Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Friday, November 22, 2024 at 3:30 PM

Guided Exercises

Part 1: Research Incident Response Documentation

4. **Describe** the purposes of an incident response policy, incident response plan, and incident response procedures.

Incident Response Policy (Section 2.3.1)
The policy establishes the organization's commitment and approach to incident response, defining its scope, purpose, and objectives. It outlines roles, responsibilities, and authority, including the ability to take control of systems and report incidents. It also includes guidelines for incident severity ratings, reporting processes, and external communication rules.

Incident Response Plan (Section 2.3.2)
The plan provides a structured strategy for implementing the incident response policy, aligning it with the organization's mission, size, and goals. It outlines resources, communication protocols, and metrics for measuring effectiveness, focusing on continuous improvement. Senior management approves the plan, integrating the incident response program into the organization's structure. Regular reviews ensure the plan remains relevant and actionable.

Incident Response Procedures (Section 2.3.3)
Standard Operating Procedures translate the policy and plan into thorough, actionable steps for the incident response team. These include detailed techniques, processes, checklists, and forms to guide the team during incidents. SOPs are tested, validated, and updated regularly to ensure accuracy and minimize errors under stress. Training allows the team to execute the procedures effectively.

5. **Identify** which document type (policies, plans, and procedures) corresponds to which risk management layer and **provide** your justification.

Incident Response Policies operate at the organizational level, setting high-level governance and expectations for incident response across the enterprise. Polices designate roles, responsibilities, and the overall scope of incident handling, ensuring alignment with the organization's mission and strategic objectives. Policies are broad and guide how to manage risk across the organization.

Incident response plans align with mission and business processes by translating organizational policies into actionable strategies that support specific functions and objectives. Plans address how the incident response program incorporates critical business operations, detailing communication, resources, and performance metrics to ensure business continuity during incidents. They act as the bridge between organizational objectives and operational execution.

Procedures focus on the information systems layer, managing the detailed processes and tools used to react to incidents within information systems. They provide step-by-step guidance for tasks, ensuring consistency and minimizing errors. These are detailed and system-specific, supporting the mission-level plans and organizational policies.

9. **Identify** three examples of external information sharing during the Equifax timeline, including the date, details, and stakeholder.

March 7, 2017 – Apache Struts Project Management Committee
The Apache Struts team announced the CVE-2017-5638 vulnerability and released a patch to notify organizations, including Equifax, of the critical security risk. This was a proactive measure to share information about the threat with all software users.

March 8, 2017 – US-CERT Notification
The United States Computer Emergency Readiness Team (US-CERT) alerted Equifax and urged them to patch the Apache Struts vulnerability promptly. This demonstrates a government and organization's effort to mitigate risks through information sharing.

March 9, 2017 – Equifax Internal Dissemination
Equifax's Global Threat and Vulnerability Management (GTVM) team forwarded the US-CERT notification internally to responsible personnel, stressing the urgency of applying the critical patch within 48 hours. This step highlights internal information sharing initiated due to an external alert.

11. **Describe** three team models.

A central incident response team consists of a single team responsible for handling incidents across the organization. This model best suits smaller organizations with minimal geographic and resource diversity. It ensures a consistent approach to incident handling, and centralized oversight simplifies communication and decision-making during incidents.

Distributed teams have multiple incident response groups, each responsible for specific logical or physical segments of the organization, such as divisions or geographic regions. This model works well for large organizations with widespread operations. While distributed teams provide localized expertise and faster responses, coordination is crucial to maintain consistency and prevent mismanagement.

A coordinating team serves as an advisory body to other incident response teams without having direct authority over them. It is used when multiple teams handle incidents independently. The coordinating team acts as a central resource, providing guidance, expertise, and recommendations to ensure consistency in incident handling. This model benefits organizations with decentralized structures.

12. **Describe** three staffing models.

In the employee-only model, the organization’s internal employees perform all incident response work. This approach ensures the team understands the organization’s specific environment, systems, and processes. However, it requires significant investment in training, staffing, and maintaining expertise across all areas of incident response. Organizations that value in-house control over sensitive data and operational decision-making will often choose this model.

In a partially outsourced model, the organization handles incident response tasks internally while outsourcing specific functions, such as 24/7 monitoring or specialized technical assistance for complex incidents. Outsourcing allows access to specialized expertise and resources. While this model reduces costs and enhances capabilities, a clear division of responsibilities between the internal staff and the outsourcer is essential.

In the fully outsourced model, all incident response tasks are managed by an external contractor, typically with an on-site presence. Organizations that need more resources or expertise often use this approach to maintain a full-time internal incident response team. Organizations using this model should strengthen oversight and basic internal incident response skills to ensure effective partnerships.

13. **Describe** eight groups within an organization that CIRT can turn to for their expertise, judgment, and abilities.

