CALIFORNIA STATE UNIVERSITY
LONG BEACH

Homework #6

CECS 378 – Spring 2021 Cappel
Due: Wednesday, April 21th prior to class (11:59 PM)

Sergio Vasquez

Chapter 8 – Intrusion Detection

1. List and briefly define four classes of intruders.

   Cyber Criminals: are either individuals or members of an organized crime group with a goal of financial reward.

   Activists: are either individuals, usually working as insiders, or members of a larger group of outsiders attackers, who are motivated by social or political causes. They are also known as hacktivists, and their skill level is often quite low.

   State- sponsored organizations are groups of hackers sponsored by governments to conduct espionage or sabotage activities. They are also known as Advanced Persistent Threats (APTs), due to the covert nature and persistence over extended periods involved with many attacks in this class.

   Others: are hackers with motivations other than those listed above, including classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation. Many of those responsible for discovering new categories of buffer overflow vulnerabilities [MEER10] could be regarded as members of this class.

2. What are three benefits that can be provided by an IDS?

   Sensor: Sensors are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion. Types of input to a sensor I ncludes network packets, log files, and system call traces.

   Analyzers: Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred. The output of this component is an indication that an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred.

   User interface: The user interface to an IDS enables a user to view output from the system or control the behavior of the system.

3. What is the difference between signature detection and rule-based heuristic identification?

Signature detection: match a large collection of known patterns of malicious data against data stored on a system or in transit over a network. The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data.

While, **Rule-based heuristic identification** involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is with the bounds of established patterns of usage.

4. Describe the types of sensors that can be used in a NIDS.

   Inline sensors: inserted into a network segment so that the traffic that it is monitoring must pass through the sensor. The primary motivation for the use of inline sensors is to enable them to block an attack when one is detected.

   Passive sensor: monitors a copy of network traffic; the actual traffic does not pass through the device. From the point of view of traffic flow, the passive sensor is more efficient than the inline sensor, because it does not add an extra handling step that contributes to packet delay.

5. What is a honeypot?

   Honeypot: are decoy systems that designed to lure a potential attacker away from critical system. Honeypots are designed to divert an attacker from accessing critical systems, collect information about the attacker's activity or encourage the attacker to stay on the system long enough for administrators to respond.

Chapter 9 – Firewalls and Intrusion Prevention Systems

1. List four characteristics used by firewalls to control access and enforce a security policy.

   Service Control: Determines the types of Internet services that can be accessed, inbound and outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number.

   Direction control: Determines the direction in which particular service requests are allowed to flow

   User Control: Controls access to a service according to which user is attempting to access it

   Behavior Control: Controls how particular services are used

2. What is the difference between a packet filtering firewall and a stateful inspection firewall?

Packet filtering firewall: It applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The firewall is typically configured to filter packets going in both directions.

Stateful inspection firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.

3. What is a DMZ network and what types of systems would you expect to find on such networks?

   DMZ network: the network just inside the external firewall, but outside the internal firewall.

   Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.

4. How can an IPS attempt to block malicious activity?

   IPS can be host-based, network-based, or distributed/hybrid. It can be anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior. IPS will analyze all the inbound and out network traffic for suspicious activities.

   Once it has detected malicious activity, it can respond by modifying or blocking network packets across a perimeter or into a host, or by modifying or block system calls by programs running a host.

5. Explain the strengths & weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, & laptops against network threats.

   a. A firewall at the network perimeter.
      Strength: - the addresses the bulk of the traffic
      - easy to refresh the strategy
      - ensure to protect against DoS assault
      Weakness: vulnerable to internal attacks and it can't have different policies for different servers/client

   b. Firewalls on every end host machine.

      Strength: - it is adaptable to the needs of each host

- protect portable workstations even if it is associated with different systems

Weakness: - many installation and configurations are required and needed to be kept update.

- It is hard to oversee strategies

- Might can prevent DOS assault

c. A network perimeter firewall and firewalls on every end host machine

Strength: First line of defense by the perimeter firewall and second line of defense provided by individual firewalls.

The perimeter firewall can have basic settings for all, the individual ones augment for specifics.

Weakness: need lots of maintenance and coordination.