CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #6

Team: 1

Participants: Zack Graas, Trevor Hagel, Jacob Forcht

Logistics

A. Get together with other students on your assigned team in person and virtually.

B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1 *(15 points)*

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

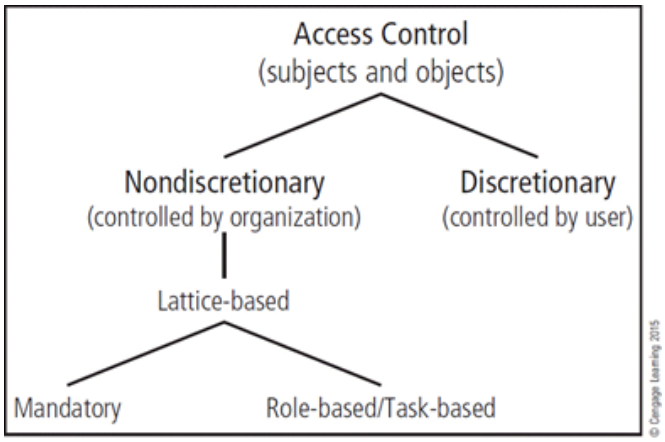

Figure 6-1 Access control approaches

.

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

A subject is a system or a user. An object is a resource. Access control is focused on if, when, where a subject can access an object. A major part of this is making sure the right subjects can access the right objects which makes sure that the subjects can accomplish their tasks.

· discretionary and non-discretionary access control

Discretionary access controls (DAC) are access controls that are based on the data user's decisions. The data users have the discretion to assign access controls that can allow the data to be shared with certain people groups or even the whole company. Non-discretionary access controls (NDACs) are access controls that are implemented by a central authority. One form of NDACs are lattice-based access controls.

· lattice-based access control

A lattice-based access control (LBAC) is an access control structure that uses a matrix of authorization that gives users access to certain areas, this also includes the information assets of subjects as users and objects. This is a type of NDAC. There are different types of lattice-based controls such as RBACs and MACs.

· mandatory access control

Mandatory Access controls are a form of lattice-based access controls where a structured data classification system rates information and users to different classification levels. These controls are based on the user's specified access level which allows them to access up to a certain level of the information. All information is rated as well as each user to a classification level. Data owners have limited control over access to information resources.

· role-based access control

Role-based access controls are a form of lattice-based access controls where access controls are based on a user's role in the organization. A user gets permissions from access controls when they are assigned a role. Note that users can have multiple roles and thus multiple sets of permissions.

Problem 2 *(5 points)*

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?

Stateful inspection is a network firewall protection method that is designed to check all network traffic in depth. Incoming network traffic is scanned and attempted to be looked up in a "flow table". This allows for a lot of customization in terms of what is allowed and what isn't. Since all traffic is analyzed before being allowed through, stateful inspection can pick out malicious traffic efficiently. The primary drawback of this approach is the large amount of processing power needed to scan and compare all traffic with the flow table.

Problem 3 *(5 points)*

How does a network-based IDPS differ from a host-based IDPS? Which has the ability to analyze encrypted packets?

One main difference between network-based IDPS (NIDPS) and host-based IDPS (HIDPS) is that HIDPS can obtain access to encrypted data going through the network while NIDPS does not. The HIDPS can use the access obtained to help make important decisions with any future attacks on the server. Another difference is that NIDPS is a hardware that can track the network traffic while HIDPS is a software that encrypts the information. The based IDPS that can encrypt the packets is HIDPS.