Management is responsible for establishing incident response policies, allocating budgets, and ensuring appropriate staffing for incident handling. Management's support is critical for enabling the incident response team's activities.

The information assurance team provides expertise during critical stages of incident response, such as prevention, containment, eradication, and recovery. Their role ensures technical measures align with the organization's security framework.

The IT support team, comprised of system and network administrators, brings technical expertise and in-depth knowledge of the organization's infrastructure, which is invaluable during incident response. Their familiarity with the systems ensures appropriate actions are performed quickly and effectively.

The legal department team ensures that the incident response policies, plans, and procedures comply with relevant laws and regulations. Their expertise is essential when an incident may result in legal ramifications, such as lawsuits or regulatory investigations.

The public affairs and media relations group manages external communications, including media inquiries and public disclosures during incidents. Their involvement is critical to controlling the narrative and maintaining trust with stakeholders.

Human Resources is involved in incidents involving employees, such as insider threats or policy violations. They assist with disciplinary actions, ensure proper documentation, and address employee-related concerns during and after incidents.

The business continuity planning group ensures that incident response aligns with broader business continuity plans to minimize operational disruptions. They refine risk assessments and continuity plans. Their expertise is crucial for maintaining critical business functions during crises.

Physical security and facilities management address incidents involving physical breaches or coordinated logical and physical attacks. They ensure that physical assets and environments are protected during incident response.

14. **Describe** four services that a CIRT can provide.

The core service of a CIRT is incident response, including detecting, analyzing, containing, eradicating, and recovering from them. The team ensures that incidents are managed efficiently to minimize damage, restore operations, and prevent future occurrences.

Many CIRTs monitor and analyze intrusion detection systems to identify and respond to potential threats. This service lets the team gain deeper insights into attacks and quickly determine appropriate actions.

CIRTs provide timely advisory distribution to the organization regarding emerging threats, vulnerabilities, and mitigation strategies. These advisories help keep stakeholders informed about critical security issues.

CIRTs contribute to building a security-conscious culture by educating and raising users' and technical staff's awareness of incident detection, reporting, and response. They may conduct workshops, create awareness materials, and share best practices.

Part 2: Research the Incident Response Life Cycle

2. **Describe** two preparation actions within the incident response life cycle.

Organizations must establish and train an incident response team to ensure readiness for addressing potential incidents. This process involves defining roles and responsibilities, providing team members with specialized training, and ensuring coordination access to resources like encryption tools, smartphones, and war rooms. These measures ensure the team can respond promptly and maintain secure, coordinated operations during incidents.

A comprehensive toolkit, including hardware and software for packet sniffing, malware analysis, and digital forensics, is essential for effective incident handling. Teams should prepare a portable "jump kit" containing necessary materials like investigative laptops, blank media, and networking equipment for immediate deployment. Organizations should maintain a library of critical resources, such as network diagrams, cryptographic hashes, and clean OS images. These proactive measures enable efficient and effective responses during incidents.

4. **Describe** the relationship between risk assessment and incident response.

Risk assessment is critical to incident response preparation because it identifies potential threats and vulnerabilities, allowing an organization to prioritize and mitigate risks before they lead to incidents. By understanding the likelihood and impact of specific risks, an organization can implement targeted controls to reduce the probability and severity of incidents, easing the load on the incident response team. Also, risk assessments help identify critical assets, enabling the organization to focus monitoring and response efforts on protecting its most valuable resources. Practical risk assessment ultimately supports a proactive approach to security, reducing the number and complexity of incidents requiring an elevated response.

6. **Describe** an attack vector that is not listed in Section 3.2.1.

An unlisted attack vector is the exploitation of Internet of Things devices. Many IoT devices, such as smart cameras, thermostats, and industrial sensors, are deployed with default configurations or weak security controls, making them susceptible to attacks. Threat actors can exploit these devices to gain unauthorized access to networks, steal sensitive data, or create botnets for DDoS attacks. IoT devices are currently an often overlooked risk to organizational infrastructure.

7. **Identify** two early warning signs or indicators of incidents.

An early indicator of a potential incident is an application or system logging multiple failed login attempts from an unfamiliar or unauthorized remote system. This behavior may signal a brute-force attack. Monitoring and responding to log activity can help prevent escalation.

Another early indicator is anomalous patterns in network traffic, such as unexpected spikes in data transfer, connections to unfamiliar external IP addresses, or unusual access to critical assets. Regular profiling of normal network activity helps identify irregularities quickly and can initiate an incident response to mitigate the threat.

8. **Describe** two methods of incident analysis.

Event correlation involves combining data from multiple logs and sources to create a comprehensive view of an incident. By analyzing these correlated events, incident handlers can determine whether an attack was successful, identify affected systems, and uncover the attacker's methods.

