

Teaching Plan

DESHPANDE ANAND RAVI

Oct 2022

Module Leader

Term

Module Name

MALWARE ANALYSIS TOOLS & TECHNIQUES

4

60

Credit Units

Contact

hrs

Wk

Begin Date

Topics

Activity/Session 1

Activity/Session 2

Assessment

1

17 Oct

Basic Static Analysis  
• Fingerprint  
• Packed Malware  
• PE Format  
• Imported Functions & DLLs

Self reading : Introduction to Malware   
  
Analysing Windows Malware  
  
Understand the essential Windows API calls made by malware to achieve specific functions such as Downloading, Hiding & creating a backdoor.  
  
Understand the basics of PE File  
format, and the PE life cycle.  
Understand basic PE identification  
techniques and techniques of  
evading packing

Analyze an unknown PE to  
determine  
• Is it packed?  
• APIs used  
• Functionality  
• What resources does it uses?

2

24 Oct

Basic Dynamic Analysis   
• Running a Malware  
• Monitoring a Process  
• Monitoring Registry  
• Monitoring Network Activity

Understand the basic Windows  
resources used by a malware: File  
R/W, Network Activity, Host  
Activity, Registry Activity

Analyze an unknown PE to  
determine  
• How to run the malware  
• Network activity  
• Host based indicators  
• What can prevent dynamic  
analysis

3

31 Oct

Assembly Language - Part 1  
• X86 Architecture  
• Instructions, Opcodes & Operands  
• Registers & Flags

Understand the basics of  
Assembly Language

Practical exercises : Creating  
simple Assembly Language  
programs.

Page 1 of 3

16 October, 2022

Last update:

• Conditionals

4

07 Nov

Assembly Language – Part 2   
• Branching   
• Loops   
• Function Calls   
• Reversing an assembly Program

Understand function calls & other programming structures: loops & branching

Graded In-Practical Assessment   
Perform Basic Static & Dynamic Analysis   
• Functionality   
• API used   
• Network Activity   
• Host Activity

Test 1 (15%)

5

14 Nov

Whitespace Activity - Understand the basics of Assembly Language

Whitespace Activity - Students practice on interpreting and writing simple assembly language programs.

Whitespace Activity - Students practice on interpreting and writing simple assembly language programs.

6

21 Nov

Advanced Static Analysis   
• Navigating IDA Pro   
• Analysing Functions   
• Graphing   
• Recognise C Constructs

Explore IDA

IDA Pro Practical to determine:   
• Major code constructs   
• Subroutines, parameters & purpose   
• Functionality of malware

7

28 Nov

Debugging Malware using OllyBDG   
• Single Step / Step Over   
• Hardware Breakpoint Conditional breakpoints   
• Memory Map

Explore OllyDBG

Debugging Malware to Find   
• Find Base address of dlls   
• Find Program specific details   
• Perform Patching

8

05 Dec

Examining malicious web pages and documents - 1

• Interacting with malicious  
websites to assess the nature of  
their threats  
• De-obfuscating malicious JavaScript using debuggers and interpreters

Introduction to tools such as Fiddler, SpiderMonkey, box-js, base64dump.py, pdf-parser.py, peepdf.py, scdbg, olevba.py, oledump.py, rtfdump.py, and  
jmp2it.

9

12 Dec

Common Test

Common Test

Common Test (30%)

10

19 Dec

Break

11

26 Dec

Break

12

02 Jan

Examining malicious web pages and documents -2

• Analyzing suspicious PDF files  
• Examining malicious Microsoft  
Office documents, including files  
with macros  
• Analyzing malicious RTF  
document files

Introduction to tools such as Fiddler, SpiderMonkey, box-js, base64dump.py, pdf-parser.py, peepdf.py, scdbg, olevba.py, oledump.py, rtfdump.py, and  
jmp2it.

Page 2 of 3

16 October, 2022

Last update:

13

09 Jan

In-Depth Malware Analysis -Part 1

• Recognizing packed malware  
• Getting started with unpacking  
• Using debuggers for dumping packed malware from memory

Graded In-Practical Assessment to  
examine malicious web pages and  
documents

Test 2 (15%)

14

16 Jan

In-Depth Malware Analysis -Part 2

• Recognizing packed malware  
• Getting started with unpacking  
• Using debuggers for dumping packed malware from memory

Introduction to tools such as Detect It Easy, Exeinfo Pe, Bytehist, CFF Explorer, Scylla, OllyDumpEx, ands Volatility.

15

23 Jan

ASSIGNMENT

ASSIGNMENT

ASSIGNMENT

Assignment 1 (40%)

16

30 Jan

ASSIGNMENT

ASSIGNMENT

ASSIGNMENT

Assignment 1 (40%)

17

06 Feb

ASSIGNMENT DEMO

ASSIGNMENT DEMO

ASSIGNMENT DEMO

Assignment 1 (40%)

18

13 Feb

Study & Exam Week

19

20 Feb

Study & Exam Week

Holiday:

Deepavali

24 Oct

-

Christmas Day

26 Dec

-

New Year’s Day

02 Jan

-

Chinese New Year

23 Jan

-

Chinese New Year

24 Jan

-

Nil

Notes on Teaching Plan:

Textbooks / Recommended Readings:

Sikorski, M., & Honig, A. (2012). Practical malware analysis: The hands-on guide to dissecting malicious software. San Francisco: No Starch Press.

Page 3 of 3

16 October, 2022

Last update: