to see what it does.
B. Gather the appropriate proof and afterward eliminate the malware.
C. Do an underlying driver examination to figure out how the malware got in.
D. Eliminate the malware right away.

(2 marks)

Q11 A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 100.

Which of the following levels of difficulty would be required to exploit this vulnerability?

A. Very difficult; perimeter systems are usually behind a firewall.
B. Somewhat difficult, would require significant processing power to exploit.
C. Trivial, little effort is required to exploit this finding.
D. Impossible; external hosts are hardened to protect against attacks.

(2 marks)

Q12 A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have to immediately remediate all vulnerabilities.

Which of the following would be the **BEST** suggestion for the client?

A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.
B. Identify the issues that can be remediated most quickly and address them first.
C. Implement the least impact of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities.
D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long time.

(2 marks)

Q13 Choose **THREE (3)** elements to be removed from an exploited system before finalizing a penetration test.

A. User accounts created.
B. Shells spawned.
C. Any files left behind.
D. Administrator account.

(2 marks)

Q14 When running an Nmap SYN scan, what will be the Nmap result if ports on the target device does not respond?

A. Open
B. Closed
C. Filtered
D. Listening

(2 marks)

Q15 A potential customer is looking to test the security of its network. One of the customer's primary concerns is the security awareness of its employees.

Which type of test would you recommend that the company performs as part of the penetration test?

A. Social engineering testing.
B. Wireless testing.
C. Network testing.
D. Web application testing.

(2 marks)

SECTION B

Q16 You are given these sites, namely www.uthm.edu.my, www.google.com.my and www.utem.edu.my. Simple Mail Transfer Protocol (SMTP), Lightweight Directory Access Protocol(LDAP) and Domain Name Server(DNS) are the protocols related to these sites. Assume that you are using Windows 10, and currently you are at root directory D (D:).

Based on the scenario, answer the following questions.

(a) Write **ONE (1)** Nmap command for port scanning.

(5 marks)

(b) Explain the command given in **Q16(a)**.

(5 marks)

Q17 ABC Corporation, a large financial institution, recently underwent a penetration testing assessment to identify security vulnerabilities in their systems. A third-party security firm conducted the testing, auditing and provided a comprehensive report with findings and recommendations for remediation. The report revealed several vulnerabilities. The company was advised to implement a password policy requiring users to create complex passwords, establish a regular patch management process, implement network segmentation to isolate critical systems, conduct a thorough code review of their web application and implement proper input validation and session management. The company was also advised to conduct regular security awareness training for all employees to educate them on best practices and raise awareness of potential security threats.

Based on the scenario, answer the following questions.

(a) List security vulnerabilities of ABC Corporation.

(10 marks)

(b) What type of security auditor that conducted the auditing for ABC Corporation?

(2 marks)

(c) Based on your answer in **Q17(b)**, justify why this type of security auditor is approached for auditing the security of ABC Corporation.

(8 marks)

Q18 (a) Differentiate between verification and validation in software testing.

(5 marks)

(b) Discuss **TWO (2)** activities in verification.

(6 marks)

(c) Discuss **THREE (3)** activities in validation.

(9 marks)

Q19 `You work for PentestPro Sdn Bhd as a Penstester. Write steps for doing pentest using ZEH methodology that contain four phases. You are required to list all steps according to Zero Entry Hacking (ZEH) methodology for internal pentesting between your pentest machine (PentestComputer) and target machine (targetServer) using vm. Assume your target IP is 161.161.161.161 or bmww.com.my`

(a) List the names for each phase in ZEH methodology.

(2 marks)

(b) Write **ONE (1)** search command using **ONE (1)** Google hack operator for phase 1.

(2 marks)

(c) Write **ONE (1)** Nmap command to find the status of http service in phase 2.

(3 marks)

(d) Write **ONE (1)** Nmap command to find the weakness in http service by finding possible admin folder in phase 2.

(3 marks)

(e) Write attack steps using metasploit commands in phase 3.

(5 marks)

(f) Write reverse shell backdoor steps using netcat commands in phase 4 between pentester and target computers.

(5 marks)

-END OF QUESTIONS-