Malware Analysis: Fall 2021

Final Project: Virtual Lab for Malware Analysis

Objective

Design and implementation of a virtual lab to perform basic and advanced malware analysis

Purpose

You will often be required to investigate malware infections within any organizational environment, and as a cybersecurity professional, you might also be asked to identify what data could have been compromised and exfiltrated during any malware infection.

Scenario

Your CISO has asked your incident response team to prepare a proposal to design and implement an in-house virtual laboratory to start analysing malware utilizing static and dynamic approaches. The CISO has anticipated no external resources to complete this project. This project has to be completed in eight weeks and all deliverables must be completed by the end of the second week of December 2018. Project success will be evaluated on weekly reports, completion of project phases and tasks, performance and acceptance. You team communication and task coordination are key factors to ensure project success.

Project Requirements

Your project must include the following:

1. Initial research and planning
2. Setup, configuration and architecture of virtual lab (Minimal configuration):

   Virtual network

   Virtual Machine # 1 for launching malware attacks

   Virtual Machine # 2 for launching malware attacks

   Virtual Machine for static analysis

   Virtual Sniffer machine
3. Selection and justification of malware analysis tools including:

   Antivirus/Antimalware tools

Sandbox tools

Debugger tools

Packet capture tools

Disassembler tools

Packing programs

Decompiler tools

Any additional tool to complete your malware analysis

4. Basic and Advanced analysis of your Malware samples (At least 2 samples):

   Analysis of Malware sample # 1

   Analysis of Malware sample # 2

   (Additional samples will be required for groups that have more than two members)

   You can select malware samples from the textbook, from the ones provided by the instructor or you can provide your own samples

5. Findings and Conclusions of your project

6. Glossary

7. References : APA Style

8. Appendices: As desired

   Appendix A shall include tools and techniques used to complete the malware analysis like screenshots, scenarios and any outcome that helped to complete your analysis.

Project Schedule

Weekly reports must be submitted on the due date. Late submissions will not be accepted

Week	Deliverables	Due date
Week 10 Nov 7-13	Weekly report 1: Project proposal (3%)	Nov 11
Week 10 Nov 7-13	Weekly report 2: Network configuration and diagrams (2%)	Nov 13
Week 11 Nov 14-20	Weekly report 3: Machine configuration and diagrams (1%)	Nov 16
Week 11 Nov 14-20	Weekly report 4: Tools for the virtual lab (1%)	Nov 20

Week 12 Nov 21-27	Weekly report 5: Malware sample selection and justification (1%)	Nov 23
Week 12 Nov 21-27	Weekly report 6: Basic analysis guidelines (1%)	Nov 27
Week 13 Nov 28-Dec 4	Weekly report 7: Advanced analysis guidelines (1%)	Dec 3
Week 14 Dec 5-11	Delivery of final project report (15%), Project presentation + demo (10%) and Project assessment (20%)	Dec 10

Additional resources to complete your project will be uploaded to D2L on a weekly basis (Resources for final project).

Weekly reports must be submitted to D2L on or before due date (Project weekly report Week 8 – Week 14)

Final project reports must be submitted to D2L on Dec 10