CSCI4323.01

Computer security

Lab #1

9/21/2022

Cyber-attacks: Explain what each of the following attacks is. Cite your source(s).

Note: Not all information published on the web are correct. Discern the validity of the information you use by, for example, comparing them with what you have learn

(a) Replay attacks- are a bracket of cyber attacks that can be carried out to gain access or hinder a system with the data that is being used in the system. A basic way to describe a replay attack is by stating that this attack is something that is replayed several times in quick succession to cause the load of this message to bog down the network. This can cause a DOS attack on the network slowing down the connectivity due to the queue of request in the network. All types of messages can be sent and replayed for this to work, there is no data changed between the original message and the replayed messages normally. This information is used from the chapter notes in class. Security-Services-vsMechanisms-rev2-09-06-2022 document on blackboard. With a simple google search a simple and easy way to counter act this attack from being used is by " Replay attacks can be prevented by tagging each encrypted component with a session ID and a component number."(Wikipedia contributors)(R1)

(b) Man in the middle attack- With MITM attacks can be simply described as a silent interception of messages and data between two parties who are communicating with one another. But unfortunately for the two parties the information is not being transmitted to each other but to a man in the middle who is intercepting and relaying the information to the other party. “MiTM cyber attacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive personal information -- such as login credentials, account details or credit card numbers -- in real time” (R2) (Yasar and Cobb). As stated by Kinza yasar, this type of attack can be a very expensive attack to the users involved. Due to the validity of information exchanged at times, the attacker can manipulate each user in to seeing what the attacker wants resulting in false information along with potential for the attacker to get deeper information and access to the users.

(c) From my general understanding of a replay attack and a denial of service attack, the attacker’s goal is for replay attack is to slow and hinder the user from accessing files. This can be done by sending several messages/files to that user to manipulate the information being received by the user. The Denial-of-service attack is very similar in the fact that the attacker’s goal is to block or hinder the user from accessing files, information, or other resources. This is done by bogging down the user’s computer and network connection with several messages and request to alter the speed and functionality of the device to prevent service to that device.

(d) Replay vs middleman attacks- Again from my understanding of these attacks is that a replay attack’s goal is to repeatedly send messages to a device or user to delay and hinder their interaction with a device or resource. With a man in the middle attack that process is allowed but the attacker has access to that information the user is sending to another user and is manipulating that information. The man in the middle only allows the user to see what information he wants them to see. All messages or data is sent to the attacker first instead of the original user it was intended for.

Question 3- In an online banking application, the customer may transfer fund between the saving account and the checking account.

A. Explain what data integrity means in this context-

    a. The information or message the customer is wanting to send to the bank should have complete data integrity meaning that the information should be correct and have consistent data. IE funds transferred by the customer should not be corrupted by a third party, and should be done with perfect accuracy.

B. Explain what origin integrity means in this context.

    a. The integrity of the message being sent should be identified that the user is the one sending the information to the online banking service. The origin integrity of this information helps prevent the bank and user from being intercepted and effected by information or a message sent from a different user. Only the information sent from the correct user has the right origin integrity.

C. Explain what availability means in this context.

    a. Is that the availability of the options the user can select, is available to the user and the online banking system. IE the withdraw system the credit and debit system are available and accessible to the customer to transfer data.

