R5934	Sub. Code
	248101

P.G. DIPLOMA EXAMINATION, NOVEMBER – 2021

First Semester

Cyber Security

INTRODUCTION TO COMMUNICATION NETWORKS AND SECURITY

(CBCS – 2020 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 2 = 20)

Answer **all** questions.

1. What is the basic principle of data compression?
2. How does GPS work?
3. Mention the four layers of TCP/IP models.
4. Specify the uses of network storage devices.
5. List the difference between a router and an access point.
6. How is SDN different from a normal network setup?
7. Define network security.
8. What is a disaster in network security?
9. How does SSL work?
10. What is mobile virtualization?

Part B (5 × 5 = 25)

Answer **all** questions, choosing either (a) or (b).

11. (a) List the pros and cons of Fiber optic cable.

Or

(b) How are microwaves used in satellite communication?

12. (a) Compare OSI and TCP reference model.

Or

(b) Explain the basics of network connectivity.

13. (a) What are the problems in wireless networks?

Or

(b) Write a note on Wide Area Networking.

14. (a) How can you minimize security risks on the internet?

Or

(b) Explain the parameters of a valuable network.

15. (a) Differentiate between PaaS, SaaS and IaaS.

Or

(b) What do you understand by an HTTP request and HTTP response?

Part C

(3 × 10 = 30)

Answer any **three** questions.

16. What is wired technology? Explain different types of wired technology

17. Explain the architecture of VOIP with a neat diagram.

18. Explain packet stitching and circuit switching with a neat diagram.

19. Discuss disaster planning and recovery management in network security.

20. Write short notes on the following.
    (a) Ajax
    (b) XML
    (c) JSON
    (d) LAMP

———————

R5935	Sub. Code 248102

P.G. DIPLOMA EXAMINATION, NOVEMBER 2021.

First Semester

Cyber Security

PRINCIPLES OF CYBER FORENSICS

(CBCS – 2020 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 2 = 20)

Answer **all** the questions.

1. Write any two strategies to prevent Cybercrime.

2. Write any two types of Cybercrime.

3. Define Blockchain.

4. What is Dark Web?

5. Define GPS Forensics.

6. What is Memory Forensics?

7. Write any two Forensics tools used for Data Recovery.

8. List any two Forensics tools used presently.

9. What is File System?

10. What is Digital Evidence?

Part B (5 × 5 = 25)

Answer **all** questions, choosing either (a) or (b).

11. (a) Briefly write about the types of Cybercrime.

Or

(b) Write the classification of Cybercriminals?

12. (a) Briefly discuss about Cybercrime against Individuals.

Or

(b) Write short note on Cybererime against Property.

13. (a) Write about (i) Database Forensics

(ii) Disk Forensic

Or

(b) Write about (i) Network Forensic

(ii) Mobile Forensic

14. (a) Briefly write how Forensic tools used for Meta data processing.

Or

(b) What are the Forensic tools used for RAM Analysis?

15. (a) What are the sources to collect Digital Evidence?

Or

(b) Write briefly about challenges with Digital Evidence.

Part C

(3 × 10 = 30)

Answer any **three** questions.

16. Explain various tools used in Cybercrime.

17. Explain detailed about Cyber War..

18. Explain detailed about Wireless Forensics, Database Forensics, and Disk Forensics.

19. What are the needs for computer Forensic Investigators? Discuss.

20. Discuss detailed about Digital evidence and collection procedure.

———————

R5936	Sub. Code 248103

P.G. DIPLOMA EXAMINATION, NOVEMBER – 2021

First Semester

Cyber Security

SECURITY OPERATIONS AND COUNTER MEASURES

(CBCS – 2020 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 2 = 20)

Answer **all** questions.

1. What is meant by 'Computer Hacker'?
2. Write the usage of CertUtil in Windows OS?
3. What is the goal of OSINT?
4. Define Google dork.
5. Differentiate HTTP and HTTPS.
6. What do you mean by Cookies?
7. What is meant by DNS spoofing?
8. Define enumeration.
9. What is the use of backups?
10. List out any four biometric tools.

Part B (5 × 5 = 25)

Answer **all** questions, choosing either (a) or (b).

11. (a) Write short notes on GentooLinux.

Or

(b) How does Kali Linux helpful in the aspect of hacking?

12. (a) Write notes on Maltego.

Or

(b) Elaborate the various features of Shodan.

13. (a) Explain web proxies.

Or

(b) Describe the implications of hacking DNS.

14. (a) Explain defending virus.

Or

(b) Write short notes on banner grabbing.

15. (a) Write a brief note on Kerberos.

Or

(b) Describe the various aspects of change management.

Part C (3 × 10 = 30)

Answer any **three** questions.

16. Explain the various aspects of Python scripting fundamentals.

17. Write detailed notes on DNS Reconnaissance.

18. Discuss the features of Nmap Scripting Engine.

19. Explain OWASP top 10 vulnerabilities.

20. Write a detailed account on identity and access management.

———————

R5937	Sub. Code 248104

P.G. DIPLOMA IN EXAMINATION, NOVEMBER – 2021

First Semester

Cyber Security

RISK MANAGEMENT AND SECURITY AUDITING

(CBCS – 2020 onwards)

Time : Three Hours Maximum : 75 Marks

Part A (10 × 2 = 20)

Answer **all** the questions.

