Algernon Priving Grounds

nmap -Pn -sC -sV -p 21,80,135,139,445,5040,7680,9998,17001,49664,49665,49666,49667,49668,4966 -oN nmap.md 192.168.163.65

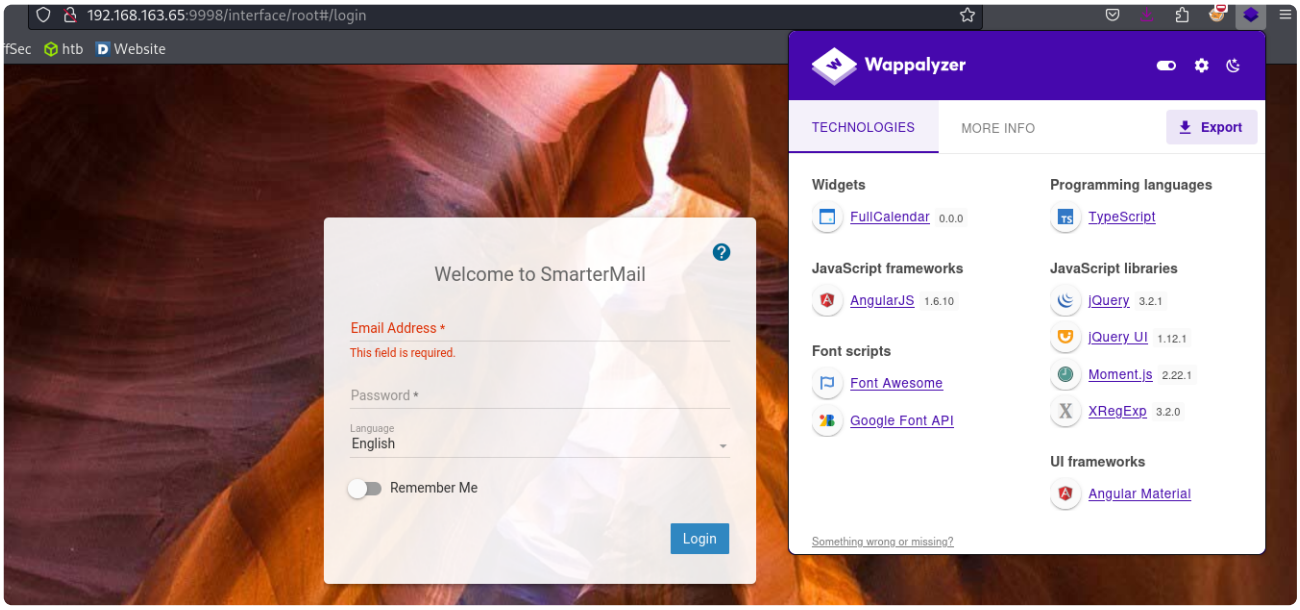
```
PORT      STATE  SERVICE       VERSION
21/tcp    open   ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  10:31PM       <DIR>          ImapRetrieval
| 05-27-24  11:03AM       <DIR>          Logs
| 04-29-20  10:31PM       <DIR>          PopRetrieval
|_04-29-20  10:32PM       <DIR>          Spool

80/tcp    open   http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
| http-methods:
|_  Potentially risky methods: TRACE

135/tcp   open   msrpc         Microsoft Windows RPC

139/tcp   open   netbios-ssn   Microsoft Windows netbios-ssn

445/tcp   open   microsoft-ds?

4966/tcp  closed unknown

5040/tcp  open   unknown

7680/tcp  closed pando-pub

9998/tcp  open   http          Microsoft IIS httpd 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: Mon, 27 May 2024 18:15:16 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

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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-05-27T18:15:19
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

```
nmap -sC -sV -p
21,80,135,139,445,5040,7680,9998,17001,49664,49665,49666,49667,49668,496
6 192.168.163.65 -oN nmap.md
```

9998

```
http://192.168.163.65:9998/interface/root#/login
```



https://www.exploit-db.com/raw/49216

```
PS C:\users\administrator\desktop> whoami /all

USER INFORMATION
----------------

User Name           SID
=================== ========
nt authority\system S-1-5-18


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
BUILTIN\Administrators                 Alias            S-1-5-32-544 Enabled by default, Enabled group, Group owner
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level Label            S-1-16-16384


PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Disabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
```