Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: (fake date)	**Entry:** 1
Description	Cybersecurity incident – phishing (Detection & Analysis)
Tool(s) used	N/A
The 5 W's	• Who: malicious hackers • What: phishing email with ransomware was opened internally, leading to loss of access to various files, and ransom note displayed. • When: prior to Tuesday 9AM (presumably, day before?) • Where: Clinic's computer network • Why: malicious hackers wanted ransom to restore the files
Additional notes	Email scanner? No segmentation / Least privilege? Lack of malware awareness? Decryptor publicly available or pay up? Mitigation and prevention?

Date:	**Entry: 2**

n/a	
Description	Wireshark packet inspection exercise (D&A)
Tool(s) used	Wireshark
The 5 W's	Capture the 5 W's of an incident. • **N/A, this is just practice of analyzing existing capture**
Additional notes	Powerful tool if you have some idea what you're looking for

Date: n/a	**Entry: 3**
Description	Packet capture exercise (D&A)
Tool(s) used	tcpdump
The 5 W's	Capture the 5 W's of an incident. • **N/A, this is just practice of a live capture and analysis**
Additional notes	Again, a powerful tool if you have some ideas what's going on

Date: n/a, 1311 hours	**Entry: 4**
Description	Investigate potential malware downloaded (D&A)
Tool(s) used	VirusTotal
The 5 W's	• Who: malicious hackers?

	• What: possible phishing email with attachment was opened internally, leading to executables created and IDS alert to SOC. • When: 1311 hours • Where: computer at company • Why: unknown at this time, probably hoping to compromise site data
Additional notes	Hash confirms well known trojan via VirusTotal via has, ip address, and host artifact. Need to update employee awareness and perhaps email filtering

Date: 7/20/2022	**Entry: 5**
Description	Alert ticket for phishing event (D&A)
Tool(s) used	Phishing response playbook
The 5 W's	Capture the 5 W's of an incident. • **Who** : Possible malicious hacker sent attachment disguised as an “encrypted” resume to HR department • **What** HR Department opened it and it appeared to have deployed on HR computer • **When** Email was sent 7/20/2022 9:30AM? • **Where** Inergy HR department? • **Why** Someone want to attack inergy for whatever purposes? So far, the trojan’s true payload remains unknown, but we’re not taking chances.
Additional notes	Escalated to L2

Date: n/a	**Entry: 6**
Description	Evaluating final report of incident 12/28/2022 1920 (Post Incident Activity)
Tool(s) used	Final Report
The 5 W's	Capture the 5 W's of an incident. • **Who** Malicious hacker? • **What** Some sort of breach occurred prior to 12/22/22, employee was notified on 12/22/22 then again at 12/28/22, when SOC was notified, then investigation started • **When** See above • **Where** company ecommerce server • **Why** ecommerce site vulnerability discovered (zero day?)
Additional notes	Remediation includes PR, disclosure, free ID protection to affected, forensic on why data exfiltration was not discovered and cut off immediately, close vulnerability in website such as URL range

---

Date: n/a	**Entry: 7**
Description	Suricata exercise with alerts, logs, and rules (D&A)
Tool(s) used	Suricata
The 5 W's	Capture the 5 W's of an incident. • **n/a exercise only, sample data alert, log, and rules tested**
Additional notes	With multiple levels of logs (fast, regular, json) knowing which to look at requires experience

NOTE: There was supposed to be another entry here, but I have problems getting Splunk to work so I was forced to skip it.

Date: ???	**Entry: 8**
Description	Analyze potential phishing attempt via Chronicle log (D&A)
Tool(s) used	Chronicle search
The 5 W's	Capture the 5 W's of an incident. • **Who** malicious phisher (suspected) • **What** several office PCs received email prompting them to sign into signin.office365x24.com, which is not a genuine MS website. • **When** 2023-01-31 roughly 1440 hours • **Where** ??? (office of wherever these employees belong to?) • **Why** Malicious actors managed to infiltrate our email spam filter and mailed several employees, two of which submitted credentials to the fake login page, probably a fake copy of MS office365 homepage, probably to steal their MS365 credentials. Interesting that same IP had previously hosted a gooqle.com host, which seems to be a fake look-alike to Google...
Additional notes	Update employee awareness to such spam, update email spam filter, put in alert for login-attempts to “sound-alike” domains or domains that contain pages such as login, signup, and so on.

NOTE: Blank entry template follows

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Reflections/Notes:
Any specific activities that are especially challenging? Not particularly, some of these are common sense and builds upon earlier tools, it's the format of the report that is a little questionable, and remember all the options in tcpdump, and know what to look for

Has my understanding of incident detection and response changed since taking this course? Not really. I expected lots of things to learn.

Were there any specific tool or concept I enjoy the most? Probably Wireshark and Chronicle, lots of interesting data to sift through, previous A+ knowledge comes in handy somewhat.