Lab 9: Simple EXE Hacking with Immunity

**Huynh Ngoc Quang – SE181838**

**Task 1: Target EXE Recon**

**Get Immunity**

A screenshot of a computer

Description automatically generated

A computer screen with a white box

Description automatically generated

**Get putty.exe**

A screenshot of a computer

Description automatically generated

**Running Putty**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

**Starting the Immunity Debugger**

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Running Putty in Immunity**

A computer screen shot of a program

Description automatically generated

A computer screen with colorful text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Finding the "login as" Code**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

**Using Breakpoints**

A screenshot of a computer

Description automatically generated

A computer screen with green text

Description automatically generated

In Immunity, from the menu bar, click **Debug**, **Restart**.

A box pops up warning you that "Process 'putty' is active". Click **Yes**.

In Immunity, from the menu bar, click **Debug**, **Run**.

A Putty window opens, as shown below.

A computer screen with colorful text

Description automatically generated

Click in the Putty window. In the "Host Name (or IP address)" box, type

**ad.samsclass.info**

At the bottom, click the **Open** button.

A black window opens, but before the "login as" message appears, the program stops, as shown below.

A screenshot of a computer

Description automatically generated

The program stopped at instruction 0041CB6E, as shown in the image above.

We'll use this instruction to hijack the program's execution.

**Task 2: Alter the Login Message**

**Removing the Breakpoint**

A screenshot of a computer

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

**Viewing the Stored Message**

In Immunity, in the CPU window, in the Assembly Code pane, right-click the intruction at address **0041CB6E** and click "**Follow in Dump**", "**Immediate constant**", as shown below.

The lower left pane shows the stored "login as" message, in hexadecimal and ASCII text.

A computer screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

**Skipping the First Letter In the Message**

A computer screen shot of a computer program

Description automatically generated

An "Assemble at 0041CB6E" box appears, as shown below.

This shows the command at this location. It's a PUSH instruction, placing the address 467C7C onto the stack. That address points to the letter "l" in the ASCII string "login as: ", as shown on the right side of the instruction line, outlined in green in the image below.

A screenshot of a computer

Description automatically generated

In the "Assemble at 0041CB6E" box, change the last character to **D**, as shown below. This will move the pointer from the "l" to the "o" in the string "login as: ".

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Running the Modified Program**

A computer screen with a black screen

Description automatically generated

**Inserting Your Name**

Now we want to change the text from "ogin as: " to your name.

Move your mouse into the lower left pane of the CPU window, which is the "hex dump" pane.

Right click, point to "**Go to**", and click **Expression**, as shown below.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

In the top left of the Hex Dump pane, point to **6F**, hold down the left mouse button, and select the entire row of 8 bytes. Then release the left button, point to **Binary**, and click **Edit**, as shown below.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Saving the Modified EXE**

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

**Running the Modified EXE**

A computer screen shot of a computer screen

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated