OS Implementation and Systems

- Privilege Escalation Techniques, and Prevention
- Buffer Overflows
- Directory Traversal
- Remote Code Execution
- Local Databases
  - Some messaging apps use sqlite for storing messages.
  - Useful for digital forensics, especially on phones.
- Windows Security Topics
  - Windows registry and group policy.
  - Active Directory (AD).
    - Bloodhound tool.
    - Kerberos authentication with AD.
  - Windows SMB.
  - Samba (with SMB).
  - Buffer Overflows.
  - ROP.
- *nix Security
  - SELinux.
  - Kernel, userspace, permissions.
  - MAC vs DAC.
  - /proc
  - /tmp - code can be saved here and executed.
  - /shadow
  - LDAP - Lightweight Directory Browsing Protocol. Lets users have one password for many services. This is similar to Active Directory in windows.
- MacOS Security
  - Gotofail error (SSL).
  - MacSweeper.
  - Research Mac vulnerabilities.