Maintaining Access with a Rootkit

Objective

The purpose of this lab is to demonstrate the final step in the network attack methodology; maintaining access. Once you have compromised a host machine as you did in the previous lab you will want to install some form of software which will allow for you to maintain persistant access to the machine. This should allow for continued access to the compromised host. Further, the software should be transparent and hidden to the end user.

To achieve this goal we will be using the HackerDefender Windows Rootkit

For each step in the lab, perform screen captures with a written explanation describing the step taken.

1.0 HackerDefender Rootkit Background

HackerDefender was written by "HolyFather" and is one of the most popular user mode rootkits for windows. The developer of this rootkit went so far as to turn it into a business where he would compile your own custom version of HackerDefender which was guaranteed to evade rootkit detection programs. This posed a challenge for the anti-malware companies as there were versions of HackerDefender that could not be detected when looking for the signature of the free version of HackerDefender.

In order to familiarize yourself with this rootkit, read the lab handout titled "HackerDefender Rootkit for the Masses" which is posted on the class website.

1.1 Root the Box

In the last lab you should have achieved remote shell from the Backtrack Linux machine to the Windows XP host. The purpose of this lab is to install HackerDefender on the WindowsXP machine and maintain this access.

BEFORE STARTING BE SURE THAT ALL OF YOUR VMS ARE POWERED ON.

Download the hackerdefender files from the lab web server to the Backtrack machine.

The lab web server is located (with the file) at the following URL:

http://10.12.1.10/hd/hd-1.0.0/

Also download netcat from the lab web server to the Backtrack 4 machine.

http://10.12.1.10/nc/nc11/

After downloading the appropriate HackerDefender files read the included readmeen.txt to further aquatint yourself with setting up HackerDefender.

Transfer HackerDefender and netcat to the WindowsXP Machine.

An extra 20 points (bonus) will be awarded if you install these using the remote exploit which you demonstrated in Lab 3. In other words if you can install and configure HackerDefender from a remote Meterpreter session you will be awarded an extra 20 points. So the maximum possible for this lab will be 120 points.

If want to forgo this 20 point bonus then you can transfer the HackerDefender rookit and netcat directly from the remote terminal session from the SFTP server provided as part of the vlab infrastructure.

First run netcat on the windows machine and transfer a file of your choice, using netcat, from the Windows/System32 directory to the Backtrack5 machine. You can choose any TCP ports that you wish for this transfer. Refer to the "Netcat Cheat Sheet" which is posted on the class website. Also google netcat and you will find plenty of references and examples.

Using the windows command "netstat" show that netcat can be seen listening on the port you selected.

Go to Windows TaskManger and demonstrate that nc.exe can be seen running.

Now configure, install and execute HackerDefender to hide the presence of nc.exe **and itself** from both Task Manager and the netstat command. Be sure to install HackerDefense as a system service.

In addition, install HackerDefender in a directory and hide that directory from normal browsing. Finally, install HackerDefender so that it starts up when the system reboots. You may do this with a Windows Registry key (google is your friend here). Then hide the HackerDefender registry key entry so that any regular user looking at the windows registry will not see the entry which you created.

Again transfer another file using netcat to verify that it is still functional.

Be sure to document each step taken using screen captures and a written explanation. Be sure to be VERBOSE in your explanations.

PLEASE BE SURE TO POWER OFF YOUR VMs WHEN YOU ARE DONE WITH YOU LAB WORK.