**CMSC 491/791 Active Cyber Defense HW 8**

**Name:**

**Due: November 20, 2019 at 7:00pm**

Summary:

This assignment has two parts. In the first part of this assignment, you are given a vulnerable C program. You must exploit the vulnerability, then patch the vulnerability while retaining program functionality. In the second part of the assignment, you must use Metasploit to exploit a vulnerability in a Windows 2008 Server VM.

Setup:

Download and unzip metasploitable-linux-2.0.0.zip from the following website:

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

In virtualbox, create a new virtual machine. It should have the type “Linux” and version “Linux 2.6 / 3.X / 4.X (64 bit)”. When you are prompted about the hard disk, choose the option for “Use an existing hard drive file” and select Metasploitable.vmdk.

You will need a second Linux VM for this lab to serve as an attacker. Kali Linux is preferred if you have it, but you can also use Ubuntu 18.04.

In the VirtualBox network settings for your Metasploitable VM, set Adapter 1 to Host-only Adapter and Adapter 2 to NAT. Do the same for the VM you are using as an attacker. Start both VMs. The username and password to the Metasploitable VM are msfadmin:msfadmin.

Use the wget command to download the provided davesemporium.c from the course website to your Metasploitable VM. Ensure that both VMs can ping each other and access the internet before proceeding.

Part 1

1. Answer the following questions regarding the source code for davesemporium.
   1. What level of user privileges does the executable need to have in order to properly function?
   2. Compile the binary using the command gcc davesemporium.c -o davesemporium. Does the binary have the correct user privileges? If not, change the owner and group of the binary so it has the correct privileges. What command did you run in order to do this?

* 1. Run davesemporium as a normal useron the Metasploitable VM. Connect to the socket from the attacker VM by using the command nc <metasploitable\_ip> 1337. When you do so, the program will not function properly. What special attribute will you need to set on the davesemporium binary in order to make it work? What command did you run in order to do this?

1. Answer the following questions regarding your exploitation technique.
   1. What type of vulnerability exists in the davesemporium binary?
   2. How would you exploit this binary? Give an example input that you could send to to the davesemporium binary in order to execute arbitrary commands on the Metasploitable VM from the attacker VM.
   3. Exploit the binary and provide a screenshot of your attacker VM sending commands to the Metasploitable VM.
2. Answer the following questions regarding your patching technique.
   1. What line/function in the source code is causing this vulnerability? What is unsafe about this call?
   2. What is a safer alternative to this function? Why is it safer? How must your source code change to implement this function?

* 1. Patch files are often used to show changes made to source code. Create your patch, then create a patch file using the command diff -u davesemporium.c davesemporium\_new.c > davesemporium.patch. Paste the contents of your patch file below.

* 1. Ensure your patch worked properly. Recompile the davesemporium binary and attempt to use the same exploit as in 2.c. Take a screenshot of your exploit failing on the patched version of the binary.

Part 2 Setup:

If you are using Ubuntu 18.04 as your attacker VM, you can install metasploit using the following instructions:  
  
<https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers>  
  
One it is installed, start Metasploit on your attacker VM with the command msfconsole.

Part 2

1. From the msfconsole, run a port scan of the Metasploitable VM. Provide a screenshot showing what services are listening and what their versions are. What command did you run to do this?
2. List one service running on the Metasploitable VM that has a vulnerability that grants remote code execution (RCE)? What is the version of this service? What is the CVE designator of this vulnerability?
3. What command did you run in msfconsole to select the exploit? What options did you set?
4. Describe the difference between a bind shell and a reverse shell. Which should you choose if you suspect that the target computer has restrictive firewall rules for inbound network traffic?
5. Select an appropriate payload in msfconsole. Which payload did you choose and why? What command did you run to do so? What options did you set?
6. Provide a screenshot showing that your exploit was successful.