# ECE4112 Course Syllabus

**ECE4112**

**Internetwork Security (2-0-3-3)**

**CMPE Degree**
This course is Elective for the CMPE degree.

**EE Degree**
This course is Elective for the EE degree.

**Lab Hours**
0 supervised lab hours and 3 unsupervised lab hours

**Course Coordinator**
Keromytis,Angelos

**Prerequisites**
ECE3600 or ECE 4110 or CS3251

**Corequisites**
None

**Catalog Description**
Hands on experimentation and evaluation of Internet Security theory, principles, and practices. Laboratory component involves implementing both defensive and offensive security techniques.

**Textbook(s)**
Peter Kim, *The Hacker Playbook 3: Practical Guide to Penetration Testing*, McGraw-Hill, 2018. (required)

Matt Monte, *Network Attacks and Exploitation: A Framework* (1st edition), 2015.(optional)

**Course Outcomes**
Upon successful completion of this course, students should be able to:
1. Plan and execute a cyber penetration test, and utilize various vulnerability vectors that can be used to achieve an attacker?s goals.
2. Integrate and apply the techniques and methodologies that are available for preventing, detecting, and countering cyber attacks; also discuss the strengths and weaknesses of these techniques and methodologies, and when each should be used.

**Student Outcomes**
In the parentheses for each Student Outcome:
"P" for primary indicates the outcome is a major focus of the entire course.
“M” for moderate indicates the outcome is the focus of at least one component of the course, but not majority of course material.
“LN” for “little to none” indicates that the course does not contribute significantly to this

outcome.

1. ( P ) An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
2. ( M ) An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
3. ( LN ) An ability to communicate effectively with a range of audiences
4. ( M ) An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
5. ( LN ) An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
6. ( M ) An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
7. ( M ) An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

**Topical Outline**

```
Legal and Moral Responsibilities
Hacking and the Law
Planning a Cyber Attack
Tools of the Trade
Network Reconnaissance Techniques
Network Mapping
Vulnerability Assessment
Network Mapping tools
Vulnerability Scanners
Man-in-the-middle attacks
Routing Hijacking
DNS Spoofing
Defenses
Gaining Access
Social Engineering Attacks
Code Injection Attacks
Memory Vulnerability Exploitation
SQL and Command Injection
Web Attacks
Web Attack Tools
Credential Stealing
Password Crackers
Sniffing
Blended Attacks
Physical Attack Tools
Wireless Network Attacks
Wireless Attack Tools
Defenses
Maintaining Access
Privilege Escalation
RootKits and Implants
Trojans and Backdoors
Lateral Movement
Command and Control
```

Defenses
Antivirus and Host-based Detection
Network Intrusion Detection
Intrusion Detection tools
HoneyNets
Forensics
Firewalls
Firewall Rules
Wireless Network Security
Defenses