As a Penetration Tester, the constant need to practice our skills is required to improve our penetration testing (PT) abilities. Thus making this process a deliberate and willful one in order to be better at our craft. As a result, this write up serves our practicing and sharing. This walk-through will guide you as you also try hacking the [Hogwarts Virtual Machine](https://www.vulnhub.com/entry/hogwarts-dobby,597/) (VM) from VulnHub in your own lab environment. Ultimately you will add something to your existing skill-set because practice makes perfect, as I was told at some point of my life.

**YOU KNOW, WE TALKING ABOUT PRACTICE.**

A castle on a hill

Description automatically generated with low confidence

**But before we get started, Public Service Announcement...**

**THIS IS ONLY FOR EDUCATIONAL PURPOSES**. **DO NOT INSTALL/RUN THIS VULNERABLE VM ON ANY PRODUCTION NETWORK**!

**WHAT WE NEED TO GET STARTED**

* Installed version of [VMWare Workstation](https://www.vmware.com/products/workstation-pro.html), [Player](https://www.vmware.com/products/workstation-player.html) or [Oracle VirtualBox](https://www.virtualbox.org/)
* Download and Import [a copy of the Hogwarts - Dobby](https://www.vulnhub.com/entry/hogwarts-dobby,597/) VM
* The imported VM and ensure that network card (NIC) set to **HOST-ONLY**
* The attacker box NIC also to be set the HOST-ONLY settings

**Reconnaissance**

The most critical part of any PT engagement is Reconnaissance, but you already know that. However, gaining a good understanding of the target will assist in focusing the attack and reduce rabbit hole pitfalls. I once found myself spending two (2) hours searching for a exploit that was right in front of me the entire time. Again RECON, RECON, RECON...Here are the steps we used to gather information against Hogwarts:

Text

Description automatically generated*NetDiscover -r 192.168.56.0/24*

Text

Description automatically generated*NMAP -sC -sV -A IPADDR --open --systems-dns*

We found a web server based on the results of the Nmap scans and noticed that the title of the page field seems a bit weird, but is it? Based on normal title, this field is an area that website normal use ("Welcome To Our Website, etc"). Therefore, the website title is unusual because it has Base64 encoded data in the title. That being said, we need to decrypt it.

Text

Description automatically generated**Draco:dG9vIGVhc3kgbm8/IFBvdHRlcg==**

So we decrypt the Base64 portion of the HTTP-Title: "echo **dG9vIGVhc3kgbm8/IFBvdHRlcg==** | base64 -d (for decode)

So close...thought we had credentials. Oh well, kept digging by performing web type scans against the host. Gathering more data about this VM provides us with an attack strategy. We should use tools such as: Nikto, DIRB, BURP and GOBUSTER to find out more.

Text

Description automatically generated*Nikto* +h http://192.168.56.110

Text

Description automatically generated*DIRB* http://192.168.56.110

Text

Description automatically generatedgobuster dir -u http://192.168.56.110 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Graphical user interface, text, email

Description automatically generatedhttp://192.168.56.110

Further investigation shows that viewing the source code of the web server provided us with some useful information in terms of web directory that GOBuster, Nikto, DIRB picked up on. **GOT IT!**

Graphical user interface, text, application

Description automatically generatedView-source:http://192.168.56.110/

Browsing to the potential hidden website directory of /alohomora, we discovered information about the "DRACO" user. Let's see the page.

A screenshot of a computer

Description automatically generated with low confidencehttp://192.168.56.110/alohomora

OK...Quick google search reveals the following:

*"What house is Draco Malfoy in The son of a Death Eater,* ***Draco*** *was raised to strongly believe in the importance of blood purity. He attended Hogwarts School of Witchcraft and Wizardry from 1991-1998 and was sorted into* ***Slytherin*** *House*"

[*https://abcnews.go.com/Entertainment/harry-potter-draco-malfoy-now-member-gryffindor/story?id=28376898*](https://abcnews.go.com/Entertainment/harry-potter-draco-malfoy-now-member-gryffindor/story?id=28376898)

**This might be credentials, but lets keep going...**

We now have potential credentials here being **username: draco and password: slytherin**, but where can we use them on this website? We need to get more data about this host. Remembering that we found a phpinfo.php in our web scan, looking at this page gave us more data about the hosts system.

