**Date: 2023-10-30**

**Entry:** 1  
**Description:** **Incident Investigation - Phishing Attack**  
**Tool(s) used:** N/A

**The 5 W's:**

* **Who caused the incident?** The incident was caused by a group of attackers using phishing emails to target employees.
* **What happened?** An employee opened a malicious email attachment, which deployed ransomware and encrypted several files on the network.
* **When did the incident occur?** The incident occurred on a Monday morning at 10:30 AM.
* **Where did the incident happen?** The incident happened at a medium-sized law firm.
* **Why did the incident happen?** The incident occurred because the employee was not cautious and clicked on a link in a phishing email, allowing the ransomware to be deployed.

**Additional notes:**  
This incident emphasizes the importance of user education on recognizing phishing attempts. Proper security measures, like multi-factor authentication, and endpoint protection software could have reduced the risk of the attack.

**Date: 2023-10-30**

**Entry:** 2  
**Description:** **Incident Investigation - Data Breach from Weak Passwords**  
**Tool(s) used:** N/A

**The 5 W's:**

* **Who caused the incident?** The incident was likely caused by an external threat actor who exploited weak password practices.
* **What happened?** Attackers were able to gain unauthorized access to the internal systems by using a brute-force attack to guess weak passwords.
* **When did the incident occur?** The incident occurred late Friday evening at around 8:00 PM.
* **Where did the incident happen?** The breach occurred in the internal network of a tech company.
* **Why did the incident happen?** The breach occurred because employees were using weak and repetitive passwords across multiple systems, making them vulnerable to brute-force attacks.

**Additional notes:**  
This incident highlights the necessity of enforcing strong password policies, including password complexity requirements and regular password changes. Implementing two-factor authentication (2FA) would have added an extra layer of protection.

**Date: 2023-10-30**

**Entry:** 3  
**Description:** **Tool Use - Wireshark Network Traffic Analysis**  
**Tool(s) used:** Wireshark

**Purpose of Tool(s):**  
Wireshark is a network protocol analyzer that captures and analyzes the traffic on a network. It’s used to inspect packets of data, helping security professionals detect malicious activity, troubleshoot network issues, and analyze how data moves across the network.

**How was it used:**  
In this activity, I used Wireshark to capture packets from the network. I analyzed the traffic to identify any unusual activity, such as unexpected connections or data exfiltration attempts. By inspecting the packet details, I was able to spot a few failed login attempts and alert the system administrator.

**Additional notes:**  
Although Wireshark can be overwhelming at first due to the large volume of data it captures, I found that using filters (such as applying a filter for failed login attempts) made the process much more manageable. It’s an essential tool for detecting anomalies and understanding what’s happening on the network.

**Date: 2023-10-30**

**Entry:** 4  
**Description:** **Tool Use - VirusTotal File Hash Analysis**  
**Tool(s) used:** VirusTotal

**Purpose of Tool(s):**  
VirusTotal is an online service that analyzes files and URLs to detect malware. It aggregates multiple antivirus engines to scan files for potential threats, and it's used by security professionals to check the safety of files or URLs before allowing them to be opened or executed.

**How was it used:**  
For this task, I used VirusTotal to analyze a suspicious file hash (SHA-256). The file had been flagged by the organization’s endpoint detection system, so I uploaded the hash to VirusTotal. The analysis revealed that the file was flagged by multiple antivirus engines, confirming that it was indeed malicious.

**Additional notes:**  
VirusTotal was extremely useful in quickly verifying the potential threat. It saved time in confirming whether the file was part of a known threat actor’s toolkit. Going forward, I would suggest integrating VirusTotal’s API into the organization's incident response process for even quicker analysis.

**Reflections/Notes:**

1. **Did you encounter any specific challenges during the activities? If so, what were they and how did you overcome them?**  
   Yes, when using Wireshark, the sheer volume of captured packets was overwhelming at first. However, after applying appropriate filters, I was able to narrow down the relevant packets, making the task more manageable. I also learned to be patient and methodical in reviewing network traffic.
2. **How has your perspective on incident detection and response evolved throughout the course?**  
   Initially, I didn’t fully grasp the complexity of incident detection and response, but now I understand how vital it is to have a systematic approach. I’ve learned how tools like Wireshark and VirusTotal fit into a larger incident response workflow, helping to quickly identify and mitigate potential threats.
3. **Was there a particular tool or concept that captured your interest the most? If so, why?**  
   I found **Wireshark** and **network traffic analysis** particularly interesting. Being able to see data moving across a network and identify potential threats in real-time was fascinating. I’m excited to continue learning more about how network traffic analysis can aid in incident detection and prevention.