

## CSCI 5345 – MALWARE ANALYSIS

**CREDIT HOURS:** 3

**PREREQUISITES:** Graduate Student status; may not be enrolled in undergraduate courses.

### CATALOG DESCRIPTION

Coverage of incorporating security technologies and methods into new and existing systems; learning how attackers expose vulnerabilities; analyzing threats; applying methods to prevent and defeat attacks; and understanding the ethical responsibilities and obligations associated with developing, acquiring, and operating software systems.

### PURPOSE OF COURSE

Learn the fundamentals of malware behavior, reverse engineering techniques, and how to use various tools to dissect and understand the functionality of malicious software. Gain practical experience in identifying different types of malware, understanding their impact, conducting comprehensive malware analysis, and developing strategies to prevent and respond to malware incidents.

### EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Describe the types of safety and security risks associated with network infrastructures.
2. Deploy appropriate countermeasures, such as layers, access controls, privileges, intrusion detection, encryption, and coding checklists.
3. Explain how adversaries are able to identify vulnerabilities and generate exploits for public and private software systems via operating systems and malware
4. Detect data exfiltration activities and conduct detailed analysis to describe the malignant logic and potential impacts.
5. Explain a variety of methods by which attackers can damage software or data associated with software via weaknesses in the design or coding of the system at the assembly level, or by infiltrating the OS with malware; and demonstrate or explain how to prevent such weaknesses.
6. Analyze threats to software systems and operational environments.
7. Design and plan for effective countermeasures such as access control, authentication, intrusion detection, encryption, and coding checklists.

### COURSE CALENDAR

This course meets for a minimum of 37.5 lecture contact hours during the semester. Students have significant assignments based on readings from the primary literature, participate in classroom discussions regarding current research topics, complete periodic homework and laboratory/programming assignments, and periodic exams in addition to the final exam. Students are expected to prepare for any class assignments

or quizzes over the material covered in class or in the reading material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

<b>CONTENT</b>	<b>Hours</b>
Introduction to Reverse Engineering.....	6
Overview and course introduction	
Common tools	
Assembly language	
File Formats .....	9
Executable files	
PDF files	
Macros	
Web files	
Static Malware Analysis .....	9
Disassembly	
Hashing, packing, and obfuscation	
Finding strings	
Imported and exported functions	
Dynamic Malware Analysis .....	9
Debugger	
Process monitoring	
Registry	
Patching	
Monitoring network traffic	
Analysis of Specific File Types .....	9
Malicious PDF analysis	
Malicious Macro analysis	
Mobile code analysis	
Malicious script analysis	
Exams (plus final) .....	3
	<b>TOTAL 45</b>

## **REFERENCES**

Eldad Eilam, Reversing: Secrets of Reverse Engineering, Wiley, 2005

Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed 7: Network Security Secrets and Solutions, Seventh Edition. McGraw Hill Osborne Media , 2012

Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 2012.

Bruce Dang, Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation, Wiley, 2014