Lab 09 - Forensics

Overview

Computer forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

[BONUS] Completare formular de feedback

Vă invităm să evaluați activitatea echipei de ISC și să precizați punctele tari, punctele slabe și sugestiile voastre de îmbunătățire a materiei. Feedback-ul vostru este foarte important pentru noi să creștem calitatea materiei în anii următori și să îmbunătățim materiile pe care le veți face în continuare.

Găsiți formularul de feedback aici [https://acs.curs.pub.ro/2018/mod/feedback/view.php?id=2010].

Vă mulțumim!

Exercises

You are a private investigator and you have 2h to solve 9 crimes. At the end of every crime you will find a flag that looks like **ISC{...}**.
Are you up to the task?

Here is your data.

All exercises can be solved on the local Linux machine.

00. Capture 1

This is traffic capture of a suspect that we've been following for a long time. Can you find anything interesting like login credentials?

Use wireshark to analyse the pcap.
Check the ports at statistics/conversations/tcp.

01. Unknown File Type

We've found this file on a confiscated machine, but we can't figure what it is. Can you help us?

Today is not your lucky day. No hints for you.

02. Hidden Flag

There is something uncanny about this image. Is it trying to give us a hint?

03. Corrupted File

During a transmission, one of our files got corrupted. Take a look and see if you can do something about it.

> Maybe there is something wrong with the header.

04. Audio Visualization

We have intercepted an alien transmission, but there is no way to understand what is it saying. Maybe we should look at it.

> Can you SEE it? Check Audacity.

05. Hidden File

There is something wrong with the size of this image. Is there anything else there?

> Use Binwalk. ”-e” option is buggy sometimes.

06. Censored

We've found a letter in the trash can of a suspect, but some of the info is censored. Do some magic and find what is underneath the black box.

> Use Google.

07. Waiting for eternity

We stared at this gif for the last hour but nothing is happening. Would you like to join us and stare at it for the next hour?

08. Capture 2

This is an USB capture of a device connected to a suspect's machine. Can you find what he's been typing?

USB Documentation [https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf]

Resources

- Hex Editor
- Wireshark
- Binwalk
- Audacity
- Image extractor
- USB documentation

11. [10p] Feedback

Please take a minute to fill in the feedback form [https://forms.gle/5Lu1mFa63zptk2ox9] for this lab.

isc/labs/09.txt · Last modified: 2020/02/19 19:25 by mihai.chiroiu