**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 6**

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

Review Figure 6-1 from your text and explain the following terms:

· subjects and object (in access control, not attack)

**The subject is the entity that is trying to access the object. A user can be a subject. The object is the resource that the subject is trying to access and contains information. A computer or document can be examples of objects.**

· discretionary and non-discretionary access control

**Discretionary access controls (DACs) provide the ability to share the resources in a peer-to-peer configuration that allows users to control and possibly provide access, or they can allow specific people or groups of people to access these resources. This is controlled by the user and the user can allow access to specific coworkers by providing them a level of access.**

**Non-discretionary access controls (NDACs) are managed by a central authority in the organization. This is controlled by the organization and branches out to lattice-based control (mandatory and role-based/task-based) in which users are assigned a matric of authorizations for particular areas of access.**

·lattice-based access control

**Lattice-based access control mens that users are assigned a matrix of authorizations. It specifies the level of access each subject has to each object, as implemented in the access control lists (ACLs) and capabilities tables. This branches into two sections, role-based/task-based access control and mandatory access control.**

· mandatory access control

**Mandatory access control is a form of lattice-based control. Users and data owners are given limited access control over access to information resources. It uses data classification schemes and each collection of information is rated and users are rated to specify the level of information they may access.**

· role-based access control

**Role-based access controls (RBACs) and task-based access control ((TBACs), sometimes used simultaneously depending on the organization, are another form of lattice-based controls. These controls are tied to a person’s duties and responsibilities. This could be there role or position in the department like job role, or task based which is tied to a particular chore or responsibility/ These controls make it easier to maintain the role or task. When a new employee gets a role or task, they will automatically receive the corresponding access. When they are removed from the role or task, their access is revoked.**

(15 pts.)

**Problem 2**

What is stateful inspection? How is state information maintained during a network connection or transaction? What is the primary drawback to the use of this approach? (5 pts.)

**Stateful inspection is one of the three subsets of packet-filtering firewalls. Packet filtering enforce address restrictions. Stateful packet inspection (SPIs) keep track of each network connection between internal and external systems using a state table. A state table tracks the state and context of each packet in the conversation by recording which station sent that packet and when. This is how information is maintained during a network transaction. The primary disadvantage is that the firewall needs additional processing required to manage and verify packet against the state table. Without this processing, the system is vulnerable to DoS and DDoS attacks. If this were to happen, the firewall would slow down because it will receive a large number of external packets and will have to compare all of the incoming packets first to the state table and then to the ACL.**

**Problem 3**

How does a network-based IDPS differ from a host-based IDPS? Which has the ability to analyze encrypted packets? (5 pts.)

**Network-based IDPS (NIDPS) is an IDPS that resides on a computer or appliance connected to a segment of an organization’s network and monitors traffic on that segment, looking for indications for ongoing or successful attack.**

**Host-based IDPS (HIDPS) is an IDPS that resides on a particular computer or server, known as the host, and monitors activity only on that system.**

**One of the biggest differences is that the NIPS resides on the network segment and monitors activities across that segment while the HIDPS resides on a particular computer or server and monitors activity only on that system.**

**The HIDPS has an advantage over an NIDPS because it can acc4ss encrypted information traveling over the network and use it to make decisions about potential or actual attacks.**