Anthem

Enumaration

Nmap

Web port80

Gobuster

```
 gobuster dir -u 10.10.145.53 -w WordLists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.145.53
[+] Threads:        10
[+] Wordlist:       WordLists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/03/22 13:39:36 Starting gobuster
===============================================================
/archive (Status: 301)
/Archive (Status: 301)
/authors (Status: 200)
/blog (Status: 200)
/Blog (Status: 200)
/categories (Status: 200)
[ERROR] 2021/03/22 13:41:58 [!] Get http://10.10.145.53/com1: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/03/22 13:41:58 [!] Get http://10.10.145.53/com2: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/03/22 13:41:58 [!] Get http://10.10.145.53/com3: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/03/22 13:42:09 [!] Get http://10.10.145.53/con: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
/install (Status: 302)
[ERROR] 2021/03/22 13:46:18 [!] Get http://10.10.145.53/lpt1: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/03/22 13:46:18 [!] Get http://10.10.145.53/lpt2: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/03/22 13:47:59 [!] Get http://10.10.145.53/nul: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/03/22 13:50:03 [!] Get http://10.10.145.53/prn: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
/robots.txt (Status: 200)
/rss (Status: 200)
/RSS (Status: 200)
/search (Status: 200)
/Search (Status: 200)
/sitemap (Status: 200)
/SiteMap (Status: 200)
/tags (Status: 200)
/umbraco (Status: 200)
===============================================================
```

