Host Exploitation

1 Host Exploitation

In the real world, networks are often compromised using vulnerabilities in the software and in 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.

1.1 Objective

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 2, we are now going to exploit the host using the information that we gathered. The target should be within the VLAB IP address range of 10.10.111.0/24.

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

1.2 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 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 you started:

http://www.offensive-security.com/metasploit-unleashed/
http://www.securitytube.net/groups?operation=view&groupId=10

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 2 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. Finally, install the *persistence* Meterpreter service. Be sure to document each step you take with both screen shots and descriptions of the commands employed.

1.3 What to Submit:

For each task, provide a complete description of your steps, include all commands used, the reason why each command was used, and screenshots of the steps employed during your attack using the Metasploit framework. Perform screen captures of both the Metasploit and target machine, show the commands used and results to prove that you have accomplished each of the following steps:

[10 pts] Determine working exploit. Explain how you found this exploit, and why did you believed it would work.
[20 pts] Obtain shell access to the Windows XP machine using the Meterpreter payload and set all necessary options correctly.
[10 pts] Transfer a file of your choice from the target machine to your Backtrack machine.
[10 pts] Perform a remote screen capture of the compromised machine using Metasploit. This can be done using an auxiliary module.
[20 pts] Install the persistence Meterpreter service on the Windows XP machine that will automatically connect back when the system boots. Reboot the Windows XP machine and show that it automatically connects back to the backtrack machine.

2 SCAPY/Python Programming

2.1 SYN Flood Attack

Definition:

A SYN flood creates massive numbers of TCP SYN packets from spoofed source addresses and directs them toward a particular TCP server. The goal is to overwhelm the server by forcing the targeted TCP stack to commit all of its resources to sending out SYN/ACK packets and wait around for ACK packets that will never come.

Objective:

1. Write a Python script to create a SYN flood attack from the BackTrack 5 machine to a specified IP address (for this lab the target will be the windows XP machine).
2. This script should implement a many to one SYN flood attack, i.e. many ports from the BackTrack5 IP address sending SYN messages to the NetBIOS service running on port **139** on the Windows XP machine.

Setup:

For this assignment we will need one prerequisite setup task. By default the Linux kernel sends an RST in response to a SYN-ACK received from the server. This is because of a lack of communication between SCAPY and the kernel. For this reason an IPTABLES rule needs to be created in the BackTrack5 machine to block any outgoing RST packets. To do this, open up a command prompt in the BackTrack5 machine and run the following code:

```
sudo iptables -A OUTPUT -p tcp -s [IPADDRESSofBT5] --tcp-flags RST RST -j DROP
```

Next verify that the command is in the output chain. To do this, use the command:

```
sudo iptables –L
```

If you don’t see the command listed under the OUTPUT chain then it wasn’t entered properly. **Note that this command will only last until you restart your BackTrack5 machine, as it is a temporary command in IPtables.

2.2 What to submit:

[15 pts] The Python script, along with a description as to what the code is doing.
[15 pts] Screen-shots with description, of both the attacker and the victim’s machine, showing the SYN flood attack in action. For the Windows machine screenshot, open a command prompt (cmd.exe) and use the command ‘**netstat –a’** to show the ‘**syn_recv’** state next to the ½ open connections being made. **Note that if the command prompt is taking a while to finish listing and becoming unresponsive you may want to open multiple and run multiple instances of that command.