

Total No. of Questions : 6]

SEAT No. :

PE-13050

[Total No. of Pages : 2

[6520]-1001
First Year M.Sc.
CYBER SECURITY
MCS-501-MJ : Malware Analysis - II
(2024 Pattern) (Semester - I)

Time : 3 Hours]

[Max. Marks : 70

Instructions to the candidates :

- 1) *All questions are compulsory.*
- 2) *Figures to the right side indicate full marks.*

Q1) Solve any Six of the following :

[6 × 2 = 12]

- a) Define Advanced Sandboxing.
- b) Define Anti-Debugging technique.
- c) What is Cryptanalysis?
- d) Define Function Reconstruction.
- e) Define Static Features in malware classification.
- f) Define Threat Feeds.
- g) What is Information Sharing Platform?

Q2) Attempt any Four of the following :

[4 × 3 = 12]

- a) What is Behavioral analysis in malware detection.
- b) Outline Anti-Analysis techniques used by malware.
- c) Describe Code Deobfuscation techniques.
- d) Mention Machine Learning limitations in Malware detection.
- e) Describe in Detail Role of Threat Intelligence in malware analysis.

P.T.O.

Q3) Attempt any Three of the following :

[3 × 4 = 12]

- a) What are Runtime hooking techniques.
- b) Explain in Brief Control Flow Graph representation.
- c) Describe Analyzing encrypted malware.
- d) What is Proactive Threat Hunting.

Q4) Attempt any Three of the following :

[3 × 4 = 12]

- a) How Memory Analysis integration is done with dynamic analysis.
- b) What are Different Malware unpacking techniques.
- c) List out Incorporating threat indicators.
- d) How Collaborative investigation is done through JACs.

Q5) Attempt the following :

- a) Attempt any TWO of the following.

[2 × 5 = 10]

- i) Give Difference between Static vs Dynamic feature extraction.
- ii) What are the Debugging techniques used in reverse engineering.
- iii) Explain in detail Incident Response workflow in malware outbreaks.

- b) Attempt any ONE of the following.

[1 × 2 = 2]

- i) Define Malware Classification with Examples.
- ii) What is Indicator of Compromise (IOC).

Q6) Write a short note. (Any Two) :

[2 × 5 = 10]

- a) Analyze Behavioral detection approaches.
- b) Explain Leveraging OSINT for cyber threat investigations.
- c) Analyze Command and Control communication patterns.



Total No. of Questions : 7]

SEAT No. :

PE-13051

[Total No. of Pages : 2

[6520]-1002
First Year M.Sc.
CYBER SECURITY
MCS-502-MJ: Intrusion Detection and Prevention System
(2024 Pattern) (CBCS) (NEP) (Semester - I)

Time : 3 Hours]

[Max. Marks : 70

Instructions to the candidates :

- 1) *Q.1 is compulsory.*
- 2) *Attempt any FIVE questions from Q.2 to Q.7*
- 3) *Figures to the right indicate full marks.*

Q1) Attempt any FIVE of following :

[5 × 2 = 10]

- a) Define False Positives and False Negatives in the context of IDS.
- b) What is Deep Packet Inspection (DPI)?
- c) State the purpose of a Honey Pot in an intrusion detection environment.
- d) Define Behavior-based Detection.
- e) What is the role of a Management Console in a distributed IDS?
- f) Define Promiscuous Mode in Network Intrusion Detection.
- g) What is the significance of Log Normalization in SIEM?

Q2) Attempt the following :

[12]

- a) Explain the working of Heuristic-based Detection with suitable examples.
[4]
- b) Discuss the impact of Network Segmentation on IDS/IPS effectiveness.
[3]
- c) Explain the SIEM Data Lifecycle from collection to archival.
[5]

P.T.O.

Q3) Attempt the following : [12]

- a) Differentiate between In-line (IPS) vs. Passive (IDS) deployment modes. [4]
- b) Explain Rootkit Detection as a specialized function of HIDS. [3]
- c) Discuss Thresholding and Throttle mechanisms used to prevent alert fatigue. [5]

Q4) Attempt the following : [12]

- a) Analyze the process of Signature Policy Development for a new zero-day vulnerability. [4]
- b) Illustrate the Components of a HIDS (Host-based IDS) with a neat diagram. [3]
- c) Compare Centralized vs. Decentralized IDS sensor management. [5]

Q5) Attempt the following : [12]

- a) Discuss the challenges of Traffic Fragmentation as an evasion tactic. [4]
- b) Evaluate the role of Threat Intelligence Feeds in modern IPS. [3]
- c) Explain the Resource Consumption limitations of performing DPI on high-speed links. [5]

Q6) Attempt the following : [12]

- a) Describe Rule-based Correlation vs. Algorithmic Correlation in SIEM. [4]
- b) Detail the deployment of IDS in a Cloud/Virtualization environment. [3]
- c) Explain how User and Entity Behavior Analytics (UEBA) enhances traditional IDS. [5]

