INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

FOOTBALL LEAKS – Stage III

2021/2022

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment will conclude the investigation of the case "Football Leaks". After having analyzed the hard drive images of the two computers located in Charles Daniels' residence (Lab Assignment II), in this exercise, you will need to investigate the computer network of the Red Hawks FC. This examination aims to finally assess the authenticity of the documents found in Charles Daniels' possession and determine if (and how) they have leaked from the Red Hawks FC. To perform this task, you will need to analyze some network traces that can can be downloaded from the course website. Just like in the previous assignment, we suggest you use Kali for performing this work.

Scenario presentation

Despite some important steps taken in the previous assignment, the results are still somewhat inconclusive. In fact, after analyzing the hard disk images of Charles Daniels' workstation and backup server, you found evidence that: (1) copies of the documents hidden inside the pen drive existed on these computers, (2) these documents reached those computers via the pen drive, and (3) Charles Daniels was given the pen drive containing the relevant documents by a third party. This third finding, in particular, is backed by a sequence of message exchanges between Charles and an individual using the Internet Relay Chat (IRC) system. The content of these messages suggests that this unknown individual may have accessed Red Hawks FC's systems and exfiltrated said documents. The investigators presented these evidences to Charles during an interrogation session and he identified this individual to be his girlfriend, Abby Chapman, who is a recent graduate of Computer Science doing an internship at Red Hawks FC.

To investigate the hypothesis of document exfiltration from Red Hawks FC, the digital forensic team – you comprised – head their way towards Red Hawks FC's facilities in possession of a warrant and meet with Frederick Balconies, the chief network administrator. You ask Frederick for relevant information and any available forensic material that can help you reconstruct the sequence of events that may have led to the exfiltration of the documents from Red Hawks FC.

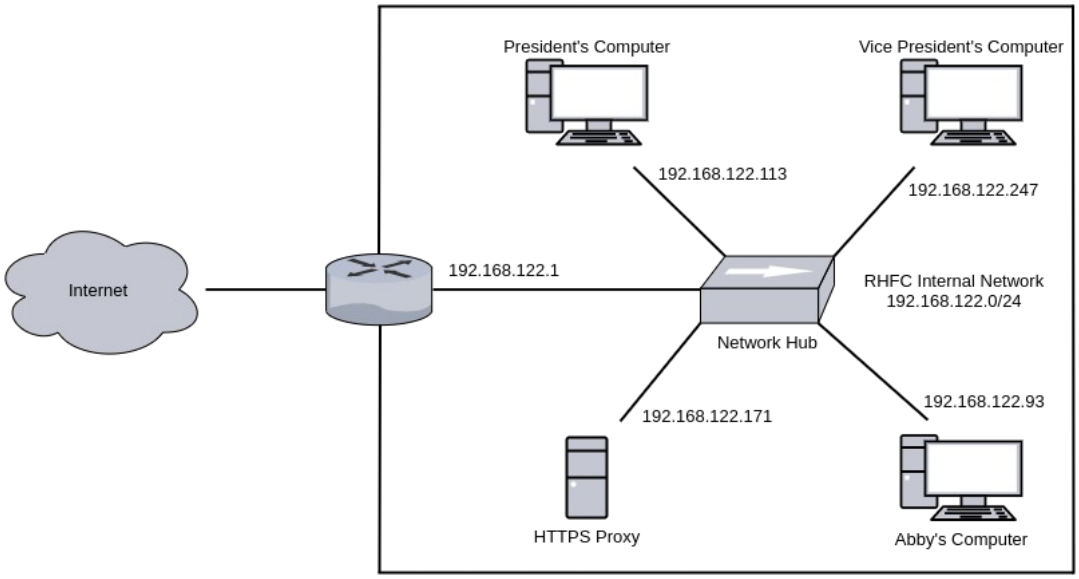

Figure 1: Diagram of the network topology covering the Red Hawks FC's network.

The figure above shows the reconstruction of the topology of Red Hawks FC's internal network (simplified). This network has one gateway router R (192.168.122.1), an HTTPS Proxy (192.168.122.171), Levy Fran Velucci's computer (192.168.122.113), Ryan Coast's computer (192.168.122.247) and Abby Chapman's computer (192.168.122.93). Mr. Ryan Coast is the Vice President of Red Hawks FC. Luckily, for security reasons, the HTTPS Proxy has also been configured to collect periodic traces of the

network traffic. Frederick was able to give you access to two pieces of data: (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/csf2122/project/csf-lab3-artifacts.zip

Additionally, Frederick also confirmed the e-mail addresses of some Red Hawks FC's collaborators:

- President Levy Fran Velucci - levyfvelucci@outlook.com
- Vice President Ryan Coast - ryancoast10@outlook.com
- Network Administrator Frederick Balconies - frederickbalconies@hotmail.com
- Intern Abby Chapman - chapmanabby1337@protonmail.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 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 Charles Daniels' computers?
4. What can you deduce from all the evidence collected in the context of the investigation? If the investigation was to continue, what should be the next steps to verify your hypotheses?

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 30^{th}. Therefore, the absolute timestamps recorded within the provided digital artifacts are skewed by two 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 two weeks, i.e., 15 days).

Deliverables

Write a forensic report that describes your findings. The deadline for this work is November 12^{th}. 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!