CSC 479/579 FINAL EXAMINATION STUDY GUIDE

PROFESSOR GODFREY C. MUGANDA

The final examination will be comprehensive, so refer to all previous study guides. In particular, pay special attention to the material from previous study guides on cryptography, especially the mathematical foundations of public key encryption, including the RSA and Diffie-Hellman schemes, and also the different techniques for buffer overflow attacks; network security, syn-flood attacks and counter-measures, attacks on DNS, smurf attacks, ARP spoofing and ARP cache poisoning.

With regard to material covered since the week 8 test, the important concepts are cross domain web security and cross-site scripting (XSS); attacks based on session hijacking where sessions are based on cookies, URL-rewriting, or hidden input variables.

Different types of malware: be able to define and distinguish among viruses, logic bombs, trojan horses, worms, techniques for virus detection, and techniques used be virus writers to evade detection.

Elementary notions about spam filters: false positives, false negatives; Elementary notions about firewalls; what we covered in class about IPSEC.