

Reg. No. :

--	--	--	--	--	--	--	--	--	--

Question Paper Code: 41883

B.E. / B.Tech. DEGREE EXAMINATION, MAY 2017

Elective

Information Technology

14UIT920 - ETHICAL HACKING AND INFORMATION FORENSICS

(Regulation 2014)

Duration: Three hours

Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 1 = 10 Marks)

- Following is not a type of firewall
 - Packet filter firewall
 - Packet inspection firewall
 - Application proxy firewalls
 - Proxy firewalls
- Correct means of DOS
 - Denial-of-service (DoS) attacks typically flood servers
 - Denial-of-service (DoS) attacks only for firewall
 - Denial-of-service (DoS) attack is dangerous attack
 - Denial-of-service (DoS) attack destroy the whole data
- Buffer overflow is based on
 - memory
 - operating system
 - firewall
 - Attack
- Following thinks which is not example of Web hacking
 - Credit card number
 - Some other website login and password
 - email address and password
 - Without internet desktop password
- Strategic planning is _____ process.
 - Day-to-day process
 - Weekly process
 - Monthly process
 - Yearly Process

6. A thread of execution is the smallest sequence of programmed instructions that can be managed independently by a scheduler, which is typically a part of the
- (a) operating system
 - (b) firewall
 - (c) Thread
 - (d) filter
7. How to protect your website from hackers
- (a) keep software up to date
 - (b) don't use trial versions
 - (c) don't use without licence software
 - (d) don't share anything
8. The goal of computer forensics is to perform a _____ while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.
- (a) Unstructured investigation
 - (b) Structured investigation
 - (c) Formatted investigation
 - (d) Un formatted investigation
9. Neural network is also called as
- (a) wireless network
 - (b) Internetwork
 - (c) Artificial Neural Network
 - (d) broadcast network
10. The word forensics means
- (a) to collect data
 - (b) to enquiry data
 - (c) destroy the evidence
 - (d) to bring to the court

PART - B (5 x 2 = 10 Marks)

11. What is the attack and list the types of attack.
12. What is firewall and usage of firewall?
13. Define strategic planning process.
14. What is Intrusion detection system?
15. Define neural networks.

PART - C (5 x 16 = 80 Marks)

16. (a) Explain in detailed about Hacking. (16)

Or

- (b) Explain in detailed about any two types of Attacks. (16)

17. (a) Explain about DOS and DDOS attack. (16)

Or

(b) Brief notes on following topics (i) Packet filter firewall (ii) Packet inspection firewall (iii) Application proxy firewalls. (16)

18. (a) Describe about fundamentals of computer fraud. (16)

Or

(b) Explain about the concept of strategic planning process. (16)

19. (a) Explain about the techniques used for protection of web sites. (16)

Or

(b) Explain about Intrusion Detection System (IDS), NIDS and HIDS. (16)

20. (a) Explain about key fraud indicator selection process. (16)

Or

(b) Explain about accounting forensics and computer forensics. (16)
