Exam Review Outline
IN618 Security

The final exam for 2016 will be held on Thursday, June 16. There will be one session at 1:00 PM and a second at 3:00 PM, both in D313. You should revise the following topics to prepare for the exam.

Risk

- Know the definition of risk. (Basically, Probability of harmful event * degree of harm from event)
- Be able to calculate an ALE.
- Understand how an ALE informs budget calculations for risk reduction measures.
- Know the difference between quantitative and qualitative risk assessment.
- Be able to use qualitative risk assessments to prioritise security decisions.

Password hashing

- Explain the algorithm for authenticating a user with hashed passwords.
- Understand the difference between hashing and two-way encryption methods. Why is hashing a good method for protecting passwords?
- Explain how using salt with hashed passwords improves their security.

Common vulnerabilities: XSS, XSRF, SQL injection

For each or these vulnerabilities:

- Explain how the vulnerability can typically be exploited.
- Explain the nature of the mistakes in coding that lead to the vulnerability and how to fix them.
- Explain the risk associated with the vulnerability - what harm can result from its exploitation and how likelihood that it may be exploited.

Buffer overflows

- Explain why buffer overflow vulnerabilities are so serious.
- Explain how buffer overflow attacks work.
- Know what coding mistakes lead to buffer overflow vulnerabilities.

Encryption

- Know the difference between symmetric key and asymmetric key encryption.
- Explain the challenge of public key distribution and verification.
- Know the difference between a self-signed key and one signed by a certifiifate authority(CA) key when setting up https.
- Know the security advantages of using public key authentication with ssh.

Port scanning

- Explain how common port scanning methods work.
- Interpret sample port scan results (produced by nmap).
- List some uses for port scanning besides reconnoitring for an attack.

Firewalls

- Know what items of information can be used in packet filtering firewall rules.
- Interpret the meaning of example firewall rules (using `iptables`)
- Explain the function of application firewalls and how they differ from packet filtering firewalls.