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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2019

Course: Cyber Forensics	**Semester: VIII**
Program: B.Tech. CS-OSS, CS-BAO	**Time 03 hrs.**
Course Code: LLBL704	**Max. Marks: 100**
Instructions: **All sections are compulsory**	**Nos. of page(s) : 2**

SECTION A

S. No.	Write short notes on the following	**Marks**	**CO**
Q 1	How is memory data collected and analyzed	**4**	**CO1**
Q 2	Identify the different types of Steganography	**4**	**CO2**
Q 3	Explain cookie poisoning	**4**	**CO3**
Q 4	Differentiate between Phishing and Pooling concepts	**4**	**CO2**
Q 5	Explain ADS	**4**	**CO3**

SECTION B

	All questions are compulsory	**Marks**	**CO**
Q 6	Explain the process of data recovery in detail	**10**	**CO3**
Q 7	Identify and explain in detail Steganography Hierarchy	**10**	**CO1, CO2**
Q 8	Describe the definition of Cyber Crime in IT Act.	**10**	**CO4**
Q 9	Identify and describe the process of acquisition of evidence **OR** Explain the process of RAID Acquisition	**10**	**CO3**

SECTION-C

	Case Study: Read the following scenario properly and answer Q10 & Q11	**Marks**	**CO**
	Org 6, globally recognized for innovative research, was informed that suspect traffic had been observed communicating with a known command and control node IP address in September 2013. An investigation into the incident found that in May 2013, a user had conducted a Google search for an updated driver for a specialist piece of software that facilitated console access to devices used in industrial control systems (ICS). The vendor name, type and the keyword ‘driver’, was specified as part of the search query. Given the uniqueness of the requested query, the legitimate vendor’s website was returned and subsequently the link clicked on, to visit the website. The user proceeded to download the required driver, which was delivered as a zip file. Extraction of this file presented a setup executable, which launched a malicious		

	DLL, and wrote multiple DLLs to the users roaming profile, at which point the user’s host became compromised with a remote access trojan (RAT). Once a user’s roaming profile has been infected any subsequent machines logged into are at risk of also becoming infected. Analysis of the malware found on the user’s host was undertaken to determine its capabilities and to extract any further information that could be used to identify STAGES OF ATTACK other compromised machines. The malware was created in March 2013 and was capable of validating its persistence, checking for, and injecting further malicious code into web browsers on the machine. Additionally, several new command and control servers were also identified through this process. Lack of reliable logging meant that it was not possible to determine the impact and whether the attacker had been able to acquire data from other systems on the network. If successful, attacks of this nature that take advantage of trusted relationships, such as vendor and consumer, can promptly and efficiently compromise large portions of a particularly niche industry. Specific Failures Leading to Compromise • Insufficient Internal Segregation Between Hosts • Machines used for ICS also used for day-to-day business • Lack of logging, either centrally or on individual hosts		
Q 10	Compare the different other technologies which could have been used to protect against these types of attacks.	**20**	**CO4, CO5**
Q 11	Critically analyze the precautionary technologies in the above scenario. OR Design a fully secure architecture to prevent such attacks.	**20**	**CO4, CO5**

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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: Cyber Forensics **Semester: VIII**
Program: B.Tech. CS-OSS, CS-BAO **Time 03 hrs.**
Course Code: LLBL704 **Max. Marks: 100**
Instructions: **All sections are compulsory** **Nos. of page(s) : 2**

SECTION A

S. No.	Write short notes on the following	**Marks**	**CO**
Q 1	Explain Cookie Storage and analysis	**4**	**CO1**
Q 2	Categorize the different steps of email forensics	**4**	**CO2**
Q 3	Identify the types of Steganography	**4**	**CO3**
Q 4	Differentiate between DOS & DDOS attacks	**4**	**CO2**
Q 5	Elucidate authentication of evidence	**4**	**CO3**

SECTION B

	All questions are compulsory	**Marks**	**CO**
Q 6	Distinguish the different methods of data hiding	**10**	**CO3**
Q 7	Clarify how data is extracted from volatile memory	**10**	**CO1, CO2**
Q 8	Distinguish and explain the IT Act definition of cyber crime	**10**	**CO4**
Q 9	Characterize and describe the Malware analysis techniques **OR** Explicate the process of physical and process memory dumps for malware	**10**	**CO3**

SECTION-C

	Case Study: Read the following scenario properly and answer Q10 & Q11	**Marks**	**CO**
	Org 4 is a mid-sized industrial products distributor with a number of small offices across the UK. In order to keep its telephone operating costs down, Org 4 adopted VoIP (Voice over IP) technology based on session initiation protocol (SIP). This allowed Org4 to roll out IP phones so that all of its staff could call each other at their many distributed offices without any call charges. It also allowed Org 4 to enter arrangements for routing its calls to the outside world. However, one month the bill for external connections was over £15,000, 30 times greater than normal. After a number of possibilities were ruled out, Org4 suspected that a security incident had occurred and commenced an investigation. SIP addresses work much like email addresses and SIP addresses for Org 4 looked like the following: sip:JoeBlow@Org 4.com.		

	When routing a call to the outside world, the system is configured to recognize the non-SIP traditional numbers and route the call through to their outbound telephone services provider. Telephone and data traffic traverse the same infrastructure, however org4 strictly segregated VoIP and corporate network traffic by virtual LANs (VLANS). However, investigation of logs showed that attackers had been abusing the system to identify Org4's SIP server and then enumerate STAGES OF ATTACK extensions. The attackers had realized that Org4 had mistakenly set up their service to allow SIP connections from unknown IP addresses to be forward through their external telephone services provider. The attackers had abused this configuration error to make calls to premium rate numbers that they controlled at a cost to Org4. The attackers had then gone on to attack the SIP infrastructure and, through exploiting weak credentials, been able to gain access and monitor calls made by Org4's employees. The investigation found that the attackers were trying to gain access to the corporate network but were unsuccessful before their access could be terminated. Specific Failures Leading to Compromise: • Misconfiguration of a network service • Weak credentials		
Q 10	Compare the different other technologies which could have been used to protect against these types of attacks.	**20**	**CO4, CO5**
Q 11	Critically analyze the precautionary technologies in the above scenario. OR Design a fully secure architecture to prevent such attacks.	**20**	**CO4, CO5**