ECE 497 Administrative Issues

ECE 222 Development

Spring 2023

# Student Objectives

Students will assist with the development of the upcoming ECE 222, *Introduction to Cybersecurity Engineering*, by providing feedback on lecture materials, homework, projects, and exams.

# Distribution of Work

ECE 222 course material has been divided into 4 categories. Each student will select a category for the semester. Students may exchange categories, but must communicate this adjustment to David as soon as possible. Categories and associated work are as follows:

1. Cybersecurity Fundamentals
   1. Review and Present Lecture Slides:
      1. Cybersecurity Threats (L2)
      2. Network Basics (L5)
      3. Network & Web Attacks (L6)
   2. Project 1 Recording
2. Penetration Testing
   1. Review and Present Lecture Slides:
      1. Steps in a Penetration Test (L8)
      2. Tools of a Penetration Test (L9)
      3. MITRE Framework (L12)
   2. Project 2 Recording
3. Buffer Overflows
   1. Review and Present Lecture Slides:
      1. Assembly and Memory (L14)
      2. Buffer Overflows (L15)
      3. Linux Forensics (L24)
   2. Project 3 Recording
4. Defense Fundamentals
   1. Review and Present Lecture Slides:
      1. Defense Tools (L18)
      2. Intrusion Detection Systems (L19)
      3. Windows Forensics (L25)
   2. Project 4 Recording
5. Cyber Law
   1. Review and Present Lecture Slides:
      1. Course Introduction (L1)
      2. Cyber Law Intro (L22)
      3. Cyber Law Case Law (L23)
   2. Mini Project (TBD)

Throughout the semester, 6 Homework assignments will be distributed along with a sample Midterm Exam and Final Exam. Completion of these assignments and exams will assist in evaluating length and difficulty, so students will be expected to complete them. Performance on these assignments will NOT impact the student’s final 497 grade.

# Lecture Schedule

Students will meet twice per week (Mondays 8 pm – 9 pm and Tuesdays 3 pm – 4 pm) to discuss course materials and observe lecture demonstrations. A tentative schedule is as follows:

|  |  |  |
| --- | --- | --- |
| Date | Topic | Presenter |
| **1/9** (8 pm – 9 pm) | Administrative Issues | David |
| **1/16** (8 pm – 9 pm) | Command Line Intro (L3) | David |
| **1/17** (3 pm – 4 pm) | Kali Linux Intro (L4) | David |
| **1/23** (8 pm – 9 pm) | Course Introduction (L1) | Camden |
| **1/24** (3 pm – 4 pm) | Cybersecurity Threats (L2) | Defensive Security |
| **1/30** (8 pm – 9 pm) | Steps in a Penetration Test (L8) | Offensive Security |
| **1/31** (3 pm – 4 pm) | Assembly and Memory (L14) | Offensive Security |
| **2/6** (8 pm – 9 pm) | Defense Tools (L18) | Defensive Security |
| **2/7** (3 pm – 4 pm) | Penetration Test Walkthrough 1 (L10) | David |
| **2/13** (8 pm – 9 pm) | Penetration Test Walkthrough 2 (L11) | David |
| **2/14** (3 pm – 4 pm) | Network Basics (L5) | Defensive Security |
| **2/20** (8 pm – 9 pm) | Tools of a Penetration Test (L9) | Offensive Security |
| **2/21** (3 pm – 4 pm) | Buffer Overflows (L15) | Offensive Security |
| **2/27** (8 pm – 9 pm) | Intrusion Detection Systems (L19) | Defensive Security |
| **2/28** (3 pm – 4 pm) | Cyber Law Intro (L22) | Camden |
| **3/6** (8 pm – 9 pm) | Buffer Overflow Walkthrough 1 (L16) | David |
| **3/7** (3 pm – 4 pm) | Buffer Overflow Walkthrough 2 (L17) | David |
| **3/13** (8 pm – 9 pm) | **No class** |  |
| **3/14** (3 pm – 4 pm) | **No class** |  |
| **3/20** (8 pm – 9 pm) | Snort Overview 1 (L20) | David |
| **3/21** (3 pm – 4 pm) | Network Web Attacks (L6) | Defensive Security |
| **3/27** (8 pm – 9 pm) | MITRE Framework (L12) | Offensive Security |
| **3/28** (3 pm – 4 pm) | Linux Forensics (L24) | Offensive Security |
| **4/3** (8 pm – 9 pm) | Windows Forensics (L25) | Defensive Security |
| **4/4** (3 pm – 4 pm) | Cyber Law Case Law (L23) | Camden |
| **4/10** (8 pm – 9 pm) | Homework Debrief | Everyone |
| **4/11** (3 pm – 4 pm) | Exam Debrief | Everyone |
| **4/17** (8 pm – 9 pm) | Project 1 Review | Defensive Security |
| **4/18** (3 pm – 4 pm) | Project 2 Review | Offensive Security |
| **4/24** (8 pm – 9 pm) | Project 3 Review | Offensive Security |
| **4/25** (3 pm – 4 pm) | Project 4 Review | Defensive Security |

# Assignment Schedule

Sample Homework and Exams will be distributed throughout the semester. A tentative schedule is as follows:

|  |  |  |
| --- | --- | --- |
| Date | Assignment | Description |
| 1/23 | Homework 1 | Cybersecurity Basics |
| 2/13 | Homework 2 | Network Basics |
| 2/20 | Homework 3 | Penetration Testing |
| 3/6 | Homework 4 | Buffer Overflows |
| 3/20 | Homework 5 | Defense Tools |
| 3/27 | Homework 6 | Cyber Law |
| 3/6 | Midterm Exam | Networks & Penetration Tests |
| 4/3 | Final Exam | Buffer Overflow, Defense, & Cyber Law |

# Projects

Each student will be assigned 1 of the 4 course projects to complete. As part of the project, a Kali Linux Virtual Box image with the necessary tools will be provided along with a VPN configuration file to access the ECE 222 server cluster. ECE 497 students will be asked to develop and record a project guide that will be provided to future students. Project descriptions are as follows:

1. Environment Basics and Scanning
   1. Students will familiarize themselves with Kali Linux and basic scanning tools. Scans will be conducted against a vulnerable machine.
   2. Deliverables – A report detailing key components of Kali Linux along with analysis of the scan results. Screenshots of scans must be included for full points.
2. Penetration Test
   1. Students will conduct a penetration test against the machine from Project 1. The objective of the test will be to obtain root access to the target machine and obtain the hidden flag.
   2. Deliverables – A report detailing the steps completed as part of the penetration test along with analysis of the exploit used to defeat the target. Screenshots of steps taken along with the root flag must be included for full points.
3. Buffer Overflow Analysis
   1. Students will examine and test the provided code to identify and exploit a buffer overflow vulnerability.
   2. Deliverables – A report detailing he provided code and vulnerability with screenshots as proof of successful exploitation.
4. Intrusion Detection Basics
   1. Students will learn how to write basic Snort rules for identifying basic attacks against a host-based IDS. Students will launch attacks against the target to verify the ruleset worked.
   2. Deliverables – A report detailing the rules that were created along with screenshot showing detection of the launched attacks.