GOVERNMENT POLLYTECHNIC, NAYAGARH

PREPARED BY :- TANMAY NATH MISHRA

SUB :- INTRODUCTION TO INFORMATION SECURITY

UNIT–1 : INTRODUCTION TO INFORMATION SECURITY

1. 2 MARKS QUESTIONS

a. What is Information Security?
b. Define CIA Triad.
c. What is confidentiality?
d. What is integrity in information security?
e. What is availability?
f. Define authentication.
g. What is authorization?
h. What is malware?
i. What is a firewall?
j. Define cyber attack.

---

2. 5 MARKS QUESTIONS

a. Explain the CIA Triad with diagram.
b. What are the basic principles of information security?
c. Explain types of security threats.
d. Differentiate between authentication and authorization.
e. Explain malware and its types.
f. What is a firewall? Explain its working.
g. Explain need of information security.

---

3. 10 MARKS QUESTIONS

a. Explain Information Security in detail and its importance.
b. Describe CIA Triad with real life examples.
c. Explain different types of cyber attacks.
d. Explain security goals and challenges in information security.
e. Discuss threats, vulnerabilities and risks.

UNIT–2 : CRYPTOGRAPHY

1. 2 MARKS QUESTIONS

a. What is cryptography?
b. Define encryption.
c. Define decryption.
d. What is plaintext?
e. What is ciphertext?
f. What is a key in cryptography?
g. What is symmetric key encryption?
h. What is asymmetric key encryption?
i. What is hashing?
j. Define digital signature.

---

2. 5 MARKS QUESTIONS

a. Explain encryption and decryption process.
b. Differentiate between symmetric and asymmetric encryption.
c. Explain Caesar cipher.
d. What is hashing? Explain with example.
e. Explain digital signature.
f. What is public key infrastructure (PKI)?

---

3. 10 MARKS QUESTIONS

a. Explain cryptography and its types in detail.
b. Explain symmetric and asymmetric encryption with examples.
c. Describe working of digital signature.
d. Explain hash functions and their applications.
e. Discuss role of cryptography in information security.

UNIT–3 : NETWORK SECURITY

1. 2 MARKS QUESTIONS

a. What is network security?
b. What is phishing?
c. Define DoS attack.
d. What is intrusion detection system (IDS)?
e. What is VPN?
f. Define spyware.

g. What is a Trojan horse?
h. What is packet sniffing?
i. Define port scanning.
j. What is social engineering?

2. 5 MARKS QUESTIONS

a. Explain phishing attack.
b. What is IDS and IPS?
c. Explain DoS and DDoS attacks.
d. What is VPN? Explain its working.
e. Explain social engineering techniques.

3. 10 MARKS QUESTIONS

a. Explain network security and its importance.
b. Describe different types of network attacks.
c. Explain firewalls and IDS in detail.
d. Explain phishing, spoofing and sniffing.
e. Discuss security mechanisms for network protection.

UNIT–IV: Security in Operating Systems

(Authentication, access control, file security, patching)

1766493227694a8c2bb636e4th Sem …

2 Marks

1. What is authentication?
2. What is access control?
3. What is biometric authentication?
4. What is patch management?
5. What is security auditing?

5 Marks

1. Explain user authentication methods.
2. What is access control mechanism?
3. Explain OS security hardening.
4. What is patch management?

10 Marks

1. Explain operating system security in detail.
2. Describe authentication and access control.
3. Discuss file system security and encryption.
4. Explain security auditing and monitoring.

UNIT–V: Web Security

(SQL Injection, XSS, CSRF, WAF, OWASP)

1766493227694a8c2bb636e4th Sem …

2 Marks

1. What is SQL injection?
2. What is XSS?
3. What is CSRF?
4. What is WAF?
5. What is OWASP?

5 Marks

1. Explain SQL injection with example.
2. What is XSS and its types?
3. Explain secure HTTP headers.
4. What is penetration testing?

10 Marks

1. Explain common web security threats.
2. Describe secure web application practices.
3. Explain SQL injection, XSS and CSRF.
4. Discuss role of WAF and OWASP.

UNIT–VI: Security Policies & Incident Response

(BCP, DRP, forensics, legal & ethics)

1766493227694a8c2bb636e4th Sem …

2 Marks

1. What is incident response?
2. What is BCP?
3. What is DRP?
4. What is digital forensics?
5. What is evidence gathering?

5 Marks

1. Explain incident response lifecycle.
2. What is BCP and DRP?
3. Explain digital forensics.
4. Write note on legal issues in cyber security.

10 Marks

1. Explain security policies and their importance.
2. Describe incident response process in detail.
3. Discuss business continuity and disaster recovery.
4. Explain legal and ethical issues in information security.