



K.R. MANGALAM UNIVERSITY

THE COMPLETE WORLD OF EDUCATION

Rollno.....

End Semester Examination, December 2024
B.Tech. Cyber Security – 1st Semester
Essentials of Cyber Security (SEC068)

Time: 2.5 hrs.

Max Marks: **50**

Note: ***All Questions are compulsory. Marks are indicated against each question.***

PART-A

Q.1 *Attempt any five questions:*

(a) What is the difference between a firewall and an intrusion detection system (IDS)?

[CO-1] [L-2] **2**

(b) Multiple Choice Questions:

i. Which encryption algorithm is widely used for secure communication?

a) RSA b) MD5 c) SHA-256 d) DES

ii. What is the primary goal of a denial-of-service (DoS) attack?

a) To steal sensitive information b) To disrupt network or system availability c) To gain unauthorized access to a system d) To spread malware

[CO-1] [L-2] **2**

(c) Fill in the Blanks:

i. _____ is a security practice that involves regularly updating software and systems.

ii. _____ is a security incident that involves unauthorized access to a system or network.

[CO-1] [L-2] **2**

(d) One Word Answer Questions:

i. A security measure that protects data from unauthorized access, use, disclosure, disruption, modification, or destruction.

ii. A security principle that ensures data is accessible to authorized users when needed.

(e) Explain the concept of zero-day vulnerabilities and how they can be exploited.

(f) True/False Questions:

- i. A honeypot is a decoy system set up to attract and trap attackers.
- ii. Biometric authentication, such as fingerprint or facial recognition, is a strong form of authentication.

(g) Explain the concept of two-factor authentication (2FA). How does it enhance security?

2x5

PART-B

Q.2 Discuss the different types of cybersecurity threats and vulnerabilities that organizations face in the modern digital landscape. In your response, highlight at least four major categories of threats, providing real-world examples.

[CO-2] [L-3] **10**

OR

Analyze the Cosmos Bank cyber-attack, discussing the following points:

- i. Attack methodology
- ii. Impact
- iii. Vulnerabilities exploited
- iv. Preventive measures
- v. Lessons learned

[CO-2] [L-3] **10**

Q.3 As a cybersecurity analyst tasked with investigating a suspected breach on a Linux server, you are required to perform the following tasks using the server's terminal:

- i. Navigate to the /var/log directory, as it is suspected to contain hidden malicious files. Use the correct command to change your current directory.
- ii. Create a subdirectory called investigation within the /var/log directory for storing relevant findings.
- iii. Copy the hidden_script.sh file into the newly created investigation folder.

[CO-2] [L-3] **10**

OR

You are working as a system administrator and have been assigned to secure a Linux server. To achieve this, perform the following tasks and answer the related questions:

- i. You need to change the ownership of a sensitive file named confidential.txt to a different user. What command will you use?
- ii. The file secure_script.sh must have its permissions modified so that only the owner has read, write, and execute access. Which command should be used?
- iii. Verify and display the current permissions of all files in the /home/admin directory. What command will you execute?
- iv. A file named shared_data.log should be updated so that the group has no access rights. Which command will accomplish this?
- v. Apply recursive changes to modify permissions for all files and directories within /project to grant read and write permissions only to the owner. What command will you use?

[CO-3] [L-4] **10**

Q.4 Discuss the following network protocols and describe at least one common vulnerability associated with each. Explain how these vulnerabilities can be exploited and suggest a mitigation strategy for each.

- i. FTP
- ii. DNS

[CO-3] [L-3] **10**

OR

As technology advances, so do cyber threats. What innovative strategies can be employed to combat the ever-evolving landscape of phishing, ransomware, and DDoS attacks?

[CO- 4] [L-3] **10**

Q.5 How can developers protect web applications from security breaches? Discuss the risks posed by SQL injection and XSS attacks.

[CO-5] [L-4] **10**

OR

Cybersecurity is a major concern in today's digital age. Password cracking techniques are commonly used by malicious actors to gain unauthorized access to systems.

- i. Explain the concept of password hashing and its role in enhancing password security.
- ii. Discuss the following password cracking techniques:

[CO- 5] [L-4] **10**