

TED (15) – 5135
(REVISION – 2015)

Reg. No.
Signature

DIPLOMA EXAMINATION IN ENGINEERING/TECHNOLOGY/
MANAGEMENT/COMMERCIAL PRACTICE — APRIL, 2019

ETHICAL HACKING

[Time : 3 hours

(Maximum marks : 100)

PART — A

(Maximum marks : 10)

Marks

I Answer *all* questions in one or two sentences. Each question carries 2 marks.

1. Define Ethical Hacking.
2. List two malwares.
3. Define foot printing.
4. Write the need of NetBIOS.
5. List two web attackers tools.

(5 × 2 = 10)

PART — B

(Maximum marks : 30)

II Answer any *five* of the following questions. Each question carries 6 marks.

1. Explain man in the middle attack.
2. Describe DNS zone transfer method.
3. Explain dumpster diving.
4. Explain Server Message Block.
5. Summarize Linux OS vulnerabilities.
6. Explain Common Gateway Interface.
7. Describe the method of war driving.

(5 × 6 = 30)

PART — C

(Maximum marks : 60)

(Answer *one* full question from each unit. Each full question carries 15 marks.)

UNIT — I

- III (a) Explain Virus, Worms and Trojan Program. Give example for each. 9
 (b) Explain Session Hijacking. 6

OR

- IV (a) Explain DDoS, Brute Force attack and Replay attack. 9
 (b) Compare Spyware and Adware. 6

UNIT — II

- V (a) Explain the different type of port scanning. 9
 (b) Explain Social Engineering. 6

OR

- VI (a) Describe the port scanning tools NMAP, Unicorn scan and Nessus. 9
 (b) Explain competitive intelligence. 6

UNIT — III

- VII (a) Explain the content of a password policy for user authentication. 9
 (b) Explain OpenVAS tool for Linux enumeration. 6

OR

- VIII Describe different steps to hardening Windows systems. 15

UNIT — IV

- IX (a) Explain three web application components. 9
 (b) Describe counter measures for wireless attack. 6

OR

- X (a) Explain three web application vulnerabilities. 9
 (b) Explain Service Set Identifiers. 6