National University of Computer and Emerging Sciences, Karachi
FAST School of Computing

Information Security
Fall 2022
Practice Question

1. List and briefly define the skill level of intruders.
2. List five examples of intrusion.
3. How are intruders classified according to skill level?
4. What is meant by security intrusion?
5. List and breifly describe the classifications of intrusion detection systems based on the source and the type of data analyzed.
6. What are three benefits that can be provided by an IDS?
7. What is the difference between a false positive and a false negative in the context of an IDS?
8. Explain the base-rate fallacy.
9. List some desirable characteristics of an IDS.
10. What is the difference between anomaly detection and signature or heuristic intrusion detection?
11. List the different types of firewalls.
12. List four characteristics used by firewalls to control access and enforce a security policy.
13. Which type of attacks is possible on a packet filtering firewall?
14. How does a traditional packet filter make filtering decision?
15. What is the difference between a packet filtering firewall and a stateful inspection firewall?
16. What is the difference between a gateway and a firewall?
17. What are the differences between an IDS, an IPS, and a firewall?
18. List the types of malicious behaviors addressed by a Host-based Intrusion Prevention System (HIPS)?
19. What are the different places an IPS can be based?
20. List at least three malicious behaviors addressed by HIPS.

Q1: As part of a formal risk assessment of the IT system of your university, you have identified the asset “integrity of stored file and database information of all the students and faculty stored on the server” and the threat “corruption, theft, loss of information from server.” Suggest reasonable values for the items in the risk register for this asset and threat with justifications for your choice.
Q2: State the difference between do and act steps of Plan-Do-Check-Act model.
Q3: List some of the key national and international standards that provide guidance on IT security management and risk assessment.
Q4: What are the key points that should be addressed by an organizational security policy?
Q5: List some of the topics that should be addressed by an organizational security policy

Q6: As part of a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset “integrity of customer and financial data files on desktop systems” and the threat “corruption of these files due to import of a worm/virus onto system.” Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices