Anthem

Anthem

Exploit a Windows machine in this beginner level challenge.

10.10.182.229

[Task 1] Website Analysis

**This task involves you, paying attention to details and finding the 'keys to the castle'.
This room is designed for beginners, however, everyone is welcomed to try it out!
Enjoy the Anthem.
In this room, you don't need to brute force any login page. Just your preferred browser and Remote Desktop.
Please give the box up to 5 minutes to boot and configure.**

#1
Let's run nmap and check what ports are open.

No answer needed

#2
What port is for the web server?

80

#3
What port is for remote desktop service?

3389

#4
What is a possible password in one of the pages web crawlers check for?

UmbracoIsTheBest!

#5

What CMS is the website using?

umbraco

#6

What is the domain of the website?

anthem.com

#7

What's the name of the Administrator

solomon grundy

#8

Can we find find the email address of the administrator?

sg@anthem.com

nmap-scan

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
-------------------------------------------------------------------------------
135/tcp  open  msrpc         Microsoft Windows RPC
-------------------------------------------------------------------------------
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
-------------------------------------------------------------------------------
445/tcp  open  microsoft-ds?
-------------------------------------------------------------------------------
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| 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: 2020-07-21T22:21:18+00:00
| ssl-cert: Subject: commonName=WIN-LU09299160F
| Not valid before: 2020-04-04T22:56:38
|_Not valid after:  2020-10-04T22:56:38
|_ssl-date: 2020-07-21T22:22:20+00:00; +4s from scanner time.
-------------------------------------------------------------------------------
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
-------------------------------------------------------------------------------
Host script results:
|_clock-skew: mean: 3s, deviation: 0s, median: 3s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-07-21T22:21:20
|_  start_date: N/A
```

Versions:

CMS: **Umbraco 7.15.4**
Web Server: **IIS 10.0**
Web FW: **Microsoft ASP.NET**
OS: **Windows Server**
JS Lib: **jQuery 1.11.0**, **MomentJS 2.10.6**, **jQueryUI 1.11.4**
JS FW: **AngularJS 1.1.5**
UI FW: **ZURB**

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/
```

SiteMap

```
<urlset xsi:schemalocation="http://www.sitemaps.org/schemas/sitemap/0.9 http://www.sitemaps.org/schemas/sitemap/0.9/sitemap.xsd">
<url>
<loc>http://10.10.202.255/</loc>
<lastmod>2020-04-05T20:37:17+00:00</lastmod>
</url>
<url>
<loc>http://10.10.202.255/archive/</loc>
<lastmod>2020-04-05T19:11:38+00:00</lastmod>
</url>
<url>
<loc>http://10.10.202.255/archive/we-are-hiring/</loc>
<lastmod>2020-04-05T21:01:02+00:00</lastmod>
</url>
<url>
<loc>
http://10.10.202.255/archive/a-cheers-to-our-it-department/
</loc>
<lastmod>2020-04-05T21:02:29+00:00</lastmod>
</url>
<url>
<loc>http://10.10.202.255/authors/</loc>
<lastmod>2020-04-05T23:13:00+00:00</lastmod>
</url>
<url>
<loc>http://10.10.202.255/authors/jane-doe/</loc>
<lastmod>2020-04-05T21:11:16+00:00</lastmod>
</url>
</urlset>
```

gobuster-scan

```
/robots.txt (Status: 200)
/rss (Status: 200)
/search (Status: 200)
/sitemap (Status: 200)
/Archive (Status: 301)
/Blog (Status: 200)
```

```
/RSS (Status: 200)
/Search (Status: 200)
/SiteMap (Status: 200)
/archive (Status: 301)
/authors (Status: 200)
/blog (Status: 200)
/categories (Status: 200)
/install (Status: 302)
/tags (Status: 200)
/1075 (Status: 200)
/1076 (Status: 200)
/1074 (Status: 301)
/1078 (Status: 200)
```

[Task 2] Spot the flags

Our beloved admin left some flags behind that we require to gather before we proceed to the next task..

#1
What is flag 1?

THM{L0L_WH0_US3S_M3T4}

#2
What is flag 2?

THM{G!T_G00D}

#3
What is flag 3?

THM{L0L_WH0_D15}

#4
What is flag 4?

THM{AN0TH3R_M3TA}

[Task 3] Final stage

Let's get into the box using the intel we gathered.

#1
Let's figure out the username and password to log in to the box.(The box is not on a domain)

No answer needed

#2
Gain initial access to the machine, what is the contents of user.txt?

THM{N00T_NO0T}

#3

Can we spot the admin password?

ChangeMeBaby1MoreTime

#4

Escalate your privileges to root, what is the contents of root.txt?

THM{Y0U_4R3_1337}

writeup

--**ran nmap -sC -sV 10.10.93.26 and found open ports → 80, 135, 139, 445, 3389**
--found robots.txt and SiteMap file on server
--ran gobuster dir -w common-dirs.txt -u http://10.10/93.26
results gobuster-scan
--found CMS is Umbraco and possible password UmbracoIsTheBest! on robots.txt page

--Googles the poem written to admininstrator and got the name solomon grundy
--email is sg@anthem.com

--found flags in source code:
flag1 in meta THM{L0L_WH0_US3S_M3T4}
flag2 in source THM{G!T_G00D}
flag3 in source THM{L0L_WH0_D15}
flag4 in meta THM{AN0TH3R_M3TA}

--started a remote desktop connecion with rdesktop 10.10.93.26
--entered user SG and pass UmbracoIsTheBest!
--found user.txt on Desktop:
THM{N00T_NO0T}

--checked box ‘Hidden Items’ in File Explorer and found backup directory
--ran cd C:\ and then dir *.txt /s /a and found restore.txt
--ran cd C:\backup and then icacls restore.txt /grant SG:F to change permissions of file
--opened restore.txt and found password ChangeMeBaby1MoreTime
--opened an admin cmd prompt with SG and ChangeMeBaby1MoreTime
--ran cd C:\ and then dir root.txt /s /a and found root.txt
--opened root.txt to get contents:
THM{Y0U_4R3_1337}