Penetration Testing Guide: Teacher’s Guide

In this lab students will be using python scripting to penetrate a vulnerable machine. The target machine is a metasploitable 2 machine. Students aren’t supposed to know that it is a Metaspoitable 2 machine. Its assumed this machine is deployed on VSphere in the same local subnetwork as the attack machine

The machine is available for download:

<https://information.rapid7.com/download-metasploitable-2017.html>

There were some very light modifications made on the same machine:

* Added a file to secret.txt to the /root directory
* Modified the /var/www/index.php file
  + Deleted the “Metaspoitable 2” text banner
  + Resarted the apache2 server sudo /etc/init.d/apache2 restart

A list of exploits for this machine is available at

* <https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide>
* <http://blog.securelayer7.net/attacking-metasploitable-2-using-metasploit/>

Not all the exploits that work in the metasploit console will work in the metasploit console library.Students will have to play with different payloads and exploits to see what works.

Here is a list of known exploits in the python library using pymetasploit3.

* ‘exploit/unix/ftp/vstpd\_234\_backdoor’
  + Payload: ‘cmd/unix/restart’
* ‘exploit/multi/samba/usermap\_script’
  + Payload: ‘cmd/unix/bind/bind\_zsh’
* ‘exploit/multi/http/tomcat\_mgr\_deploy’
  + Payload:’java/shell/bind\_tcp’

There are comments in each of the answer scripts going over how the scripts work. In the scripts 10.50.1.78 is the ip of the target machine.