UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2023/2024

COURSE NAME	:	SECURITY ASSESSMENT AND TESTING
COURSE CODE	:	BIS 33703
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2024
DURATION	:	3 HOURS
INSTRUCTIONS	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA ☐ Open book ☒ Closed book 3. STUDENTS 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

PART A

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

Q1 Which of the following best describes Open-Source Intelligence (OSINT)?

(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) Information gained by source code analysis of free and open-source software (FOSS).

(d) Any information or data obtained via publicly available sources that is used to aid or drive decision-making processes.

(2 marks)

Q2 Which of the following, can be used to search for vulnerable CCTV connected to the Internet?

(a) Maltego.

(b) OSINT Framework.

(c) Shodan.

(d) Censys.

(2 marks)

Q3 Which technique is used during passive reconnaissance to map IP address to a domain name?

(a) DNS zone transfer.

(b) Reverse DNS lookup.

(c) Investigation.

(d) Forward DNS lookup.

(2 marks)

Q4 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)

Q5 What is the process of assessing a target to collect preliminary knowledge about systems, software, networks, or people that directly engaging the target?

(a) Reconnaissance.

(b) Passive information gathering.

(c) Web searching.

(d) Active information gathering.

(2 marks)

Q6 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)

Q7 Which of the following has meterpreter embedded in it?

(a) Metasploit.

(b) Wireshark.

(c) Nmap.

(d) Backdoor.

(2 marks)

Q8 Which of the following is a commonly used technique for identifying interesting services?

(a) Vulnerability scanning.

(b) Port scanning.

(c) Traffic analysis.

(d) All of the above.

(2 marks)

Q9 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)

Q10 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)

Q11 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)

Q12 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)

Q13 Which of the following command can be used to start metasploit?

(a) msfconsole.

(b) msf.

(c) msframework.

(d) All of the above.

(2 marks)

Q14 Which of the following are suitable for post-exploitation phase?

(a) Gain shell control.

(b) Obtain screenshot.

(c) Initiate key logging.

(d) All of the above.

(2 marks)

Q15 Which of the following requires vulnerability detection of their web applications through crowd sourcing?

(a) Penetration test.

(b) Meterpreter.

(c) Bug bounty.

(d) Metasploit.

(2 marks)

PART B

Q16 Suppose You are given these sites, namely www.uthm.edu.my, www.google.com.my and www.utem.edu.my. Simple Mail Transfer Protocol (SMTP), http,secure shell, and https 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 only **ONE (1)** Nmap command for port scanning multiple domains by storing the domains in a text file d:\web.txt.

(5 marks)

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

(3 marks)

(c) What is the content of d:\web.txt?

(2 marks)

Q17 Answer the following questions.

(a) Write a meterpreter command for gaining shell control.

(2 marks)

(b) Write commands used for creating listener and connecting virtual machines (VM) for bind shell backdoor.

(6 marks)

(c) Write a meterpreter command for listing available processes.

(2 marks)

(d) Write a meterpreter command changing to another process with process ID (PID) 486.

(3 marks)

(e) Write a meterpreter command to capture the screen.

(2 marks)

Q18 You work for PentestPro Sdn Bhd as a Penstester trainer. You are required to setup a demo for creating a backdoor for training new staff.

(a) Illustrate your bind shell backdoor demo environment using virtual machines (VM) and use appropriate label. Assume that these VM are using IPv4 Class B address.

(5 marks)

(b) Write commands used for creating listener and connecting VM for bind shell backdoor.

(5 marks)

(c) Illustrate your reverse shell backdoor demo environment using VM and use appropriate label. Assume that these VM are using IPv4 Class A address.

(5 marks)

(d) Write commands used for creating listener and connecting VM for reverse shell backdoor.

(5 marks)

(e) Which backdoor type is more suitable for target that resides behind a firewall? Justify your answer.

(5 marks)

- END OF QUESTIONS -