SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Cyber Forensics - Practical Assignments

A list of practical assignments for a Cyber Forensics course, along with problem statements, objectives, and answers for each assignment. Please note that the answers will be concise and focused on guiding the student through the process rather than providing the complete solution. The purpose of these assignments is to enhance hands-on skills in various areas of cyber forensics. Here are 10 assignments covering the topics you mentioned:

Assignment 1: Apache2 Log Analysis

Problem Statement:

An Apache2 web server has been compromised, and you need to analyze the server logs to identify the attack vectors and determine the extent of the breach.

Objective:

1. Analyze Apache2 access and error logs to identify suspicious activities.
2. Determine the source of the attack and the vulnerabilities exploited.
3. Recommend mitigation measures to prevent future attacks.

Answers:

1. Look for unusual patterns in access logs, such as excessive 404 errors or repeated requests for specific files.
2. Check for any suspicious IP addresses in the logs and investigate the corresponding activities.
3. Patch or update vulnerable software, implement intrusion detection systems (IDS), and tighten server security configurations.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 2: Customizing SIEM Tools

Problem Statement:

You are tasked with customizing a Security Information and Event Management (SIEM) tool to monitor specific network and system events in a corporate environment.

Objective:

1. Configure the SIEM tool to collect and analyze relevant logs.
2. Create custom alerts and rules to detect potential security incidents.
3. Generate reports for management based on the collected data.

Answers:

1. Set up log sources (e.g., firewall, antivirus, DNS) to feed into the SIEM.
2. Define rules to trigger alerts based on specific conditions (e.g., multiple failed login attempts).
3. Create regular reports summarizing security incidents, trends, and compliance.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 3: Windows Log Analysis

Problem Statement:

A Windows workstation has been compromised, and you need to analyze the event logs to identify the attack vector and the actions taken by the attacker.

Objective:

1. Analyze Windows event logs (Security, Application, System) to identify anomalous activities.
2. Reconstruct the attacker's actions and timeline.
3. Recommend actions to remediate the compromise and improve security.

Answers:

1. Look for failed login attempts, unusual account activity, and process execution events.
2. Trace the attacker's activities by analyzing the timestamps and event sequences.
3. Isolate the compromised system, remove malware, update patches, and enhance security policies.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 4: USB Data Theft

Problem Statement:

An employee is suspected of stealing sensitive company data using a USB drive. You need to investigate the incident.

Objective:

1. Identify the USB devices connected to a specific workstation.
2. Analyze the content of the USB drives for any unauthorized data.
3. Determine the extent of the data theft and gather evidence for potential legal action.

Answers:

1. Check Windows registry and device logs to identify USB devices connected.
2. Use forensic tools to analyze the USB drive, looking for sensitive files or evidence of data transfer.
3. Present findings, including timestamps, file hashes, and user activity logs, to support legal proceedings if needed.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 5: Windows Forensics

Problem Statement:

A Windows server has been compromised, and you need to conduct a thorough forensic analysis to understand the attack, identify the attackers, and gather evidence for further action.

Objective:

1. Conduct a full disk image acquisition of the compromised Windows server.
2. Analyze the acquired image to identify malware, artifacts, and signs of intrusion.
3. Extract relevant information to support incident response and legal proceedings.

Answers:

1. Use forensic imaging tools to create a copy of the server's hard drive.
2. Analyze the image for malware, suspicious files, and system configuration changes.
3. Document findings, such as malicious files, network connections, and timestamps, to present as evidence if necessary.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 6: Linux Forensics

Problem Statement:

A Linux server has experienced a security breach. You are tasked with conducting a forensic investigation to determine the scope of the attack and identify potential vulnerabilities.

Objective:

1. Perform disk imaging of the compromised Linux server.
2. Analyze system logs, user activity, and network traffic to identify the attack vector.
3. Recommend security improvements to prevent future incidents.

Answers:

1. Use Linux-based tools to create a disk image of the compromised server.
2. Analyze logs, such as syslog and auth.log, for unusual activity and potential vulnerabilities.
3. Implement security measures, such as patching, user access controls, and intrusion detection, based on the findings.

Assignment 7: Android Forensics

Problem Statement:

A suspected mobile device contains evidence of illegal activities. You need to perform Android forensics to extract relevant data.

Objective:

1. Acquire a forensically sound image of the Android device.
2. Analyze the image to recover deleted files, messages, and application data.
3. Document the findings for use in a legal investigation.

Answers:

1. Use forensic tools compatible with Android devices to create an image of the target device.
2. Recover deleted files, parse messaging apps, and extract relevant data from the image.
3. Create a comprehensive report, including extracted data, timestamps, and details of relevant applications.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 8: Data Recovery

Problem Statement:

A user accidentally deleted critical files from their workstation. You need to recover the deleted files without damaging existing data.

Objective:

1. Identify the appropriate data recovery tools and techniques for the specific file system.
2. Recover the deleted files and verify their integrity.
3. Educate the user on best practices for preventing data loss.

Answers:

1. Select a suitable data recovery tool compatible with the file system and storage medium.
2. Use the recovery tool to scan for deleted files, select the desired files for recovery, and ensure their integrity.
3. Provide the recovered files to the user, along with recommendations for data backup and file recovery.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 9: RAM Forensics

Problem Statement:

A compromised system has suspicious processes running in memory. You need to analyze the system's RAM to identify the malicious activity.

Objective:

1. Capture a memory dump of the compromised system's RAM.

2. Analyze the memory dump for running processes, injected code, and other artifacts.

3. Determine the nature of the attack and recommend appropriate actions.

Answers:

1. Use a memory acquisition tool to capture a RAM dump of the compromised system.

2. Analyze the memory dump using volatility or a similar tool to extract running processes, network connections, and injected code.

3. Identify the malicious processes, their behavior, and any other relevant information for incident response and remediation.

SEDULITY SOLUTIONS & TECHNOLOGIES
Website: www.sedulitygroups.com
Email: contact@sedulitygroups.com
Phone: +91-9312903095

Assignment 10: Data Acquisition

Problem Statement:

You are investigating a cyber incident and need to acquire evidence from a suspect's computer while ensuring data integrity.

Objective:

1. Acquire a forensically sound image of the suspect's computer.
2. Maintain chain of custody and ensure data integrity during the acquisition.
3. Prepare the acquired data for analysis while adhering to best practices.

Answers:

1. Use a forensically sound imaging tool to create an image of the suspect's computer.
2. Document the acquisition process, including timestamps, digital signatures, and the hardware used.
3. Verify the integrity of the acquired image using hashes, and securely store the image for analysis while following standard procedures.

These assignments cover a range of topics in cyber forensics, from log analysis and forensics to mobile and memory forensics. Remember that the "Answers" provided are meant to guide the students in the right direction and encourage them to think critically about the process of investigating and analyzing digital evidence. Each assignment should be conducted within a controlled and ethical environment, adhering to legal and organizational guidelines.