Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May2020

Course: Cyber Forensic **Semester: VIII**
Program: B.Tech CSE (CCVT+Mainframe+OSS+TI+BAO+BFSI) **Time : 03 hrs.**
Course Code: LLBL704 **Max. Marks: 100**

Instructions: Attempt all Sections

SECTION A

Attempt all questions. Each question carries 2 marks **[60 marks]**

S.No.		Marks	CO
Q1	Key logger is a _____ a. Firmware b. Antivirus c. Spyware d. All of the above	2	CO1
Q2	To protect yourself from computer hacker, you should turn on a _____. a. Script b. Firewall c. VLC d. Antivirus	2	CO1
Q3	What is the default port number for most web servers? a. 20 b. 27 c. 80 d. 87	2	CO2
Q4	What is the maximum character Linux supports in its filenames? a. 8 b. 128 c. 256 d. Unlimited	2	CO2
Q5	A DNS translates a domain name into what? a. Binary b. HEX c. IP d. URL	2	CO3
Q6	In OSI model, the dialogue control and token management are responsibility of _____. a. Session Layer b. Network Layer c. Transport Layer d. Data Link Layer	2	CO2
Q7	The main purpose of data protection act is to _____. a. protect privacy b. prevent virus c. increase security d. reduce failure	2	CO3
Q8	Why would a hacker use a proxy server? a. for stronger connection b. for ghost server c. for remote access d. for hiding malicious activity	2	CO1
Q9	What type of symmetric key algorithm using a streaming cipher to encrypt information? a. RC4 b. Blowfish c. SHA d. MD5	2	CO1
Q10	Which of the following is not a factor in securing the environment against an attack on security? a. education of attacker b. system configuration c. network architecture d. business strategy	2	CO1
Q11	What type of attack uses a fraudulent server with a relay address? a. NTLM b. MITM c. NetBIOS d. SMB	2	CO2
Q12	To hide information inside a picture, what technology is used? a. Rootkits b. Bitmapping c. Steganography d. Image Rendering	2	CO3
Q13	Which phase of hacking performs actual attack on a network or system? a. Reconnaissance b. Maintaining Access c. Scanning d. Gaining Access	2	CO3
Q14	Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking. a. Local Networking b. Social engineering c. Physical Entry d. Remote Networking	2	CO4
Q15	What is the purpose of a Denial of Service attack? a. Exploit weakness in TCP/IP stack b. Execute Trojan c. Overload a System d. Shutdown a system	2	CO4
Q16	What are some of the most common vulnerabilities that exist in a network or system?	2	CO4

	a. Newly installed application b. Commercial software packages c. Open source application d. Security Policies		
Q17	What is the sequence of a TCP connection? a. SYN-ACK-FIN b. SYN-SYN-ACK-ACK c. SYN-ACK d. SYN-ACK-ACK	**2**	**CO5**
Q18	Why would a ping sweep be used? a. identify live system b. locate live system c. identify open ports d. locate firewalls	**2**	**CO5**
Q19	Performing hacking activities with the intent on gaining visibility for a social/political situation is called _____. a. cracking b. analysis c. hacktivism d. exploitation	**2**	**CO5**
Q20	What is the most important activity in system hacking? a. information gathering b. cracking passwords c. escalating privileges d. covering tracks	**2**	**CO4**
Q21	Sniffing is used to perform _____ fingerprinting. a. passive stack b. active stack c. scanned d. passive banner grabbing	**2**	**CO5**
Q22	Phishing is a form of _____. a. spamming b. identity theft c. impersonation d. scanning	**2**	**CO5**
Q23	The DSS Signature Uses Which Hash Algorithm? a. MD5 b. SHA2 c.SHA1 d. does not use hash	**2**	**CO1**
Q24	Which Of The Following Is A Class Of Computer Threat? a. DoS attack b. Phishing c. Stalking d. Soliciting	**2**	**CO2**
Q25	_____ social engineering refers to person-to-person interaction to get the required/desired information. a. Human Based b. Computer Based c. Cyber Stalking d. Botnet	**2**	**CO2**
Q26	_____ is a popular IP address and port scanner. a. Cain and Abel b. Snort c. Angry IP Scanner d. Ettercap	**2**	**CO3**
Q27	Which of the following is independent malicious program that needs no host program? a. trap doors b. Trojan horse c. virus d. worm	**2**	**CO4**
Q28	Unsolicited commercial email is known as _____. a. Spam b. Malware c. Virus d. Spyware	**2**	**CO3**
Q29	Unauthorized access in a network _____ issue. a. Performance b. Reliability c. Security d. None of the above	**2**	**CO2**
Q30	What security tradeoff occurs while using Intrusion detection system? a. Change in permission b. login failure c. change in privilege d. performance degradation	**2**	**CO4**
	SECTION B **Attempt all questions. Each question carries 10 marks** **[40 marks]**		
Q31	Discuss the Digital Forensic life cycle phases.	**10**	**CO1, CO3**
Q32	Elaborate on the relevance of OSI model to Computer Forensics.	**10**	**CO2, CO4**
Q33	Describe the key provisions made under the Indian ITA 2000. **OR** What is Cyber Forensic Investigation? Differentiate between auditing and Cyber Forensic Investigation with respect to following elements: Definition, Objectives, Scope and Methodology.	**10**	**CO4**
Q34	Discuss about techniques for obtaining password for the purpose of accessing a system. Explain them **OR** Explain the various challenges to Indian Law and Cyber Crime Scenario in India	**10**	**CO5**