

HOMWORK 4

ENTS 689i Network Immunity Fall 2008

Instructions

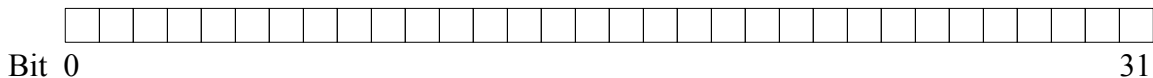
This assignment is **NOT** a group assignment. Each student should turn in their own set of answers. You should not collaborate for this assignment.

Answer each of the following questions and send your responses in ASCII (.txt) or PDF format to **awalters@4tphi.net** no later than **12:01am EST on November 17th, 2008 (midnight Sunday night)**. All other formats will receive **NO CREDIT**. Any mail arriving later than 12:01am on Monday morning (as determined by my mail server's time stamp) will be considered late. The standard course grading policy will apply for late homework on this assignment. If you turn in several copies of this assignment, the last one received will be graded and all others discarded.

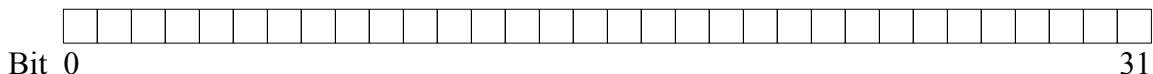
Questions

- (10 points) What are two reasons for using layered protocols? What are two disadvantages to using layered protocols?
- (10 points) Consider a system with an n-layer protocol stack. Applications generate messages of length M bytes. At each of the layers, an h-byte header is added. What fraction of the network bandwidth is filled with headers? Briefly explain how bandwidth would be affected if the packets were fragmented?
- (20 points) In slide 17 (“Programming Example (client)”), we made a call to the subroutine `htons()`. What is the purpose of this function call? Please show, by filling in the boxes (in binary), how the following 32-bit number, `0x11223344`, would be stored using both big-endian and little-endian byte orders. Assume big-endian bit order for both cases.

Big-Endian



Little-Endian



- (10 points) Pfleeger, Chapter 7, exercise 19.
A port scanner is a tool useful to an attacker to identify possible vulnerabilities in a potential victim's system. Cite a situation in which someone who is not an attacker could use a port scanner for a nonmalicious purpose?
- (10 points) Briefly explain (~1 paragraph) what SQL Injection is. Explain (1 paragraph) a defensive mechanism that could be used to mitigate this threat.
- (10 points) In the context of network security, what is the purpose of the Demilitarized Zone

(DMZ)? Name one server you are likely to find in the DMZ. Why would it improve a company's network security to place that server in the DMZ?

7. (15 points) In class, we described a type of distributed denial of service attack called a "reflector" attack. Describe how I could use each of the following protocols to perform the attack? (Provide details as to the "type" of packet or datagram that would need to be sent to the "reflector" and the response it would generate.)
 - a) (5 points) TCP
 - b) (5 points) UDP
 - c) (5 points) ICMP
8. (5 points) Explain what factors make defending a network from distributed denial of service such a challenging problem?
9. (10 points) One of the biggest challenges we have discussed is IP address spoofing. Does either SSL or IPSec help solve this problem? If so, how?