[CRT11]

UNIVERSITY OF BOLTON

CREATIVE TECHNOLOGIES

BSC COMPUTER NETWORKS & SECURITY

SEMESTER TWO EXAMINATION 2018/2019

SECURITY FUNDAMENTALS

MODULE NO. SEC4003

Date: Friday 24th May 2019 **Time: 10:00 – 12:00**

INSTRUCTIONS TO CANDIDATES:

There are TWO sections in this exam Section A and B.

Section A: COMPULSORY with 25 parts.

Section B: There are FOUR questions. Answer THREE questions only.

All questions carry equal marks.

Individual marks are shown within the question.

Creative Technologies
Bsc Computer Networks & Security
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003.

Section A – COMPULSORY you must answer ALL 25 parts

This is a multiple choice question consisting of twenty-five parts each carrying equal marks. Each part has four possible answers of which ONLY ONE is correct. To indicate your selection, you should write down the question number and indicate which answer you have selected.

1) Which of the following statements best describes a white-hat hacker?

a) Security professional
b) Former black hat
c) Former grey hat
d) Malicious hacker

2) Which statement accurately describes the evolution of threats to network security?

a) Threats have become less sophisticated while the technical knowledge needed by an attacker has grown.
b) Internal threats can cause even greater damage than external threats.
c) Internet architects planned for network security from the beginning.
d) Early internet users often engaged in activities that would harm other users.

3) What type of ethical hack tests accesses to the physical infrastructure?

a) Internal network
b) Remote network
c) External network
d) Physical access

Section A continues over the page….

PLEASE TURN THE PAGE….

Creative Technologies
Bsc Computer Networks & Security
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003.

Section A continued….

4) What security solution can be used to mitigate a DoS attack?
- **a)** Virus scanning
- **b)** Intrusion protection system
- **c)** Applying user authentication
- **d)** Data encryption

.

5) The security, functionality, and ease of use triangle illustrate which concept?
- **a)** As security increases, functionality and ease of use increase.
- **b)** As security decreases, functionality and ease of use increase.
- **c)** As security decreases, functionality and ease of use decrease.
- **d)** Security does not affect the functionality and ease of use.

6) What are the components of the CIA triad security model?
- **a)** Communications, intrusions and attacks
- **b)** Cryptography, internet and availability
- **c)** Connections, integrity and attacks
- **d)** Confidentiality, integrity and availability

7) Which term best describes a hacker who uses their hacking skills for destructive purposes?
- **a)** Cracker
- **b)** Ethical hacker
- **c)** Script kiddie
- **d)** White-hat hacker

8) Which of the following is a tool for performing foot printing undetected?
- **a)** Whois search
- **b)** Traceroute
- **c)** Ping Sweep
- **d)** Host scanning

Section A continues over the page….

PLEASE TURN THE PAGE….

Creative Technologies
Bsc Computer Networks & Security
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003.

Section A continued….

9) Which of the following is not an encryption standard?
- **a)** DES
- **b)** AES
- **c)** ARP
- **d)** RSA

10) What is the next immediate step to be performed after footprinting?
- **a)** Scanning
- **b)** Enumeration
- **c)** System hacking
- **d)** Bypassing an IDS

11) Which of the following is a type of social engineering?
- **a)** Shoulder surfing
- **b)** User identification
- **c)** System monitoring
- **d)** Face-to-face communication

12) What is the best way to prevent a social-engineering attack?
- **a)** Installing a firewall to prevent port scans
- **b)** Configuring an IDS to detect intrusion attempts
- **c)** Increasing the number of help desk personnel
- **d)** Employee training and education

13) Dumpster diving can be considered which type of social-engineering attack?
- **a)** Human-based
- **b)** Computer-based
- **c)** Physical access
- **d)** Paper-based

Section A continues over the page….

PLEASE TURN THE PAGE….

Creative Technologies
Bsc Computer Networks & Security
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003.

Section A continued….

