Exercise-4

Vineeth Mylavarapu
ID.801337050
College of Computing and Informatics

Question-3:

A computer system provides protection using the Bell-LaPadula policy. How would a virus spread if (a) the virus was place on the system at system low (the compartment dominated by all other compartments)? Justify your answer. (b) the virus was place on the system at system high (the compartment that dominates all other compartments)? Justify your answer.

A. Placing the virus in the system low compartment, which is dominated by all other compartments in the Bell-LaPadula policy, would result in its inability to spread to compartments with higher security levels. The reason for this is that the policy only permits the flow of data from higher to lower security levels and not vice versa. Consequently, the virus would be restricted to the system low compartment and incapable of altering or accessing data in higher security level compartments.

B. In case the virus was introduced to the system high compartment - the one that dominates all other compartments under the Bell-LaPadula policy, it would propagate to all other compartments in the system. This is possible because the policy permits data flow from higher security levels to lower security levels, not in reverse. Therefore, since the system high compartment dominates all others, the virus would have the ability to access and modify all the data in the system, as well as propagate itself to other compartments through data modifications.

For the virus to spread in either scenario, it must have appropriate privileges to read, write, or execute data in the target compartments. The Bell-LaPadula policy is designed to restrict access to data in a manner that restricts the virus's propagation only to the compartments for which it has the necessary permissions. In this way, the spread of the virus is controlled and limited to only those compartments that meet the required access criteria.

Question-4:

Classify the following vulnerabilities using the RISOS model. Assume that the classification is for the implementation level. Justify your answer. (a) The presence of the “wiz” command in the send mail program (see section 20.2.8). (b) The failure to handle the IFS shell variable by load module (see section 20.2.8). (c) The failure to select an Administrator password that was difficult to guess (see section 20.2.9).

A. Insufficient identification, authentication, or authorization flaws are present if the "wiz" command is included in the send mail program. As a result, remote users can easily guess the permissions of the mail-sending server and execute commands as if they were that user. Additionally, the actual user is misidentified in this scenario.

B. This is an incomplete parameter validation error if the load module does not handle the IFS shell variable. Since the shell variable is a global parameter, it can influence how the program is run even though it is not a command line or function parameter. The variable would not be validated to verify its value, if it only includes acceptable values.

C. If an easy-to-guess Administrator password is selected, the identification, authentication, or authorization flaw will be inadequate. In such a situation, the authentication process would fail to establish the correct user association with the internal identity representation. Therefore, it is important to select a complex password that is not easily guessable to ensure that the authentication method operates effectively.