Q7) Attempt the following : [12]

- a) Describe the Maintenance Lifecycle of an IDS (Tuning, Patching, and Testing). [4]
- b) Explain Protocol Anomaly detection specifically for the HTTP/HTTPS protocol. [3]
- c) Discuss Traffic Rate Limiting and Shunning as active response techniques in IPS. [5]



Total No. of Questions : 5]

SEAT No. :

PE-13052

[Total No. of Pages : 2

[6520]-1003

F.Y. M.Sc. (Cyber Security)

MCS503 - MJ : DIGITAL IMAGE PROCESSING

(2024 Pattern)(Semester - I)

Time : 2 Hours]

[Max. Marks : 35

Instructions to the candidates:

- 1) Question No. 1 is compulsory.
- 2) Solve any Three questions from Q.2 to Q.5.

Q1) Attempt any FIVE of the following :

[5 × 1 = 5]

- a) Define digital image.
- b) What is image acquisition?
- c) Define histogram equalization.
- d) What is Fourier Transform?
- e) Define lossless compression.
- f) What is feature extraction?
- g) Define dilation operation.

Q2) Attempt the following :

[4 + 4 + 2 = 10]

- a) Explain the fundamentals of image processing.
- b) Describe image representation techniques and histogram concept.
- c) Define degradation model.

Q3) Attempt the following :

[4 + 4 + 2 = 10]

- a) Explain Run-Length Encoding with suitable example.
- b) Describe thresholding techniques in image segmentation.
- c) Define template matching.

P.T.O.

Q4) Attempt the following :

[4 + 4 + 2 = 10]

- a) Explain spatial filtering methods for noise removal.
- b) Describe machine learning approaches in image classification.
- c) Define erosion operation.

Q5) Attempt the following :

[5 + 5 = 10]

- a) Explain transform coding and JPEG compression.
- b) Describe multispectral and hyperspectral imaging with applications.



Total No. of Questions :5]

SEAT No. :

[Total No. of Pages : 2

PE13053

[6520]-1004

F.Y.M.Sc. (Cyber Security)

MCS-510-MJ: DIGITAL PAYMENTS & ITS SECURITY

(2024 NEP Pattern) (Semester-I)

Time : 2 Hours]

[Max. Marks : 35

Instructions to the candidates:

- 1) *Question No. 1 is compulsory.*
- 2) *Solve any Three questions from Q.2 to Q.5.*
- 3) *Question 2 to 5 carry equal marks.*

Q1) Attempt any Five of the following:

[5×1=5]

- a) Define online banking.
- b) What is QR code payment?
- c) Define Peer-to-Peer (P2P) payment system.
- d) What is Two-Factor Authentication (2FA)?
- e) Define PCI DSS.
- f) What is behavioral analytics?

Q2) Attempt the following:

[10]

- a) Explain types of digital payment systems. **[4]**
- b) Describe benefits and challenges of digital payments. **[4]**
- c) Define cross-border transaction compliance. **[2]**

P.T.O.

Q3) Attempt the following: [10]

- a) Explain behavioral analytics in fraud prevention. [4]
- b) Describe role of digital identity in fraud mitigation. [4]
- c) Define payment fraud detection. [2]

Q4) Attempt the following: [10]

- a) Explain blockchain technology in digital payments. [4]
- b) Describe smart devices and wearable technologies in payments. [4]
- c) Define CBDC. [2]

Q5) Attempt any TWO of the following: [10]

- a) Explain accessibility and inclusion in digital payments. [4]
- b) Describe cross-border payments and global interoperability. [4]
- c) Explain user-centric design in digital payment applications. [2]



Total No. of Questions :5]

SEAT No. :

PE13054

[Total No. of Pages : 2

[6520]-1005

F.Y. M.Sc. (Cyber Security)

MCS-512-MJ: WIRELESS SECURITY

(NEP 2024 Pattern) (Semester-I)

Time : 2 Hours]

[Max. Marks : 35

Instructions to the candidates:

- 1) *Question No. 1 is compulsory.*
- 2) *Solve any Three questions from Q.2 to Q.5.*
- 3) *Question 2 to 5 carry equal marks.*

Q1) Attempt any Five of the following:

[5×1=5]

- a) What is encryption in wireless communication?
- b) Expand WEP.
- c) Define WIDS.
- d) What is jamming attack?
- e) What is secure Wi-Fi connectivity?
- f) Mention any one of the IoT security risk.

Q2) Attempt the following:

[10]

- a) Explain the need for wireless security measures. **[4]**
- b) Describe MAC filtering and access control mechanisms. **[4]**
- c) Write two advantages of BYOD policy implementation. **[2]**

Q3) Attempt the following:

[10]

- a) Explain WPA2 security mechanisms. **[4]**
- b) Discuss wireless honeypots and their use in threat detection. **[4]**
- c) State two steps in periodic Wi-Fi security audits. **[2]**

P.T.O.

