UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET		
COURSE CODE	:	BNS 3333
COURSE	:	ETHICAL HACKING & NETWORK DEFENCE
SEMESTER/SESSION	:	SEM 2, SESSION 2024/2025
DURATION	:	3 HOURS

Instructions:

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

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

THIS BOOKLET CONTAINS 6 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

a) Besides of main hacker classes (Black Hat, White Hat, Grey Hat, and script kiddies), list **THREE (3)** other types of hackers. (3 marks)

b) In the process of ethical hacking, there are several steps involved before successfully get the target. Describe these **TWO (2)** processes of hacking below:
   i. Reconnaissance (2 marks)
   ii. Gaining Access (2 marks)

c) Ain stopped by her favorite coffee shop to grab her afternoon drink. She placed her order, paid the clerk, and waited while the baristas worked furiously to fulfill the backup of orders. Ain pulled out her phone, opened the wireless client, and connected to what she assumed was the coffee shop's free wireless network. However, sitting in a corner of the store, a hacker had just set up an open "rogue" wireless hotspot posing as the coffee shop's wireless network. When Ain logged onto her bank's website, the hacker hijacked her session and gained access to her bank accounts. Another term for rogue wireless hotspots is "evil twin" hotspots.
   i. Elaborate how do threat actor typically manipulate victim into connecting to evil twin hotspots? (2 marks)
   ii. Once connected, threat actor able to engage in various malicious activities and tactics. State **FOUR (4)** common tactics used by hackers once a victim has connected to an evil twin hotspot? (4 marks)
   iii. Explain **TWO (2)** mitigation strategies that we can do to protect ourselves from falling victim to evil twin hotspots when using public Wi-Fi networks? (4 marks)

QUESTION 2

a) Azrin has received an attachment via e-mail. He downloaded the attachment without his consent and without fully verifying the source. After a while, his PC developed symptoms consistent with computer virus infection.

i. Describe another **THREE (5)** indication of a virus attack on a computer. (6 marks)

ii. Besides opening an email attachment, explain **TWO (2)** other ways how computer can get infection from computer virus. (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 another **THREE (3)** reasons what do Trojan creator looking for. (6 marks)

c) Describe **THREE (3)** threats introduced by reconnaissance attack. (6 marks)

d) Reconnaissance is the first step in penetration testing framework. There are two types of reconnaissance active and passive. Answer following questions:

i. Distinguish **TWO (2)** differences between passive and active reconnaissance. (8 marks)

ii. You visit the LinkedIn page of the target company, hoping to get some of their employee names. State what type of reconnaissance activity is this? (1 mark)

iii. State **THREE (3)** tools that can be used to perform a passive reconnaissance attack. (3 marks)

QUESTION 3

```
kali@kali:~$ sudo nmap -sS -sU -p 22,80,111,53,137 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 15:57 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT    STATE         SERVICE
22/tcp  open          ssh
53/tcp  closed        domain
80/tcp  open          http
111/tcp closed        rpcbind
137/tcp filtered      netbios-ns
22/udp  closed        ssh
53/udp  open          domain
80/udp  closed        http
111/udp closed        rpcbind
137/udp open|filtered netbios-ns

Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
kali@kali:~$
```

Figure 1: Port scan in Kali Linux

a) Putri performed port scan using Kali Linux. Answer following question based on **Figure 1:**

i. State the nmap syntax (command argument) that has been used by Putri to performed the port Scan in **Figure 1.** (1 mark)

ii. Name type of port scanning technique is performed by Putri. (2 mark)

iii. State the target in this scanning (1 mark)

iv. State how many targets ports TCP. (1 mark)

v. State how many ports are shown to be open. (1 mark)

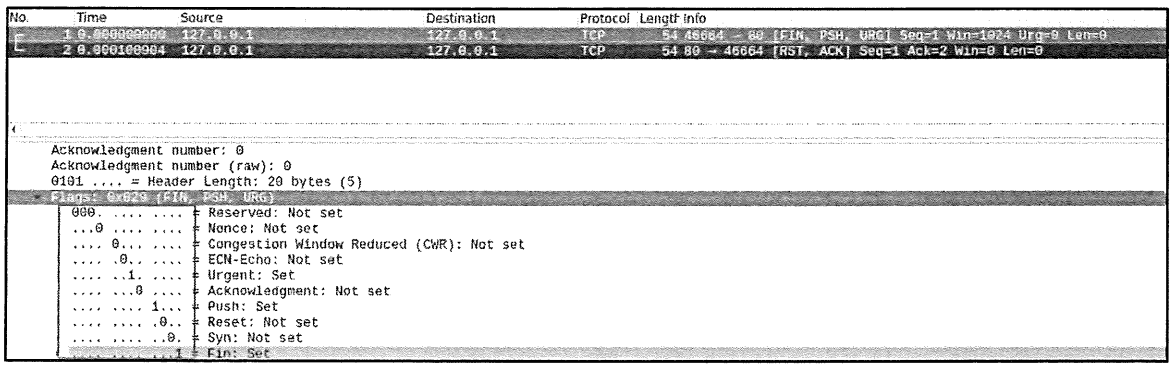

Figure 2: Port Scan

b) **Figure 2** shows a port scanning that viewed as a packet capture in Wireshark. Answer following question according to **Figure 2**.

