**Internal Memorandum**



**To: Dr. Regner, CISO**

**From: Ahmed Almass and Mike Carlson**

**RE: Virtual Lab for Malware Analysis**

**2018-10-23**

**Introduction**

Further to our recent discussion, in your offices on Tuesday, October 23rd, 2018; the ISS group has put together the following project plan for your proposed internal malware analysis lab. You have asked us to *design and implement a virtual lab to perform basic and advanced malware analysis and to demonstrate its effectiveness* to management by December 10th, 2018.

**Purpose**

As you know, our specialized accounting services for the para-military community requires a high level of discretion for our clients. Working in hostile political and operational environments means there is a high chance of malware in their accounting submissions. Our company must be prepared to deal with the receipt of malware infected files from our clients in-house. Although we are required to provide Revenue Canada with documented expense statements, the information is legally protected. Never-the-less, the information contained therein could compromise our clients in ongoing operations in foreign jurisdictions, if it were to be leaked from our offices. We can expect nation-state level hacking attempts from foreign governments. Our reputation for dealing with Revenue Canada and providing secure accounting service is the core of our business (excuse the triple entendre!).

The objectives are therefore twofold:

* Investigate malware infections within our organizational environment; and,
* identify what data may be compromised and ex-filtrated during any malware infection.

**Physical Requirements**

The minimum physical requirements outlined, in our meeting, for the lab were:

1. A Virtual network
2. Virtual Machine # 1 for launching malware attacks
3. Virtual Machine # 2 for launching malware attacks
4. Virtual Machine for static analysis
5. Virtual Sniffer machine
6. Antivirus/Antimalware tools

**Resources**

The project currently has no formal budget and involves the two staff assigned to the project: Messr’s Almass and Carlson. Since the project has no formal budget and there is a limited time frame it is intended that materials will be obtained from existing computer resources and those that can be purchased with petty cash requisitions, which means individual purchases that are individually under $1,000.00 in Canada or $1,000 from foreign jurisdictions. The budget is detailed on the attached spreadsheet.

**Project Organization**

Most of the work in the company is organized with a traditional project management system. This system has served the company very well with accounting services that are typically repetitive from year to year. In the case at hand, the company, and our department, has not built a malware lab previously and it is proposed that an alternative procedure be used. The suggested procedure is the Agile development program, which now dominates software development.

There are some very fundamental differences. Although there is defined structure to Agile Development, the process is far more iterative. Short term goals, of limited scope, are picked in a series of “sprints”. The goal is to have an operational product being developed, even if it is limited in scope. When the sprint is completed, the progress is reviewed, objectives reset and adjustments made based on the cumulative experience developed on the project to date. This system has proven to be the most effective in IT product development over the last two to three decades.

A rough project plan was discussed during our meeting, with the following objectives:

|  |  |  |
| --- | --- | --- |
| **School Fall Term Week:** | **Objective:** | **Submisson Date:** |
| Week 8, Oct 22-28 | Report 1: Project proposal (3%) | Oct 29 |
| Week 9, Oct 29-Nov 4 | Report 2: Network configuration and diagrams (2%) | Nov 5 |
| Week 10, Nov 5-Nov 11 | Report 3: Machine configuration and diagrams (1%) | Nov 12 |
| Week 11, Nov 12-Nov 18 | Report 4: Tools for the virtual lab (1%) | Nov 19 |
| Week 12, Nov 19-Nov 25 | Weekly report 5: Malware sample selection and justification (1%) | Nov 26 |
| Week 13, Nov 26-Dec 2 | Weekly report 6: Basic analysis guidelines (1%) | Dec 3 |
| Week 14, Dec 3-Dec 9 | Weekly report 7: Advanced analysis guidelines (1%) | Dec 9 |
| Week 15, Dec 10-14 | Delivery of final project report (15%),  Project presentation + demo (10%) and Project assessment (20%) | Dec 1 |

A Gant chart has been prepared based on the above, as shown below and on the attached. However, this should be regarded as a rough outline and not a strict plan, in keeping with Agile development.

****

**Summary**

On Tuesday, October 23rd, 2018, CSO assigned our team to *design and implement a virtual lab to perform basic and advanced malware analysis and to demonstrate its effectiveness* to management by December 10th, 2018. There are two main objectives investigate malware infections within our organizational environment, identify what data may be compromised and ex-filtrated during any malware infection.

In terms of project management our team will be using agile software development structure method. To keep on track there will be a weekly task. This means a weekly meeting to review progress and a second part to set the goals for the next “sprint”. There will be a weekly summary report until the project is complete.

The project will have need some resources. The estimated budget for the resources is $3,240.00. The budget may change. However, if it is apparent that it will be a significant upward change, i.e. more than 10 percent, we will notify you for your approval. The budget will cover servers, routers, switches, resource hackers, IDA Pro, input and output devices. It is intended that the lab will be located in the basement where there is existing space for a lab.

As with all projects of this scale, it is often difficult to predict which methods will be necessary to address any unforeseen obstacles and inaccuracies that may arise. Any methods that are introduced into our research later on will be outlined and elaborated on in our final report.

**Personnel**

Ahmed Almass Malware analyst

Email address: ahmed.almass@edu.sait.ca

Phone number (403) 667 1234

Mike Carlson Manager Malware analyst

Email address: mike.carlson@edu.sait.ca

Phone number (403) 399 7151

**Authorization**

Thank you for taking the time to review proposal. Please indicate your approval below. If you have any questions or concerns, please contact us directly at the coordinates above.

**CSO Project Management Project Management**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Regner Mike Carlson Ahmed Almass

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mercenary Accounting Corps Ltd.** |  |  |  |  |
| **Proposed Malware Analysis Lab** |  |  |  |  |
|  |  |  |  |  |
| **Budget Item** |  |  |  | **Amount** |
| HP-DL380 Gen 5 from ERA (used) |  |  |  | $300.00 |
| HP-DL380 Gen 6 from ERA (used) |  |  |  | $300.00 |
| 2 x HP-DL380 Gen 7 from ERA (used) |  |  |  | $300.00 |
| 3 x HP-DL-580 Gen 7 (ex SANs) |  |  |  | $0.00 |
| Monitors, Keyboard, Mice and hard drives |  |  |  | $500.00 |
| IDA Pro (USD – purchased from Belgium) |  |  |  | $1,000.00 |
| PfSense firewall (free ware) |  |  |  | $0.00 |
| OllyDebug |  |  |  | $0.00 |
| Sysinternals (Microsoft) |  |  |  | $0.00 |
| Programming Tools |  |  |  | $200.00 |
| ClamAV (freeware) |  |  |  | $0.00 |
| Burp Suite commercial edition |  |  |  | $250.00 |
| Router and switch also from ERA |  |  |  | $200.00 |
| Variety of OS’s |  |  |  |  |
|  | Kali OS |  |  | $0.00 |
|  | VMware ESX | SAIT licence | |  |
|  | Parrot | free |  |  |
|  | Windows 10 | (Memory Express) | | $140.00 |
|  | Windows 8 | SAIT licence | | $0.00 |
|  | Windows XP | SAIT licence | | $0.00 |
|  | Ubuntu 18 |  |  | $0.00 |
|  | Ubuntu 16 |  |  | $0.00 |
|  | Ubuntu 14 |  |  | $0.00 |
| Hiew |  |  |  | $0.00 |
| Resource Hacker |  | (buy full edition) | | $50.00 |
|  |  |  |  |  |
|  |  |  |  | **$3,240.00** |