Profiling measures the characteristics of normal network and system activity to identify deviations that may signal an incident. This process includes monitoring baseline bandwidth usage, file integrity, and application behaviors. When abnormal activities are detected, they can be alerted for analysis. Profiling helps incident responders identify subtle threats that might have gone unnoticed.

9. **Identify** three examples of incident documentation.

An incident logbook records all facts about an incident as it unfolds. This logbook includes timestamps, system events, and observed file changes, ensuring an accurate chronological account.

An issue tracking system organizes all information about an incident in one place. This system tracks information such as the current status, a summary of the incident, related indicators, and actions taken by handlers.

Chain of custody forms documents how evidence is collected, stored, and accessed. These forms record who handled the evidence when it was accessed, and for what purpose. This ensures the evidence's integrity and admissibility in court.

10. **Identify** three factors for incident prioritization.

The functional impact factor measures how the incident affects the organization's ability to provide services. Prioritization considers the current and potential future impact on critical system functionalities if the incident is not contained.

The information impact factor evaluates how the incident affects the confidentiality, integrity, and availability of sensitive or proprietary information. Understanding the scope of information compromise helps assess the severity and prioritization of the incident.

The recoverability factor examines the resources and effort needed to restore operations to normal. Prioritization depends on balancing the time and resources required against the possible advantages of recovery measures.

13. **Identify** two instances of incident notification in the Equifax timeline involving top-level management.

Notification from US-CERT on March 8, 2017
On March 8, 2017, the United States Computer Emergency Readiness Team (US-CERT) notified Equifax about the Apache Struts vulnerability (CVE-2017-5638) and the need to apply a patch. This notification was an external communication from a national cybersecurity entity to Equifax's top-level teams.
Internal Notification by Equifax GTVM Team on March 9, 2017
On March 9, 2017, Equifax's Global Threat and Vulnerability Management (GTVM) team disseminated the US-CERT notification internally via email. The communication instructed relevant personnel to address the critical Apache Struts vulnerability.

15. **Summarize** four actions performed in the third phase of incident response.

Containment: Strategies are executed to limit the incident's impact, such as disconnecting affected systems, turning off certain functions, or redirecting attackers to a sandbox environment for monitoring without causing further damage.

Evidence Gathering: Evidence is collected and preserved for incident resolution and potential legal proceedings, adhering to chain-of-custody procedures and documentation.

Eradication: Steps are taken to eliminate the root cause of the incident, such as removing malware, disabling compromised accounts, and addressing vulnerabilities exploited.

Recovery: Systems are restored to normal operation, which includes rebuilding affected systems, restoring backups, applying patches, and monitoring to ensure the incident does not reoccur.

16. **Describe** an example of the two-way communication between the second and third phases of incident response.

When a malware infection is detected during the analysis phase, the incident response team might discover additional infected hosts or new indicators of compromise while containing the malware. These findings go back through the analysis phase to refine detection devices, such as updating IDS signatures or adjusting network monitoring activities.

18. **Summarize** three actions performed in the fourth phase of incident response.

In the post-incident activity phase, organizations focus on learning from the incident and improving future responses:
1 -- They hold a lessons-learned meeting to evaluate what happened, how the incident was handled, and identify areas for improvement.
2 -- An incident report is prepared, documenting the chronology, impact, and costs, which can serve as a reference for similar incidents and as evidence.
3 -- Collected incident data is analyzed to identify trends, justify resource allocation, and measure the effectiveness of the incident response team.

19. **Describe** the purpose of the feedback mechanism between the fourth phase to the first phase.

The feedback mechanism between the fourth phase, post-incident activity, and the first phase, preparation, ensures continuous improvement in the incident response process. Lessons learned from incidents, including identified weaknesses, trends, and gaps in resources or procedures, inform updates to preparation activities such as policies, training, and security controls. This process strengthens the organization's ability to prevent similar incidents, enhance detection, and respond more effectively in the future. Organizations create a proactive security posture by applying understandings acquired from previous incidents.

Challenge Exercise

- What type of team/staffing model could be adopted at Acme based on the given information? Why?

Given Acme Corporation's small size and limited security awareness, a Central Incident Response Team with a partially outsourced staffing model would be ideal. The central team model works well for smaller organizations, allowing a single team to handle all incidents. A partially outsourced model would enable Acme to use external expertise to monitor and detect incidents.
Assumption: Acme needs more resources and expertise for an entirely internal CIRT but can afford to contract for outsourced coverage.

- Assume that the Acme Corporation had a comprehensive set of incident response procedures. What procedure would apply to the incident described above? Why?

The procedure that would apply to this incident is the incident response phases: **Preparation, Detection and Analysis, Containment, Eradication, and Recovery**. The **detection and analysis** step involves verifying and analyzing the abnormality to confirm it as a security incident, which would have been accomplished when the administrator identified exploitation of CVE-2017-0143. The **containment** would kick off isolating the compromised Windows domain controller and disabling the attacker's access, which would be essential to prevent further data breaches. The **eradication and recovery** would mitigate the vulnerability by patching CVE-2017-0143, removing the malicious executables. Recovery would include restoring critical services from a secure, verified backup.

