**Portfolio activity:**

**Incident handler's journal**

**\*All dates in this portfolio activity are not real\***

Scenario 1

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

| **Date:**  28 February 2024 | **Entry:**  #001 | | |
| --- | --- | --- | --- |
| Description | Ransom attack, all companies files have been encrypted | | |
| Tool(s) used | None for this case | | |
| The 5 W's  (of an incident) | * **Who :** Incident caused by unethical hackers(unknown) * **What** :All company files have been encrypted * **When** :Tuesday 9:00am * **Where**: A healthcare company. * **Why**: because employees opened a malicious email that contained malware. | | |
| Additional notes | Should the company pay the ransom in order to receive the decryption key or should they attempt to decrypt it themselves? | | |

| Reflections/Notes: Employees need to be taught about phishing attacks ,how to identify a potential phishing email and how to handle a situation with suspicious emails. |
| --- |

# 

Scenario 2

# In this scenario, you’re a security analyst investigating traffic to a website.You’ll analyze a network packet capture file that contains traffic data related to a user connecting to an internet site. The ability to filter network traffic using packet sniffers to gather relevant information is an essential skill as a security analyst.

You must filter the data in order to:

* identify the source and destination IP addresses involved in this web browsing session,
* examine the protocols that are used when the user makes the connection to the website, and
* analyze some of the data packets to identify the type of information sent and received by the systems that connect to each other when the network data is captured.

| **Date:**  3 March 2024 | **Entry:**  #002 | | |
| --- | --- | --- | --- |
| Description | Analyzing my first packets | | |
| Tool(s) used | Wireshark | | |
| The 5 W's | As this is not an incident there is no who,what,where,when or why. | | |
| Additional notes | At first glance, the interface was very overwhelming. | | |

| Reflections/Notes: In this activity i learned how to open saved packet capture files within Wireshark ,how to view high-level packet data such as source(src) and destination(dst) IP addresses ,protocols of different packets, and how use filters to inspect detailed packet data such as the ip.adr ,ip.dst ,udp.port, tcp.port.  I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. I can see why it's such a powerful tool for understanding network traffic and I’d love to learn more about how to use it accurately in a way that benefits your company.  I did this all on a virtual machine which was provided to me by my course provider but I would love to learn more on how to use them in real world situations. |
| --- |