DIGITAL FORENSICS MODULE CHALLENGE

If you have any questions, please ask them in the ""forensics-module" channel, under the "Operation Chimera" category on the SBT Discord server.

If you feel you're familiar with what Digital Forensics is, and how to conduct a simple investigation, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' on the first page before attempting the Challenge.

What will I need for this Challenge?

- Virtualbox (https://www.virtualbox.org/wiki/Downloads)T
- Kali Linux VM (https://www.kali.org/downloads/)
- Here's a YouTube guide to help you set up a Kali VM: (https://www.youtube.com/watch?v=FVmWMogGX4Q)
- **Challenge Disk Image** (.zip file for ease-of-use. Download this to your Kali VM, unzip, and get going!) (http://bit.ly/ChimeraDFZip)

Challenge Brief:

The SOC has received an anonymous report that a user is potentially exfiltrating data from the company. An image of the user's hard drive has been taken, and you are responsible for analyzing the contents of a perfect copy to find any evidence of malicious activity. Using your newly developed skills, search through the folders and files using techniques to uncover 4 pieces of hidden information (**each piece of evidence will contact the text {1 of 4} or something similar**). Keep a record of all information you find that may be relevant to the investigation and write a short report on what you believe is going on. The report should include the following information (report template below):

- **Hidden information you have found**
- **Methods used to retrieve information**
- **The locations/files of the information**
- **A conclusion on the activity you have discovered**

Some useful commands include the following:
(Remember you can view the manual page for tools by using "man *command*" *to get useful information!)*

- **Strings** (Allows us to find hidden text strings in image and audio files)
- **ls -a** (Allows us to find hidden files in the current directory from terminal)
- **Cat <file>** (Allows us to find hidden text strings in image and audio files)
- **Fcrackzip** (Allows us to crack password protected .zip files)
- **Steghide** (Allows us to retrieve files hidden in image and audio files - http://steghide.sourceforge.net/documentation/manpage.php)

- **File <file>** (Allows us to see what the true file-type the file is, even if the extension has been changed to trick us)

STARTING POINT - You have been told that the most recent file on the hard-drive was an email and attachment in the “Saved Emails” directory. It is suggested you start there. Below are some tips for your investigation:

- Always keep an eye out for hidden files that start with a ‘**.**’ - use ‘ls -a’ in a terminal to view these files!
- Look at the directories and files both in the Kali Linux GUI, and Command-Line!
- This challenge is based on a narrative. You will be gently guided to find some pieces of evidence. Remember to look in all folders, and check all files, especially ones that look strange!
- If you need to bypass a password-protected .zip, follow the training material and use fcrackzip with the rockyou.txt word list.
- If you get stuck, ask people in the forensics module chatroom on the Discord! Work together, learn together.

Read to submit your Challenge? Head over to the website and click on the ‘Challenge Submission’ button under the Digital Forensics module.

Evidence Piece 1 of 4	
Name of original file containing evidence [10]	
Full file path (right-click > parent folder value + filename) [5]	
File type [5]	
Time found (Date - DD/MM/YYYY + Time) [5]	
Method (+ commands) used to find file [10]	
Explain how the information was hidden [10]	
What information was included in the file? (Don’t copy-paste the file content, explain exactly what it is) [10]	

Evidence Piece 2 of 4	
Name of original file containing evidence [10]	
Full file path (right-click > parent folder value + filename) [5]	
File type [5]	
Time found (Date - DD/MM/YYYY + Time) [5]	
Method (+ commands) used to find file [10]	
Explain how the information was hidden [10]	
What information was included in the file? (Don't copy-paste the file content, explain exactly what it is) [10]	

Evidence Piece 3 of 4	
Name of original file containing evidence [10]	
Full file path (right-click > parent folder value + filename) [5]	
File type [5]	
Time found (Date - DD/MM/YYYY + Time) [5]	
Method (+ commands) used to find file [10]	
Explain how the information was hidden [10]	
What information was included in the file? (Don't copy-paste the file content, explain exactly what it is) [10]	

Evidence Piece 4 of 4	
Name of original file containing evidence [10]	
Full file path (right-click > parent folder value + filename) [5]	
File type [5]	
Time found (Date - DD/MM/YYYY + Time) [5]	
Method (+ commands) used to find file [10]	
Explain how the information was hidden [10]	
What information was included in the file? (Don't copy-paste the file content, explain exactly what it is) [10]	

Investigation Report	
Provide a brief conclusion on what information was being stolen, how it was hidden, and how the suspect was getting it out of the company (Look at how many marks this question is worth, to ensure you write enough) [25]	