C1002

Total Pages : 4 Roll No. .....

MIT (CS)-203/PGDCS-07

Advanced Cyber Security Techniques

(MSCCS-18/PGDCS-17)

2nd Semester Examination, 2022 (June)

Time : 2 Hours] **Max. Marks : 80**

Note : This paper is of Eighty (80) marks divided into two (02) Sections A and B. Attempt the questions contained in these sections according to the detailed instructions given therein.

SECTION–A
(Long Answer Type Questions)

Note : Section 'A' contains Five (05) long answer type questions of Twenty (20) marks each. Learners are required to answer any Two (02) questions only. (2×20=40)

1. Answer the following :

(a) What is a difference between network based and host-based intrusion detection and prevention system? (5)

(b) Discuss the various placement of intrusion detection and prevention system in a network. (5)

(c) What do you understand by log management, how it is different from security information and event management? (5)

(d) What is a signature-based detection, how it is different from anomaly detection? (5)

2. Answer the following :

(a) Explain importance of data backup. (5)

(b) Write note on Uninterruptable and backup power supplies. (5)

(c) What is data center security? (5)

(d) Explain different Tiers of datacentes. (5)

3. Answer the following :

(a) Explain Dan Kaminsky's DNS cache poisoning. (5)

(b) Explain concept of DNS and common threats to DNS server. (5)

(c) Explain threats to email servers and countermeasures. (5)

(d) Write note on security threats to database servers. (5)

4. Answer the following :

(a) Write note on malware scanning and content filtering with respect to email server. (10)

(b) Discuss Blacklisting and Whitelisting approach of input validation. (10)

5. Answer the following :

(a) What is XSS vulnerability and how it could be exploited by the attacker. (7)

(b) What is sandboxie? How can you safely run a browser with sandboxie? (7)

(c) Explain principle of least privilege. (6)

SECTION–B

(Short Answer Type Questions)

Note : Section 'B' contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any Four (04) questions only. (4×10=40)

1. Answer the following :

(a) Discuss Current threat landscape. (5)

(b) Discuss possible attacks on Internet trust infrastructure. (5)

2. Write a note on Network Device Resiliency and Survivability.

3. Answer the following :

(a) Describe the phrase "security with in SDLC". (5)

(b) Write a short note on CSRF. (5)

4. Answer the following :

(a) What is a spear phishing attack? (5)

(b) Write a note on Operation Aurora Attack. (5)

5. Answer the following :

(a) Write note on DoS/DDoS attack. (5)

(b) Explain end-point security. (5)

6. Answer the following :

(a) Discuss threats to ICT from manmade or natural disasters. (5)

(b) Explain importance of ICT equipment disposal policy. (5)

7. Answer the following :

(a) Write note on malware scanning and content filtering with respect to email server. (5)

(b) What is XSS vulnerability and how it could be exploited by the attacker. (5)

8. Answer the following :

(a) Discuss Blacklisting and Whitelisting approach of input validation. (5)

(b) Explain Microsoft Baseline Security Analyser. (5)