Midterm-2 Study guide:

Part IV: Network Security and Malware

- Malware
  - What are worms?
  - What are viruses?
  - How do worms and viruses propagate?
  - How to detect worms/viruses and other kind of malware?
  - What are the countermeasures a malware could use to avoid detection? (Polymorphism, metamorphism, etc)
- Network Protocol Security
  - What are the general Layer 1, 2 threats?
  - What can you do with spoofing? When can you perform a blind spoofing?
  - What are the security issues with TCP? (disruption, injection, rate-management, blind spoofing, etc)
  - What are DHCP related security issues?
  - What are DNS related security issues? How does cache poisoning work? What is Kaminsky attack and what is the defense against it?
- Denial of Service attacks and defenses
  - Smurf amplification and the general idea about amplification attacks.
  - What is TCP SYN flood? What are the possible defenses? What are syncookies?
  - What is the general idea behind a DoS prevention proxy?
  - DNS DoS attack, why and how does that work?

Part V: Web Security

- Web security threat models
  - Understand the different threat models: web attacker, network attacks, OS/ Malware attacker
- Browser security goals and architecture
  - What are the browser security goals?
  - What security mechanisms are used in modern browser security architecture? (isolation, etc.)
  - What is the same Origin Policy?
- Web application vulnerabilities
  - Command Injection vulnerabilities and defenses
  - SQL Injection
    - vulnerabilities and defenses
    - Prepared statements
  - Cross-Site Scripting (XSS)
    - Three types of vulnerabilities and attacks (Reflected, Stored, DOM-based)
    - Defenses
  - CSRF
    - Vulnerabilities

        - Defenses: Nonce-based defense and Origin-header based defense

Part VI: Mobile Security

- Android security architecture
    - What are the goals of the android security architecture?
    - How does application sandboxing help achieve the desired goals?
    - How does the application signing work in android? How does that help in achieving the desired security goals?
    - Application permissions, what are those and how could a malicious application use these permissions to its advantage?
    - Understand common android app vulnerabilities