# Mid-Term Outline

1) Buffer Overflows
   a) Stack overflows
   b) Heap overflows
   c) Format string attacks
2) Components of Operating System
   a) Boot Process details
   b) Attacks against hardware
3) Address Space Layout Randomization
   a) What it is
   b) How it works
4) Data Execution Protection
   a) What it is
   b) How it works
5) Cryptography
   a) Hashes
      i) What they are
      ii) How they work
   b) Monoalphabetic ciphers
   c) Transposition ciphers
   d) Polyalphabetic ciphers
   e) Vignere cipher
   f) Stream ciphers
   g) Block ciphers
      i) Block cipher modes
   h) Asymmetric cryptography
      i) Four properties
   i) Diffie Hellman
   j) Digital Signatures
   k) Attacks against cryptography
6) Threat Modeling
7) Attack Surface Analysis
8) Access Control
   a) Setuid issues
9) Chroot jails
   a) Setting up
   b) Requirements
   c) Concerns
   d) Breaking out of