Host Exploitation

1.0 Objective

In real world networks are often compromised using vulnerabilities in the software and services that they host. This also happens to be one of the easiest ways to gain access given the easy availability of exploits and frameworks that are used to quickly build one. The aim of this exercise is to gain understanding of basic exploitation techniques used by hackers & pen-testers alike and understand the post-exploitation possibilities.

Using the single ip address on which you performed reconnaissance in lab two we are now going to exploit the host using the information which we gathered. Again the target should be within the ip address range of 10.10.111.0/24 in the ISIS lab.

DO NOT TARGET ANYTHING OUTSIDE OF THIS IP ADDRESS RANGE. IN ADDITION, THIS EXERCISE MUST BE PERFORMED WITHIN THE CONFINES OF THE ISIS LAB.

1.1 Exploit Discovered Hosts

To do this exercise, you'll need to have a thorough understanding of the Metasploit Exploit Framework – this is a community project that is widely used in Infosec. The tool is used to perform authorized penetration testing, IDS signature detection and exploit research.

Task:

Thoroughly research the Metasploit framework and familiarize yourself with its use. There are a number of resources available on the web. Here are a few to get your started:

http://www.offensive-security.com/metasploit-unleashed/

http://www.securitytube.net/Security-Tools-Video-List.aspx

You will also find some resources on the class Wiki which might prove to be helpful

Now, use Metasploit to compromise the single Windows XP machine on which you performed your reconnaissance in Lab 2. You will need the information gained in lab two to effectively target your attack against a known vulnerability.

Gain shell access and transfer a file of your choice from the target machine to your Backtrack machine. Also perform a remote screen capture *using Metasploit* of the compromised machine. You will need to use an auxiliary module to do this. Be sure to document each step you take with both screen shots and descriptions of the commands employed.

1.1 What to Submit

What to submit:

- Screenshots of the steps employed during your attack using the Metasploit framework along with a complete description of your steps. Perform screen captures of both the Metasploit machine and the target machine to prove that you have accomplished shell access to the remote target.