Reg.No: | | | | | | | | |

SNS College of Technology, Coimbatore-35.
(Autonomous)
B.E/B.Tech- Internal Assessment -III
Academic Year 2023-2024(ODD)
Fifth Semester
Computer Science and Engineering

A

19CSE304 - Cyber Security

Time: 1.5 Hours **Maximum Marks: 50**

Answer All Questions

	PART - A (5x 2 = 10 Marks)	**CO**	**Blooms**
1.	Outline the concept of Honeypots . A honeypot is a security mechanism that creates a virtual trap to lure attackers.	CO4	Und
2.	Distinguish between passive and active analysis of malicious code. There are two main techniques to analyze the behavior of malicious code: 1. Passive analysis: Record the state of the system before and after the infection. Then, compare these states to determine what changed 2. Active analysis: Actively monitor and record malicious code actions during execution.	CO4	Ana
3.	Recall the concept of Intrusion Detection System. An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.	CO4	Und

4.	List few web threats for organizations.		CO5	Und

Industrial espionage
IP-based blocking
IP-based cloaking
Cyber terrorism
Confidential information leakage

5.	Spell few security risks of social computing.		CO5	Ana

Usersphere
Recipientsphere
Jointsphere

PART–B (13+13+14 = 40 Marks)

6.	(a)	Elaborate in detail about the Memory Forensics.	13	CO4	Und

Memory forensics refers to finding and extracting forensic artifacts from a computer's physical memory. This section explains the importance and capabilities of memory forensics and the tools used to support incident response and malware analysis.

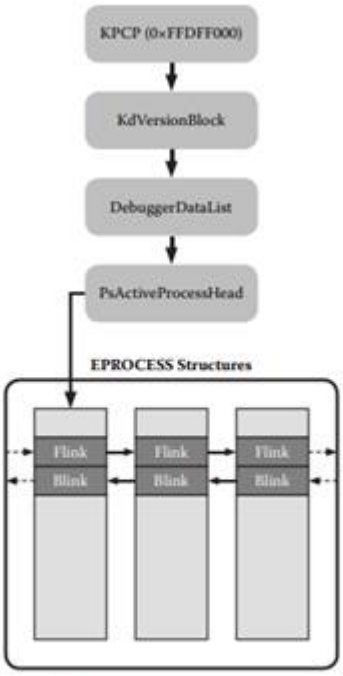


Exhibit 5-1 The path used by Volatility to locate the EPROCESS object list.

Capabilities of Memory Forensics
Memory Analysis Frameworks
Dumping Physical Memory
Finding Hidden Processes
Volatility Analyst Pack

(or)

(b) Examine the usage and application of honeypots and discuss the organization structure of honeypots and discuss the working of Honeypots in computer. 13 CO4 Ana

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource

Honeypots fit into two different classifications based on the level of system interaction available to the attacker. **Low-interaction honeypots** emulate vulnerable services and applications to entice inbound exploit attempts from attackers. Emulation occurs by mimicking real network responses to inbound connections allowing an attack to progress to completion. The attacks do not compromise the honeypot because the honeypot itself is not vulnerable; rather, it follows along by emulating vulnerabilities. Logs of the activity capture the exploit attempt, and postattack analysis provides information to protect other production devices from falling victim to the attack. The second type of honeypots, known as **high-interaction honeypots**, utilize actual services and vulnerabilities to attract inbound attacks. The use of real services provides detailed information on the steps involved in exploitation and the postcompromise activity. This type of honeypot requires close and constant observation because the system is likely to fall victim to compromise. High-interaction honeypots also need extra security measures to contain subsequent attacks or malicious code propagation.

