CSCI 5345 – REVERSE ENGINEERING

CREDIT HOURS: 3
PREREQUISITES: Admittance in graduate program in Cyber Security
RECOMMENDED PREREQUISITE COURES:

CSCI 3341 Algorithm Analysis;
CSIT 4355 Enterprise Security or CSCI 4347 Cyber Security Concepts and Practice

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 and understand the threats to an operating environment through examination of both operating systems and malware. Practice practical reverse engineering on various operating systems (PC, Linux, OSX). Study threats and prevention techniques applied to various OS threats. Examine both application and OS level vulnerabilities, including malware. Examine and learn how to defend against networking attacks.

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.

CONTENT **Hours**

Introduction to Reverse Engineering 3
- Overview and course Introduction
- Common tools

Application-level Vulnerabilities.....9
- Stack vulnerabilities
- Heap vulnerabilities

OS-level Vulnerabilities.....9
- DLLs
- DLL injection
- Authentication, Authorization and Credentials

Malware 9
- Malware categories
- Malware and obfuscation
- Coding malware
- Malware forensics

Miscellaneous Threats 9
- Networking attacks
  - Routing
  - Remote exploitation
- Cyber defense

Exams (plus final).....6

TOTAL 45

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

Attendance Policy:
Attendance will be taken at the beginning of each class. If you have 3 unexcused absences, then your final grade will be reduced by one letter grade. If you have 4 unexcused absences, you will receive an "F" in the course. To receive an excused absence a written and signed notice is required within three class days of the absence. If you miss class without approval of your instructor, you will receive a grade of zero on the missed assignment. Authorized absences must be approved by your instructor in advance of the absence unless you have an emergency or illness. Make-up work must be completed outside of normal class hours and within one week following an excused absence. It is your responsibility to see your instructor and make arrangements for make-up work.

Academic Integrity (*A-9.1*)
Academic integrity is a responsibility of all university faculty and students. Faculty members promote academic integrity in multiple ways including instruction on the components of academic honesty, as well as abiding by university policy on penalties for cheating and plagiarism.

Definition of Academic Dishonesty
Academic dishonesty includes both cheating and plagiarism. Cheating includes but is not limited to (1) using or attempting to use unauthorized materials to aid in achieving a better grade on a component of a class; (2) the falsification or invention of any information, including citations, on an assigned exercise; and/or (3) helping or attempting to help another in an act of cheating or plagiarism. Plagiarism is presenting the words or ideas of another person as if they were your own. Examples of plagiarism are (1) submitting an assignment as if it were one's own work when, in fact, it is at least partly the work of another; (2) submitting a work that has been purchased or otherwise obtained from an Internet source or another source; and (3) incorporating the words or ideas of an author into one's paper without giving the author due credit.

Please read the complete policy at http://www.sfasu.edu/policies/academic_integrity.asp

Withheld Grades - *Semester Grades Policy (A-54)*
Ordinarily, at the discretion of the instructor of record and with the approval of the academic chair/director, a grade of WH will be assigned only if the student cannot complete the course work because of unavoidable circumstances. Students must complete the work within one calendar year from the end of the semester in which they receive a WH, or the grade automatically becomes an F. If students register for the same course in future terms the WH will automatically become an F and will be counted as a repeated course for the purpose of computing the grade point average.

Students with Disabilities
To obtain disability related accommodations, alternate formats and/or auxiliary aids, students with disabilities must contact the Office of Disability Services (ODS), Human Services Building, and Room 325, 468-3004 / 468-1004 (TDD) as early as possible in the semester. Once verified, ODS will notify the course instructor and outline the accommodation and/or auxiliary aids to be provided. Failure to request services in a timely manner may delay your accommodations. For additional information, go to http://www.sfasu.edu/disabilityservices/.

Mental Health Statement

SFASU values students' mental health and the role it plays in academic and overall student success. SFA provides a variety of resources to support students' mental health and wellness. Many of these resources are free, and all of them are confidential.

On-campus Resources:

SFASU Counseling Services
www.sfasu.edu/counselingservices
3rd Floor Rusk Building
936-468-2401

SFASU Human Services Counseling Clinic
www.sfasu.edu/humanservices/139.asp
Human Services Room 202
936-468-1041

Crisis Resources:
Burke 24-hour crisis line 1(800) 392-8343
Suicide Prevention Lifeline 1(800) 273-TALK (8255)
Crisis Text Line: Text HELLO to 741-741