Reg. No. : | | | | | | | | | | | | |

Question Paper Code : K1362

M.C.A. DEGREE EXAMINATION, AUGUST/SEPTEMBER 2016.

Third Semester

DMC 7301 — SECURITY PRACTICE

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define the term threat environment.
2. Distinguish between cyber war and cyber error.
3. Give the five modes of operation of Block cipher.
4. What are the differences between SSL version 3 and TLS?
5. Define basic access control terminology.
6. Define Auditing.
7. How data can be protected while it is being transmitted?
8. List the advantages of data centers.
9. What is meant by Buffer overflow?
10. Define Inference.

PART B — (5 × 16 = 80 marks)

11. (a) Explain how criminals have become the dominant attackers today, describe the types of attacks they make and discuss the modes of cooperation. (16)

Or

(b) Explain risk analysis in detail. (16)

12. (a) Explain how electronic signatures, including digital signatures, digital certificates, and key-hashed message authentication codes (HMAC) work. (16)

Or

(b) (i) Explain quantum security. (8)

(ii) Explain cryptographic systems including VPNs, SSL, and IPsec. (8)

13. (a) Describe how central authentication servers work. (16)

Or

(b) (i) Explain the working of Network Address Translation (NAT) in detail. (8)

(ii) Describe some difficult problems associated with Firewalls. (8)

14. (a) What is Virtualization? What are the advantages of using virtual machines? (16)

Or

(b) (i) What kind of risks do web service and e-commerce service create for corporations? Explain in detail. (8)

(ii) Describe the intrusion response process for major incidents. (8)

15. (a) (i) Explain the common principles behind Secure Coding. (8)

(ii) What are the vulnerabilities occurred in OWASP/SANS? (8)

Or

(b) Explain in detail about C Secured Software Development Life Cycle (16)

Reg. No. : | | | | | | | | | | | | | |

Question Paper Code : FM3129

M.C.A. DEGREE EXAMINATIONS, FEBRUARY/MARCH 2020
Fourth Semester (Elective)
DMC 7007 – ETHICAL HACKING AND CYBER FORENSICS
(Regulations 2013)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. List the five steps in ethical hacking.
2. What are the three types of hackers ?
3. What is the use of computer forensics in law enforcement ?
4. List the vendors of forensics services.
5. What are the factors that affect back-up ?
6. List the different types of Evidences.
7. List the tools needed for an intrusion response to the destruction of data.
8. What do you mean by a clock filter ?
9. What is the role of Global military alliance ?
10. Differentiate between threats and attacks.

PART – B **(5×13=65 Marks)**

11. a) How is network host hacking performed in ethical hacking ? Explain about ethical hacking in motion. (13)

(OR)

b) Describe in detail, the foundations for ethical hacking. (13)

12. a) Illustrate the recovery mechanism and the data backup in detail. (13)

(OR)

b) Discuss the various types of computer forensics technology. (13)

13. a) Explain the steps in processing computer evidence. (13)

(OR)

b) With a neat sketch, explain how Authenticode works with VeriSign Digital IDs. (13)

14. a) Discuss in detail about network forensics data visualizer with its main components. (13)

(OR)

b) Describe the digital evidence collection procedure and explain how to authenticate the electronic evidences. (13)

15. a) Explain the new tools used in terrorism and write the tactics of terrorists and rogues to attack networks. (13)

(OR)

b) Explain how is military protected against threats ? Discuss about tactics of the military. (13)

PART – C (1×15=15 Marks)

16. a) Create a Case Study on : Fighting cyber-crime with risk management techniques. (15)

(OR)

b) Analyze common authentication methods used for network security. (15)

Reg. No. : | | | | | | | | | | | | | |

Question Paper Code : BS2380

M.C.A. DEGREE EXAMINATION, AUGUST/SEPTEMBER 2017.

Fourth Semester – Elective

DMC 7007 — ETHICAL HACKING AND CYBER FORENSICS

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is Ethical Hacking?

2. Mention the various types of Ethical Hacking.

3. List the Vendors of Forensics Services.

4. Define Computer Forensics.

5. Why data recovery is needed?

6. What is authentication?

7. How to do identification on data?

8. Mention the types of attacks in network.

9. List out the tactics in the threats.

10. What are ways to block the threats?

PART B — (5 × 13 = 65 marks)

11. (a) How Ethical Hacking is done in the network hosts? Explain with various methods. (13)

Or

(b) (i) How the application is hacked? (6)

(ii) Discuss the Operating System Hacking. (7)

12. (a) (i) Write short note on intrusion detection system. (7)

(ii) Discuss the Forensics Services. (6)

Or

(b) (i) Explain the various types of the Forensics Technologies. (7)

(ii) Write about the DoS attacks. (6)

13. (a) Discuss about the Evidence collection and data seizure in data recovery. (13)

Or

(b) Describe the computer image verification and authentication process. (13)

14. (a) (i) Explain about the Electronic Evidence. (7)

(ii) Explain the methods to collect electronic evidence. (6)

Or

(b) Discuss how to reconstruct the Past Events. (13)

15. (a) (i) How to fight against Macro threats? (6)

(ii) Write the steps to be followed for protecting the Information Arsenal. (7)

Or

(b) Explain the different tactics followed by the military against threats. (13)

PART C — (1 × 15 = 15 marks)

16. (a) Create a Case Study on: Trojan horse and Ransom ware. (15)

Or

(b) Analyze the verification methods used in Aadhaar. (15)

———————

Reg. No. : | | | | | | | | | | | | |

Question Paper Code : F5028

M.C.A. DEGREE EXAMINATION, FEBRUARY/MARCH 2019.

Fourth Semester — (Elective)

DMC 7007 — ETHICAL HACKING AND CYBER FORENSICS

(Regulations 2013)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Distinguish between hacker and normal user.

2. Write the need of ethical hacking.

3. Is your personal information used against you, to do crime. Justify.

4. Name the vendors of forensics services.

5. Write the need of data recovery system.

6. Which type of evidence is subject to the perceived reliability of the witness?

7. List out the any two network forensics tools.

8. What is the need of electronic evidence?

9. Why terrorists and rogues have an advantage in Information Warfare?

10. What is HERF Gun Information Weapon?

PART B — (5 × 13 = 65 marks)

11. (a) Briefly discuss about the ethical hacking in motion. (13)

Or

(b) (i) How ethical hacking is done in an operating System? Explain. (6)

(ii) Illustrate any two hacking applications. (7)

12. (a) (i) Explain in detail about Law Enforcement computer Forensic technology. (6)

(ii) Write short notes on Firewall security systems. (7)

Or

(b) Describe about the computer forensics service in detail. (13)

13. (a) Explain about the computer image verification and authentication. (13)

Or

(b) (i) Write the rules of evidence used in computer forensics evidence collection. (6)

(ii) A parent was concerned that her son was accessing unwanted Web sites from his computer. Each time the computer was checked by a technician, no evidence was found. How would a Computer Forensics Service go about investigating this incident? (7)

14. (a) (i) Brief about the discovery of electronic evidence. (6)

(ii) Write short notes on identification of data. (7)

Or

(b) Illustrate about the reconstructing the past events. (13)

15. (a) (i) Write the role of global military alliances. (6)

(ii) What to do when terrorists keep attacking? Explain. (7)

Or

(b) Explain the IW tactics of the Military five elements of information operations, command and control warfare (C2W), covering both offensive and defensive applications. (13)