Course Readings

Textbook
The Art of Memory Forensics by Ligh, Case, Levy, and Walters

References:

1. Intel documentation of IA-32 and x64 processors
2. Papers to be distributed by the instructor

Tools used:

- Hands-on with
  1. Various memory acquisition tools, such as dumpit, RAM capture, Memoryze, etc.
  2. Memory analysis tools, such as redline, WINDOWScope, etc.
  3. Volatility Framework (current version)

Course Description

This course is based on the intel processor architecture employed in Windows, Linux and MacOS operating systems. The student will learn how memory is assigned to processes, how memory data structures can be exploited by malware, and what is available for forensic analysis of memory. Students will do scores of Labs on recognizing process data structures in memory, memory acquisition, and use of a set of tools to catch the malware while preserving evidence from live memory analysis.

This is a 3 credit-hour graduate level course.

Goals and Objectives

As a result of this class a student should be able to:

1. Identify the use of virtual memory by operating systems as a protected mode in modern processor architecture
2. Use memory acquisition tools for Windows, Linux and MacOS
3. Recognize process memory block and vulnerabilities associated with it
4. Demonstrate proficient use of tools for detection and alienation of malware in memory while the computer is operating without losing its value as legally presentable evidence

How the Course Works

This online course employs several methods of delivery and learning activities including online lectures and presentations, reading and written assignments, examinations, e-mail, and electronic access of information. The course is designed around seven modules. It is important to pay attention to the varying length of each module.
Grading Criteria

Grading Assessments (Note: A grade rubric will be provided for each assessment)

Please Note: All sections will do exactly the same assessments. Instructors may use additional resources in their emails to students.

A typical rubric for reports consists of:

- how focused the discussion is
- at least two scientific citations and references
- language accuracy
- description accuracy

A typical rubric for Labs will include:

- accuracy of results
- accuracy of analysis
- error-free language

Grading Scale:

- A = 900-1000 points
- B = 800-899 points
- C = 700-799 points
- F = 0-699 points

List of all assessments:

1. Understand intel-IA-32 memory address management, register functions and FLAGS. Write a program to convert between linear and physical memory addresses. **Week 1-2**

2. Obtain a memory dump from website and apply a given tool to extract key information from it.
- Use itto to get a memory dump from your computer.
- This should not be in the raw format--Use another tool to convert the dump into raw format.

4. Use a privilege analysis tool and analyze a rootkit.

5. Analysis of the process environment block (PEB), communications ports and Windows registry for malware hunting.


7. Rootkit detection techniques.

8. Disk artifacts from memory, event reconstruction, and timelining.

10. Do a project to demonstrate the ability to handle a case independently / set up lab.

**Student Responsibilities**

**Time Management**

Students are expected to spend 10 hours per week on the course materials and assignments. Out of 10 hours, students are expected to spend approximately 3 hours per week to read the material and another 3 hours/week for the homework and discussions.

**Attendance**

Since this is an on-line course, there is no mandatory attendance policy. However, students are expected to actively participate in the discussions, homework submissions, and journal writing. Each of these components is graded and counted toward the final grade.

- If an extraordinary situation has occurred that requires your time and attention which will prevent submitting your work on time, please notify your instructor.

**Utilizing Online Components**

Refer to the START HERE section within the Blackboard menu.

**Course Policies**

**Online Classroom Conduct (Netiquette)**

Students are expected to follow good Netiquette rules. Netiquette is the accepted behavior for online participation. The following is a list of general guidelines for this course:

- Check your grammar and spelling
- Keep your comments focused on the topic
- Strive to write succinctly and clearly
- Share your knowledge and include supportive evidence for your comments
- Do not use all capital letters as that is viewed as shouting
- Avoid flaming—disrespectful language is unacceptable

**Tests and Make-ups**

Exams will be proctored. The ODU policy regarding tests and make-up exams will be followed.

**Plagiarism and academic integrity**

University/ACM rules apply to academic integrity
The instructor may use Turnitin or similar tool(s) to check for plagiarism/cheating in reports.

**Course Disclaimer**

Every attempt is made to provide a syllabus that is complete and provides an accurate overview of the course. However, circumstances and events may make it necessary for the instructor to modify the syllabus during the semester. This may depend, in part, on the progress, needs, and experiences of the students.

**University Policies**

**Honor Pledge**

"I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community, it is my responsibility to turn in all suspected violators of the honor system. I will report to Honor Council hearings if summoned."

By attending Old Dominion University you have accepted the responsibility to abide by this code. This is an institutional policy approved by the Board of Visitors. For more information please visit the Honor Council.

**Educational Accessibility and Accommodations**

Students are encouraged to self-disclose disabilities that have been verified by the Office of Educational Accessibility by providing Accommodation Letters to their instructors early in the semester in order to start receiving accommodations. Accommodations will not be made until the Accommodations Letters are provided to instructors each semester.