SIM GLOBAL EDUCATION

UNIVERSITY OF WOLLONGONG AUSTRALIA

School of Computing and Information Technology

Student to complete:

Family name	
Other names	
Student number	
Table number	

CSCI369
Ethical Hacking

Final Examination Paper
Session 3 2022

Exam duration	3 hours
Start time	10:00 am
End time	1:00 pm
Weighting	50% of the subject assessment
Marks available	50 marks
Directions to students	Marks for each question are shown beside the question. All answers must be hand-written with a **BLACK** or **DARK BLUE** pens.

Part A: Multiple Choice Questions (MCQs) (Total 15 marks)

1. What is the main purpose of ethical hacking? **(1.0 mark)**

A) To compromise systems

B) To steal data

C) To identify vulnerabilities from a defensive standpoint

D) To earn money unethically

2. What is OSINT? **(1.0 mark)**

A) Operating System Interface

B) Open Source Internet Technology

C) Open Source Intelligence

D) Overly Secure Intrusion Tool

3. Which OSI layer does TCP operate on? **(1.0 mark)**

A) Network

B) Transport

C) Session

D) Presentation

4. What is a port scan? **(1.0 mark)**

A) A method to identify active hosts

B) A way to determine which ports are open

C) Scanning an entire operating system

D) A network firewall configuration check

5. ARP stands for: **(1.0 mark)**

A) Advanced Routing Protocol

B) Apple Repair Protocol

C) Address Resolution Protocol

D) Active Route Poisoning

6. What does MITM stand for? **(1.0 mark)**

A) Maximum Internet Traffic Management

B) Man-In-The-Mirror

C) Man-In-The-Middle

D) Mandatory Internal Transfer Mechanism

7. What is brute force in the context of password cracking? **(1.0 mark)**

A) Using the strongest algorithm to encrypt passwords

B) Trying every possible password combination

C) Physically forcing someone to reveal their password

D) Cracking a password by applying a huge computational force

8. What is a zero-day vulnerability? **(1.0 mark)**

A) A vulnerability unknown to vendors

B) A vulnerability that has zero impact

C) A vulnerability patched on the same day it is discovered

D) A vulnerability that affects zero devices

9. Which of the following is a type of social engineering attack? **(1.0 mark)**

A) Port Scanning

B) SQL Injection

C) Phishing

D) Brute Force

10. What is WPA2? **(1.0 mark)**

A) Web Password Algorithm 2

B) Wireless Protected Access 2

C) Wi-Fi Protected Access 2

D) Web Port Authentication 2

11. What does APT stand for? **(1.0 mark)**

A) Advanced Persistent Threat

B) Apple Protocol Transfer

C) Access Point Traversal

D) Automated Penetration Test

12. What is ransomware primarily designed to do? **(1.0 mark)**

A) Encrypt files and demand a ransom

B) Steal passwords

C) Infect multiple devices on a network

D) Perform a DDoS attack

13. What type of privacy tool is Tor? **(1.0 mark)**

A) Firewall

B) Antivirus

C) Virtual Private Network

D) Anonymity Network

14. What does NAT stand for? **(1.0 mark)**

A) Network Area Technology

B) Network Address Translation

C) Natural Attack Time

D) Network Automation Tool

15. What is SSL? **(1.0 mark)**

A) Simple Security Layer

B) Secure Socket Layer

C) Secure Sync Link

D) Socket Security Layer

Part B: Calculation (Total 2 marks)

Please show your calculations.

16. What is the information entropy H of two binary password of length 12? **(2.0 marks)**

Part C: Short Answer Questions (Total 10 marks)

Please answer the following questions in a sentence or two.

17. What is the key difference between a black hat hacker and a white hat hacker? **(1.0 mark)**

18. Explain the term "information gathering" in the context of ethical hacking. **(1.0 mark)**

19. Describe the function of the OSI model. **(1.0 mark)**

20. What is the significance of conducting a vulnerability scan? **(1.0 mark)**

21. Explain ARP poisoning and its implications. **(1.0 mark)**

22. What are DNS attacks? Provide an example. **(1.0 mark)**

23. Explain the concept of "password entropy." **(1.0 mark)**

24. Describe one common vulnerability and how it can be exploited. **(1.0 mark)**

25. What is spear phishing and how does it differ from generic phishing? **(1.0 mark)**

26. Explain how WPA2 improves upon the security features of WPA. **(1.0 mark)**

Part D: Essay Questions (Total 23 marks)

Please provide a paragraph-length response to the following questions.

27. Discuss the ethical responsibilities that come with hacking and information gathering. **(4.0 marks)**

28. Describe the TCP/IP model and explain how capturing network traffic can assist in identifying vulnerabilities. **(4.0 marks)**

29. Discuss in detail the methods and countermeasures concerning ARP Poisoning and Man-in-the-Middle attacks. **(5.0 marks)**

are essentially the same except that WPA2 is based on stronger crypto functions like AES, CBC– MAC and etc.

rability scanning: This scan is to find weaknesses or problems

30. Provide a comprehensive guide on creating secure passwords and discuss the impact of vulnerabilities in password security. **(5.0 marks)**

31. Evaluate the importance of social engineering tactics within the broader context of cybersecurity, and discuss various tools and strategies for privacy and security against threats like Zero-Day, APT, and Ransomware. **(5.0 marks)**

End of Examination