**Will Pond**

Setting up the DNS by having the right hostname and ipaddress

**A computer screen with a black screen

Description automatically generated**

Building the container images

A screenshot of a computer

Description automatically generated

Starting the containers

A screen shot of a computer

Description automatically generated

Getting the container ID

A screen shot of a computer code

Description automatically generated

Looking inside the vul.cgi

A screenshot of a computer

Description automatically generated

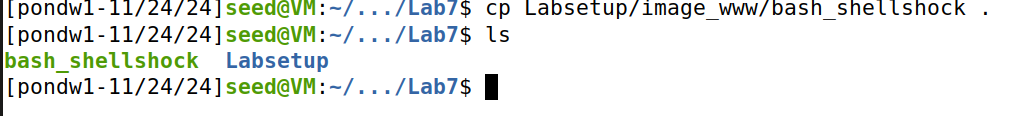
Making sure that I can access the website

A screenshot of a computer

Description automatically generated

**TASK1**

Copying the image\_www as bash\_shellshock



Created a C file named vul.c and wrote this program to run the attack

A screen shot of a computer

Description automatically generated

Copying the bash shellshock to the bin folder

A screen shot of a computer

Description automatically generated

Linking it to bin/sh and making sure it is linked

A screen shot of a computer

Description automatically generated

Making a setuid of vul and creating an environment variable foo and executing it to get the rootshell.

A screenshot of a computer program

Description automatically generated

Changing the linking to bin/bash and repeating the process again. After executing the vul program the attack fails

A screenshot of a computer

Description automatically generated

**TASK2**

Looking inside the getenv.cgi file

A computer screen with text

Description automatically generated

Making sure the website is accessible and getting HTTP request with environmental variables

A computer screen shot of a computer screen

Description automatically generated

Running this command curl -v www.seed-server.com/cgi-bin/getenv.cgi to print out the header of the HTTP

A screenshot of a computer

Description automatically generated

Running this command curl -A "my data" -v www.seed-server.com/cgi-bin/getenv.cgi using -A to define the user and sets the User-Agent.A computer screen shot of a computer

Description automatically generated

Running this command curl -e "my data" -v www.seed-server.com/cgi-bin/getenv.cgi the -e is use for refer URL



Running this command curl -H "AAAAAA: BBBBBB" -v www.seed-server.com/cgi-bin/getenv.cgi -H is use for a custom header to the server

A computer screen shot of a computer

Description automatically generated

**Conclusion of TASK2**

You can still launch the Shellshock attack, but the attack does not depend on CGI program code contents. It uses A CGI script to run but you can go through the URL from the server so you can run any arbitrary command to do it.

**TASK3**

Launching the shellshock command for the ls-l from the server

**A black screen with white text

Description automatically generated**

**Checking it in the rootshell**

**A screenshot of a computer

Description automatically generated**

Launching the shellshock command for the etc/passwd from the server

**A screenshot of a computer

Description automatically generated**

**Checking it in the rootshell**

A screenshot of a computer

Description automatically generated

Getting the process ID from the server

A black screen with a black background

Description automatically generated

Creating the a file inside the tmp folder from the server

A black screen with a black background

Description automatically generated

Showing that it has been created from the server

A black and white screen

Description automatically generated

Delete the file from the server

A screen shot of a computer

Description automatically generated

Also Checking it in the rootshell

A black and white screen with a black background

Description automatically generated with medium confidence

Deleting the file from the server

A black and white screen

Description automatically generated

Also checking it in the rootshell

A black screen with white text

Description automatically generated

**Question1**

Will you be able to steal the content of the shadow file /etc/shadow from the server? Why or why not? The information obtained in Task 3.B should give you a clue.

A black screen with white text

Description automatically generated

You cannot steal content of the shadow file because /bin/cat because you are not access it as root.

**Question2**

HTTP GET requests typically attach data in the URL, after the ? mark. This could be  
another approach that we can use to launch the attack. In the following example, we attach some data  
in the URL, and we found that the data are used to set the following environment variable:

Can we use this method to launch the Shellshock attack? Please conduct your experiment and derive  
your conclusions based on your experiment results?

