Extra Credit Option #2:

Understanding the Incident Response Mindset

Background Information

Cliff Stoll's book the "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" is revered as one of the first cases where forensic analysis was used to identify computer intruders. In the mid-1980s, the were ill-established computer forensic practices and Cliff Stoll's book exemplifies this point. Through analyzing discrepancies in an accounting system, he then manages to identify anomalous network connectivity on his network. Throughout the book, you'll learn how he tracked the hackers back to Russia and engaged with several key governmental players.

Objective

Gain a thorough understanding of the analytic mindset associated with computer forensic and the incident response process.

Assignment

Read and answer the questions below about the "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" by Cliff Stoll.

A PDF version is available here: https://vxheaven.org/lib/pdf/The%20Cuckoo's%20Egg.pdf

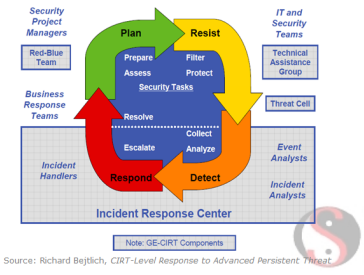
1) What is the book's premise?

2) How did Cliff reconcile the accounting error? How long did the investigation take place?

3) How was the news of the intrusion received by the Lawrence Berkeley National Laboratory? What challenges did Cliff encounter in his hunt to identify the hackers and why is it important to get management buy-in before initializing such a massive incident response effort?

4) What computer systems and networks did the hackers break into? What operating system were these computers and networks running? What application did the hackers exploit? What type of files were they looking for?

5) What did Cliff do to identify the hacker's presence on the network?



6) What private sector entities did Cliff contact to help in his investigation? How did they support him? What information did he need to provide them with to enable them to do their job?

7) What US Government entities were contacted to include other US National Labs? How did Cliff find their contact information? How was Cliff's findings received by them?

8) What award(s) was Cliff given for his work?

9) How was the news of the intrusion received after it was made public?

10) What insights did this book provide you with as it relates to incident response and computer forensics? What processes are in place today to report such a crime/hack? What parties should be contacted?

11) How do you think reading this book will help you in the future in both your academic career and post-graduation?