**Incident handler's journal**

| **Date:**  11/18/2023  1:41 PM | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Documenting a ransomware attack on a small healthcare clinic after the incident has occurred.  This entry occurs in the Post-incident Recovery phase of the NIST Incident Response Lifecycle; however, this entry also includes steps from the Containment, Eradication, and Recovery stages, and the Detection and Analysis stage. | | |
| Tool(s) used | None | | |
| The 5 W's | * **Who**: Ransomware Group * **What:** Infected Healthcare Clinic systems with ransomware * **When:** Tuesday morning, at approximately 9:00 a.m * **Where:** A Small Healthcare Clinic * **Why:** An employee fell for a phishing attack and downloaded malware which gave the hackers access to the companies systems. After gaining access they encrypted all critical files with their ransomware. In return for gaining back access to the files, the group wants a large amount of money. | | |
| Additional notes | 1. What training did employees have to help mitigate social engineering attacks? 2. If they had training then where did the training fail? 3. What training now needs to take place? 4. What access controls could have prevented or mitigated this attack? | | |

| **Date:**  11/23/2023  3:12pm | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet using Wireshark.  This occurs in the Detect and Analysis phase of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | Wireshark | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/AA | | |
| Additional notes | Used Wireshark to analyze a pcap file inside a windows environment. This is the first time I got to use wireshark since learning about it during my degree. I really enjoyed focusing more into the program. | | |

| **Date:**  11/23/2023  3:15pm | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet using TCPDump.  This occurs in the Detection and Analysis stage of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | TCPDump | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A | | |
| Additional notes | Using TCPDump to capture a pcap of some simulated network activity on linux. This was my first time using TCPDump but not my first time hearing about it. | | |

| **Date:**  11/21/2023  2:53pm | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Employee downloads and opens a suspicious file, and it downloads EXE’s on the computer.  This occurs in the Detection and Analysis stage of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Employee * **What:** Employee received and opened an attachment from a suspicious email which then installed a bunch of unauthorized EXE files on the computer * **When:**   + **1:11 p.m.:** the employee received the email   + **1:13 p.m.:** The employee successfully downloads and opens the file.   + **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer.   + **1:20 p.m.:** An intrusion detection system detects the executable files and sends out an alert to the SOC. * **Where:** Financial Services Company * **Why**: The employee in question received an email with a password protected spreadsheet. This email included the password. The employee then opened the spreadsheet which dropped a payload of EXE’s onto their computer which the IDS picked up. | | |
| Additional notes | 1. Who sent this email? 2. Did the employee open any of these executable files? 3. What was the motive behind this email and payload? | | |

| **Date:**  11/21/2023  3:53pm | **Entry:**  5 | | |
| --- | --- | --- | --- |
| Description | Using a Phishing Incident Response Playbook  This occurs in the Detection and Analysis stage of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | Phishing Incident Response Playbook | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: HR Employee * **What**: Received a Phishing email and opened the attached file. * **When**: 1:20pm * **Where**: Financial Service Company in the HR department * **Why**: A HR employee received and fell for a Phishing email which compromised their computer | | |
| Additional notes | 1. What training has the company given on Phishing 2. Is opening email attachments something HR needs the ability to do?   This was one of my first looks at an official playbook though I have done similar things before but I never connected that to being a playbook necessarily. | | |

| **Date:**  11/21/2023  3:13pm | **Entry:**  6 | | |
| --- | --- | --- | --- |
| Description | Unauthorized access to customer personal identifiable information (PII) and financial information.  This contains steps from every stage of the NIST Incident Response Lifecycle as this details everything from the start to the end of an incident. | | |
| Tool(s) used |  | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Unknown Threat actor * **What**: A threat actor gained access to PII and financial information of customers. Approximately 50,000 customer records were stolen. * **When**: Approximately 3:13 p.m., PT, on December 22, 2022 * **Where**: Mid-sized retail company * **Why**: After stealing the information the threat actor emailed an employee and demanded $50,000 in crypto currency. They gained access by exploiting a web vulnerability and performing a forced browsing attack that then allowed them to modify the order number in the url and access purchase confirmation pages which contained the customer PII and financial information. | | |
| Additional notes | 1. Why did the threat actor email that specific employee? 2. Could said employee know the threat actor? 3. Was this a known vulnerability? 4. If known then why was it not fixed? 5. If it wasn’t known then why wasn’t it known? | | |

