Manual/Walkthrough

Before starting the challenge, all documents from the **Resources** page of the site should be printed and arranged at a workstation. These documents contain hints and information that are necessary to complete the challenge.

1. Log into each account (information will be found on the Employee ID Cards, the employee that we want to Look at mostly are Jaime and Sam)
    - Jaime; **User:** j.graves2 **Pass:** CavsFan123
    - Sam; **User:** s.carters7 **Pass:** smokedsalmon24

2. Search through emails for suspicious information
    - Sam will have emails that make him sort of suspicious
    - Jaime will have a very suspicious folder!
    - The emails are labeled **Subject: Quick Access Check** and **A New Transaction From sreniram66**

3. In this folder in Jaime's email, you will find a transaction containing an IP address and a suspicious conversation with an external figure.
    - This email conversation contains hashed login information for an unknown and malicious FTP connection information

4. Decrypt the hashed login information by using an online MD5 Decrypter. The exact decrypter is given in the conversation. Here is the correct login information.
    - Host: **73.118.209.254**
    - User: **carters**
    - Pass: **seahawks**

5. Go into FTP, where you will find the 3 stolen files that then point to Sam.

6. You will find that Sam has 3 locked files in his file explorer. Each of these locked files has a password.
    a. Each Password in the FTP has a Password Reminder/Hint and the password's themselves are found through the process of open source intelligence (OSINT) and will be found through the Company Social Media Feed and physical documents gathered from the employee desk.

       (lowercase no spaces)
       -> my best friend's last name

       -> model of my first car

       -> my home city

clientDatabase.pdf **Hint:** “my best friend's last name” **Answer:** hansen

- This answer can be found on a company social media post from Sam.

employeeInformation.pdf **Hint:** “model of my first car” **Answer:** cruze

- This answer can be found in a physical clue, which is Sam’s Parking Pass. This parking pass labels the make and model of their car.

productRoadmap.pdf **Hint:** “my home city” **Answer:** seattle

- This answer has been alluded to all over the game. Sreniram66 is mariners backwards, relating to the Seattle baseball team. Sam’s password is smokedsalmon24. He has emails from StormKraken Coffee in Seattle. Their password for the FTP is seahawks the NFL team from Seattle, It is spread everywhere!

7. Once all the passwords have been entered, the student will complete a brief Incident report write up that covers the game and acts as a debrief as well as a certificate of completion. A copy of a completed incident report can be found below as well as on the **Resources** page of the site.

INCIDENT REPORT TEMPLATE

REPORTED BY: BASTION INVESTIGATION TEAM

DATE OF REPORT: DATE OF COMPLETION 00/00/0000

TITLE/ROLE: CYBER FORENSIC INVESTIGATOR

INCIDENT NO.: 00346

INCIDENT INFORMATION

INCIDENT TYPE: SENSITIVE DATA BREACH

DATE OF INCIDENT: DATE OF COMPLETION 00/00

LOCATION: 6425 PENN AVE

CITY: PITTSBURGH

STATE: PENNSYLVANIA

ZIP CODE: 15206

SPECIFIC AREA OF LOCATION (IF POSSIBLE): BASTION OFFICES

INCIDENT DESCRIPTION:

BRIEF INCIDENT DESCRIPTION- SHOULD WALK THOUGH THE MAJOR PIECES OF DATA BREACEHED AND METHODOLOGY

NAME/ROLE/CONTACT OF PARTIES INVOLVED:

1. SAM CARTERS, BASTION EMPLOYEE, S.CARTERS7@BASTION.COM
2. JAIME GRAVES, BASTION EMPLOYEE, J.GRAVE2@BASTION.COM
3.

NAME/ROLE/CONTACT OF WITNESSES:

1. NAME OF STUDENT 1
2. NAME OF STUDENT 2
3. NAME OF STUDENT 3

POLICE REPORT FILED? YES

PRECINCT: 12

REPORTING OFFICER: CARTER SAMSOM

PHONE NUMBER: (412) 123-4567

FOLLOW UP ACTION:

BRIEF RECCOMENDATION OF FOLLOW UP ACTION

SUPERVISOR NAME: NAME OF INSTRUCTOR

SUPERVISOR SIGNATURE: DIGITAL SIGNATURE OF INSTRUCTOR

DATE: DATE OF COMPLETION 00/00/0000