UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

COS 330

Practical 1

Specification

Release Date: 06 August 2014

Due Date: 12 August 2014 (23H59)

Instructions

In this practical you are required to create an application that unveils your thorough understanding of computer security so far. You are allowed to use programming languages and technologies of your choice, as long as you can upload the application and download it from the CS website for demonstration, and as long as those applications work in the lab or virtual environment provided to you.

Note: The aim of this practical is NOT to test anything other than Computer Security concepts that you are expected to know by now.

Upload a zip archive of your code onto the CS website by the specified due date. If you do not demonstrate your program in one of the practical sessions, then you will not be allocated any marks (even if you did upload), i,e, you must be present in person at the demo sesison to be able to receive a mark.

Everything that you submit might be checked for plagiarism. Instances of plagiarism will be dealt with in a serious manner.

Background

So far you are expected to understand the theory behind *assets, vulnerabilities, threats, identification and authentication (*Refer to Chapter 1 of the prescribed textbook*).*

This practical will help you identify assets and how to protect them from unauthorized access (i.e. possible exploitation). That is, only **legally known** people must be allowed to gain access to the asset(s).

Task 1 [15 Marks]

Your application should address all of the following properties:

- Your application must contain a registration functionality to allow *identification* of people when trying to access the perceived asset. [1]
- Registered users must have one of three access levels described below [2]
    - Level One: No Read/Write Permission
    - Level Two: Read Permission
    - Level Three: Read/Write Permission
- The above mentioned access levels are in relation to a file stored in your system (e.g. Text File). This will serve as your *asset*. [2]
- After registration, the registered user must receive a **UNIQUE** *authentication* code that will be used for logging into the application. [7]
- Consequently you will need to use some form of network communication mechanism for you to send an authentication code to the user. (Refer to COS 332).
- The Application must give users access based on their access levels. [3]

Task 2 [5 Marks]

Introduction to the Metasploit framework

This section of the practical is meant to introduce you to the Metasploit Framework, which is an ongoing computer security project that provides resources for researching vulnerabilities and developing exploit code so that an administrator can assess the weaknesses in their system, and employ the appropriate counter measures to facilitate the weakness.

You are advised to frequent the following website as it will be paramount to these practicals: http://www.offensive-security.com/metasploit-unleashed/Metasploit_Fundamentals .

Basic Terms

Vulnerability: A weakness which allows an attacker to break into or compromise a systems security.

Exploit: Code which allows an attacker to take advantage of a vulnerable system.

Payload: Actual code which runs on the system after exploitation.

It is important to understand these terms as they will be used quite frequently.

In this task we are going to start up a database service as well as a Metasploit service, so that we can get a "feel" of how these services work.

First we need to start up our database. [1 Mark]

The database is going to keep a record of every action that we are going to do to a target, so that we can review these records if we wish.

Metasploit uses a PostreSQL database to record the actions that are done in the framework and this database is also built into Kali Linux.

The command to start up the database is as follows:

service postgresql start

You should get a message back, this message should contain the PostgreSQL database version.

Once this is done we now must verify that our database is indeed running, to do so type in the command:

ss –ant

A list of running services should be displayed in the console, the one we are looking for is the one that is **listening on port 5432**.

If you cannot see this service, please contact an assistant as you cannot continue.

Starting up the Metasploit services [2 Marks]

Now we can get started with Metasploit. To start the service, type the commands:

service metasploit start

Once this service has started, we are going to start the Metasploit Frameworks Console.

The console allows us efficient access to virtually all of the options available in the Metasploit Framework. To start it up, we type in the command:

msfconsole

This may take a while to start up, but when it is done it will be noticeable that you have entered into the interface. Take note of the **msf >** instead of the conventional **root@kali** on the left side of the console.

Check that the Interface is connected to the database

As previously mentioned, the database is a very important tool, because it keeps records of all our states so that we can review them later. And it is thus very important to ensure that the interface is connected to it. We do so by typing the following command into the terminal.

db_status

You should get a message that states that we are connected to the database, if not, please contact an assistant at this point.

Finally [2 Marks]

We want to make sure that our interface can actually see our windows **virtual machine**, to do so we must ping out machine. To avoid Kali having to send a lot of packets to the machine we must tell it how many to send. We prefer that you send 10 packets and if none of them are lost, we know that our connection is well established.

Do so by typing the command.

ping –c 10 ADDRESS

-c : tells the ping command how many packets to send.

ADDRESS: This is the IP address of your Win7 virtual machine. To obtain this, type **ipconfig** into the console (cmd) of your windows machine. It is listed under Ethernet adapter Local Area Connection.

Total Mark: 20