UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET		
COURSE CODE	:	BNS 3333
COURSE	:	ETHICAL HACKING & NETWORK DEFENSE
SEMESTER/SESSION	:	SEM 2, SESSION 2023/2024
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) Instead of to preventing hacker and fighting against terrorism from gaining access to information breaches, justify another **THREE (3)** reasons why it is important that organizations hire an ethical hacker. (6 marks)

b) Describe **ONE (1)** characteristic for each types of hackers below:
   i. Script Kiddies (2 marks)
   ii. White Hat (2 marks)

c) Besides Black Hat, White Hat, Grey Hat and Script Kiddies, list **THREE (3)** other types of hacker. (3 marks)

d) Describe an example of these two categories of vulnerability below:
   i. Weak or default credentials (2 marks)
   ii. Human-factor (2 marks)

e) Distinguish **TWO (2)** scopes between black-box testing and white-box testing. (8 marks)

f) Name the penetration testing framework that focuses on the testing of web applications. (Write the Full name) (1 mark)

g) The red team can use various cyber kill chains to summarize and assess the steps and procedures of an engagement. List **SIX (6)** techniques use in Lockheed Martin Kill Chain. (6 marks)

h) Besides Lockeheed Martin Kill Chain, state **TWO (2)** other examples of Cyber Kill Chain. (2 marks)

QUESTION 2

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

b) Reconnaissance is the first step in ethical hacking and 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 **TWO (2)** tools can be used to perform an active reconnaissance attack. (2 marks)

QUESTION 3

a) Taufiq 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. List **FIVE (5)** other reasons indication of a virus attack on a computer. (5 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 **THREE (3)** other reasons what do Trojan creator looking for. (6 marks)

QUESTION 4

```
grumpy-ghost@kali:~$ sudo nmap -p1-5000 -sS 10.10.245.20 -Pn -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:30 EST
Initiating Parallel DNS resolution of 1 host. at 19:30
Completed Parallel DNS resolution of 1 host. at 19:30, 0.04s elapsed
Initiating SYN Stealth Scan at 19:30
Scanning 10.10.245.20 [5000 ports]
Discovered open port 3389/tcp on 10.10.245.20
Discovered open port 53/tcp on 10.10.245.20
Discovered open port 21/tcp on 10.10.245.20
Discovered open port 80/tcp on 10.10.245.20
Discovered open port 135/tcp on 10.10.245.20
Completed SYN Stealth Scan at 19:30, 30.05s elapsed (5000 total ports)
Nmap scan report for 10.10.245.20
Host is up, received user-set (0.14s latency).
Scanned at 2021-01-11 19:30:29 EST for 30s
Not shown: 4995 filtered ports
Reason: 4995 no-responses
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 127
53/tcp   open  domain        syn-ack ttl 127
80/tcp   open  http          syn-ack ttl 127
135/tcp  open  msrpc         syn-ack ttl 127
3389/tcp open  ms-wbt-server syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 30.16 seconds
           Raw packets sent: 10015 (440.660KB) | Rcvd: 26 (1.144KB)
```

Figure 1. Result of scanning in Kali Linux

a) Amirah performed an nmap scan using Kali Linux as illustrated in Figure 1. Answer following question based on Figure 1:

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

ii. Name type of port scanning is performed by Amirah. (2 marks)

iii. State the target IP address. (1 mark)

iv. State how many target ports. (1 mark)

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

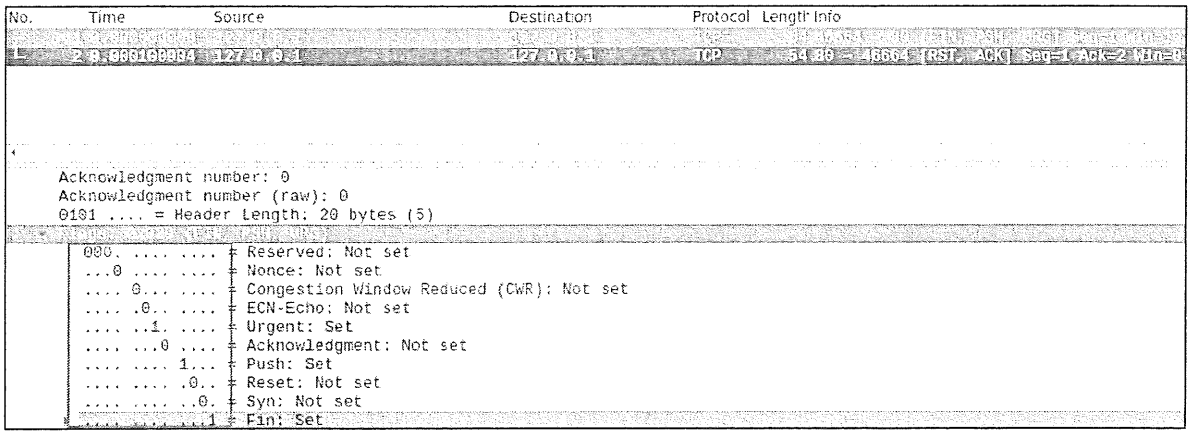

Figure 2. Result of Scanning in Wireshark

b) Figure 2 shows a result of 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. Explain your reason to support your answer. (3 marks)

ii. State open or close port? Explain your reason to support your answer. (3 marks)

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

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

QUESTION 5

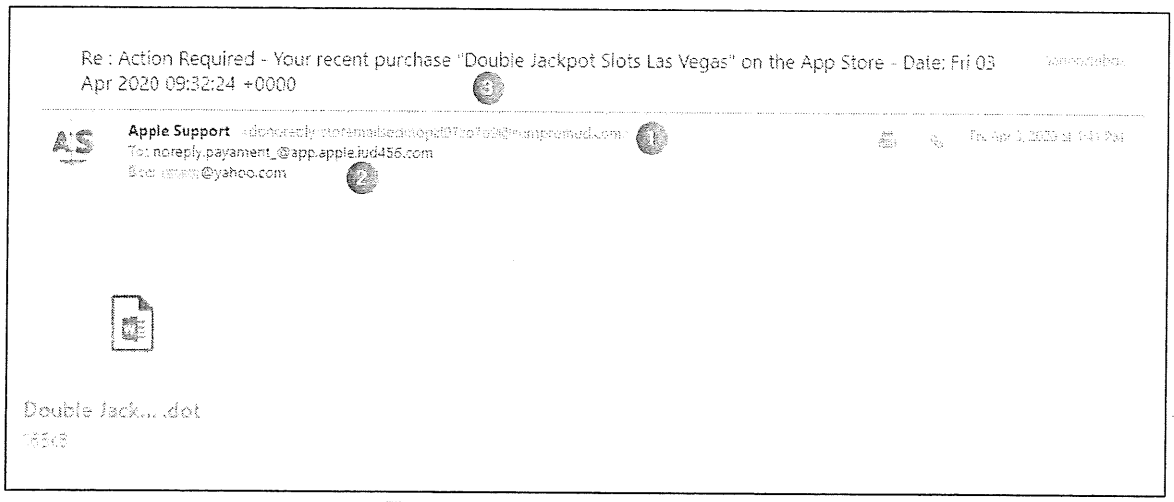

Figure 3. Email Sample

a) As a 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 as indicate in email sample. (1 marks)

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

b) Define these two types human-based social engineering techniques below. How can individuals protect themselves from with these types of social engineering? Provide **TWO (2)** specific examples or recommendations to support your answer.

   i. Shoulder Surfing (5 marks)

   ii. Dumpster Diving (5 marks)

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