**Chapter 5: Firewall & IDS/IPS**

1. Firewall overview
2. What is a FW?
   * Point of control & monitoring
   * Interconnect networks of different trust
   * Impose restriction on network services
   * Auditing and controlling access
   * Perimeter defense
3. Characteristics
   * All traffic must pass through FW
   * Only authorized traffic defined by the security policy are allowed to pass
   * Immune to penetration
   * Access Policy? List of authorized traffics: Address range, protocols, applications and content types. Developed by the organization’s IS risk assessment and policy
4. Limitations
   * The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out or mobile broadband capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in
   * Capability for traveling employees and telecommuters.
   * The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
   * An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
   * A laptop, PDA, or portable storage device may be used and infected outside the corporate network and then attached and used internally
5. Four General control techniques:
   * Service control
   * Direction control
   * User control
   * Behavior control
6. Firewall &Filtering types
   * Packet filtering (per packet) 🡪 Stateless
   * Session filtering (per session) 🡪 Stateful
7. Common types of FW
8. Packet-filtering routers:

* forward/discard packet based on the rules match
* Two default policies:
  + Discard: prohibit
  + Forward: permit
* Advantages, Weaknesses
* Application-level gateways (proxy server)
  + Advantages,
  + Weaknesses

1. Circuit-level gateways
2. Bastion host:

* Packet-filtering router + Bastion host (single-homed)
* Packet-filtering router + Bastion host (dual-homed)
* Screened-subnet firewall

1. Network-based/Host-based firewall
2. Intrusion Detection
3. Intruders
   1. Examples
   2. Behavior
      * Target acquisition/Information gathering
      * Initial access
      * Privilege escalation
      * System exploit
      * Maintaining access
      * Covering tracks
4. Intrusion Detection System (IDS)
   1. Components
      * Sensors
      * Analyzers
      * User interfaces
   2. Basic Principles
      * Intruder/Authorized user behavior
      * False positives/False alarms vs False negatives
   3. The Base-Rate Fallacy
   4. Requirements
   5. Detection Techniques
      * Anomaly detection (Statistical, Knowledge based, Machine-learning)
      * Signature/Rule-based detection
   6. HIDS vs NIDS
5. Snort
6. IPS
7. HIPS vs NIPS
8. Snort Inline

**Questions**

**Firewall**

1. List three design goals for a firewall.
2. List four characteristics used by firewalls to control access and enforce a security policy.
3. What information is used by a typical packet filtering firewall?
4. What are some weaknesses of a packet filtering firewall?
5. What is the difference between a packet filtering firewall and a stateful inspection firewall? What is an application-level gateway?
6. What is a circuit-level gateway?
7. Why is it useful to have host-based firewalls?
8. What is a DMZ network and what types of systems would you expect to find on such networks? What is the difference between an internal and an external firewall?
9. How does an IPS differ from a firewall?
10. What are the different places an IPS can be based?
11. How can an IPS attempt to block malicious activity?
12. Problems 9.5, 9.6, 9.7 on pages 332, 333, 334

**Intrusion Detection System**

1. List and briefly describe the steps typically used by intruders when attacking a system.
2. Provide an example of an activity that may occur in each of the attack steps used by an intruder. Describe the three logical components of an IDS.
3. Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?
4. What are three benefits that can be provided by an IDS?
5. What is the difference between a false positive and a false negative in the context of an IDS? Explain the base-rate fallacy.
6. What is the difference between signature detection and rule-based heuristic identification?
7. Describe the types of sensors that can be used in a NIDS.
8. What are possible locations for NIDS sensors?