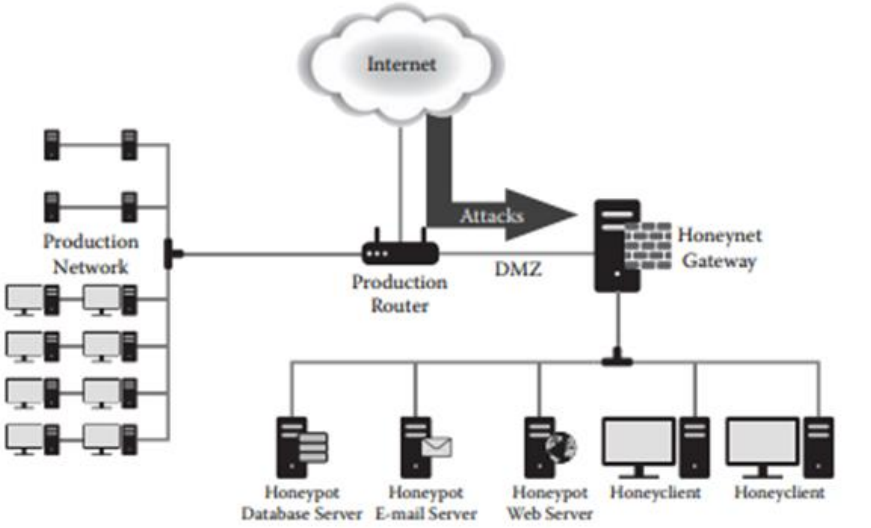
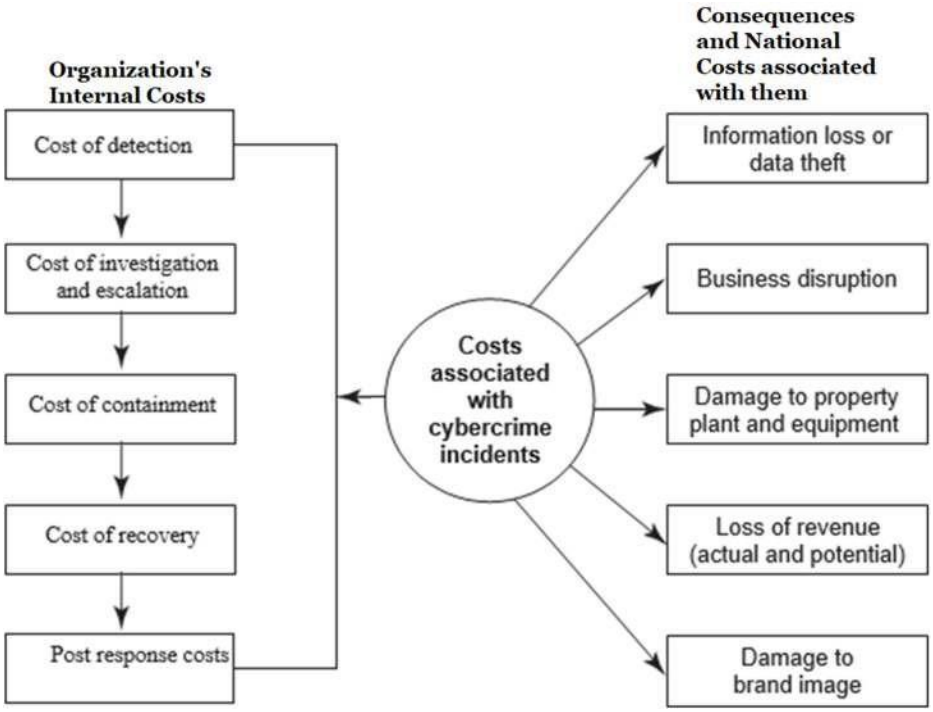


Exhibit 5-3 A honeynet infrastructure.

7. (a) Discus in detail about the cost of cybercrimes and IPR issues related to the organization. 13 CO5 Und



(or)

(b) Discover the security risks and perils of social media marketing and discuss about the associated challenges and preventive measures. 13 CO5 Ana

Social Media Marketing: Security Risks for Organizations • Social media marketing has become dominant in the industry and is used extensively. • There are security problem (privacy threats) related to "social media marketing" or "social computing". • Exposures to sensitive PII and confidential business information are possible if due care is not taken by organizations. According to a survey, usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. My Space is used by 6% of the organizations.

8. (a) Analyze the different aspects of Automated Malicious Code Analysis System. 14 CO4 Und

Behavioral analysis, the process of running an executable in a safe environment and monitoring its behavior, is one way to determine what malicious code does.

Common analysis features include the following

• File system
• Windows Registry content
• Running processes
• Listening ports
• Memory contents

There are two main techniques to analyze the behavior of malicious code:
1. Passive analysis: Record the state of the system before and after the infection. Then, compare these states to determine what changed
2. Active analysis: Actively monitor and record malicious code actions during execution.

Exhibit 5-6 An automated malicious code analysis cycle.

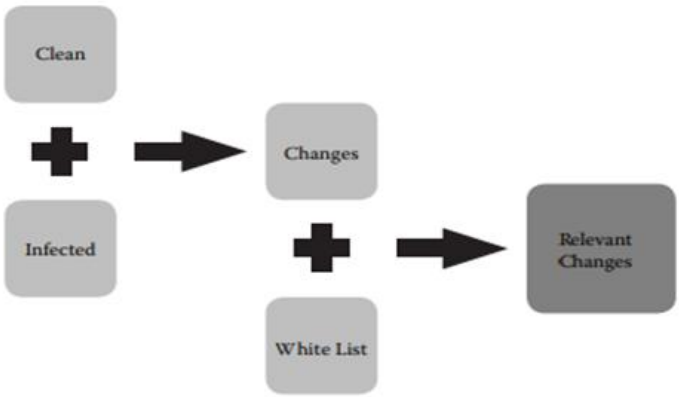


Exhibit 5-7 A passive analysis comparison process.

(or)

(b) Consider the scenario a organization is affected by security and privacy implications, identify the concept involved in threats for organization and its techniques and recommend few tips to prevent from web threats. 14 CO5 Ana

The following are the Internet and Web Threats to Organizations:
• Employee wasting time on social networking sites and its impact on employee productivity.
• Monitoring and Controlling Employees' web usage.
• Keeping security systems with up-to-date patches.
• Legal and regulatory compliance risks such as employee visiting inappropriate websites and accidental disclosure of

information.
• Keeping internet bandwidth free for applications such as live video conferencing, YouTube, and online training videos.
• Monitoring cell phones/smart phones usage and security threats imposed by handheld devices.
• Protecting multiple offices and locations because of globalization.

****

(Note: Und-Understand Rem-Remember Ana-Analyze App-Apply)

Prepared By Verified By HoD