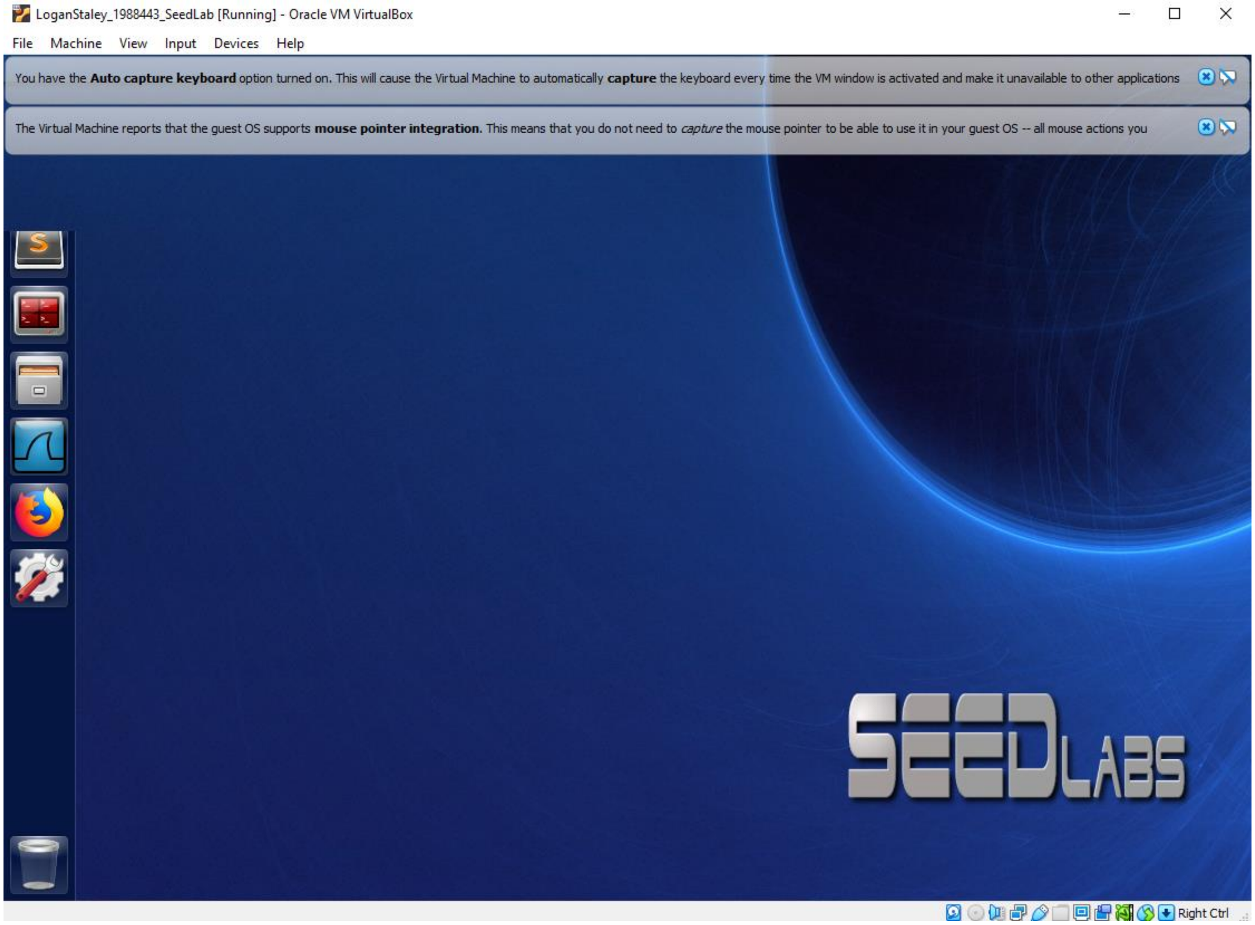
D. Explain what confidentiality means in this context.

    a. Is that the personal information of the customer is correct and has the be correct for the customer to access and request data from the online banking system. IE Bank pin, password, username not only that but the bank should not have this information available to the public for others to intercept and access.

E. Explain what non-reputability means in this context.

    a. This is a vital system to have in the online banking system, this is for when a customer claims to not have transferred the money from banking accounts to other accounts in the system. Non-reputability provides legal evidence for the bank to have to prove that the customer was the one whom transferred the correct amounts to the correct locations.

Hands on LAB-


LoganStaley_1988443_SeedLab [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
SEEDLABS
Right Ctrl

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you

Questions For Virtual machines-

a) What is a virtual box? Hint: Explain its relationship to the operating system. What is the role played by the virtual box?

   a. A virtual box is a machine that is run virtually inside of the computer, this can be done separately from the base computer it is running on. To the advantage of not having major effects on the host Computer. This allows for the computer to have multiple operating systems for flexibility. Each OS has its hardware capacity restricted to not alter or tax the main operating system.