1. Define Job Rotation.
2. What are SLAs?
3. What is the main work product of a Security Assessment?
4. Define Vulnerability Scans.
5. Expand COBIT.
6. What is ITIL framework?
7. What is Document and Technical Review?
8. Define Graybox testing.
9. What is PIDS?
10. Define Unified Communications.

Part B (5 × 5 = 25)

Answer **all** questions, choosing either (a) or (b).

11. (a) Identify the elements of risk with a neat diagram.

Or

(b) Write short note on Risk Responses in detail.

12. (a) What are the components of SCAP? Explain in detail.

Or

(b) Explain Account Management Reviews.

13. (a) What are the various mechanisms used in NIST 800-53A

Or

(b) Explain the various activities supported by NIST 800-53A.

14. (a) Write short note on Security Audit? Explain its types.

Or

(b) What the practices followed in Auditing Security? Explain.

15. (a) Write short note on access control in intrusion detection.

Or

(b) Identify the endpoint protection in infrastructure security.

Part C

(3 × 10 = 30)

Answer any **three** questions.

16. Discuss the need to perform a balanced risk assessment. What are the techniques that can be used and why is this necessary?

17. Explain Code Review and Testing process in detail.

18. Describe the DREAD risk assessment model.

19. Explain the security testing frameworks in detail.

20. Describe the categories of secure remote access.

———————

R5938	Sub. Code
	248501

P.G. DIPLOMA IN CYBER SECURITY EXAMINATION, NOVEMBER – 2021

First Semester

WIRELESS NETWORK FORENSICS

(CBCS – 2020 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 2 = 20)

Answer **all** questions.

1. State the importance of audit logs.
2. What are the types of network attacks?
3. What are the information available in a log file?
4. What are the components in a routing table?
5. How can you collect evidence from the web?
6. What is chain email?
7. What are active and passive wireless attacks?
8. Explain : PDA generic states.
9. What can a criminal do with an iphone?
10. What is jail breaking?

Part B (5 × 5 = 25)

Answer **all** questions, choosing either (a) or (b).

11. (a) Give an account on network forensics.

Or

(b) Explain DNS poisoning techniques.

12. (a) Give an account on the tools used for locating IP addresses.

Or

(b) Explain the tools used in router forensics.

13. (a) Explain the steps for investigating crime over internet and web.

Or

(b) Give an account on email forensic tools.

14. (a) How can one determine wireless fields strength and map wireless zones and hot spots?

Or

(b) Give an account on PDA security issues.

15. (a) How can one acquire device Info and sys Info file from iPod / iPhone?

Or

(b) Give an account on blackberry forensics.

Part C

(3 × 10 = 30)

Answer any **three** questions.

16. Explain the use of various tools for investigating network traffic.

17. Explain the different types of web attacks and the tools used for investigating them.

18. Give a detailed account on web security.

19. Explain recovery with respect to iPod and iPhone forensics.

20. Explain PDA forensics steps and the tools used for them.

———————

R5939	Sub. Code
	248201

P.G. DIPLOMA EXAMINATION, NOVEMBER – 2021

Second Semester

Cyber Security

INFORMATION SECURITY STANDARD, AND CYBER LAWS

(CBCS – 2020 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 2 = 20)

Answer **all** questions.

1. Distinguish between threats and attacks.

2. What is the difference between law and ethics?

3. What is security standard?

4. What do you mean by Information System? What is the need of Information System?

5. What is Cyber Security and How it is different from Information Security?

6. Describe security risk and analysis?

7. Write a short note on (a) Credit/Debit Cash (b) Digital Signature (c) E-Cash

8. Elaborate the term access control?

9. What do you mean by policy? why it is developed and reviewed?

10. Write a short note on (a) Patent Law (b) Copy write Law (c) IPR.

Part B $(5 \times 5 = 25)$

Answer **all** questions, choosing either (a) or (b).

11. (a) How can be Intrusion Detection system is the backbone of Information. system? Justify along with its categories?

Or

(b) Define Vendor challenges and user challenges for application security?

12. (a) Describe Risk management. List the components of risk management.

Or

(b) List various risk models. Explain.

13. (a) Discuss about Protect Card holder Data.

Or

(b) What are vulnerabilities? List any two vulnerabilities.

14. (a) Distinguish between direct attacks and indirect attacks on a computer network.

Or

(b) What are the issues and problems in modern era that leads to implement cyber laws?

15. (a) How will you verify electronic signatures in India.

Or

(b) Narrate the attributes of Data messages.

Part C ($3 \times 10 = 30$)

Answer any **three** questions.

16. Explain about the security controls in an information management system

17. Explain about ISO/IEC 38500 in detail

18. How will you implement strong access control measures?

19. Explain about symmetric encryption and how it differs from asymmetric encryption systems

20. Explain in detail about Data messages.

———————