i. Name type of port scanning is performed in **Figure 2**. (3 mark)

ii. State open or close port? (3 mark)

iii. Illustrate a diagram sequence of scanning between attacker (IP Address:?) and target (IP Address:?) associate with **Figure 2**. (4 marks)

iv. State the nmap syntax (command argument) to perform this scan. (1 mark)

QUESTION 4

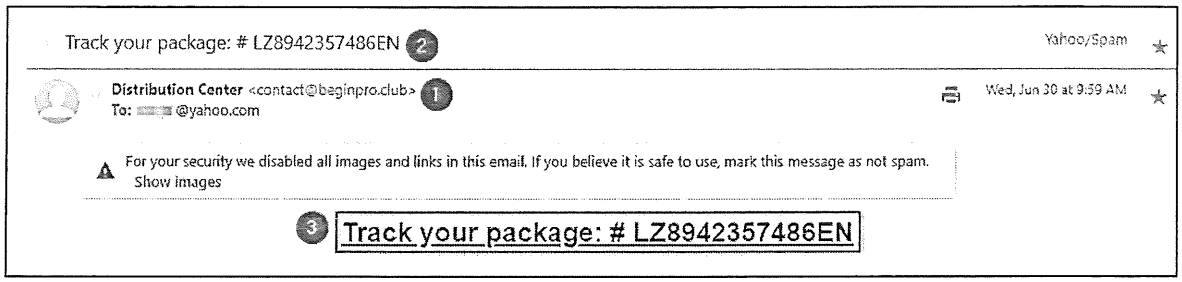

Figure 3: Email Sample

a) Amirul received a suspicious e-mail. As Security Operation Centre (SOC) Analyst, you have been tasked to investigate a suspicious e-mail sample as shown in **Figure 3** by answering the following questions:

i. Name type of computer-based social engineering attack did Amirul become a victim of. (1 marks)

ii. As illustrated in **Figure 3**, justify **THREE (3)** points to prove that the e-mail sample is malicious. (6 marks)

b) General phishing is a simple, mass phishing attack which does not target anyone, although they may aim for large groups (e.g., PayPal users, or Amazon customers. The general phishing campaign targeting large scale audience.
Define additional two types social engineering techniques below and state type of campaign.

i. Spearphishing (3 marks)

ii. Whaling (3 marks)

c) Explain **ONE (1)** factor why humans' behaviour can be vulnerable to Social Engineering attack. (2 marks)

QUESTION 5

a) Name the framework focuses on the testing of web applications. (Write the full name. (1 mark)

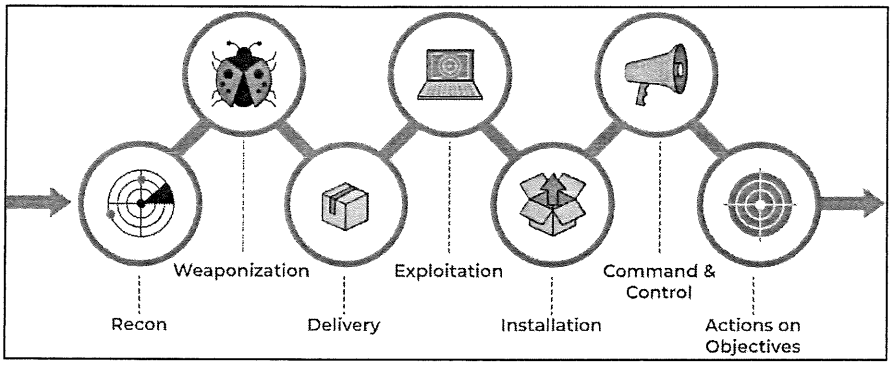

Figure 4: Lockheed Martin Cyber Kill Chain

b) The red team can use various cyber kill chains to summarize and assess the steps and procedures of an engagement. **Figure 4** shows the techniques use in Lockheed Martin Kill Cyber Chain are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control and Action on Objectives.
Explain each purpose of **SEVEN (7)** techniques in Lockheed Martin Cyber Kill Chain. (14 marks)

c) Besides Lockheed Martin Kill Chain, state **TWO (2)** other examples of cyber kill chain. (2 marks)

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