i310 (IAC) - Midterm Review

Computer Labs (summary & lessons learned)

Computing Security rests on what elements ? Goals of Computing Security ?

Classes of integrity mechanisms

Broad classes of threats (according to text)

Define/Describe specific threats (snooping, DoS, masquerade)

Risk Cube

Understand security policy and/versus security mechanisms (how do they complement each other)

Hurdles to overcome that limit/delay implementation of security policy/implementation

Authentication (methods, adv/disadv)

Define cryptography (according Bishop definition)
Transpositional ciphers
Subsitutional ciphers

Briefly describe public key encryption

What is a man-in-the-middle attack - how relevant to crypto ?

Principle of Tranquility

Role Based Access Control – can you give an example

DNS (Domain Name Service), and what is its role in host identity ?

What makes an entity trustworthy ?

What is Software Assurance ?

What is a cookie ? Its role in security ?

Briefly describe malicious logic (according Bishop definition)

Briefly describe Trojan Horse

Describe Boot Sector Infector

Differentiate dynamic and static software scanners

Describe TSR (Terminate and Stay Resident) virus

What is meant by command and control ?

Pillars of IA (Information Assurance)?

Stuxnet, Conficker

NIST Stages of pen testing

Differentiate white box and black box pen testing?

Common vulnerability found in systems?

SCADA (what is – why relevant)

Components and strategies of enterprise security perimeters

Enterprise IA/CyberSec versus Platform

Able to describe what polices you would implement (and security mechanisms implemented) in different scenarios (i.e. small/large companies).

Hashing - common uses of hashing?

Symmetric-key and Public-key cryptography?

Basic types of ciphers.

Different cryptanalytic attacks

Motivations for creating and deploying malware?

Spear phishing? Give an example of a spear phishing attack

Mechanisms employed by malware for exfiltrating data?

Using indicators to detect or block malicious traffic on a network?

What is obfuscation? How does it apply to malware?