**Homework #6 Answers**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, April 21th prior to class (11:59 PM)

**Homework #6 is focused on Chapter 8 and Chapter 9. There are 10 total questions all worth 10 points each (100 pts total).**

**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 outsider attackers, who are motivated by social or political causes
* **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.

1. What are three benefits that can be provided by an IDS?
   1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
   2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
   3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.
2. What is the difference between signature detection and rule-based heuristic identification?

**Signature approaches** match a large collection of known patterns of malicious data against data stored on a system or in transit over a network. **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 within the bounds of established patterns of usage.

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

An **inline sensor** is inserted into a network segment so that the traffic that it is monitoring must pass through the sensor. A **passive sensor** monitors a copy of network traffic; the actual traffic does not pass through the device.

1. What is a honeypot?

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

**Chapter 9 – Firewalls and Intrusion Prevention Systems**

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

* **IP Address and Protocol Values**: Controls access based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer

characteristics.

* **Application Protocol**: Controls access on the basis of authorized application protocol data.
* **User Identity**: Controls access based on the users identity, typically for inside users who identify themselves using some form of secure authentication technology, such as IPSec.
* **Network Activity**: Controls access based on considerations such as the time or request, or other activity patterns.

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

A **traditional packet filter** makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context. A **stateful inspection packet filter** tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as

shown in Table 9.2. 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.

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

Between internal and external firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. 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.

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

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

1. Explain the strengths & weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, & laptops against network threats.
2. A firewall at the network perimeter.

Here are the strengths.

(1) It mediates all incoming traffic from external hosts and can protect against many attacks by outsiders.

(2) It is easier to manage and to update policies, because of single central location.

(3) It protects against some kinds of DoS attacks launched from the outside.

Here are the weaknesses.

(1) It has no protection against malicious insiders.

(2) It has no protection for mobile laptops while they are connected to other networks.

(3) It has no protection if laptops get infected while travelling and then spread infection when they re-connect to our internal network.

1. Firewalls on every end host machine.

Here are the strengths.

(1) It protects against malicious insiders and infected internal machines as well as outside attackers.

(2) It protects laptops even while they are travelling and connected to other networks.

(3) It may be easier to customize firewall protection on a per machine basis.

Here are the weaknesses.

(1) It is potentially more difficult to manage policies, due to the number of machines whose rulesets must be configured and updated.

(2) Uncooperative users may be able to modify settings or disable firewalls on their own machines, and viruses/worms may be able to do the same to machines they infect.

(3) It is potentially less resistant to DDoS, since DoS attacks can still flood internal network links.

(4) Depending upon firewall configuration, it may block legitimate internal traffic and/or make some internal services harder to use.

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

Here are the strengths.

(1) Layered defense provides redundancy in case one firewall fails.

(2) It can easily update policy against external attacks if a new threat develops, which gives some time to update the rulesets on internal hosts.

(3) Strengths (a)(1) and (b)(1)–(3) also apply.

Here are the weaknesses.

(1) Potential for over blocking of legitimate traffic, since traffic flows only if permitted by both firewalls.

(2) Weaknesses (b)(1), (b)(4) also apply