Security of IT Systems

Institute of Distributed Systems | Winter Semester 2018/2019
Nicola Fröhlich, Amir Hosh, Dominik Lang
Prof. Dr. Frank Kargl, Dr. Elmar Schoch

Exercise 5: Network Forensics

Overview

In this exercise sheet, an excursion to digital forensics will take place. Specifically, 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. This means you need to **explain your answers**.

Submission

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

Task 1: Working Environment Setup (0)

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 (2)

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.

a) *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 that Ann has sent to her contact
- All further information gathered is optional

b) *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 the following information:

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

Submission:

- *a2/* (the directory name)
- a)
  - *a2/a.txt*: add all documentation/explanations/answers/sources/etc. to this file
- b)
  - *a2/b.txt*: add all documentation/explanations/answers/sources/etc. to this file
- if applicable, add all other/extracted files to the directory *a2/*

Task 3: Capture the Flag (6)

The main task also involves a PCAP file: *task3pcapctf.pcapng*. This PCAP file is of a recorded 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.

You will be in the shoes of the great forensic investigator Bob, and your task is to uncover the data that has been hidden and secretly transferred by Alice. You will need a sharp sense, some basic understanding of network protocols and a little background in forensics. Document your steps, even the ones that have failed and led to no information. This way, an easy understanding of the events that led to your success can be guaranteed. The more documentation you submit, the more partial points you get.

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

Tips and hints will be provided via Moodle, to help you if you get stuck. Feel free to submit scripts/etc. that you used to help you solve the task.

Hint: yeah, you already tried to extract the archive, didn't you? Well, too bad you don't have the passw0rd. Oh, look at this cute cat picture: `https://bit.ly/2RZmhkt`!

Submission:

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

Task 4: Lecture/Exercise Evaluation (2)

Submission:

- *a4/* (the directory name)
  - *a4/lecture-evaluation.txt*: add all replies to this file
  - *a4/exercise-evaluation.txt*: add all replies to this file

Please answer the following questions to your best knowledge. This will help us evaluate the maturity of our project and aid us in making it better. First of all, some questions to the lecture:

1. *Prior Knowledge:* What prior knowledge do you have in the subject digital forensics?
2. *Related Lectures:* I have prior knowledge from the following lectures:
   - "Grundlagen der Rechnerarchitektur"
   - "Grundlagen der Rechnernetze"
   - "Grundlagen der Betriebssysteme"
   - "Sicherheit in IT-Systemen"
3. *Understanding of Digital Forensics:* Do you have a better understanding of digital forensics after the lecture? What do you understand under digital forensics?
4. *Train of Thought:* Was there a clear train of thought regarding the topics discussed in the lecture? If not, where did you miss it?
5. *Practical Compliance:* Was there an adequate relation to the practical use of digital forensics? Did the real case at the beginning underline that?
6. *Slides and Script:* Were you able to create a connection between presented slides and the corrosponding topic in the script? If no, what was missing? (you can download the script in Moodle - Exercise Session Material)
7. *Overall Opinion:* What was your overall opinion of the concept of the created lecture, especially the dedicated script on top of the slides? (you can download the script in Moodle - Exercise Session Material)
8. *Interactivity:* How did you like the concept of interactivity between lecturer and student?
9. *Positive Reinforcement:* How did you like the fact that positive reinforcement was used to reward participation in the lecture?
10. *Zen Presentation:* The created slides are so called "Zen-Slides"; less bulletpoints more keywords. Was the slide design a welcomed feature? Did it complicate the understanding of the topics explained?
11. *Be Creative:* We would like to receive more feedback, suggestions and your thoughts on possible improvement!

Following, a few questions regarding the exercise. Please answer those after the processing of tasks 2 and 3 of this sheet:

1. *Lecture and Exercise:* Was there a clear connection between lecture and exercise? Where was such an connection missing?

2. *Clarity:* Was the exercise clear? If not, what was unclear?
3. *Level of Complexity:* Were the tasks adequate? Were they too easy or too hard? Please explain your answer.
4. *Exercise and Tasks:* Did the exercise help you in solving the tasks? If no, why not? What was missing?
5. *Practical Compliance:* Was there a practical compliance of the exercise and the tasks? Where would you wish for more practical relevance?
6. *Be Creative:* We would like to receive more feedback, suggestions and your thoughts on possible improvement!