**Internal Memorandum**



**To: Regner Sabillon, CISO**

**From: Ahmed Almass and Mike Carlson**

**RE: Weekly Report 4 – Malware Lab**

**2018-11-12**

**Introduction**

The lab currently has two victim virtual machines and one Kali analysis/sniffer machine. The virtual lab will eventually have a series of tools to analysis the malware; which will cover both malware techniques, static and dynamic. The REMnux with inet have also been installed.

Based on the provisional timetable below, we appear to be still more or less on

|  |  |  |
| --- | --- | --- |
| **School Fall Term Week:** | **Objective:** | **Submission 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 |

The budget has not changed. Some changes have been made to the backlog list – for items completed.

Cheers,

Ahmed Almass Malware analyst

Email address: [ahmed.almass@edu.sait.ca](mailto:ahmed.almass@edu.sait.ca)

Phone number (403) 667 1234

Mike Carlson Manager Malware analyst

Email address: [mike.carlson@edu.sait.ca](mailto:mike.carlson@edu.sait.ca)

Phone number (403) 399 7151

|  |  |
| --- | --- |
|  |  |
| **Analysis Tools:** |  |
| **ApateDNS v1.0** | on Win 7 vm |
| **Autoruns v13.51** | on Win 7 vm |
| **Process Explorer V16.1** | on Win 7 vm |
| **Process Monitor V3.20 (ProcMon)** | on Win 7 vm |
| **CaptureBAT V2.0.0-5574** | on Win 7 vm |
| **CFF Explorer x86** | on Win 7 vm |
| **Dependency Walker v2.2.6000** | on Win 7 vm |
| **Exeinfo PE v0.0.4.2** | on Win 7 vm |
| **FileAlyzer V2.0.5.57** | on Win 7 vm |
| **McAfee FileInsight V2.1 Hex Editor** | on Win 7 vm |
| **Hex Editor Neo V6.20 Hex Editor** | on Win 7 vm |
| **IDA Pro Free V5.0** | on Win 7 vm |
| **Md5deep - Windows** | on Win 7 vm |
| **OllyDbg V1.10 - 32-bit** | on Win 7 vm |
| **OfficeMalScanner V0.54** | on Win 7 vm |
| **OleDump** | on Win 7 vm |
| **Peid V0.95** | on Win 7 vm |
| **Pestudio 8.54** | on Win 7 vm |
| **PEView V0.9.9.0** | on Win 7 vm |
| **Regshot V1.9.0 x86** | on Win 7 vm |
| **Rekall V1.5.2 Furka x86** | on Win 7 vm |
| **Resource Hacker V4.2.5** | on Win 7 vm |
| **Mandiant Memoryze V3.0** | on Win 7 vm |
| **Upx V3.91 - Packer** | on Win 7 vm |
| **WinDbg V6.11.1.404 - Windows Debugger** | on Win 7 vm |
| **Wireshark Win32 V1.10.1** | on Win 7 vm |
| **Burp Suite Pro** | on Win 7 vm |
| **iNetsim** | Independent vm |