Schedule and outline

Texts

Certified Ethical Hacker Version 9 Cert Guide - Denoted CHE for readings below

Week 1

- Topics:
  - Intro s1
  - Ethical Hacking s2
  - Information gathering s3
- Readings: CEH1-3
- Labs: p1

Week 2

- Topics:
  - Vagrant & Virtualbox
  - Authentication s4
  - MFA
  - BIOMETRICS
  - Rainbow tables
  - Passwords
  - Gaining Access
    - Local password attacks
    - Privilege escalation
  - Physical Security
  - Hacking windows or linux without knowing password.
    - Rescue cd
    - Hirens
    - Reset SAM
  - Bios security
- Readings: CEH4
- Labs:
  - p2
  - p3

Week 3

- Topics:
  - OS Security
  - Maintaining Access
    - Rootkit s5
    - Trojan and Backdoor
- Labs:
  - p4

Week 4

- Topics:
More OS Security
Armitage
zero day exploits
security updates and patches
Data Hiding: [s6]
Review [here]
Man in the middle project [p5]

Test 1
Presentation

---

**Week 5**

- Topics:
  - Network attacks with SCAPY
  - replay
  - DOS
- Readings:
  - Scapy slides 1
- Projects:
  - [p6]
  - [p7]

---

**Week 6**

- Topics:
  - More scapy
  - Malware
  - Ransomware
- Readings:
  - CEH Chapter 5
  - Ransomware
  - Linux ransomware
- Projects:
  - [p6]
  - [p9]

---

**Week 7**

- Topics:
  - firewalls/acls
  - iptables [ppt more]
- Readings:
- Projects:
  - [p10]
  - [p11]

---

**Week 8**

- Topics:
  - Malware conclusion
  - Social Engineering Toolkit
- Readings:
Week 9

- Review
- Test 2
- Topics:
  - Application security
- Readings:
  - Read the section “Finding and Exploiting XSS Vulnerabilities” to the “Summary” at the end of XSS.
    - [this book](#)
    - Slides
- Projects:
- Presentations?

Week 10

- Topics:
  - Application security
- Readings:
- Projects:
- Presentations?

Week 11 - 13

- Topics:
  - Application Security
    - [https://sourceforge.net/projects/mutillidae/](https://sourceforge.net/projects/mutillidae/)
  - XSS, CSRF, injection
  - Software Security
    - Buffer overflows
  - Database injections
  - Jails, Containers
- Readings:
- Presentations?
- Test 3

Week 14 - 15

- Topics:
  - Monitoring and Intrusion Detection
  - Honeynets
  - snort (base, placid)
  - HIDS vs NIDS
  - Cloud security
  - Mobile?
- Cryptography
- Policies & Access control
- Forensics
- Steganography
- Fun random stuff?

Readings:

- Test 4