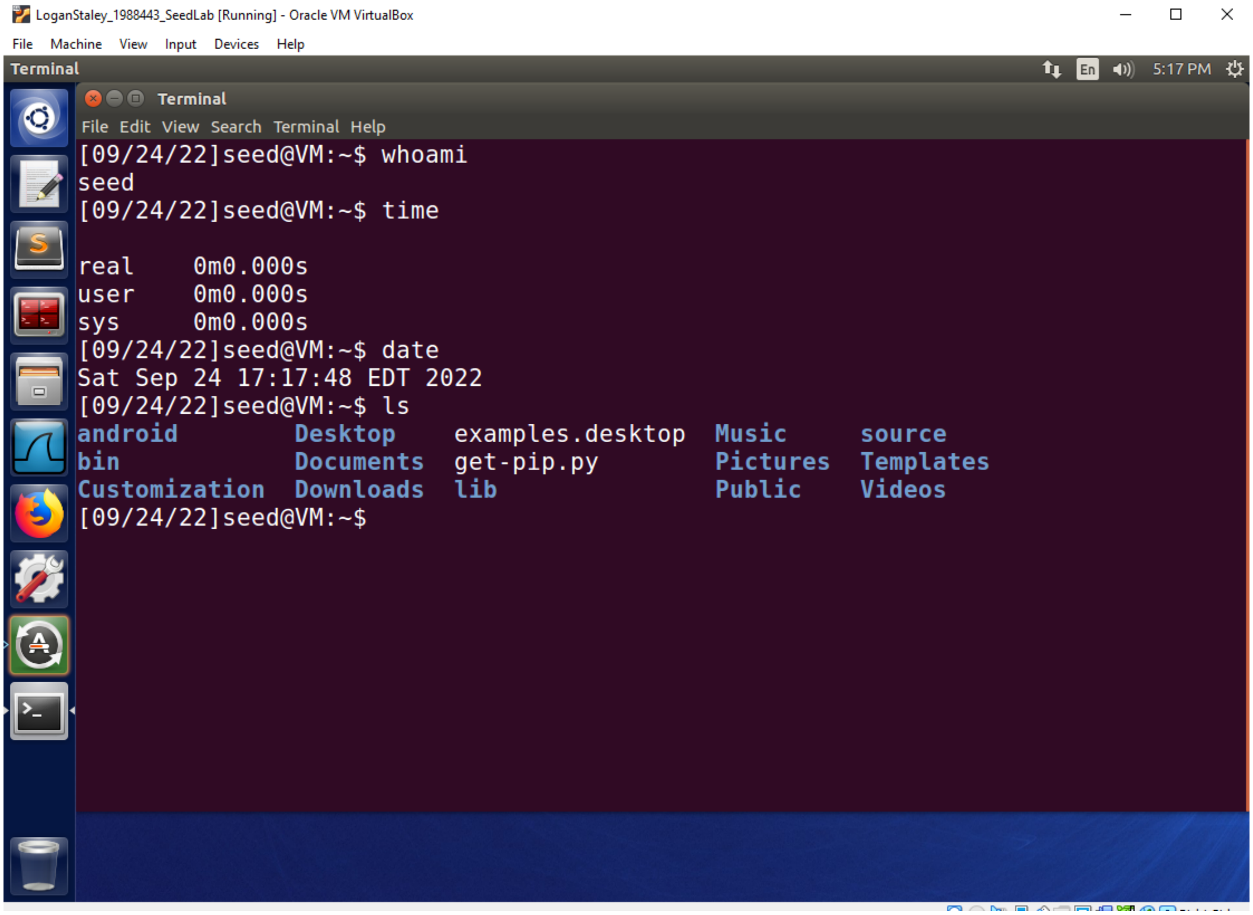
b. What is the role played by the SEED Ubuntu16.04 VM image?

    i. The image file that is provided is a template for the virtual machine to use to create the operating system from the ISO file. This is a good way to capture a image of an OS of a computer or device and recreate that in a virtual machine on a different device to find problems with the Operating system if needed. In this specific case the image file is vital in setting up the ubuntu operating system and having it set up in the exact way needed for this example.

c. How many VMs can you run simultaneously within a virtual box

    i. This is an open-ended question, there is no limit that the virtual machine software to restrict the number of virtual machines. Its more of the case for the host computer that the virtual machine is running on. This factor is up to the hardware and design of the computer.

d. Here is the screen shot showing the process defined in this question is accurately completed.


LoganStaley_1988443_SeedLab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
5:17 PM
Terminal
File Edit View Search Terminal Help

```
[09/24/22]seed@VM:~$ whoami
seed
[09/24/22]seed@VM:~$ time

real	0m0.000s
user	0m0.000s
sys	0m0.000s
[09/24/22]seed@VM:~$ date
Sat Sep 24 17:17:48 EDT 2022
[09/24/22]seed@VM:~$ ls
android        Desktop    examples.desktop  Music     source
bin            Documents  get-pip.py        Pictures  Templates
Customization  Downloads  lib               Public    Videos
[09/24/22]seed@VM:~$
```

References

(R1)- Wikipedia contributors. (2022, August 26). Replay attack. In *Wikipedia, The Free Encyclopedia*. Retrieved 19:46, September 24, 2022, from https://en.wikipedia.org/w/index.php?title=Replay_attack&oldid=1106843242

(R2) - Yasar, Kinza, and Michael Cobb. "What Is a Man-in-the-Middle Attack (MITM)? - Definition from Iotagenda." *IoT Agenda*, TechTarget, 28 Apr. 2022, https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.