CSCI 641, Spring 2017
Midterm Review

Topics to Study:

1. Security Lifecycle
2. Threat Modelling
    a. Attack trees
    b. STRIDE
    c. Data Flow Diagrams
    d. Process Flow Diagrams
3. Intrusion Detection and Prevention
4. Firewalls
5. Network attacks
    a. TCP/IP
    b. DNS
    c. DDoS
    d. Worms
6. Secure protocols:
    a. DNSSEC
    b. TLS (???)
7. Pen Testing
    a. Reconnaissance
    b. Scanning

Sample Questions

1. Suppose a business wants to develop and implement a web based portal to allow its business partners to transfer proposals and other related documents in a secure manner. How will you apply the phases of the security lifecycle to develop this portal?
2. WhatsApp is a free to download messenger app for smartphones. WhatsApp uses the internet to send messages, images, audio or video. The service is very similar to text messaging services however, because WhatsApp uses the internet to send messages, the cost of using WhatsApp is significantly less than texting. Whatsapp is adding passwords: what is the threat model that they want to protect their users from?
3. What custom IDS rule would you write to prevent Smurf attacks in your network? Can you filter these attacks with a firewall rules? The syntax for Snort alerts is:
   alert proto src_ip src_port direction dst_ip dst_port (*options*)
   Where option can be any generic rule that you would like to use, like for example:
   num_of_SYN_packs > 1000/sec
   Do not worry if the syntax of your options is not exactly the syntax used by snort.
4. Explain how DNSSEC prevents DNS Cache Poisoning.
5. If you had the scope and ip addresses for an external/internal penetration test/assessment how would you start?

6. What tools would you run to scan/recon a network? what ports would you scan? what commands would you run?