ICS014 ICS Lab 6 Using SimpleHTTPServer

Lab Objective

The objective of this lab is to understand Siimple HTTP Servers. Python's SimpleHTTPServer is a quick solution for serving the files in a directory via HTTP.

In this lab, you will learn to:

- Use Python's SimpleHTTP Server to pass a reverse_tcp payload to an end device

Lab Environment

This lab requires a wireless laptop or PC with Kali Linux flash drive and the ICS lab kit.

Lab Duration

10 minutes

Lab Tasks

Run Python's SimpleHTTPServer with optional HTML files

Lab Scenario

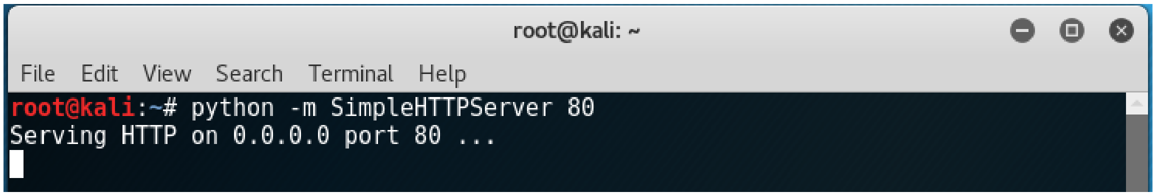
Once a payload has been created, the attacker will use various methods to trick the victim into clicking on it. For this lab, the victim will connect to a Web server and download an update for the DoMore PLC. A simple HTTP server will be used to store the reverse_tcp payload.

Step 1- Connecting to the Kali Wireless Access Point

1.
2. For this lab, connect Kali to the external Wireless Access Point that is associated with the lab. The internal LAN network is 192.168.30.x and is DHCP. The public facing IP Address of the WAP is a static address of 209.165.10.3, which simulates the public network. The public address will be used in this lab and was configured with Veil-Evasion. Refer to the figure below for topology addressing

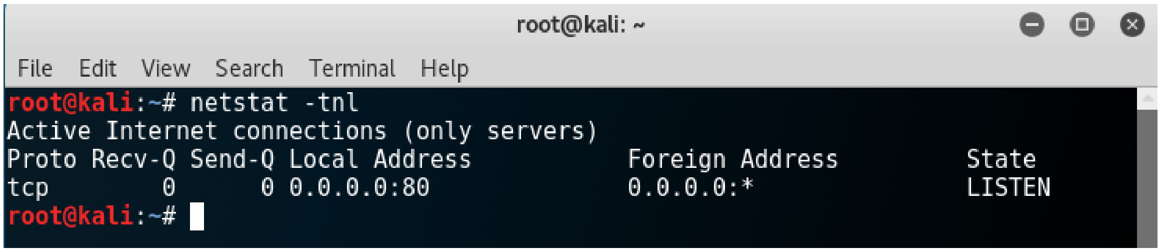
Step 2- Create a SimpleHTTPServer

1. Open a terminal prompt in Kali Live and change the directory to where the payload is stored. For this lab, the payload is stored on the Kali Desktop under the user root. Run the command shown in the output below. Use the port **80** that was created with Veil-Evasion (port 4444).



```
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

2. Open another terminal and use the **netstat –tnl** command to verify the port is listening.



```
root@kali:~# netstat -tnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
root@kali:~#
```

3. To stop the HTTP server at any time, just press Ctrl C

4. The payload is now attached to the Web server and ready for deployment when the victim connects.