**PERFORMANCE PHASE–SENIOR CYBER CAPABILITIES DEVELOPER**

**WINDOWS EXAM**

**MODULE STRUCTURE**

You will do all of your work for this exam on a virtual machine (VM).

To unlock the VM, the password is “vagrant” (all lowercase).

On the left side of the desktop, you will find a folder entitled, “Exam,” that contains the 4 modules you will be working on.

When opening IDA Pro from the desktop, if it asks for a license server, enter 192.168.10.14

With the exception of Modules #4 and #5, it is a good idea to spend some time reviewing each of the test case files per module to see the data being passed to your function and the expected results.

**Modules #1 and #2: User Mode Modules**

* This exam uses Microsoft Visual Studio.
* Both modules are in the *Eval.sln* solution file in the *Exam/Windows* directory.
* After opening up the solution file:
* To see your code for Module 1 in Visual Studio, navigate to the “Solution Explorer” window and look for the *WindowsUMPart1* directory.
* To see your code for Module 2 in Visual Studio, navigate to the “Solution Explorer” window and look for the *WindowsUMPart2* directory.
* For User Mode Part 1, develop your code in the provided *WindowsUMPart1.cpp* file.
* For User Mode Part 2, develop your code in the provided *WindowsUMPart2.cpp* file.
* Both *WindowsUMPart1.cpp* and *WindowsUMPart2.cpp* files contain instructions on how to complete the modules.
* After completing each module, take a screenshot and save it in the same directory where you have your source code.

**Module #3: System-level Driver Module**

* This exam uses Microsoft Visual Studio.
* The module is in the *Eval.sln* solution file in the *Exam/Windows* directory.
* After opening up the solution file, to see your code in Visual Studio, navigate to the “Solution Explorer” window and look for the *Evaldriver* directory.
* Go to the *Source Files* directory and develop your code in the *main.cpp* file.
* The instructions and requirements for this module are in the *main.cpp* file.
* You are provided two VMs: A Development VM called vagrant\_windows\_eval and a Sandbox VM called vagrant\_windows\_driver.
* The Sandbox VM is used to load and run your driver code. It also safeguards your Development VM from crashing.
* On the Development VM, use the helper script entitled *load\_driver.ps1* located in the *Exams/Windows* folder when you are ready to load and run your module on the Sandbox VM.

***NOTE:*** The *load\_driver.ps1* script will do the following: Contact your Sandbox VM; stop the service on your Sandbox VM that runs the driver; transfer your driver code to the Sandbox VM; and restart the service running the new driver code on the Sandbox VM.

* You can run your code with the executable called *DriverTest.exe* located in the *DrvTest* folder on the Sandbox VM desktop. Run this from the command prompt.
* When debugging this module from the Development VM, you will use WinDbg. You will find the debugging key in the *Exam/resources/debugging\_key.txt* file.
* Once you have completed the module, take a screenshot and save it in the same directory where you have your source code.

**Module #4: Vulnerability Research/Reverse Engineering and Exploitation Module**

* This module is in the *Exam/RE\_VR* directory.
* The instructions are found in the *Instructions.txt* file.
* Develop your code in the provided *client.py* file to accomplish tasks #2 and #3 from the *Instructions.txt* file.
* Develop your Assembly code in the *RE\_VR/shellcoder/shellcode\_gen/shellcode.S”* file.
* Document your findings in the *research.txt* file.
* The grading criteria consists of a code review and whether or not a valid image file is returned from the remote server.
* Once you have completed the module, take a screenshot and save it in the same directory where you have your source code.

**General Information**

The provided function header names and parameters must remain the same in your source code.

All of your solutions must be persistent.

You may spend as much time as desired on each module. You may complete the modules in any order—you do not have to complete one module before moving to another module.

Note: If you pull the modules out of your exam folder, the modules will not build!

You will be graded upon completion of work and code functionality. You will not be graded on coding or format standards.

Do not delete your code even if you think it may be incorrect or incomplete. This could show the logic you used even in an area you may not be strong in, which could increase your score.

Do not close or stop the VM. Leave it in the state it was when you finished.

When your exam is complete, zip the exam folder and upload it to the web application in the browser where you opened your account today.