# Question Bank for Final Exam

1) Explain the different purposes (to attack, to defend, to monitor) of each of the following in the context of network security?

a) Port Scanning
b) Honeypot
c) Traffic analyzer

2) What are the critical parameters of a TCP session that need to be known to hijack the session?

3) Explain how TCP session hijacking could lead to an ACK storm?

4) Differentiate between local session hijacking and blind session hijacking.

5) Explain how are the following attacks launched and explain a prominent solution to mitigate or prevent these attacks:

a) Smurf attack
b) SYN flood attack
c) Tiny fragmentation attack
d) Session hijacking attack
e) Echo-Chargen attack

6) Explain how the following attacks are launched and their consequences

a) Teardrop attack
b) Traffic redirection attack

7) Explain the terms "zombie" and "botnet" and their role in launching a distributed denial of service attack.

8) Explain how would use a firewall (and what category) for each of the following scenarios. You need to justify your selection:

a. An organization wants to give remote login access for its employers to their office computer. The office computers could differ in the operating system employed and do not have a strong authentication mechanism.
b. A network administrator wants to restrict clients from downloading beyond a certain number of bytes from a file server over a time period.
c. A network administrator wants to restrict a client from using beyond a threshold bandwidth on the server network
d. A company wants to set up an online price list so that outsiders can see the products and prices offered. It wants to be sure that (a) no outsider can change the prices or product list and (b) outsiders can access only the price list and not any of the more sensitive files stored inside.

9) What is the difference between a proxy firewall and a reverse proxy firewall? Explain their use.

10) What is the advantage of using a Demilitarized Zone (DMZ) in a network? What would be the nature of machines that you would deploy in a DMZ network and why?

11) Mention some of the significant characteristics that are unique representative features of a “personal” firewall when compared to the other three categories of firewalls discussed in class?

12) What is the advantage of using multiple layers of firewalls? Among the four categories of firewalls we discussed in class, explain the sequence of firewalls that you would deploy to protect an organization's network, starting from its connection to the public Internet all the way to the internal hosts. Justify why you recommend that sequence.

13) Differentiate between a network-based IDS and a host-based IDS.

14) Compare the signature-based IDS and anomaly-based IDS based on their underlying fundamental working principle. What kind of attacks they can and cannot capture, if any? Explain with an example for each IDS.

15) Differentiate between an "active" IDS and a "passive" IDS. What is the advantage of an active IDS over a passive IDS? Explain the difference with an example.

16) Differentiate between a false positive and a false negative? Between the "signature-based" and "anomaly-based" IDS, which one can lead to more false positives and/or more false negatives? Why?

17) Explain the sequence of steps in the IPSec security association (SA) establishment. How is it identified (globally unique) and used in IPSec?

18) What are the two protocols/headers developed for IPSec? What features each of these two provide?

19) Differentiate between the IPSec transport mode and tunnel mode.

20) What are the three significant attacks (that we discussed in the slides/lecture) that could be prevented by employing a packet filter firewall.

21) Explain the "default-deny" and "default-allow" options of filtering packets through a firewall. What are the pros and cons, if any?