Course Syllabus

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 - interspersed

- 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 systems
- Introduction to networking
  - TCP/IP
  - socket programming
  - network protocols: HTTP, FTP, DNS
- Basic math
  - probability
  - discrete math
  - number theory

Social

- Social engineering
- Psychology
- Physical access
- Phishing
- Social networks
- User interface redressing
  - Clickjacking, tapjacking, tabnabbing, cursorjacking, likejacking, ...
- Defenses

**Web**

- Engines
  - Dorks
  - Pushpins
- Web Apps
  - SQL injection
  - cross-side scripting (XSS)
  - cross-side request forgeries (CSRF)
  - open relay
  - Same-Origin Policy bypasses
  - denial of service (DoS)
- Defenses

**Network**

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

**Software**

- Interface errors
  - metric-English
  - java-C
- Code analysis
  - Taxonomy of coding errors
- Overflows
  - buffer, stack, heap
  - format string
- Return-oriented programming (ROP)
  - return to libc
- Binary analysis
- Reverse engineering
- Fuzzying
- Shellcode
  - executables
    - port binding, reverse bind, meterpreter, ...
  - No-Op (NOP) sleds
  - polymorphism
  - Detection
    - Virtual Machines, debugging
- Defenses
  - Address space layout randomization (ASLR)
  - Data execution prevention (DEP)
  - Stack canaries

**Operating system**

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

**Disk**

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

Advanced

• Applied Cryptography
  • fundamentals
    ■ confidentiality
    ■ integrity
    ■ availability
    ■ non-repudiation
  • hashing
    ■ DES, Message-Digest 5 (MD5)
    ■ Secure Hash Algorithm (SHA-1, -2, -3)
    ■ Advanced Encryption Standard (AES)
    ■ Hash modes
      ■ Electronic CodeBook (ECB)
      ■ Cipher Block Chaining (CBC)
      ■ Galois/Counter Mode (GCM)
      ■ Elements
        ■ Initialization Vector (IV)
        ■ Key, length
    ■ hash chains, Merkle trees
    ■ bitcoin
    ■ Key-hashed message authentication code (HMAC)
  • attacks
    ■ rainbow tables
    ■ birthday attacks
    ■ modification
    ■ length extension
  • symmetric-key encryption
    ■ Attacks/defenses
  • public-key encryption
    ■ RSA
    ■ Attacks/defenses
      ■ blinding, padding, timing, random faults, lattices
• Smartphones
  • security models
    ■ full disk encryption
    ■ paranoid networking
    ■ signed binaries
- ARM-based overflows
- Subsystems
  - sensors, SIM, baseband processor, assisted GPS

Footnotes

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