Course and Contact Information

Course: Computer Science, Network Defense Part 2, 6907, 10
Semester: Spring 2018
Meeting time: Wednesday 06:10PM - 08:40PM: 01/17/18 - 04/25/18
Location: Tompkins Hall 405

Instructor

Name: Matthew Norris
Campus Address: Tompkins Hall 405
Phone: 202.994.7181
E-mail: mnorris@gwu.edu
Office hours: Prior to class - available upon request

Name: Kevin Yasuda
Campus Address: Tompkins Hall 405
Phone: 202.994.7181
E-mail: kevinyas@gwu.edu
Office hours: Prior to class - available upon request

Bulletin Course Description

Continuation of CSCI 6542. Concepts of the modern attack life-cycle of computer systems. Offensive methods of attack and persistence. Defensive network and host based methods of detection and prevention. History and literature related to advanced attacks. Simulation of attacks and defenses of computer systems.

Prerequisites

Computer Science 6542 - Computer Network Defense

Required Text(s)

- There are no required materials.

Learning Outcomes:

As a result of completing this course, students will be able to:

1. Analyze the architecture of a modern malware variant
2. Discuss various mechanisms used by malware authors to accomplish their goals and tradeoffs inherent
3. Evaluate malware kill chains and explain various components
4. Apply various techniques to identify sample malware on the host level
5. Apply various techniques to identify sample malware on the network level
6. Develop a wholistic plan to identify previously unknown malware on a sample system
7. Analyze cloud service provider security models to determine risk impacts for the customer and cloud service provider(s)

Class Schedule

Schedule subject to change - notification will be provided in class.

Date	Topic(s) and readings	Assignment(s) Due
1/17	Introduction / Special Topic	
1/24	Communication Mechanisms	
1/31	Building Defenses	Homework 1 Due
2/7	Building Defenses P2	Homework 2 Due
2/14	Dynamic/Behavior Analysis	
2/21	R&D Fair	Defense Practical Due
2/28	Windows Domains and Authentication	Homework 3 Due
3/7	Lateral Propagation	R&D Fair
3/14	SPRING BREAK (no class)	
3/21	Domain / Lateral Compromise	Practical 1 Due
3/28	Memory Analysis	Homework 4 Due
4/4	Domain Compromise 2	Practical 2 Due
4/11	Exfil Mechanisms	
4/18	IOC Creation and Handling	Homework 5 Due
4/25	Cloud Security	Practical 3 Due
5/2	Designated Monday	
5/9	Final	Homework 6 Due
NOTE: In accordance with university policy, the final exam will be given during the final exam period and not the last week of the semester		

Assignments and Grades

Grading

Below is a list what will be counted and percentages assigned:

- Homework (30%)
- Lab discussion/participation (10%)
- Practicals (30%)
- Final Exam (30%)

Assignments

Assignments are subject to change - notification will be provided in class.

Assignment	Description
Homework #1	Homework #1 will be assigned after the Introduction lecture and will focus on malware propagation techniques.
Homework #2	Homework #2 will be assigned after the Communications Mechanisms lecture and will focus on malware techniques to avoid network detection.
Homework #3	Homework #3 will be assigned after the Dynamic analysis lecture and will focus on the application of dynamic malware analysis.
Homework #4	Homework #4 will be assigned after the Lateral propagation lecture and will focus on network attack methodology.
Homework #5	Homework #5 will be assigned after the Memory Analysis lecture and will focus on the application of memory based analysis techniques to detect and identify malicious software.
Homework #6	Homework #6 will be assigned after the IOC Creation and Handling lecture and will focus on the application of a communicating network security indicators.

University Policies

University Policy on Religious Holidays

1. Students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance.
2. Faculty should extend to these students the courtesy of absence without penalty on such occasions, including permission to make up examinations.
3. Faculty who intend to observe a religious holiday should arrange at the beginning of the semester to reschedule missed classes or to make other provisions for their course-related activities

Support for Students Outside the Classroom

Disability Support Services (DSS)
Any student who may need an accommodation based on the potential impact of a disability should contact the Disability Support Services office at 202-994-8250 in the Rome Hall, Suite 102, to establish eligibility and to coordinate reasonable accommodations. For additional information please refer to: gwired.gwu.edu/dss/

Mental Health Services 202-994-5300
The University's Mental Health Services offers 24/7 assistance and referral to address students' personal, social, career, and study skills problems. Services for students include: crisis and emergency mental health consultations confidential assessment, counseling services (individual and small group), and referrals.
counselingcenter.gwu.edu/

Academic Integrity Code

Academic dishonesty is defined as cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and the fabrication of information. For the remainder of the code, see:
studentconduct.gwu.edu/code-academic-integrity