Name:

Enrolment No:

UPES

UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2020

Course: IT Network Security **Semester: VII**
Program: B. Tech (CSE + CSF) **Time : 03 hrs.**
Course Code: CSF4001 **Max. Marks: 100**

SECTION A

1. Each Question will carry 5 marks, there are six questions in this section.
2. Instruction: Complete the statement / Select the correct answer(s).

S. No.		Marks	CO
Q 1	OSINT collection frameworks are used to effectively manage sources of collected information. Which of the following best describes open-source intelligence? a.) Company documentation labeled "Confidential" on an internal company storage share requiring authentication. b.) Press release drafts found on an undocumented web page inside a company's intranet. c.) Any information or data obtained via publicly available sources that is used to aid or drive decision-making processes. d.) Information gained by source code analysis of free and open-source software (FOSS).	**5**	**CO2**
Q 2	A user reports that he cannot gain access to a shared folder. You investigate and find the following information: • Neither the user nor any groups the user is a member of have been granted permissions to the folder • Other users and groups have been granted permissions to the folder, • Another IT person on your team reports that he updated the permissions on the folder recently. Based on the information in this scenario, which type of access control is in use? a.) RBAC b.) Rule-based Access Control c.) MAC d.) DAC	**5**	**CO3**
Q 3	Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to	**5**	**CO2**

	attract attackers. Which of the following techniques should the systems administrator implement? a.) Role-based Access Control b.) Honeypot c.) Rule-based Access Control d.) Password Cracker		
Q 4	Assume you've managed to dump the password hashes of an account database. Which of the following if true, would render rainbow tables ineffective at cracking at least one. a.) Large salt value was added to the password inputs before being hashed b.) Database includes thousands of unique password hashes c.) Passwords were hashed with MD5 Algorithm d.) Passwords were hashed with SHA-1 Algorithm	**5**	**CO3**
Q 5	Your company is rapidly expanding its public cloud footprint, especially with Infrastructure as a Service (IaaS), and wants to update its authentication solution to enable users to be authenticated to services in the cloud that are yet to be specified. The company issues the following requirements: • Minimize the infrastructure required for the authentication • Rapidly deploy the solution • Minimize the overhead of managing the solution. You need to choose the authentication solution for the company. Which solution should you choose? a.) Federated identity solution b.) Cloud-based identity service c.) Multi-factor authentication solution d.) Third-party identity service	**5**	**CO4**
Q 6	You are conducting an analysis of a compromised computer. You figure out that the computer had all known security patches applied prior to the computer being compromised. Which of the following statement is true about this incident? a.) The computer seems to have configuration management agent issues b.) The computer has configuration management policy mismatch c.) The system was compromised by a Zero-Day Exploit d.) The computer does not have anti-malware enabled.	**5**	**CO4**
SECTION B **1. Each question will carry 10 marks, there are five questions in this section.** **2. Instruction: Write short / brief specific notes.**			
Q 7	Explain Firewall Rules, Firewall types and Firewall technologies with diagrams.	**10**	**CO2**

Q 8	Mention at least five types of IDS Alerts. What is the difference between False Positive and True Negative alerts? Give one example.	**10**	**CO3**
Q 9	Describe TCP/IP and OSI models with examples and diagrams.	**10**	**CO1**
Q 10	Explain with diagram the functions of the protocols used in each layer of OSI model.	**10**	**CO1**
Q 11	What is Risk? Describe the Levels, Phases, Matrix involved in Risk Management. OR Describe the OSI reference model and illustrate their functions with examples.	**10**	**CO4**

SECTION-C

1. Each Question carries 20 Marks.

2. Instruction: Write long answer with diagram wherever required.

Q 12	What do you understand by Incident Handling and Response? Describe the Roles & Responsibilities of Incident Response teams involved in mitigating an incident. OR Describe Penetration Testing Methodology in detail. Mention at least five tools you would use for conducting a Pen Test on Web and Mobile Applications.	**20**	**CO5**