INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

STORM AREA 51 – Stage III

2019/2020

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment will conclude the investigation of the case “Storm Area 51”. After having identified some leaked secrets in a pen drive (Lab Assignment I) and obtained evidence that these secrets have likely been downloaded from a remote computer (Lab Assignment II), in this exercise you will follow this latest clue in an attempt to finally discover the authorship of the data leakage. This will be achieved by analyzing two network traces that can be downloaded from the course web site. To solve this exercise, you will need to develop your skills primarily in traffic analysis. Just like in the previous assignments, we suggest you to use the Kali Linux distribution for performing this work.

Scenario presentation

Despite some important steps that were made in the previous assignment, the results are still somewhat inconclusive. In fact, after analyzing the hard disk images and memory dumps extracted from the computers of Matty and Tim, you found evidence that (1) these secrets have been copied into Matty’s pen drive from Tim’s computer, (2) that these secrets have been downloaded from a remote machine, and (3) that the download was performed by a script that was sent to Tim by email from an anonymous mailer service. After inspecting the script, it was possible to identify the IP address of the remote machine from where the secrets have been obtained. This IP is 10.10.9.14.

With the help of your teammates, you learn that this IP address is owned by Area 51. This prompts you to head your way towards their facilities and meet with Bryan Reynolds, the chief network administrator. Bryan tells you that the IP address 10.10.9.14 is statically assigned to the workstation of a high-ranked USAF military with clearance to classified information. As it turns out, the name of this officer is Justin Roberts: Matty’s older brother. In light of these findings, you ask Bryan for relevant information and any available forensic material that can help you reconstruct the sequence of events that led to the exfiltration of secrets from Area 51.

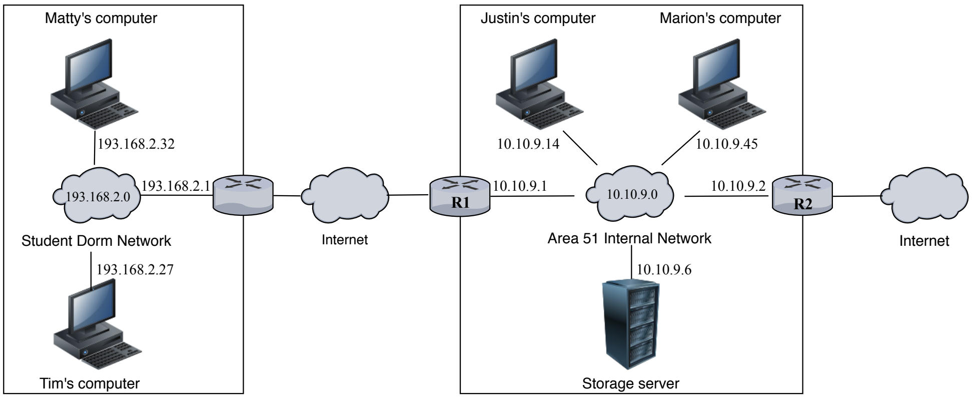

Figure 1: Diagram of the network topology covering both the student dorm and the Area 51 networks.

The figure above shows the reconstruction of the network topology involving the relevant stakeholders of our case. In particular, it shows the student dorm’s network (193.168.2.0/16) and the Area 51 internal network (10.10.9.0/16) where Tim’s computer (193.168.2.27) and Justin’s computer (10.10.9.14) are connected, respectively. The internal network of Area 51 has one gateway router R (10.10.9.1). In addition to Justin’s computer, there are two machines connected to this network: Marion’s computer (10.10.9.45) and a storage server (10.10.9.6). Marion Schneider is the secretary of Justin Roberts. The storage server is a dedicated server for storing the classified data in Area 51. It can be accessed over SSH by accredited users. The only user with access credentials is Justin Roberts.

Luckily, for security reasons, the gateway has been configured to collect periodic traces of the network traffic, and Bryan was able to give you access to some network traces obtained from the gateway (R) sometime before the secrets have been exposed. Moreover, we also have access to the SSH logs maintained by the storage server. The respective files can be downloaded from the course's website or directly from the following links:

- `http://turbina.gsd.inesc-id.pt/csf1920/area51_trace.tar.gz`
- `http://turbina.gsd.inesc-id.pt/csf1920/area51_ssh_log.tar.gz`

In this exercise, your job is to analyze these digital artifacts and answer the following questions. Justify your answers by providing all the relevant evidence you can find. Make sure to explain your hypotheses and how you have proceeded to validate them.

1. Do you find any evidence of transfers involving the leaked secrets (or the files containing the leaked secrets) in the analyzed network traces?
2. Can you explain how the leaked secrets have been retrieved from the storage server?
3. Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the secrets ended up in Tim's computer?
4. What can you tell about the identity of the person(s) responsible for leaking the secrets?

Note: Given that this exercise was emulated in a virtual environment, i.e., we used virtual machines interconnected by virtual networks running on a single host, the network configuration has been greatly simplified when compared with a real world setting. For example, there are no firewalls deployed in the networks and no NAT translation is in place. For the sake of simplicity, you should assume hypothetically that the private IP addresses associated with the stakeholder's computers are public IP addresses.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is December 13th. Until then, you must upload to Fenix a compressed zip file containing three deliverables:

- **Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend that you use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All relevant evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.
- **Auxiliary Items:** Programs, scripts, and additional documents that you have produced during the investigation which are important to justify your results must also be included.

Good luck!