INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

FAKE NASA – Stage III

2022/2023

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment will conclude the investigation of the “Fake NASA” case. After analyzing the hard disk images of two computers found in Carl Seagal’s residence (Lab Assignment II), you will need to investigate the computer network of NASA’s headquarters in Washington, DC. This examination aims to assess the authenticity of the documents obtained by Prof. Seagal and determine if (and how) they were leaked from NASA’s facilities. To carry out this task, you need to analyze network traces available from the course website. As in the previous assignment, we suggest you to use Kali to solve this exercise.

Scenario presentation

In the previous assignment, you have made some considerable progress, but the results are still inconclusive. By analyzing Prof. Seagal’s workstation and backup server, you found evidence that: (1) the backup server contained copies of the documents hidden inside the pen drive, (2) these documents were transferred there from the pen drive, and (3) the pen drive was given to Carl Seagal by a third party, someone by the name of Megan Polanski. This third finding, in particular, is supported by a few email exchanges and IRC messages between Prof. Seagal and an individual identified by the email address “`megan.polanski@mail.com`” and the IRC username “`MPolanski`”, respectively. These messages suggest that they had arranged a meeting where Megan handed over the pen drive to Prof. Seagal.

During an interrogation session, the FBI confronted Carl with these findings and he confirmed the identity of this person. Megan Polanski is an old friend of his. They studied together at MIT in the nineties. After graduating in Computer Science, Megan worked at Google for several years and was recently hired as the technical director of NASA aeronautics department in Washington, DC. She is married to Chris Cox, who incidentally holds the position of associate administrator at NASA’s headquarters.

Based on this information, the FBI decided to pursue the investigation by following their lead on Megan Polanski. Holding a search warrant, they made their way to NASA’s headquarters looking for evidence of document exfiltration authored by Megan. The FBI team – you included – met with Roy Pinto, the head of the IT department. Roy helped you to learn the topology of the local network infrastructure and gave you access to forensic material that might help discover if and how the documents were stolen.

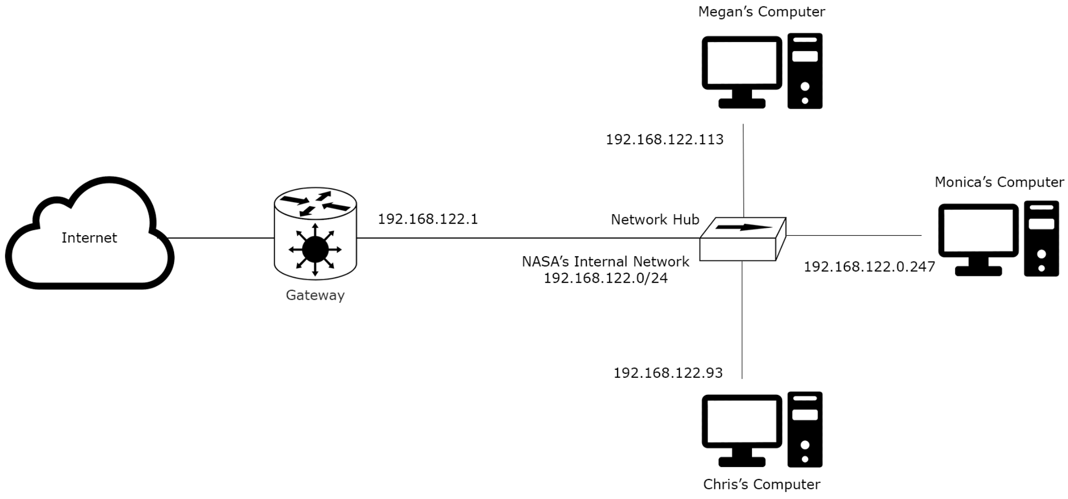

Figure 1: Diagram of the simplified network topology at NASA’s headquarters.

The figure above shows the reconstruction of the topology of NASA headquarters’ network (simplified). This network has a gateway which implements both a router and a HTTP Proxy (192.168.122.1), Chris's computer (192.168.122.93), Monica Sky's computer (192.168.122.247) and Megan Polanski's computer (192.168.122.113). Ms. Monica Sky is the personal assistant of Chris. Luckily, for security reasons, the HTTPS Proxy has also been configured to collect periodic traces of the network traffic. Roy managed to give you access to: (1) a network trace, and (2) the HTTPS proxy key file, all obtained sometime before the actions investigated in the previous assignments. The HTTPS proxy key file enables forensic analysts to decrypt the traces of HTTPS traffic intercepted by the proxy. This file can be provided directly to Wireshark. Both artefacts are enclosed inside a zip file that can be downloaded from:

- `https://turbina.gsd.inesc-id.pt/csf2223/project/csf-lab3-artifacts.zip`

Roy has also confirmed the following e-mail addresses:

- Megan Polanski - `megan.polanski@mail.com`
- Chris Cox - `chris.nixon.cox@mail.com`
- Monica Sky - `monica.lsky@mail.com`
- Roy Pinto - `roy.pinto@mail.com`

In this exercise, your job is to analyze the digital artifacts provided above 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 documents in the analyzed network traces? What can you tell about the source and authenticity of these documents?
2. What can you tell about the identity of the person(s) responsible for leaking the secrets?
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 Carl Seagal's computers?
4. From all the collected evidence in this investigation, what can you deduce about the motivation of the actor(s) responsible for the data exfiltration?

Note: Given that this exercise was emulated in a virtual environment, please consider that:

1. We used virtual machines interconnected by virtual networks running on a single host. As a result, 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.
2. The trace collection started really on October 22th. Therefore, the absolute timestamps recorded within the provided digital artifacts are skewed by 3 weeks in comparison to the timestamps of Lab Assignment II. For the purpose of your timeline, you must adjust the times of this trace to match those of the previous assignment (subtract those 3 weeks, i.e., 21 days).

Deliverables

Write a forensic report that describes your findings. The deadline for this work is November 4th. 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!