LIGHTHOUSE LABS

FINAL PROJECT - STUDENT GUIDELINES

Table of Contents

Date: February 2022

Version: 1.0

Introduction

Welcome to your final project! This project consists of a scenario where a company has received a potential threat and you are brought in as the Security Consultant to investigate the cyber security incident. In this document, you will find instructions, guidance, and key resources to successfully complete the project.

Technical Prerequisites

As part of this investigation, you will need to install a few basic tools on your computer that will aid you with analyzing the artifacts.

1. **Packet Analyzer**
    a. Wireshark (https://www.wireshark.org/download.html/)
    Available for Windows, Linux, and MacOSX operating systems

2. **Text Editor (any of them)**
    a. Notepad++ (https://notepad-plus-plus.org/downloads/)
    Available for Windows operating systems

    b. Sublime Text (https://www.sublimetext.com/3)
    Available for Windows, Linux, and MacOSX operating systems

Install the listed tools for your operating system type and ensure they can run properly. All tools are free and do not require any special licensing.

Scenario

Premium House Lights, Inc, an Ontario-based boutique company that sells and installs luxury lighting for upscale buildings, has received a suspicious extortion email to the company's Customer Support mailbox. Premium House Lights hired you as the Security Consultant to support them with the investigation of this potential incident.

The extortion email sent to the support mailbox states the following:

```
From: 4C484C@qq.com
To: support@premiumhouselights.com

Hello,

We will go right to the point. We are in possession of your
database files, which include sensitive information about your
customers.

You wouldn't want this information to be out on the internet,
would you? We will release this information on
https://pastebin.com if you don't deposit 10 BTC to the following
wallet ID:

                    1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

by Monday at 10:00AM UTC.

To demonstrate to you that we aren't just playing games, here is a
snippet of your customer database table:

+------------------+-----------------+--------------+
| contactFirstName | contactLastName | phone        |
+------------------+-----------------+--------------+
| Carine           | Schmitt         | 40.32.2555   |
| Jean             | King            | 7025551838   |
| Peter            | Ferguson        | 03 9520 4555 |
| Janine           | Labrune         | 40.67.8555   |
| Jonas            | Bergulfsen      | 07-98 9555   |
+------------------+-----------------+--------------+

Now the ball is in your court to make the right decision and take
action. There will be no negotiations on the price.

// The 4C484C Group
```

Currently, Premium House Lights does not know if the claims in the email are true, and they are also not sure if they have been compromised. Premium House Lights is interested in having a full Root Cause Analysis done, along with a detailed report.

Environment Artifacts

Premium House Lights provided network, application, and database artifacts that were collected during and after the alleged incident, to help you with the investigation:

- **Company Network Diagram**
  - *phl_network_diagram.png*
- **Wireshark Captures**
  - *phl_webserver.pcap*
  - *phl_database.pcap*
- **Application Access Logs**
  - *phl_access_log.txt*
- **Session Logs**
  - *phl_database_shell.txt*
- **Database Logs**
  - *phl_database_access_log.txt*
- **Database data**
  - *phl_database_tables.db*

Note: All artifacts are safe to download and analyze, they do not include any malicious files.

Instructions

The Root Cause Analysis report that you need to produce should be able to tell a story about the attack and be built in such a way that allows both technical and non-technical audiences to understand what happened and what is the path towards resolution.

The report should include the following sections and subsections:

1. Executive Summary
2. Incident Timeline
3. Technical Analysis
   a. Attack origin
   b. What happened (with the related evidence)
   c. What was accessed
   d. When were things accessed
   e. Insight into the hacker’s attack methodologies
   f. What and where were the weaknesses that allowed for this incident to occur
4. Recommendations
   a. Ransom payment guidance
   b. Steps to contain & remediate the incident
   c. Steps to recover & restore business functions

    d. Post-incident recommendations: how should the company protect itself against such attacks in the future
5. Appendix

Note: Use the *Root Cause Analysis Template* to structure your reports. You will need to make a copy of the document in order to fill it in.

Guidelines

In real-life security breach scenarios, analysts often don't have a clear picture or complete information to understand exactly what happened in a breach until they start diving into the investigation itself. You will need to use all the information you have and draw conclusions based on the evidence collected during the investigation.

Here are some high-level recommendations as you go about this project:

1. Take your time and investigate each artifact.
2. Understand what story the logs tell, and how this may help shed light on the incident.
3. Pay attention to the order of events based on timestamps to build a more accurate incident timeline.
4. Use external resources (linked at the bottom of this document) to get inspiration on how to carry out a post-mortem analysis if you get stuck or have no leads.
5. The company in this scenario provided some initial information, however, it's important to note that companies may not always have a clear understanding of what they have running in their networks, or how things are configured.

Evaluation

The project will be evaluated as pass or fail, however, it will include comprehensive qualitative feedback. The purpose of the qualitative feedback is to understand how well overall the report went as well as where you can improve in the future. This is also an opportunity to add a relevant project to your portfolio to help impress potential employers/ show them your process for handling this type of scenario.

The project should be submitted in the Final Project Info doc in PDF format (not through Docebo).

DUE DATE: Week 11, Day 3.

Bonus Task: Design a Secure Network

******This is a bonus task and is NOT mandatory. It should only be performed once the assignment has been fully completed and does not count towards the requirements of the project.******

How would you recommend the company design its network differently? What would the ultimate network security design look like that would improve the company's overall security posture?

Build a diagram of a strongly secure network which would greatly enhance the chances that such a company never experiences this incident again. Make sure you annotate it properly to detail each component & security control fully.

Note: The diagram must be delivered in PDF format.

Useful Resources

There are a variety of online resources you can refer to for inspiration when writing a report. As previously mentioned, you can use the template provided to create your report, or, you can create a custom template that works for you as well. What matters is that the important information is captured.

Post Mortem Templates

- Root Cause Analysis Template for Students (provided separately)
- GitHub Post Mortem Template Repositories
- Atlassian Post Mortem Template

Breach Post Mortem Reports from Project Days in Bootcamp:

- Equifax Post Mortem Analysis Report
    - GAO Report
- Target Post Mortem Analysis Report
    - Kill Chain Analysis of the Target Breach
- Capital One Breach Case Study
    - Technical Analysis

Packet Analysis Cheat Sheets

- Wireshark Cheat Sheet #1
- Wireshark Cheat Sheet #2