UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET

COURSE CODE	:	BNS 3333
COURSE	:	ETHICAL HACKING & NETWORK DEFENSE
SEMESTER/SESSION	:	1-2022/2023
DURATION	:	3 HOURS

Instructions:

1. This booklet contains **5** questions. Answer **ALL** questions.
2. All answers should be hand written on your own answer booklet.
3. Write legibly draw sketches wherever required.
4. If doubt, raise your hands and ask the invigilator.

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE TOLD TO DO SO

THIS BOOKLET CONTAINS 4 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

a) Distinguish **FOUR (4)** differences between Hacking and Ethical Hacking. (8 marks)

b) Define these types of hackers

i. Grey Hat (2 marks)

ii. Scrip Kiddies (2 marks)

c) Defense in depth is a security strategy in which several protection layers are placed throughout an information system. Justify **TWO (2)** reasons why this layer is effective to prevent the intrusion. (4 marks)

d) Instead of to preventing hacker and fighting against terrorism from gaining access to information breaches, justify another **TWO (2)** reasons why it is important that organizations hire an ethical hacker. (4 marks)

QUESTION 2

a) Define the footprinting. (2 marks)

b) Give **FOUR (4)** examples of footprinting methodology. (4 marks)

c) Describe **FOUR (4)** processes involved in footprinting a target. (8 marks)

d) Justify **ONE (1)** reason why performing a footprinting on a target organization may provide a complete profile of the organization's security posture. (2 marks)

e) Name **TWO (2)** examples of footprinting tools and explain their purposes. (4 marks)

QUESTION 3

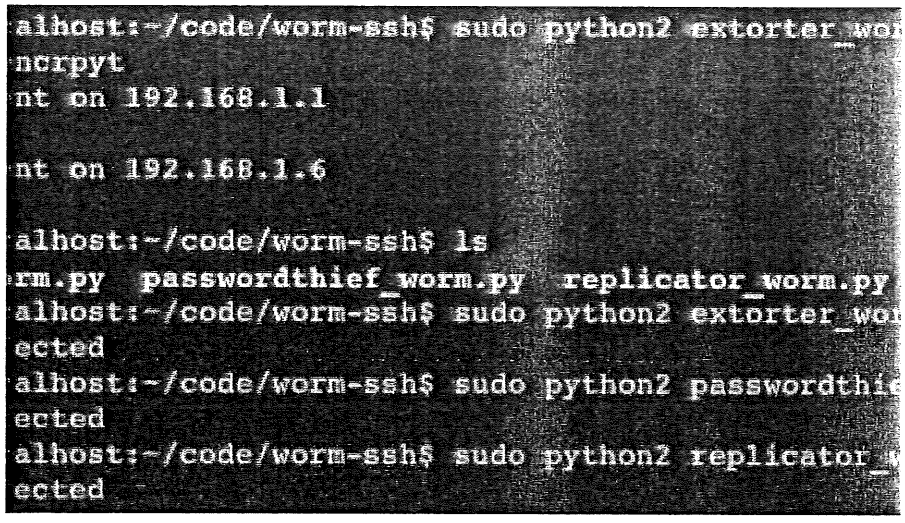

Figure 1: Malware signature

a) Amalia has found an USB drive in a Network Security Lab. Without her consent, she has mounted the USB drive in her laptop without checking properly the source. After a while, her computer has suddenly showed the symptom of malware infection.
   i. State the malware infection based on Figure 1. (1 mark)
   ii. Briefly explain **THREE (3)** malware features from your answer (i).(6 marks)
   iii. Describe **TWO (2)** countermeasure against malware infection from your answer (i). (4 marks)

b) Trojans are built for a variety of purposes, including the theft of personal information such as credit card numbers and passwords. Justify **ONE (1)** other reasons what do Trojan creator looking for. (2 marks)

c) Define these network attack.
   i. Spoofing Attack (2 marks)
   ii. Man-in-the-middle Attack (2 marks)

d) Gives **THREE (3)** examples of attack against encrypted data. (3 marks)

QUESTION 4

a) State **FOUR (4)** purposes of Scanning Phase. (4 marks)

b) Stealth Scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfer.

i. Illustrate a diagram the process of OPEN port XMASS Scan. (4 marks)
(Attacker: 10.0.0.6, Victim 10.0.0.8:23)

ii. Briefly explain the process in question b(i) (4 marks)

iii. Illustrate a diagram the process of OPEN port Null Scan. (4 marks)
(Attacker: 10.0.0.6, Victim 10.0.0.7:23)

iv. Briefly explain the process in question b(iii) (4 marks)

QUESTION 5

a) Adila receives notifications that she is receiving mail, phone calls, and other information requests. Additionally, she has discovered certain issues with his credit checks, such as bad debts and loans in which she did not engage.

i. Name type of attack did Adila become a victim of. (2 marks)

ii. Explain **TWO (2)** countermeasures what can you do if you fall victim to the attack mention in Question (a)(i). (4 marks)

b) Impersonation is a common human-based social engineering technique where an attacker pretends legitimate or authorized person. Demonstrate a situation below (which is different from lecture note) on how attacker perform impersonation tricks and gathers sensitive information about the target.

i. Posing as Important User (4 marks)

ii. Posing as Repairman (4 marks)

c) Give **THREE (3)** examples for these type of Social Engineering:

i. Computer-based Social Engineering (3 marks)

ii. Mobile-based Social Engineering (3 marks)

---------- End of Questions ----------