CIS 214 Midterm Review Guide

Chp. 1 – 8

This is not an exhaustive list – but meant to help identify areas to review.

Types of hackers – motivations, means, opportunity.

Role of ethical hackers and legal limitations and dangers.

What characteristics of information must be protected by IT Security?

Threat vs. Vulnerability

Active vs. Passive attacks

Types of attacks: TAP (Technical, Administrative, Physical)

Phases of an attack

Footprinting phase – info gathering

Scanning methods: (for the Hands-on, being able to look at Wireshark capture/nmap output will be very useful.) What flags are associated with different types of scans? Methods (Examples –this list is not exhaustive –Syn/Ack, XMAS, Stealth Scan, Fin, Null)

Differences between Port scanning, Network Scanning, Vulnerability scanning.

Types of Pen Tests: White-/Gray-/Black-box

Enumeration - The legal line in the sand = accessing systems

Fingerprinting – active/passive –

Cryptography

Symmetric and Asymmetric Algorithms

Hashing Algorithms

PKI Concepts

Attacks on Cryptosystems

What are the characteristics of strong encryption?

Confidentiality, Integrity, Authenticity/Non-Repudiation, Access Control  
Malware types  
Windows security – Users/Groups/Access Controls/SAM DB/SIDs

Types of Users: Local Service, Network Service, System, Current User  
What is one of the most attacked services in Windows?

What is the tool, included with all Windows OSes, used to troubleshoot

issues with this service?

Launching Metasploit –What command is used?

Exploits –What are the exploits doing?

Payloads –What is a payload?

Meterpreter Shell –How does it work? What are some things we can do with a Meterpreter Shell?

Wimax – what is it?

MIMO

Wireless is 802.??

WEP/WPA/WPA2; preshared keys.

Bluetooth basics and its vulnerabilities/attacks.

What flags are associated with different types of scans? Methods (Examples –this list is not exhaustive –Syn/Ack, XMAS, Stealth Scan, Fin, Null)

Resources and Lab Review:

Review labs completed.

When reviewing labs examine Wireshark capture/nmap out exercises)

In addition, use the Metasploit PDF and video included in this Module’s Review Page.