14) What port number does FTP use?
- **a)** 21
- **b)** 25
- **c)** 23
- **d)** 80

15) What does the TCP RST command do?
- **a)** Starts a TCP connection
- **b)** Restores the connection to a previous state
- **c)** Finishes a TCP connection
- **d)** Resets the TCP connection

16) What is the proper sequence of a TCP connection?
- **a)** SYN-SYN-ACK-ACK
- **b)** SYN-ACK-FIN
- **c)** SYN-SYN-ACK-ACK
- **d)** SYN-PSH-ACK

17) Which step comes after enumerating users in the CEH hacking cycle?
- **a)** Crack password
- **b)** Escalate privileges
- **c)** Scan
- **d)** Cover tracks

18) Why would an attacker want to perform a scan on port 137?
- **a)** To locate the FTP service on the target host
- **b)** To check for file and print sharing on Windows systems
- **c)** To discover proxy servers on a network
- **d)** To discover a target system with the NetBIOS null session vulnerability

Section A continues over the page….

PLEASE TURN THE PAGE….

Creative Technologies
Bsc Computer Networks & Security
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003.

Section A continued….

19) What is enumeration?
- **a)** Identifying active systems on the network
- **b)** Cracking passwords
- **c)** Identifying users and machine names
- **d)** Identifying routers and firewalls

20) What is the process of hiding text within an image called?
- **a)** Steganography
- **b)** Encryption
- **c)** Spyware
- **d)** Keystroke logging

21) What is privilege escalation?
- **a)** Creating a user account with higher privileges
- **b)** Creating a user account with administrator privileges
- **c)** Creating two user accounts: one with high privileges and one with lower privileges
- **d)** Increasing privileges on a user account

22) What is the recommended password-change interval?
- **a)** 30 days
- **b)** 20 days
- **c)** 1 day
- **d)** 7 days

23) What type of password attack would be most successful against the password T63k#s23A?
- **a)** Dictionary
- **b)** Hybrid
- **c)** Password guessing
- **d)** Brute force

Section A continues over the page….

PLEASE TURN THE PAGE….

Creative Technologies
Bsc Computer Networks & Security
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003.

Section A continued….

24) What is the first thing a hacker should do after gaining administrative access to a system?

a) Create a new user account
b) Change the administrator password
c) Copy important data files
d) Disable auditing

.

25) Asymmetric encryption is also referred to as which of the following?

a) Shared key
b) Public key
c) Hashing
d) Block

END OF SECTION A

PLEASE TURN THE PAGE….

Creative Technologies
Computing Pathways
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003

Section B – Answer ANY THREE questions

Question 1

a) With the aid of examples and diagrams, explain the Threat, Vulnerabilities, the Risk and control elements in the Network Security. **(7 marks)**

b) Assess the Network scanning common techniques, stress on a sweeping and port scan.

Support your answer with examples of using hping3, fping, nmap, and ultra-scan? **(8 marks)**

c) Evaluate the vulnerabilities scanning techniques, discuss the Nessus scanner and website vulnerabilities scanners architecture, and support your answer with examples and diagrams. **(10 marks)**

Question 2

a) Discuss the Enumerations concept, methods and tools?
State the steps and techniques to perform the enumerations. **(8 marks)**

b) Explain the Firewalls Design Principles and types, talk about the need for the Honeypots to protect the networks? **(10 marks)**

c) Evaluate the DOS and DDOS in term of Bandwidth/throughput, Protocol and software vulnerabilities attacks? **(7 marks)**

Section B continues over the page….

PLEASE TURN THE PAGE….

Creative Technologies
Computing Pathways
Semester Two Examination 2018/2019
Security Fundamentals
Module No. SEC4003

Section B continued….

Question 3

a) Discuss in details the Information Security Controls, types of controls and the impact elements? **(10 marks)**

b) Explain the Access Control Mechanisms using Reference Monitor and the Architecture Integration? **(7 marks)**

c) Appraise Spoofing Attack, expanding on ARP and RARP, IP, DNS Spoofing? Highlight on Spoofing Defenses to secure and protect the network. **(8 marks**

Question 4

a) What is Steganography, Digital Watermarking and Steganalysis? Discuss with details the type and the Future of the Steganalysis. **(10 marks)**

b) Discuss the System hacking steps and methodology, talk about the Password Attacks, Password Security, Technical password vulnerabilities and the Password Attacks – TYPES? **(8 marks)**

c) Describe what is meant by the following terms: Virus, Worm and a Trojan? **(7 marks)**

END OF QUESTIONS