Assignment 3

Due 11:59PM, March 10, 2017

(This document has been updated as of March 10, 2017)

In this assignment you will have an opportunity to write an exploit to remotely gain control on a host.

Attack Scenario

The **victim machine** is a RedHat9 machine that has the vulnerable web server nweb running. The RedHat9 machine is hosted in the class Infrastructure with IP address: **10.247.49.156**; the nweb service is running under port **8888**. You will need to write an exploit generator for this target. You exploit will be sent to the target machine, and it needs to return a shell to the **attack machine,** at IP address: **10.247.49.145**.

You need to first develop the exploit on your own laptop like we did in the class. Then you can change payload to test the exploit on the real target. You are given an account on the attack machine. Login using **username: *attack,* password: *password***

Tools

Before launching your attack in the target victim machine. You should first make the exploit work on a victim that you control. The RedHat9 image is given and can be downloaded from the following link: https://drive.google.com/open?id=0BzkPm4m1AGy4N3Z4TldfNXRudlU

1. Download the **redhat9.ova** file and import it to your VMware software.
2. Login to the redhat9 virtual machine with username: ***root***, the password should be empty by default.
3. The nweb should be already compiled under the default directory (to install by yourself, please refer to the class instruction file), run the nweb program and test the website to make sure it is working.
4. Develop the exploit, make it work on your local RedHat9 VM.
5. Adjust your exploit to use the payload for returning the shell to the attack machine. Launch the exploit towards the victim machine on the infrastructure, and get a shell on the **attack machine**.

You will need a debugger to observe the crashed program and gather important information for developing your exploits. In the class we used gdb to open a core file (please refer to the class instruction file).

You will need to search for the “jump code” in shared library to indirectly jump to your shellcode. You will first need to identify which library code to search. One Redhat9 VM, do:

ldd nweb

You will find the shared library path. Pick the library you want to use, and copy it to Kali. Use the following Metasploit command to search for instructions that jump through ESP:

msfelfscan –j esp file_to_be_scanned

There will be multiple entries returned. You need to pick one address that has no zero byte in it (why?)

For generating shellcode, you will need to use Metasploit. The payload and encoder you are going to use are still the same: **linux/x86/shell_reverse_tcp** and **x86/alpha_mixed**.

For the final testing (step 5), since everyone would be using the same attack machine, please choose your own port number for your shellcode in this step, so that it is unlikely to conflict with another person's port number.

Submission

Submit a zip file that contains:

1. Source code of your exploit generator that will compromise the victim machine on the infrastructure. Your exploit generator must print the exploit to the standard output. Make sure the shell is returned to the attack machine (**10.247.49.145**). *If you cannot make your exploit work on the infrastructure but made it work on your local machine, submit both the non-working exploit generator and the working one on local machine. The local exploit shall return the shell to local host 127.0.0.1 at port 4444.*

2. One page report that documents a) how to execute your program from command line; b) which port number the shell is sent to; c) whether your exploit works (locally or in the infrastructure); d) how you developed the exploit; and e) if you cannot finish, your progress and what was the problem you encountered.