Computer Security: Laboratory 5

February 9th 2023

Vulcan IP : **10.6.18.173**

Set up ssh jump tunnel	ssh -L port1:10.6.18.176:80 you@10.6.18.173
Deep scan with nmap	nmap -A <host>

Important: In this lab you are allowed to work either individually or in groups of up to 2.

For the next 3 laboratories you will be working with your own virtual machine. Your task in this laboratory is to examine the machine for security problems and attempt to fix them. We will guide you through some of them, but you should not assume they are the only problems on the machine.

You have a week to secure your machine, and create two "flags" as described below. By 12.00 next Wednesday you should place a copy of your virtual machine in the shared directory: */home/students*

In next week's laboratory we will activate all the submitted machines, and you can then attempt to break into as many as you like. A (very) small prize of candy will be provided to the student or group who gets the most points. Points will be awarded for flags obtained from other machines, and for detecting successful attacks on your machine, weighted by the number of students in your group.

Rules of Engagement

The machine must retain its functionality, you cannot disable the website or remove any software.

1. The website must stay online and functional, attached to its SQL database, but you are allowed to modify the WWW pages as you like, preserving their visible text content.
2. You cannot delete existing user accounts from the system.
3. As usual in Computer Security, anything that is not expressly forbidden is permitted, you can for example turn on accounting or install monitoring packages if you like.

Virtual Machine Setup

1. Take a copy of the *\tmp\Lab5-wilbur.ova* file to your home folder on vulcan. Please rename it to your group id, eg. group1.ova (Group Id's for the lab should be chosen from the Lab5_6 group.
2. *"wilburwhateley/+yog_sototh"* is the login/password for a superuser of the machine in order for you to be able to secure the machine.
3. To be able to alter the mysql database you need to log into it as the mysql 'root' user. The password for the root user is *"_theGate&Thekey"*. To access the mysql database, you use the command *mysql -u root -p* and then input the root password.
4. To run the machine, you should use virtualbox on vulcan. To do that, do the following:
   - From the command terminal on Vulcan using ssh -X or -Y.
   - Run *virtualbox* (Note, there is also a command line interface if you prefer, *vboxmanage*)
   - In the VirtualBox GUI, select the "file" menu, and then "import appliance".
   - Select the .ova file you copied from /tmp
     - *IMPORTANT*
     - You will need to set the network mode to 'bridged adapter' in the machine settings.
     - Under the network settings (when the machine is powered off) press the refresh MAC button a few times to make sure you have a unique MAC address.
   - You should now be able to run the machine, if you log into it using the console you can find its IP address using the terminal command 'ip addr', and then ssh to it normally.
   - You should now be ready to continue with the lab.
5. Create two files called FLAG, which can either be text or an image of your choice (Files should be different), and place one in the admin account's directory, and one in the root directory. Set file permissions so that they are owned by the account whose directory they are in.

Metasploit search

Metasploit allows you to search for an exploit to use.

1. Start the metasploit console with the 'msfconsole' terminal command.
2. Type 'search' along with any search term you'd like
3. If your search yields any results you can simply type 'use #' substituting '#' with the index of the exploit search found.
4. Now you can use metasploit normally.

Securing your Machine

1. As usual, probe the machine.
   - nmap scan it for open ports and services
   - If you find a Web server, use nikto and/or dirb to look for problems
   - Use metasploit search to look for issues with any exposed programs
2. You may well find that the web server is misconfigured.
   (a) Which web server is the machine using to host its content?
   (b) Use the search function in metasploit or searchsploit to see if there is an existing exploit for the web server.
   (c) Is the web server somehow leaking unnecessary information? (hint: check the response headers)
   (d) Look at the server configuration files to see if the web server can somehow access files or directories that it should not be able to access.
3. It seems there is an "SQL injection vulnerability" on the website.
   (a) Look at the code for the blog, is there something you could do to the PHP source code to prevent SQL injection attacks?
4. Check the users on the machine to see if there are any weak passwords
   (a) For a list of the users that can log in on the system you can look at which lines have a "*/bin/bash*" in the */etc/passwd* file.
   (b) You can then use an SSH brute force program such as metasploit's *scanner/ssh/ssh_login* to test each login against a password dictionary.
5. Is all software up to date?
6. Other checks may well be useful.

Advanced

1. Port Scan Atack Detector is a lightweight tool that collects data on scans, this will let you see attack attempts on your machine. (apt install psad - `https://cipherdyne.org/psad/`
2. SNORT (`snort.org`) is an intrusion detection system.
