826

Total pages : 04 Roll No. .....

MIT (CS)-203/PGDCS-07

Advanced Cyber Security Techniques

(MSCCS-18/PGDCS-17)

Examination 2021 (Winter)

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 x 20=40)

Q.1. Answer the following :

a. Write a short note network security.(5 marks)

b. Discuss emerging threats to Cloud computing and Internet of Things.? (5 marks)

c. Discuss five common attacks possible on computer networks with example? (5 marks)

d. What is MTM attack, discuss impact of MITM. (5 marks)

P.T.O.

Q.2 Answer the following :

a. What do you mean by infrastructure security? (5 marks)

b. Why Maintenance, Monitoring and Analysis of Complete Audit Logs is critical control? (5 marks)

c. Discuss importance of Penetration Tests and Red Team Exercises. (5 marks)

d. Discuss any 4 critical security control in detail. (5 marks)

Q.3 Answer the following :

a. What are the best practices to log management. (6 marks)

b. What are the event log entries that indicate loggin through different ways(remote, interactive, non-interactive, local)on windows server platforms? (7 marks)

c. List out Advantages of full disk encryption. (7 marks)

Q.4 Answer the following :

a. Proper error handling is important in web application. Discuss. (5 marks)

b. What is SRP? HOW CAN it prevent a malware running from %appdata% directory? (5 marks)

c. What are MACRO's in the context of office applications. What are the threats they pose? (5 marks)

d. What can be done to restrict physical access to authorized wireless devices? (5 marks)

Q.5 Answer the following :

a. What is fuzzy hashing? HOW SSDEEP being advantageous over md5hash sum? (10 marks)

b. What are honeypots? Compare the various technologies in practice? (10 marks)

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 x 10=40)

Q.1 What is a firewall? discuss different type of firewall filtering.

Q.2 Answer the following :

a. Write note on TIA-942 standard. (5 marks)

b. Write note on environmental risk assessment. (5 marks)

Q.3 Answer the following :

a. What is Defense in Depth approach. (5 marks)

b. What is DNS cache poisoning. (5 marks)

Q.4 Answer the following :

a. Discuss SQL injection attack with example. (5 marks)

b. Security is a continuous process. explain. (5 marks)

P.T.O.

Q.5 Answer the following :

a. List out some of the advantage of wireless LAN over Wired networks? (5 marks)

b. List out WPA attacks and the impacts? (5 marks)

Q.6 Answer the following :

a. How waterholing attack is considered a well known method to perform APT? (5 marks)

b. Discuss SYN flooding and UDP flooding. (5 marks)

Q.7 Answer the following :

a. Explain Microsoft Baseline Security Analyser. (5 marks)

b. What are the best WLAN security practices to follow as a home user? (5 marks)

Q.8 Answer the following :

a. What is the role of Remote Access Trojan in APT? (5 marks)

b. Explain threats to email servers and countermeasures. (5 marks)

****