This procedure is critical because it provides a structured approach to limiting damage, investigating the incident, and ensuring compliance with PCI DSS. It also addresses the risk of insider threats.

- Think about the external entities that Acme should contact about the incident. Identify one entity and provide your justification. Identify one external entity that should not be contacted and provide your justification.

External Entity to Contact:
Acme should contact the **Payment Card Industry Security Standards Council** to report the breach because this incident involved a critical insider attack targeting customer credit card numbers. Being transparent with PCI-SSC helps maintain compliance and builds trust with customers.
External Entity Not to Contact:
Acme should not contact the **media or press**. Acme should complete a thorough investigation and prepare a controlled public relations strategy with input from legal counsel.

- Which internal stakeholders should the CIRT contact and why?

The CIRT should contact the following internal stakeholders:
1. Senior Management: To ensure they are aware of the severity of the incident and the potential impact on the organization's revenue, reputation, and compliance status. Their involvement is critical for decision-making, resource allocation, and reinforcing the importance of security awareness.

2. Legal Department: Assess the incident's legal implications, especially since PCI DSS compliance and credit card information theft are involved.

3. Human Resources: Manages the employee who was the insider threat, including taking disciplinary action or terminating the employee and addressing any policy reviews.

4. IT Support and System Administrators: Assist with technical mitigation, including containing and eradicating the threat on any impacted systems, recovering data, and securing the systems.

- After recovering from this incident, which services should the CIRT provide to Acme? Why?

After recovering from the incident, the CIRT should provide **intrusion detection and monitoring** services to proactively identify and alert the organization about future threats or suspicious activities. The team should also conduct security **education and awareness training** to address Acme's need for more security awareness.

- Acme had not made preparations for cyber incidents, including this incident. Identify two preparation actions that could have prevented or mitigated the effects of this incident and provide your justification.

By using **user activity monitoring and least privilege access policies**, Acme could have detected unusual behavior patterns thorough user activity monitoring, such as an employee accessing unauthorized files. Enforcing a least privilege policy would ensure that users, including employees, only have access to resources required for their job roles. A least privilege policy would have restricted the employee’s ability to exploit the vulnerability and access sensitive data.

By using **regular vulnerability management and patch management**, Acme could have conducted routine vulnerability scans and applied patches to address known vulnerabilities like CVE-2017-0143. A structured patch management program provides critical vulnerability mitigation.

- What was the attack vector for this incident?

The attack vector for this incident exploited a critical vulnerability, CVE-2017-0143, associated with the Microsoft Windows SMBv1 protocol. This vulnerability allowed the attacker, an insider, and an Acme employee to exploit the domain controller to gain unauthorized access and manipulate files. This vulnerability is associated with the EternalBlue exploit, which indicates the system did not have a proper patch management policy and was not updated regularly. The insider threat shows a lack of internal controls and monitoring to detect and prevent malicious activities from trusted employees.

- What were the early warning signs and indicators of the incident?

Early warning signs and indicators were anomalies observed on the Windows Domain Controller. These included renamed files and the presence of new executables with suspicious names, which strongly suggested unauthorized activity. A technical analysis confirmed exploiting a critical vulnerability (CVE-2017-0143). The discovery of these signs should have prompted immediate escalation and analysis to validate the incident and take action.

- Identify two criteria for determining the appropriate strategy that should be adopted in the containment phase and provide your justification.

The first criteria would be potential damage to and theft of resources.

Justification: The critical vulnerability exploited, CVE-2017-0143, allowed unauthorized access and the attacker, an insider, to steal customer credit card numbers. Since Acme must comply with PCI DSS, failing to mitigate this could lead to severe financial, reputational, and legal consequences.

The second criteria would be the need for evidence preservation.

Justification: Evidence of the exploitation is critical for internal examination and legal action. As the attacker was an insider, preserving the evidence is essential to assure accountability and to understand the methods used in the attack. Properly documenting the chain of custody assures the evidence remains admissible.

- Identify two types of post-incident activities that should be performed and provide your justification.

A meeting to **review the lessons learned** should be conducted to review the elements of the insider threat incident. This meeting can involve exploring the timeline of the breach, the exploited vulnerability, and the response actions. The goal is to identify gaps in Acme's incident response procedures, security awareness, and technical controls.

Acme should perform a **policy and procedure update review**. Based on the findings, it is critical to update the incident response policies and security protocols. Acme should revise its access control policies to limit administrative privileges and adopt measures to monitor abnormal employee behavior. Conducting regular internal audits can be introduced to mitigate the risk of future insider threats and to meet compliance with PCI DSS.