The following course syllabus is tentative and may change or be reordered as the semester unfurls. It is also likely that some topics will be skipped for sake of time.\(^{(1)}\)

## Background

- Laws and Ethics
  - Jailed hackers
- Introduction to system programming
  - Intel Assembly
  - C/C++
  - low-level debugging
  - memory management
- Introduction to operating systems
  - shell
  - access permissions
  - file system
- Introduction to networking
  - TCP/IP
  - socket programming
  - network protocols: HTTP, FTP, DNS
- Basic math
  - core discrete math
  - core number theory

## Social

- Social engineering
  - Psychology
  - Physical access
  - Phishing
- Social networking
- User interface attacks
  - Clickjacking, tapjacking, tabnabbing, cursorjacking
- Defenses

### Web

- Google dorks
- SQL injection
- cross-side scripting
- cross-side request forgeries
- Defenses

### Network

- Fingerprinting
  - Operating Systems
  - Applications
- Port scanning
- Protocol mangling
  - Packets in packets
- Wireless network cracking
- Defenses
  - tar pits
  - honeypots

### Software

- Code analysis
  - Taxonomy of coding errors
  - Overflows
    - buffer, stack, heap overflow
    - format string overflow
  - Return-oriented programming
    - return to libc
  - Binary analysis
  - Reverse engineering
  - Fuzzing
- Shellcode
  - port binding
  - reverse bind
  - NOP sleds
  - polymorphism
- VM detection
- Interface errors
  - metric-English
  - java-C
- Defenses
  - Stack canaries
  - Address space layout randomization

## Operating system

- Access control
  - executability
  - groups, users
  - password hashes
- Privilege escalation
  - password cracking
  - suid/sgid scripts
- Denial of Service
  - Fork bombs
- Backdoors
  - Rootkits
  - Trojans/worms/viruses
  - BOTs and BOTNETs
- Defenses

## Disk

- Structure
- Hidden files/directories
- Deletion/undeletion
- Forensics
- Defenses

## Advanced

- Cryptography
  - hashing
    - MD5, SHA1
    - birthday attacks
    - rainbow tables
    - hash chains, Merkle trees
  - symmetric-key encryption
    - ciphers, DES, 3DES, AES
- public-key encryption
  - RSA
    - attacks - factor attacks, Pollard rho, bad keys
  - signatures, authentication, steganography
  - general attacks
    - blinding, padding, timing, random faults, lattices
- Android attacks
  - sensors, SIM, adaptors, baseband processor, agps

Notes

1: In other words, this syllabus tells you nothing absolute about the course contents.