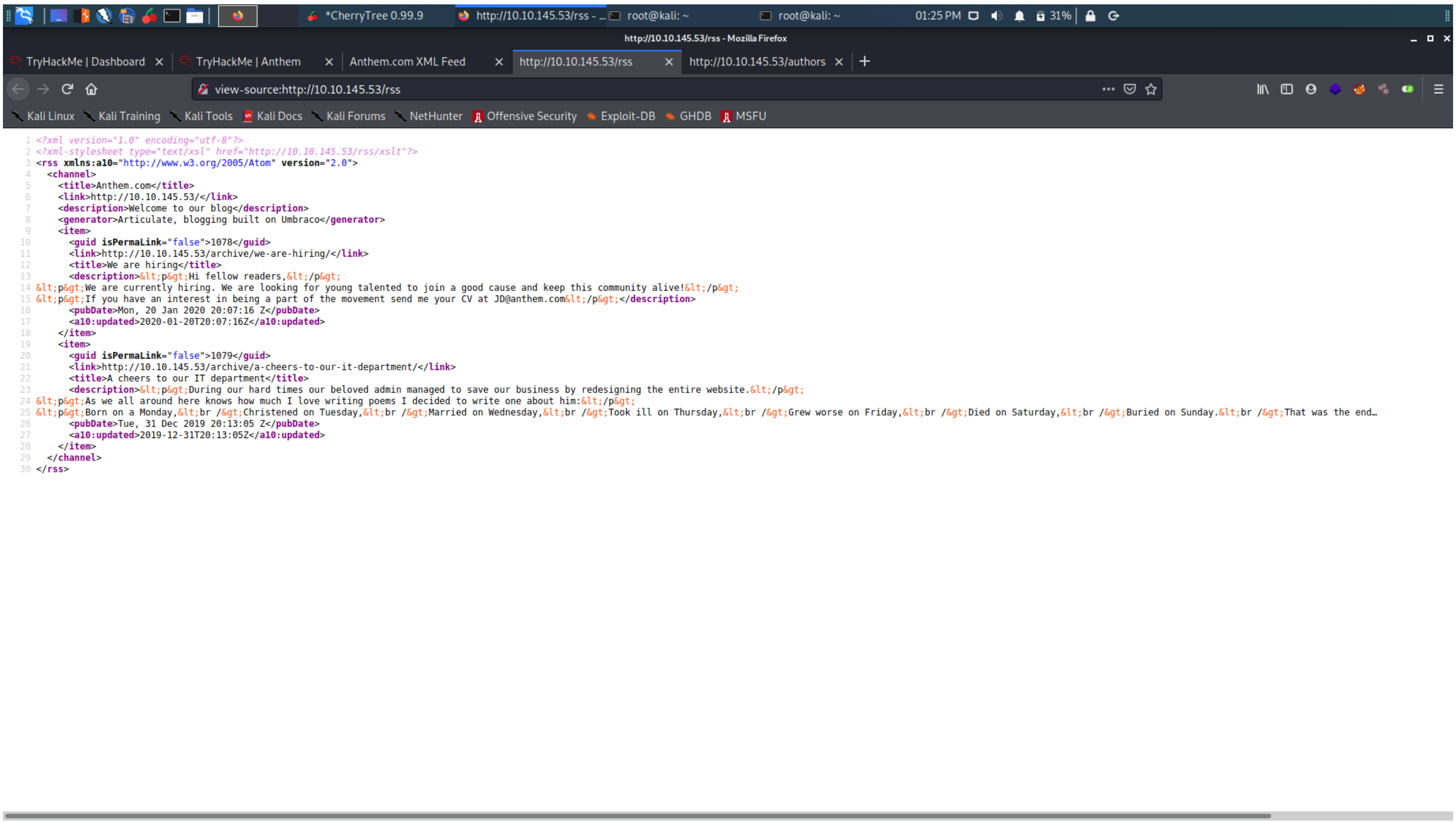
Robots.txt

```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

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

XML document

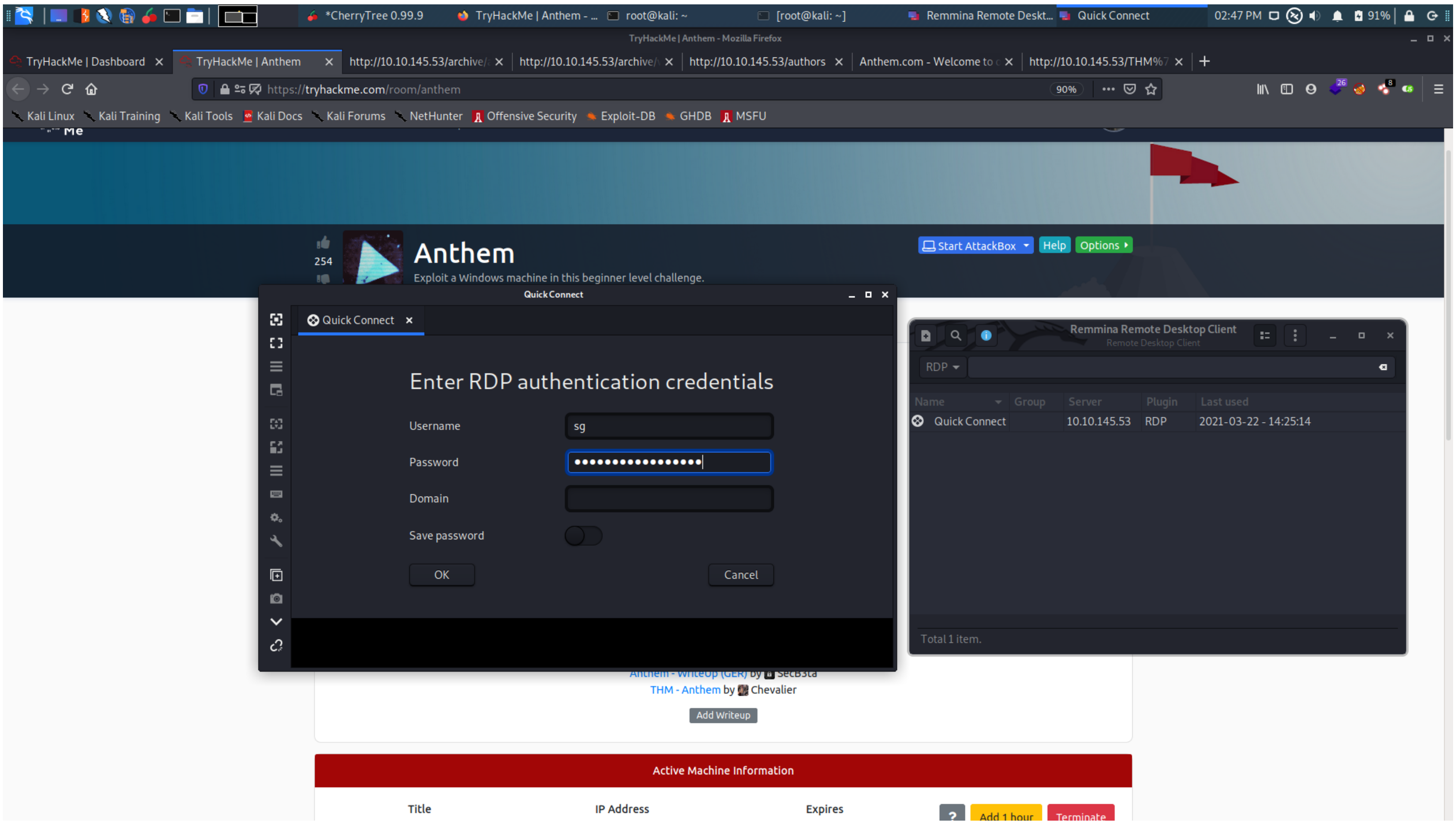