**A screenshot of a computer

Description automatically generated**

No, you cannot use a query parameter can make the attack work or trying to encode

**TASK4**

Find the ipaddress by using ipaddress command

A screenshot of a computer

Description automatically generated

Find the ipaddress of root by using ipaddrsss

A screenshot of a computer

Description automatically generated

Running this command get the reverse shell

A black square with white text

Description automatically generated

Then listen on port 9090 and got the reverse root shell

A screenshot of a computer program

Description automatically generated

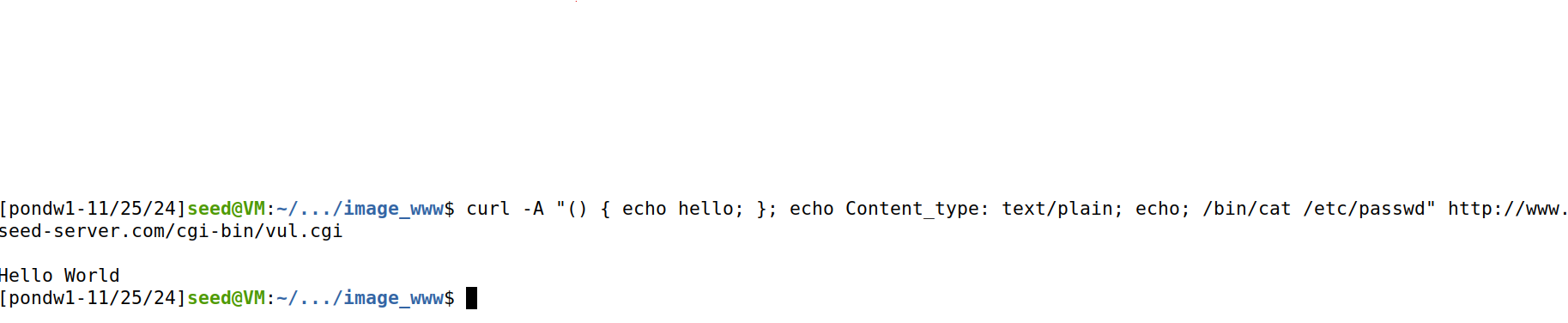
**TASK5**

Editing the vul.cgi and taking out the shell shock using nano

**A screenshot of a computer

Description automatically generated**

Repeating the process of Task3 part A



Repeating the process of Task3 part B

A black and white background with text

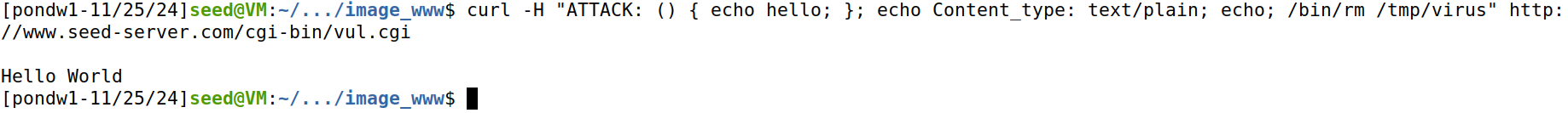
Description automatically generated

Repeating the process of Task3 part C

A black and white screen

Description automatically generated

Repeating the process of Task3 part D



**Observation For TASK5**

**ALL the attacks failed**

**LAB REFLECTION**

In this Lab I was able to explore and complete all tasks involving Shellshock. At the beginning of the lab, I had to set up the ipaddress and domain name of the attack. Then I did the standard setup for the lab like lab5 and lab6. In TASK1 I played around with Bash Function by linking it to lab’s website to see if the attack is possible.

TASK2 I was able to pass Data to Bash using Environment Variables. First using the browser and getting HTTP requests Than using the curl command with different options to get different forms of Headers. TASK3 was all about Launching the Shellshock Attack. The first attack was getting the etc/passd file, and I had to use -A approach to the command to make it work. Then it was the Process ID using -e approach to command to make it work. Next it was creating a file and deleting files inside the tmp folder which I had to use -H approach to the command to make it work.

TASK4 was getting Reverse Shell using Shellshock Attack. You first have gotten the ipaddress of the local machine and then the rootshell ipaddress. Then I use the curl with -A option with environment variable to get the reverse shell of the root user. TASK5 was Patching the Bash by editing vul.cgi and removing shellshock from #!bin/bash then redoing TASK3. After redoing TASK3 none of the attacks worked.