Master of Computer Applications
MCAE501: Cyber Security
UPC-223402501
Semester-V
OBE Examination,Nov./Dec.-2021
Year of Admission: 2019

Time-Three hours   **Max. Marks: 70**

Note: Answer any four questions. All questions carry equal marks.

Q1.	a) Why computer crime is considered as a separate category of crime? Is computer crime hard to prosecute? Justify your answer. Highlight few of the laws defining certain aspects of crime against or using computers.
	b) How would you compare modern cyber-attacks from traditional external attacks? What methods does a social engineering hacker use to gain information about a user's login ID and password? How would this method differ if it targeted an administrator's assistant versus a data entry clerk?
Q2.	a) Suppose you accidentally find someone's password and use it to get into a system. Is this hacking? Justify your answer.
	b) Someone sends you a "game". When you run it, it logs you into an IRS server. Is this hacking? Justify your answer.
	c) How does screened host architectures for firewall differ from screened subnet firewall architectures? Which one of the above offer more security for the information assets that remain on the trusted network?
Q3.	What is the difference between penetration testing and vulnerability assessment? Is penetration testing still important if the company has a firewall? Who needs penetration testing and why do they need it? What are the legal steps involved in penetration testing? Also list out some hurdles faced during penetration testing.
Q4.	Write a short note for each of the following and also mention how these are related to cyber security: • SCADA • PLC • RTUs • MTUs • HMI
Q5.	a) Which approach of malware analysis is based on software engineering technique? How is it different from other approaches of malware analysis? What are the advantages and disadvantages of various approaches of malware analysis?
	b) Are there any indicators that file is packed or obfuscated? If yes, list and describe these indicators? What host or network based indicators could be used to identify the malware on infected machines?

Q6.	a)	Some sites (e.g. Yahoo) ask the user to view an image containing some text and enter the characters seen there on the screen as an added level of authentication. What is the reason for this and how does it work? What is it called? Compare this method with 2-way authentication method of security measures.
	b)	Why the combination of SCADA and IoT sometimes is referred to as Industry 4.0? Explain the different approaches of security measures in SCADA?

.

.