CS336 Homework Assignment #6

Due: Friday Dec 10th, 2021 5:00pm.
Points: 100 pts

1. (10 pts) Can link and end-to-end encryption both be used on the same communication? What would be the advantage of that? Cite a situation in which both forms of encryption might be desirable.

2. (10 pts) Recall that packet reordering and reassembly occurs at the transport level of the TCP/IP protocol suite. A firewall will operate at a lower layer, either the internet or data layer. How can a stateful inspection firewall determine anything about a traffic stream when the stream may be out of order or damaged?

3. (5 pts) Cite a reason that an organization might want two or more firewalls on a single network.

4. (5 pts) One form of IDS starts operation by generating an alert for every action. Over time, the administrator adjusts the setting of the IDS so that common, benign activities do not generate alarms. What are the advantages and disadvantages of this design for an IDS?

5. (5 pts) Should a network administrator put a firewall in front of a honeypot? Why or why not?

6. (10 pts) How can a website distinguish between lack of capacity and a denial-of-service attack? For example, websites often experience a tremendous increase in volume of traffic right after an advertisement with the site's URL is shown on television during the broadcast of a popular sporting event. That spike in usage is the result of normal access that happens to occur at the same time. How can a site determine that high traffic is reasonable?

7. (5 pts) Explain why spam senders frequently change from one email address and one domain to another. Explain why changing the address does not prevent their victims from responding to their messages.

8. (10 pts) Why does a web server need to know the address, browser type, and cookies for a requesting client?

9. (5 pts) What is clickjacking attack? Suggest a technique by which a browser could detect and block clickjacking attacks?

10. (10 pts) You have forgotten your password, so you click on "forgot my password" to have a new password sent by email. Sometimes the site tells you what your password was; other times, it sends you a new (usually temporary) password. What are the privacy implications of each approach?

11. (10 pts) Suppose a telephone company maintained records on every telephone call it handled, showing the calling phone number, the called phone number, and the time, date, and duration of the call. What uses might the telephone company make of those records? What uses might commercial marketers make? What uses might a rival telephone company make? What uses might a government make? Which of those uses violate individuals' privacy rights?

12. (10 pts) Consider the first step of the common attack methodology we describe, which is to gather publicly available information on possible targets. What types of information could be used? What does this use suggest to you about the content and detail of such information? How does this correlate with the organization's business and legal requirements?

13. (5 pts) Distinguish between copyright, patent, trade secret, and trademark (in your own words).