```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" href="http://10.10.145.53/rss/xslt"?>
<rss xmlns:a10="http://www.w3.org/2005/Atom" version="2.0">
  <channel>
    <title>Anthem.com</title>
    <link>http://10.10.145.53/</link>
    <description>Welcome to our blog</description>
    <generator>Articulate, blogging built on Umbraco</generator>
    <item>
      <guid isPermaLink="false">1078</guid>
      <link>http://10.10.145.53/archive/we-are-hiring/</link>
      <title>We are hiring</title>
      <description>&lt;p&gt;Hi fellow readers,&lt;/p&gt;
&lt;p&gt;We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!&lt;/p&gt;
&lt;p&gt;If you have an interest in being a part of the movement send me your CV at JD@anthem.com&lt;/p&gt;</description>
      <pubDate>Mon, 20 Jan 2020 20:07:16 Z</pubDate>
      <a10:updated>2020-01-20T20:07:16Z</a10:updated>
    </item>
    <item>
      <guid isPermaLink="false">1079</guid>
      <link>http://10.10.145.53/archive/a-cheers-to-our-it-department/</link>
      <title>A cheers to our IT department</title>
      <description>&lt;p&gt;During our hard times our beloved admin managed to save our business by redesigning the entire website.&lt;/p&gt;
&lt;p&gt;As we all around here knows how much I love writing poems I decided to write one about him:&lt;/p&gt;
&lt;p&gt;Born on a Monday,&lt;br /&gt;Christened on Tuesday,&lt;br /&gt;Married on Wednesday,&lt;br /&gt;Took ill on Thursday,&lt;br /&gt;Grew worse on Friday,&lt;br /&gt;Died on Saturday,&lt;br /&gt;Buried on Sunday.&lt;br /&gt;That was the end…
      <pubDate>Tue, 31 Dec 2019 20:13:05 Z</pubDate>
      <a10:updated>2019-12-31T20:13:05Z</a10:updated>
    </item>
  </channel>
</rss>
```

RDP port 3389

Remnina connect

Username is sg and password is UmbracoIsTheBest!



Enter RDP authentication credentials

Username: sg

Password: ●●●●●●●●●●●●●●●●●

Domain:

Save password

Name	Group	Server	Plugin	Last used
Quick Connect		10.10.145.53	RDP	2021-03-22 - 14:25:14

Total 1 item.

Quick Connect
OK
Cancel
Remmina Remote Desktop Client
RDP
Anthem
Exploit a Windows machine in this beginner level challenge.
Start AttackBox
Help
Options
THM - Anthem by Chevalier
Add Writeup
Active Machine Information
Title
IP Address
Expires
Add 1 hour
Terminate
https://tryhackme.com/room/anthem

Exploitation

Post exploitation

Loot

Credentials

####   jane and doe possible usernames

Password found on robots.txt   Umbracoisthebest!

### A blog post showed a poem about admin,upon googling it we found the poem was written by solomon grundy and this is admin name.HIs email is sg@anthhem.com

###RDP
sg:UmbracoIsTheBest!

##Administrator on windows file password
ChangeMeBaby1MOreTime

Flags

###Flag 1   found in wearehiring blog

THM{L0L_WH0_US3S_M3T4}

### Flag2 found in main page

THM{G!T_G00D}

##Flag3 found in jobseeking blog

THM{L0L_WH0_D15}

###Flag4 found in cheers for it department blog

THM{AN0TH3R_M3TA}

### User Flag

THM{N00T_NO0T}

### Root Flag

THM{Y0U_4R3_1337}

POC

1- Main webpage code analysis gave us our flag#2 THM{G!T_G00D}

2- Author directory on webpage gave us our flag#3 THM{L0L_WH0_D15}

3- robots.txt gives us a possible password Umbracoisthebest!

4- We are hiring blog had our first flag THM{L0L_WH0_US3S_M3T4}

5- A blog post showed a poem about admin,upon googling it we found the poem was written by solomon grundy and this is admin name.HIs email is sg@anthhem.com

6- second blog had our 4th flag THM{AN0TH3R_M3TA}

7- Now we connect to the machine using remnina [Remnina connect]

8- Now we got a file in backup folder but we couldnt read it so we changed it permissions by goind to properties,security and edit permissions then adding our usergroup

9- Password is ChangeMeBaby1MOreTime

10- NOw we can login as admin

11- Root flag is THM{Y0U_4R3_1337}