A picture containing text

Description automatically generatedhttp://192.168.56.110/phpinfo.php

Great information about the running Operating System (OS), Database and other useful information. This information is could be critical in discovering privilege escalation to root access to the system. However, let's not jump ahead of ourselves.

But wait we did find a **/log path** web directory as well. After navigating to that URL path, we base64 password and a hint.

Graphical user interface, text, application, chat or text message

Description automatically generatedhttp://192.168.56.110/log

Using Burp Suite, we were able to use the decoder tab to decrypt Base64 encoded pass ("**OjppbGlrZXNvY2tz**") to decrypted ("**::ilikesocks**");

Graphical user interface, text, application, email

Description automatically generated

The hint suggest that **/DiagonAlley** is another web directory path to research. I kid you not **WordPress**...FUN!

Graphical user interface, text, application, email

Description automatically generatedhttp://192.168.56.110/**DiagonAlley**

We found a WordPress site, let's try to get to the wp-login.php page. It works.

Graphical user interface, application

Description automatically generatedhttp://192.168.56.110/**DiagonAlley**/wp-login.php

Stepping back a bit, lets run **WPSCAN** against the WordPress site to see if we can gather more information about version, plugins, users, etc. for this website.

Text

Description automatically generated

This is a good place to pause the reconnaissance process at this time and focus on path to exploitation. But first let's reflect on what we know about the Hogwarts VM in order to successfully exploit the system.

**WHAT WE KNOW NOW**

* NMAP reveal *port 80/http* - This is a website
* Potential username and Base64 encoded value is in the ***http-title***
* Decoded base64 http-title value translate to: ***"too easy no? Potter"***
* We found ***/alohomora/*** in the web source on the index page
* Browsing to the ***/alohomora/***, we found a hint of the password for ***username: Draco***
* Based on the hint found on ***/alohomora/*** ; the question for password as to "What is the house of Draco?" web search revealed password of *"****slytherin"***
* Browsing to **/log** web directory and another base64 encoded value was found. Upon decoded it, another password was found (**"::ilikesocks**")
* The hint for web directory of ***/DiagonAlley*** brought us to ***WordPress website***
* We ran ***WPSCAN*** and examine the results which provide us addition details about the Hogwarts website.

Now for the FUN part you've been waiting on….**LETS GOOOOO**!!!

**EXPLOITATION**

A picture containing text, businesscard, vector graphics

Description automatically generated

We use the credentials collected for RECON.

Graphical user interface, text

Description automatically generatedhttp://192.168.56.110/**DiagonAlley**/wp-admin/

We are in. We navigate to the Theme-editor within WordPress. Selected the footer.php file. We add our PHP-reverse-shell script

Graphical user interface, text, application

Description automatically generated**http://192.168.56.110/DiagonAlley/wp-admin/theme-editor.php?file=footer.php&theme=amphibious**

**Setup listener**

Text

Description automatically generated

Switch user from **www-data** to **dobby**.

Graphical user interface, text

Description automatically generated with medium confidence

Searching and read FLag1.txt with VI.

Text

Description automatically generated

vi flag1.txt "Harry potter this year should not go to the school of wizardry"  
flag1{28327a4964cb391d74111a185a5047ad}

Get a copy of LinPeas from GitHub @ <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite>. Upload to the system to perform POST-EXPLOITATION Recon.

Text

Description automatically generated

Notice that the LinPeas stated that a SUID bit set in **/usr/bin/find** does not drop the elevated privileges and may be exploited to access the file system, escalate or maintain privileged access as a SUID backdoor.

Text

Description automatically generated

/usr/bin/find . -exec /bin/sh -p \; -quit

***Syntax***

Text

Description automatically generated

Setup ROOT listener to catch ROOT SHELL.

Text

Description automatically generated

**LOOT**

GIMME DAT LOOT... We were able to location the **proof.txt** file under the **root/Desktop** which is displayed below.

Text

Description automatically generated

proof.txt

We successfully performed reconnaissance, exploitation and looting of the Hogwarts VulnHub VM.

A picture containing tool

Description automatically generated