**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 6**

Names of team members: William Brown, Taylor Payne, Corey Cooley, & John Hopson

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)

· discretionary and nondiscretionary access control

· lattice-based access control

· mandatory access control

· role-based access control

(15 pts.)

1. *A subject refers to the information system user in order to determine their permissions. An object relates to the information system, asset, or resources that the subject is authorized for, or unauthorized for.*
2. *Discretionary access controls are implemented in a p2p network where users decide general, unrestricted, or specific access to the resources in the network. Non-discretionary access control is authority-based and has a central command creating the rules.*
3. *Lattice-based access control is is a non-discretionary control where separate fibers come together and form a matrix, and users are given permissions to access certain areas.*
4. *Mandatory Access Controls are a form of lattice-based controls where data classification is used to decide which users access what type of data under different types of classification.*
5. *Role-based access controls are another form of lattice-based controls where different roles within the company or information system allow you access data based on that role.*

**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 a type of firewall that tracks each network connection between internet and external systems, using a state table to speed up filtering of communications. The information is maintained during a transaction using the state table, and the table tracks the context and state of each packet that is apart of the conversation. The primary drawback of this approach is more processing.*

**Problem 3**

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

*A network-based IDPS sits on a specific machine on a network, and monitors for indications of successful attacks. There are two types of network-based IDPS’, one that monitors wireless networks, and one that monitors patterns for abnormalities.*

*A host-based IDPS is installed on specific computers and monitors activity and system files on that specific device. Host-based IDPS can use encrypted data, unlike NIDPS and it can also exist in an environment that has complicated switching.*