CSc 4222/6222 – Assignment #4

Deadline: Tuesday, October 24th (midnight) / Late Deadline: Friday, October 27th (noon)

Make sure to justify all of your answers clearly
No handwritten submissions

1. Jill lives in a large apartment complex and has a Wi-Fi access point that she keeps in her apartment. She likes her neighbors, so she doesn't put any password on her Wi0Fi and lets any of her neighbors use her Wi-Fi from their nearby apartments if they want to access the Internet. What kinds of security risks is Jill setting herself up for?

2. How many bytes are devoted to header and footer information (with respect to all layers of the IP protocol stack) of an Ethernet frame that contains a TCP packet inside it?

3. Suppose you suspect that your session with a server has been intercepted in a man-in-the-middle attack. You have a key, *K*, that you think you share with the server, but you might be only sharing it with an attacker. But the server also has a public key, K_p, which is widely known, and a private secret key, K_s, that goes with it. Describe how you can either confirm you share *K* with the server or discover that you share it only with a man-in-the-middle. Also, be sure your solution will not be discovered by a packet sniffer.

4. You are the system administrator for a provider that owns a large network (e.g., at least 64,000 IP addresses). Show how you can use SYN cookies to perform a DOS attack on a web server. Show how to defend against this DOS attack.

5. Suppose the transaction ID for DNS queries can take values from 1 to 65,536 and s randomly chosen for each DNS request. If an attacker sends 1.024 false replies per request, how many requests should he trigger to compromise the DNS cache of the victim with probability 99%?

6. Suppose DNS IDs were extended from 16 bits to 32 bits. Based on a birthday paradox analysis, how many DNS request and equal number of fake responses would an attacker need to make in order to get a 50% chance of succeeding in a DNS cache poisoning attack?

7. During a *FIN scan*, a FIN packet is sent to each port of the target. If there is no response, then the port is open, but if an RST packet is sent in response, the port is closed. The success of this type of scan depends on the target operating systems – many Oss, including Windows, have changed the default behavior of their TCP/IP stacks to prevent this type of scan. How? Also, how could an intrusion detection system be configured to detect a FIN scan?

Undergrads – answer any 3 of the following questions. Grads – answer all 5 of the following questions.

8. In the three-way handshake that initiates a TCP connections, if the SYN request has sequence number 156955003 and the SYN-ACK reply has sequence number 883790339, what are the sequence and acknowledgment numbers for the ACK response?

9. Either party in an established TCP session is allowed to instantly kill their session just by sending a packet that has the reset bit, RST, set to 1. After receiving such a packet, all other packets for this session are discarded and no further packets for this session are acknowledged. Explain how to use this fact in a way that allows a third party to kill an existing TCP connection between two others. This attack is called a *TCP reset attack.* Include both the case where the third party can sniff packets from the existing TCP connection and the case where he cannot.

10. Describe a firewall rule that can prevent IP spoofing on outgoing packets from its internal network.

11. Explain why a large value for the TTL (time-to-live) of replies to DNS queries does not prevent a DNS cache poisoning attack.

12. Describe the types of rules that would be needed for a rule-based intrusion detection system to detect a smurf attack.