Cybersecurity

LAW 20310, Fall 2019

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

Instructors:

Scott Shapiro, scott.shapiro@yale.edu

Sean O'Brien, sean.obrien@yale.edu

Laurin Weissinger, laurin.weissinger@yale.edu

Office Hours:

Laurin Weissinger – Thursday, 11:00am–12:00 noon, Baker Hall 438

Sean O'Brien – Thursday, 4:30pm–5:30pm, Baker Hall 438

Scott Shapiro – Tuesday, 4:00pm–5:00pm, SLB 325

Course Websites: Various resources for the class will be made available via the websites listed below, including video lectures, lecture slides, project source code, and student hacks.

1. Yale Canvas – https://yale.instructure.com/courses/48400
2. Cyberlab Website – https://cyberlab.yale.edu/
3. More 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: The class will make use of Virtual Machines (VMs) and VirtualBox to run them. Please see https://yale.box.com/s/7n12mfd7au19dgei1n0hmzyqs38vnmx8 for instructions and required files.

Course Requirements:

- **Attendance** – It is very important to attend each class. Attendance is mandatory.
- **Homework** – Most classes conclude with a take-home assignment. It will be graded as ✓+, ✓, or ✓–
- **Blog Post** – Write one blog post for www.cyberlab.yale.edu. The post can be about cybersecurity policy, cyberlaw, or a technical issue. Combining these themes is encouraged.
- **Final Project** – Video demonstration of three attacks/hacks with accompanying written description. Due by the last day of class. Alternatively, you can do two hacks and one essay.
- **Grading** – Homework (25%); Blog Post (15%); Final Project (60%).

Disability Statement: Students with documented disabilities should contact the Yale University Resource Office on Disabilities by email to rod@yale.edu, or by telephone at 203.432.2324, to request accommodation for examinations or other course-related needs. The Resource Office on Disabilities will work directly with the Registrars Office on accommodations.

Course Outline:

Week 1 – Practical Cybersecurity (08/27)

1. Our Approach
2. Information Security
    - Confidentiality
    - Integrity
    - Availability
3. Introduction: Virtualization
4. Command Line Interface (CLI)
5. The File-system Tree

Week 2 – Get to Know Your Operating System (09/10)

1. Admin / Root Access
2. The Kernel
3. User space
4. Processes
5. Rootkits

Week 3 – Identity & Access Control (09/17)

1. Permissions as a Structural Design for Security
2. Creating Users & Groups
3. Authentication
4. Principle of Least Privilege
5. Sandboxing Isolation
6. Privilege Escalation Attacks
7. ACLs
8. Breaking etc/shadow
9. Credentials & cracking

Week 4 – Computers & Operating Systems (09/24)

1. Which ones exist?
    - Unix

- Linux
- macOS
- DOS
- Windows
- Android
- iOS

2. Compare & contrast
3. Other computers
    - Mainframes
    - IoT
    - Industrial Control Systems
    - Cars, Planes & Ships, ...

Week 5 – Networking I (10/01)

1. Networking History
2. Client/Server Model
3. Networking Models (OSI & TCP/IP)
4. Physical & Internet Infrastructure
5. TCP/IP & UDP
6. Changing Your Network Identification

Week 6 – Networking II (10/08)

1. Request/Response via the Web
2. State
3. Ports, Sockets & Session Management
4. Network Address Translation (NAT) & Network Devices
5. Virtual Private Networks
6. Distributed Denial-of-Service (DDoS)
7. Man-in-the-Middle Attacks (MITM)

Week 7 – Encryption (10/15)

1. Obfuscation Hashes
2. Public/Private Keys

3. RSA algorithm
4. HTTP Encryption (SSL/TLS)
5. E-mail Encryption (PGP/GPG)
6. Certificates
7. Weaknesses
8. Back-doors

Week 8 – Networking III (10/22)

1. Identifiers: Domain Names & the DNS
2. DNS, IP addresses & Policy
3. Firewalls
4. Proxies & Reverse Proxies
5. Network-based Intrusion Detection & Prevention Systems
6. Content Delivery Networks & Anycast

Week 9 - Penetration Testing (10/29)

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

Week 10 – Anonymity & The Dark Web (11/05)

1. Onion Routing (Tor)
2. Censorship Circumvention
3. Configuring TOR
4. Sharing Files Anonymously

Week 11 – Chains of Trust (11/12)

1. Trusted Software Distribution
2. Software Verification
3. Hardware Assurance

4. Certification: TCSEC, ITSEC, CTCPEC, and Common Criteria
5. Free & Open-Source Software
6. Open-Source Hardware

Week 12 – Cybercrime (11/19)

1. Types of Cybercrimes
2. Varieties of Malware
3. Fraud & Phishing
4. Data Breaches
5. Cryptomarkets
6. Cryptocurrencies & Transactions
7. Challenges for Attack Attribution
8. Social Engineering

Week 13 – Cybersecurity (12/03)

1. What is InfoSec?
2. Confidentiality, Integrity, Availability
3. Risks & Vulnerabilities
4. Data & other Toxic Assets
5. Zero Day Attacks
6. Attack Scenarios
7. Mitigation
8. Operational Security (OPSEC)
9. Information Security Standards