Exam 1 Topics

Exam #1 Review

> Format will be a mix of TF, multiple choice, fill in the blank, short answer.

Intro

- Know the difference between Confidentiality, Integrity, and Availability (CIA), and how they can be applied in a scenario
- What is the difference between a Threat and a Vulnerability and an Asset
- What is the type of Virtual Machine we are using in class?

Cryptography

- Understand the differences between symmetric and asymmetric encryption
- Understand the basic process of encrypting and decrypting
- Understand what role a salt plays in encryption and decryption and how it is stored
- Understand what role encoding has if it is not encryption
- Understand which algorithms are used, how they are used, and which ones should not be used
  - How: What is PBDKF2 used for? How is it different than AES?
  - Not: Should we use DES and ECB?
- Understand what hashing is and how do we use it
  - How can hash tables be attacked
- Understand what a digital signature is and why is it used

Certificates

- Understand what a CA is and what a Root CA is
- Understand how certificates are used with TLS.
- What is the Let's Encrypt service, what does it offer?
- What type of encryption is used with TLS
- Understand basic TLS handshake

Network Security

- Understand how protocols can be attacked (e.g. TCP SYN)
- Understand basics of TCP and IP and the responsibilities of each protocol
  - How IP and Port are used together
- Understand how to define a network zone for a network diagram, what role firewalls play in creating a zone

- Understand differences in firewalls such as packet filter and stateful
- Understand basic ways of scanning a network and finding information about a network using whois, nmap, etc
- Understand what service DNS provides and how it can also be attacked

Operating System Security

- Understand principle of least privilege and how we can apply it in OS security
- Understand important of updating packages, regularly checking services, checking logs, etc
- How to harden an operating system and core software such as Apache and SSH

Malware and Threats

- What is a virus and a trojan?
- What is spyware and malware?
- What is phishing?

Overall

- Be able to evaluate an argument from a security perspective using what we have learned in class and make a counter argument or support an argument.