Introduction to Digital Forensics

Institute of Distributed Systems | Semester
Supervisor
Lecturer

Exercise 5: Network Forensics

Overview

In this exercise sheet we will be looking at network forensics. The task's goal will be, as with all capture the flag tasks, to find the hidden flag.

As usual, you are free to use resources on the Internet. However, in each task, make sure you explain all steps taken. That means you need to **explain your answers**.

Submission

Please follow the submission guidelines given at the end of the assignments and in *Exercise Sheet 1*.

Task 1: Working Environment Setup (X)

To be able to solve this task, let us start with the preparation of our working environment. First of all, start with preparing a virtual machine. For this sheet, a Kali Linux distribution is recommended. You can find suitable Kali Linux virtual machines under `https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/`. Other Linux distros, and even Windows, are also suitable, but the effort of installing all needed packages is not worth it.

Submission:

- No need to submit anything for this task, just get your working environment up and running.

Task 2: Wireshark (X)

This task's goal is getting you comfortable with Wireshark. Wireshark is pre installed in Kali Linux, so just grab the provided PCAP files and start searching for clues. There are two provided PCAP files, and for each of those, a minimum of gathered information is required. Read the documentation of Wireshark under `https://www.wireshark.org/docs/wsug_html/`, or if you already worked with it, just get cracking. Feel free to create scripts (e.g. Python) to automate string and file extraction from PCAP files or use already available libraries from the Internet.

- *task2pcap1.pcap*: The captured PCAP is of an IM communication between Ann (192.168.1.158) and her

contact at a rival company. Please verify the integrity of the PCAP file. The MD5 hash should read: *d187d77e18c84f6d72f5845edca833f5*. We are looking for:

  - The user name of Ann's IM contact
  - The first captured text of the IM conversation
  - The name of the attached file, Ann has sent to her contact
  - All further information gathered is optional

- *task2pcap2.pcap*: Ann is a fugitive and she is on the run! The captured PCAP was of an email conversation of Ann and her lover. Please verify the integrity of the PCAP file. The MD5 hash should read: *cfac149a49175ac8e89d5b5b5d69bad3*. Find out following information:

  - The email address of Ann
  - The body of the email Ann sent to her lover
  - The name of the attachment Ann has sent with the email
  - ALl further information gathered is optional

Submission:

- *a2/* (the directory name)
  - *a2.txt*: add all documentation/explanations/answers/sources/etc. to this file

Task 3: Capture the Flag (X)

The main task also involves a PCAP file: *task3pcapctf.pcapng*. This PCAP file is of a session involving TLS and FTP. This suspicious transmission is the main evidence provided. With the help of the tools introduced in the exercise, and your newly acquired proficiency in Wireshark, take a look at the PCAP file and try to find the hidden flag.

Please verify the integrity of the PCAP file. The MD5 hash should read: *d6c6b47b0f944966b1afc355c84ed593*.

Tipps and hints will be provided via Moodle, to help you if you get stuck.

Hint: yeah, you already tried to extract the archive, did'nt you? Well, too bad you dont have the passw0rd. Oh, look at this cute cat picture: `https://bit.ly/2RZmhkt`!

Submission:

- *a3/* (the directory name)
  - *a3.txt*: add all documentation/explanations/answers/sources/etc. to this file