| **Date:**  11/23/2023  3:19pm | **Entry:**  7 | | |
| --- | --- | --- | --- |
| Description | Reviewing a final report after the incident detailed in entry #6.  This occurs in the Post-incident Activity stage of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | Final Report | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A | | |
| Additional notes | I reviewed a simulated final report that occurred after the incident that was recorded in journal entry 6.  This was a interesting read and I had several questions:   1. Why wasn’t Perform routine vulnerability scans and penetration testing taking place already? 2. How easy is it to detect for IDOR 3. How could this have not been tested for or seen as an issue? 4. How common is it to have issues with IDOR | | |

| **Date:**  11/23/2023  3:21pm | **Entry:**  8 | | |
| --- | --- | --- | --- |
| Description | Exploring signatures and logs with Suricata and learning how to read them. This could be in the Detection and Analysis stage of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | Suricata | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A | | |
| Additional notes | I explored Suricata along with how to view and read logs and signatures from it. | | |

| **Date:**  11/23/2023  2:45pm | **Entry:**  9 | | |
| --- | --- | --- | --- |
| Description | Investigating a Chronicle alert triggered for office365 sign-ins that link to a known drop site.  This could be in the Detection and Analysis stage of the NIST Incident Response Lifecycle and/or Post-incident Activity stages depending on where in the incident im doing these queries. | | |
| Tool(s) used | Chronicle | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Ashton Davidson’s pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc * **What**: Possible successful Phishing attack * **When**: 1-31-2023 at 2:40PM * **Where**: Company * **Why**: Alert suggests a possible successful Phishing attack on several user PCs from office365. The url accessed and logged in using user credentials uses a known drop site for logs and stolen user logins as noted by ET Intelligence Rep List. The resolved IP also includes a high severity IP associated with Phishing. | | |
| Additional notes | I have used similar types of programs to Chronicle when I used KACE. However Chronicle is much more specifically for not only asset listing but also alerts whereas KACE can track these things but it’s much more focused on asset management. | | |

| **Date:**  11/23/2023  3:24pm | **Entry:**  10 | | |
| --- | --- | --- | --- |
| Description | Performed a search query with Splunk and investigated the query.  This could be in the Detection and Analysis stage of the NIST Incident Response Lifecycle and/or Post-incident Activity stages depending on where in the incident im doing these queries. | | |
| Tool(s) used | Splunk | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A | | |
| Additional notes | I explored Splunk and performed a search qwerty inside of it. | | |

| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   I didn’t find any specific activity challenging necessarily but some of the info used for them was. Such as trying to learn the different log languages and how they are structured took a little longer to stick than most anything else. If I had to say something then I might mention TCPDump, using it is easy but reading the output of it was challenging at first and I need more practice.   1. **Has your understanding of incident detection and response changed after taking this course?**   I have done things that would be under incident detection and response but it never occurred to me to even call it that. I did not understand how detailed you could get and how many different tools were out there to detect and respond to incidents. I’m used to KACE, AD, and some ticket softwares but I never understood where people got all of the other information till this course.   1. **Was there a specific tool or concept that you enjoyed the most? Why?**   I really love the investigation part of Cyber Security so being able to use Splunk and Chronicle was really great! Chronicle was laid out really nicely and is something I wish was covered in my degree program. Splunk is also really nice but I enjoy the extra built in features and user interface of Chronicle more. |
| --- |