CSC 437/539 Computer Security
Instructor: Dr. Natarajan Meghanathan

Question Bank: Firewalls and Intrusion Detection Systems

Firewalls

1) How could a network administrator prevent the servers in his internal protected network from directly communicating and exchanging SSL/public-key certificates with the clients in the Internet?
2) 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 (at least three firewalls, one from each category) 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.
3) Explain how stateful firewalls can be used to prevent each of the following: (a) TCP session hijacking and (b) TCP SYN flooding.
4) Why we do not run any other application program on a computer hosting a firewall.
5) Is firewall – hardware like a computer or a software program? Clarify the terminology and justify your answer.
6) Mention two significant characteristics that are unique representative features of a "personal" firewall when compared to the other three categories of firewalls discussed in class?
7) Compare the location and use of a firewall vis-à-vis an intrusion detection system? How do they typically complement each other?
8) 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?
9) What is the difference between a proxy server and a reverse proxy server? Explain their use.
10) Explain, with two significant reasons, why a firewall alone cannot secure a network?
11) Discuss the pros and cons of using the black-list approach (default-allow) and the white-list (default-deny) approach of filtering packets through a firewall.
12) What is "egress" filtering and "ingress" filtering?
13) What is the difference between the two Unix-based firewalls: "IPchains" and "IPtables"? Which one would you prefer and why?
14) Explain the three significant attacks (that we discussed in the slides/lecture) that could be prevented by employing a packet filter firewall.
15) Explain how would use a firewall (and what category) for each of the following scenarios. You need to justify your selection:
    a. A bookstore lists the books on sale through its website. We do not want any client to launch a SQL injection or XSS/XSRF attack when they attempt to access the website.
    b. 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.
    c. A user wants to prevent an XSRF attack to be launched when he opens an email on his PC.
    d. A network administrator wants to restrict clients from downloading beyond a certain number of bytes from a file server over a time period.
    e. Auditing a network security attack (i.e., trace the sequence of packets that have entered and/or left an organization's network)

Intrusion Detection Systems

1) Discuss two significant advantages (strengths) and disadvantages (weaknesses) of the network-based IDS (NIDS) vis-a-vis a host-based IDS (HIDS).
2) 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? Give a concrete example to illustrate the working of these two categories of IDS.

3) 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.

4) What are the typical source of information for an NIDS and a HIDS to analyze? Briefly explain how they use these to detect any potential intrusion to the environment they are monitoring.

5) 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?

6) What are the different categories of "anomaly-based" IDS that we discussed in the lecture? Give an example to briefly explain the functioning of each.

7) (a) What is a honeypot and a honeynet? What is the difference in the purpose of deploying a honeynet compared to deploying a regular IDS? Give an example to illustrate the difference.
(b) What roles can honeynets play with regards to identifying the sources of spam emails? How?

8) What are some of the beneficial and malicious effects of employing packet sniffers?