CSC 479 WEEK 8 TEST STUDY GUIDE

GODFREY MUGANDA

Concepts from the Lab 3/Homework assignment: digital certificates, keystores, creating keys, SSL programming, and using the cipher classes in Java.

Operating Systems and Application Security: Need to protect hibernation files, BIOS protection using passwords.

Password security and salting, encryption vs cryptographic hashing in implementation of password systems, dictionary attacks.

Application memory map (data, code, stack and heap), parameter passing and function calling conventions, base / frame pointer registers, program counter registers, stack pointer registers, buffer overflow and stack smashing attacking, shell code, code injection into the stack, techniques for facilitating buffer overflow attacks: NOP sledding, Trampolining, Return to libc.

Counter measures for buffer overflow attacks: Address space layout randomization, Use of a canary.

Netword Security: ARP spoofing, gratuitous ARP and ARP cache poisoning, smurf attacks, DNS attacks, DNS cache poisoning, subdomain DNS cache poisoning, DNSSEC as discussed in the text.

SYN Flooding attacks and counter measures, different types of SYN flood attacks: direct, distributed, with and without spoofed IP source addresses, host-based countermeasures such as SYN cookies and SYN cache, network-based countermeasures using firewalls and proxy servers: defenses by having a firewall / proxy server spoof syn-acks or acks to the initiator or to the server.

IPSEC (if covered in Tuesday lecture).