# INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

## FORENSICS CYBER-SECURITY

MEIC, METI

# Lab Assignment III

## DEEP BREACH – Stage III

2020/2021

nuno.m.santos@tecnico.ulisboa.pt

# Introduction

This assignment will conclude the investigation of the case "Deep Breach". After having analyzed the hard drive images of the two computers located in Rick Chick's residence (Lab Assignment II), in this exercise, you will need to investigate the computer network of XFarma. This examination aims to finally assess the authenticity of the documents published on PharmaLeaks and determine if (and how) they have leaked from XFarma. To perform this task, you will need to analyze some network traces that can can be downloaded from the course website. You will also have at your disposal a new vulnerability analysis framework named VulcaN for which you have contributed with your work in Lab Assignment I. This exercise will help you develop various skills, especially in traffic analysis and malware / software analysis. 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 Rick Chick's workstation and backup server, you found evidence that: (1) copies of the alleged email by Mr. John Carson and the technical report authored by Dr. Penelope Pearson existed on these computers, (2) that these documents have been downloaded from a Dropbox link, and (3) that Rick Chick has probably hired the services of a third party to obtain these documents on his behalf. This third finding, in particular, is backed by a sequence of email exchanges between Rick and an individual using the email address N16H70WL_services@protonmail.com. A plausible hypothesis suggested by the content of these emails is that this unknown individual may have hacked into XFarma's systems and exfiltrated said documents.

To investigate this hypothesis, the digital forensic team – you comprised – head their way towards XFarma's facilities in possession of a warrant and meet with Liam Sanders, the chief network administrator. Liam informs you that the only system available externally to the Internet was XFarma's website. This website was powered by Node.js and consisted of a web application written in JavaScript. You start wondering whether the potential hacker may have exploited a vulnerability in this web application to escalate its privileges into XFarma's network. In light of this possibility, you ask Liam 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 XFarma.

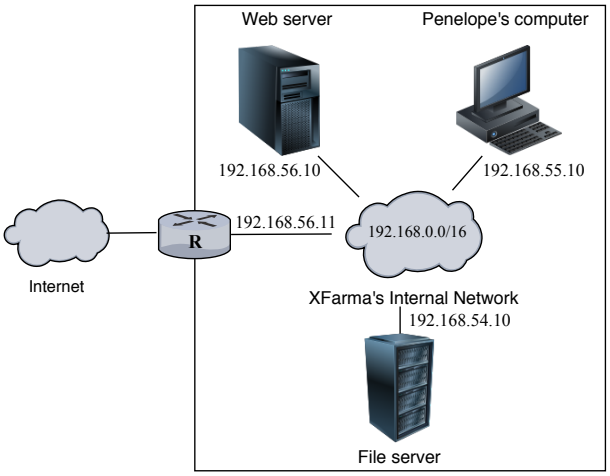


**Figure 1:** Diagram of the network topology covering the XFarma network.

The figure above shows the reconstruction of the topology of XFarma's internal network (simplified). This network has one gateway router R (192.168.56.11). In addition to the web server (192.168.56.10), there are two machines connected to this network: Penelope's computer (192.168.55.10) and a file server (192.168.54.10). The file server is a dedicated server for storing the classified data in XFarma. It can be

accessed over SSH by accredited users. Luckily, for security reasons, the gateway has been configured to collect periodic traces of the network traffic, and Liam was able to give you access to some traces obtained from the gateway (R) sometime before the documents have been exposed. These traces can be downloaded from:

- https://turbina.gsd.inesc-id.pt/csf2021/project/xfarma-trace.zip

Unfortunately, due to data collection restrictions imposed by the warrant, it was not possible to obtain a hard disk image of any of these machines. Analyzing the web server, in particular, would help determine the source of the hypothetical breach. Nevertheless, to overcome this limitation, Liam was able to give you the source code of the web application deployed on XFarma's web server. To further help you analyze potential vulnerabilities in this application, you can use a new tool that we collectively developed in Lab Assignment I: VulcaN. VulcaN is a framework that allows you to look up information about vulnerabilities in *npm* packages. As a result of your effort (and our manual validation), it is possible to use VulcaN to determine the sources and sinks of reported vulnerabilities. This information is instrumental to help identify potential attack vectors on a given application. (Watch this demo to learn how to start, stop and use the framework). You can obtain the web application and VulcaN from:

- https://turbina.gsd.inesc-id.pt/csf2021/project/xfarma-webapp.zip
- https://turbina.gsd.inesc-id.pt/csf2021/project/vulcan-framework.zip

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 solid evidence that the web application has been exploited?
2. Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the authenticity of the documents that appeared on PharmaLeaks?
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 Rick Chick's computers?
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 $11^{th}$. 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!