

# CYBERSECURITY

LAW 20310, Fall 2018

---

**Time:** Tuesday 10:00am – 12:00 noon    **Place:** 40 Ashmun (Baker Hall), Rm 120

---

## Instructors:

- Scott Shapiro, [scott.shapiro@yale.edu](mailto:scott.shapiro@yale.edu) & Sean O'Brien, [sean.obrien@yale.edu](mailto:sean.obrien@yale.edu)
- Assisted By - Laurin Weissinger, Cybersecurity Fellow, [laurin.weissinger@yale.edu](mailto:laurin.weissinger@yale.edu)

**Office Hours:** TBD

## Course Websites:

1. Canvas CMS - <https://yale.instructure.com/courses/38230>
2. Additional Resources - <https://github.com/seandiggity/yls-cybersec>

**Description and Objectives:** This course is an introduction to cybersecurity, privacy, anonymity, and cryptography via hands-on activities. Students will learn cybersecurity and networking concepts so that they may better engage issues at the policy and regulatory level.

**Technical Requirements:** A laptop computer is required for each class. We will be utilizing a Command Line Interface (CLI) on each laptop. Students will communicate and control Raspberry Pi mini-computers via the Secure Shell (SSH) protocol. Please install the software below on the laptop you will use in class.

- Hyper - <https://hyper.is> (Command Line Interface / Terminal Emulator)
- Filezilla Client - <https://filezilla-project.org> (SSH / SFTP Client)
- Atom - <https://atom.io> (Text Editor)
- Git for Windows - <https://gitforwindows.org> (Windows users only, required for SSH)

## Course Requirements:

- **Attendance** - It is very important to attend each class – indeed, attendance is mandatory.
- **Homework** - Each class will conclude with a take-home assignment. These must be completed to the satisfaction of the instructors.
- **Exam** - Your grade will be based on a take-home final exam.

## Course Outline:

### Week 1 – Practical Cybersecurity

1. Our Approach
2. Digital Self-Defense
3. Classroom Network Diagram
4. Command Line Interface (CLI)
5. Raspberry Pi Assembly

## **Week 2 – Get to Know Your Mini-Computer**

1. Command Line Basics
2. Controlling Your Raspberry Pi via SSH
3. Client/Server Model
4. Intro to File Permissions
5. Edit a File

## **Week 3 – Operating Systems**

1. What is an OS?
2. The Filesystem Tree
3. Superusers
4. The Kernel
5. Userspace

## **Week 4 – Ownership & Permissions**

1. Admin / root Access
2. Permissions as a Structural Design for Security
3. Principle of Least Privilege
4. Sandboxing & Isolation
5. Privilege Escalation Attacks

## **Week 5 – Normative Structure of a Network**

1. IP Address, Physical Address
2. Networking Models & Protocols (OSI Model)
3. Internet Infrastructure
4. Request/Response via the Web
5. Distributed Denial-of-Service (DDoS)

## **Week 6 – Network Attacks**

1. Domain Names
2. DNS Poisoning
3. Changing Your Pi's Network Identification
4. Ports & Firewalls
5. Man-in-the-Middle Attacks (MITM)

### **Week 7 – Secrecy & Encryption**

1. Obfuscation & Hashes
2. Public/Private Keys
3. HTTP Encryption (SSL/TLS)
4. E-mail Encryption (PGP/GPG)
5. Weaknesses

### **Week 8 – Information Security**

1. Data as a Toxic Asset
2. What is InfoSec?
3. Confidentiality
4. Integrity
5. Availability

### **Week 9 – Anonymity & The Dark Web**

1. Onion Routing (Tor)
2. Virtual Private Networks (VPNs)
3. Censorship Circumvention
4. Sharing Files Anonymously
5. Cryptomarkets

### **Week 10 – Cybercrime**

1. Cryptocurrency & Transactions
2. Ransomware
3. Fraud & Phishing
4. Data Breaches
5. Challenges for Attack Attribution

### **Week 11 – Chains of Trust**

1. Trusted Software Distribution
2. Software Verification
3. Hardware Assurance
4. Free & Open-Source Software
5. Static Analysis

## **Week 12 – Penetration Testing**

1. Cross-Site Scripting (XSS)
2. SQL Injection Attacks
3. Delivering Payloads
4. Metasploit Framework
5. Using Metasploit

## **Week 13 – Threat Modeling**

1. Risks and Vulnerabilities
2. Zero Day Attacks
3. Attack Scenarios
4. Mitigation
5. Operational Security (OPSEC)