

Core Impact Tutorial

digg this story

Discuss in Forums {mos_smf_discuss:J. Peltier}

By Justin Peltier, Chief Technology Officer, Peltier Associates

How tough is it to really compromise a system? In a previous column we answered that question with a tutorial using MetaSploit[®] to penetrate a common vulnerability, RPC-DCOM. This month we will look to perform another common vulnerability penetration using the Core Impact utility. In future columns we will look at other common penetration testing utilities and conclude the series with a Shoot Out Review of each framework in a head-to-head test. NOTE: While not a free utility like MetaSploit[®], demo versions of the product are available from the manufacturer as well as a chance to WIN A FREE COPY OF CORE IMPACT!

The mission of this tutorial is to compromise a Microsoft IIS web server with the SSL PCT handshake vulnerability (also known as THCIISLAME) in order to run a SYSTEM level shell. So, let's get to work.

1. Click on the Core Impact Icon.

This should launch the Core Impact GUI. In the left hand pane of the GUI, click on the icon to open a "New Workspace." In the window that opens, fill in the information to look something like the figure below:

Once you have finished configuring the project details. Click on the "next" button. This should open the license dialog box. Just click on "next" as the license should already be set up. This should open the passphrase dialog box. Set the passphrase for your system to password. Once you have set the passphrase, move your mouse around in the box on the right hand side until the blue bar underneath the box is filled. If you have done this correctly your GUI should look like the figure below:

Once you have a window that looks similar to the one above, click on "Next". This will open the completion dialog box. On this screen, click "Finish". This should launch the Core Security console. It should look like the figure below. Take a few minutes to find the different panes in the console.

2. Now that we are inside the console, go to the Entity View pane and right click on the "localhost" icon and select "New Host" from the drop down menu.

3. You should now see the New Host dialog box. Change the fields on your system to match the IP address of your target system with the vulnerable function.

4. Once you have finished the configuration of this screen click on "OK".

5. If you look at your Core Impact console you should now see the a new icon with a Microsoft Windows® logo and the IP address that you entered in the previous step next to it. We now need to add some additional information about this device for our lab to be successful. To do this click on View and the Entity Properties from the Menu Bar with the newly created object highlighted. This should open and Entity Properties dialog box, and it should look like the figure below.

Click on the + sign next to the OS to extend the configurable options. Do the same for the properties menu that appears next. Once you have done this you should have four items to configure:

- Build Number
- Edition
- Service Pack
- Version

Set your properties to match the figure below:

Once you have the properties set, click on the close icon in the upper right hand corner to return to the console workspace.

6. In the console click on the tab in the Modules Pane to switch the review from RPT (Rapid Penetration Test) to Modules.

7. From the Modules list click on the Exploits icon followed by the Remote icon and scroll through the list until you see SSL PCT Handshake Overflow Exploit. Click on this exploit.

8. Once you single click on the name of the exploit, details about the exploit will appear in the Details about the Module pane (which is located at the bottom of the console).

9. Drag the exploit over to your Web Server icon in the Agents pane. This action should produce a dialog box like the figure below:

10. Leave all of the options set to the default and click on the "OK" button. This will execute the exploit against the web server.

11. In the Agents pane of the console, click on the + sign next to your web server icon. You should see a new item named level0(0) under your web servers icon. This means that the attack was successful and a return connection from the web server has been made to your attack system. This exploit only loads the connection into memory, but does not leave any files on the hard drive of the web server. Clicking on the Log/Debug tab of the Execution Module Status pane should also let you know that the attack was successful.

12. Your web server is now exploited. Let's see if we can do something with it. In the Modules pane of the console find the icon for Shells and select the Mini Shell.

13. Drag and drop this shell on the level0(0) agent in the Agents pane. This should pup up a DOS like window. This should look something like the figure below.

14. This shell uses primarily Linux commands. Type the command help into the window to see what we can do with this shell.

At this point you have a shell running on the vulnerable system with SYSTEM level permissions. You can start and stop processes, delete and insert files, and create backdoors using rootkits or Trojan files.

Mission Accomplished!

Editorial Comment

As a reminder, this article is simply meant to be a tutorial and not a review of the product. But don't be disappointed... a full review off all exploit frameworks will be coming in the next few months in a Shoot Out Review.

Stay Tuned... Next Tutorial will cover Immunity CANVAS