Microsoft Defensive Cybersecurity Training

Windows security

Final Project

November 2019

Contents

Windows Security – Final Project **1**

Abstract 1

The Story 1

Content 2

Deliverables 2

Evaluation Method 3

Windows Security – Final Project

Abstract

In this project you will play the role of a Security Consultant hired by the Fabrikam company. Fabrikam was recently the victim of a targeted intellectual property theft. Your mission will consist in 2 parts. First, you will deliver a forensic report and then, present a remediation plan.

The Story

Fabrikam is one of the largest steel firm in the world. It is a global company, employing nearly 200,000 people worldwide and present in every major economic area. Company's yearly revenue is around $50 billion.

For the past decade, Fabrikam has worked hard to design special steel products to fit highly demanding markets like space industry or nuclear power plants. All this R&D work is what makes the business value of Fabrikam.

Two months ago, the company was on the point to publicly announce a new kind of steel alloy which could endure extremely high temperatures with limited physical deformation. This industrial breakthrough is what could make nuclear fusion a commercially viable reality for production of electricity.

Unfortunately, few days before the announcement, one of the competitors of Fabrikam announced a similar product which they plan to sell at half the price of Fabrikam's. Soon, it was clear in the mind of Fabrikam leaders that their intellectual property had been stolen. Internal investigations demonstrated that the password of the lead researcher, in charge of the project, was compromised and suspicious authentications from his user account were reported on the main server. This machine is hosting all the data for the project.

As soon as the relation between the data breach and the incident regarding researcher's password was made, Fabrikam's security officer requested that a full memory dump of the user's laptop be captured and mandated your company to perform a forensic analysis. Because the laptop was never restarted, he expects that any trace of potential malware infection be kept intact.

Alongside with the forensic analysis, Fabrikam's security officer also asked you to drive a project to enhance the security of Fabrikam's workstations.

From organizational point of view, there is a central IT division in charge of providing recommendations, guidance and governance. But each company branch has its own environment (including own AD forest) and its own IT department tasked with administration and security operations. There is no real cooperation between IT departments and the central IT team. This is something you may have to deal with.

Content

All content is available at https://mscsecstrg.blob.core.windows.net/public/WinSec_ECE_2019.zip

The archive contains:

- Memory dump you will analyze
- Public symbols for the dump
- Windows Debugger (WinDBG). Provided as convenience, you are free to use another version if you've already installed one.
- MSInfo32 export. Will help to map devices with their drivers.

Deliverables

The expected deliverables are:

- The forensic report
  - This is a written report you will deliver in electronic format (aka. no paper print)
  - The scope of the report is only the memory dump analysis. Don't ask customer for any other element.
  - The more insights from the attack you can provide, the higher your grade
  - Every aspect you reveal about the attack must be supported by a technical analysis
  - Any analysis you perform must be repeatable based on your writings so that other expert can check your work. Be explicit about how you work.
  - Remember that you are selling your expertise, the more expert we think you are, the higher your grade. Do not hesitate to explain all aspects of the attack so that even a non-technical person can understand it.
  - You are free to choose the structure but, report must include:
    - how the attack works
    - how we can detect it
- A PowerPoint-like presentation. The content of the presentation is completely up to you, but it must include:
  - A risk analysis
  - Clear relation between the risks and associated mitigations with a clear explanation on how the proposed solutions will mitigate the risks
  - Macro planning for the deployment of your solution, including all major phases of the project
- A 12 minutes oral presentation of your proposal

Accepted formats for the presentation are PowerPoint or PDF.

The presentation will occur on December 13th. You will use the presentation to support your talk.

Each group will have exactly 12 minutes to present its work. At the end, you will leave the forensic report and the presentation file. 12 minutes is a short time period.

You are expected to be on time. Any late arrival will be decremented from your 12 minutes allocation.

Presentation will be performed in French.

There will be 1 Q&A exchange with the customer. The process to ask questions is:

1. Formalize the list of questions you have for the customer in an Excel, Word or text document
2. Send it to the customer before December 2nd 23:55
3. Customer will answer questions starting on December 3rd

Q&A constraints:

- You can upload as many questions as you want but customer will only read the last uploaded document
- Customer won't answer any question sent after December 3rd

Evaluation Method

This paragraph explains how your work is going to be evaluated during the presentation session.

At all time, keep in mind that the goal of the project is to train yourself into real-life delivery of a security project. It particularly means that you must not underestimate the non-technical aspects of the project.

Important criteria which will determine the success or failure of your performance:

- Ability to demonstrate relevance of any technical product or functionality. Security costs money and the organization won't spend money in a solution if it does not see the value.
- Ability to demonstrate knowledge of security threats, products or features by being able to explain it in a concise and simple way to a non-expert public (CIO, CISO, …) in a very short amount of time
- Ability to understand the complexity of solutions by being able to determine a reasonable amount of effort to deploy proposed technology
- Presentation skills