Q4) Attempt the following: [10]

- a) Explain the role of wireless security protocols. [4]
- b) Discuss integration of IoT with wireless access control. [4]
- c) Write two benefits of AI-based wireless threat detection. [2]

Q5) Attempt any TWO of the following: [10]

- a) Explain WPA vs WPA2 vs WPA3 evolution and improvements. [5]
- b) Discuss security implications of Wi-Fi 6 and 5G together. [5]
- c) Explain 802.1X enterprise authentication. [5]



Total No. of Questions : 5]

SEAT No. :

PE13055

[Total No. of Pages : 2

[6520]-1006

First Year M.Sc. (Cyber Security)

MCS-514-MJ : IT ACT. 2000 IN CYBER SPACE

(2024 NEP Pattern) (Semester - I)

Time : 2 Hours]

[Max. Marks : 35

Instructions to the candidates:

- 1) *Question No. 1 is compulsory.*
- 2) *Solve any Three questions from Q.2 to Q.5.*
- 3) *Questions 2 to 5 carry equal marks.*

Q1) Attempt any Five of the following.

[5×1=5]

- a) When was the IT Act enacted?
- b) Define electronic contract.
- c) Define intermediary under IT Act.
- d) What is adjudication in cyber law?
- e) What is data breach?
- f) Mention any one contemporary legal challenge in cyber law.

Q2) Attempt the following.

[10]

- a) Explain scope of the IT Act 2000. **[4]**
- b) Describe unauthorized copying and data theft offenses. **[4]**
- c) State any two procedures used in cybercrime investigation. **[2]**

P.T.O.

Q3) Attempt the following. [10]

- a) Explain legality of electronic contracts. [4]
- b) Discuss balancing freedom and regulation for intermediaries. [4]
- c) Mention two requirements of consent and notice in data protection. [2]

Q4) Attempt the following. [10]

- a) Explain objectives of the IT Act. [4]
- b) Discuss functions of cyber appellate mechanisms. [4]
- c) State any two future challenges in cyberspace regulation. [2]

Q5) Attempt any Two of the following. [10]

- a) Explain digital signatures and their legal recognition. [5]
- b) Discuss international cyber law cooperation and challenges. [5]
- c) Discuss landmark judicial precedents in cyber law. [5]



Total No. of Questions : 6]

SEAT No. :

PE13056

[Total No. of Pages : 2

[6520]-1007

First Year M.Sc. (Cyber Security)

MCS -531-RM: RESEARCH METHODOLOGY

(NEP 2024 Pattern) (Semester - I)

Time : 3 Hours]

[Max. Marks : 70

Instructions to the candidates:

- 1) *All questions are compulsory.*
- 2) *Figures to the right indicate full marks.*

Q1) Solve any Six of the following.

[6×2=12]

- a) Define the term 'Research'.
- b) List two primary objectives of conducting research.
- c) What is the main difference between Research Methods and Research Methodology?
- d) Define 'Plagiarism'.
- e) Name two software tools used for identifying predatory publications.
- f) What is the meaning of 'Conflict of Interest' in publication ethics?
- g) Define 'Research Integrity'.

Q2) Attempt any Four of the following.

[4×3=12]

- a) Explain the significance of research in modern society.
- b) Describe three essential characteristics of a good researcher.
- c) Briefly explain the 'Ex Post Facto' research design.
- d) What are the aims of sampling in a research study?
- e) Distinguish between a Research Proposal and a Research Paper.

P.T.O.

Q3) Attempt any Three of the following. [3×4=12]

- a) Explain the necessity of defining a research problem clearly.
- b) Briefly describe 'Action Research' with an example.
- c) What is 'Self-Archiving' in the context of SHERPA/RoMEO?
- d) Explain the role of Google Scholar in literature review.

Q4) Attempt any Three of the following. [3×4=12]

- a) Differentiate between Probability and Non-Probability sampling methods.
- b) Explain the 'Case Study' method of data collection.
- c) Describe the layout of a standard Research Report.
- d) Discuss the ethical guidelines provided by COPE(Committee on Publication Ethics)

Q5) Attempt the following:

a) Attempt any Two of the following. [2×5=10]

- i) Elaborate on the different types of Plagiarism with examples.
- ii) Explain the steps involved in the Research Process.
- iii) Discuss the various of Research Designs (Exploratory, Descriptive and Diagnostic).

b) Attempt any One of the following. [1×2=2]

- i) What is the purpose of an 'Oral Presentation' in research?
- ii) Define 'Simple Regression Analysis'.

Q6) Write a short note. Any two. [2×5=10]

- a) Explain the techniques of data processing (Editing, Coding and Tabulation).
- b) Discuss the importance and sources of Literature Review.
- c) Explain the measures of Central Tendency and their application in research.

