

TryHackme Offensive Security

Introduction – writeup

Room : Offensive Security Intro Name : Neha Liz Thomas

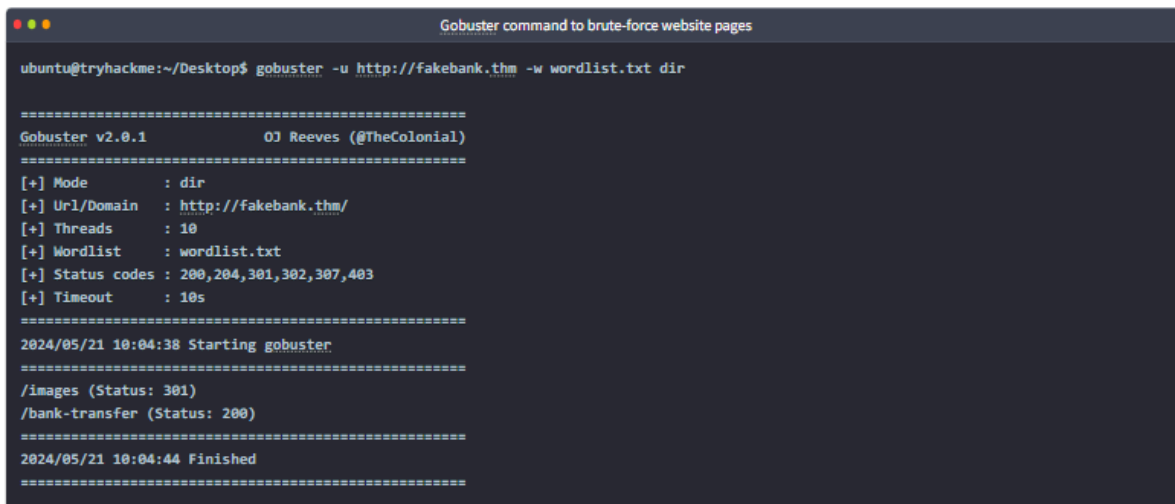
A virtual environment was launched with a fake banking website. The objective was to simulate an attack and gain unauthorized access.

1. Launched the virtual machine and navigated to the simulated banking interface.
2. Employed Gobuster to enumerate concealed directories.
3. Discovered and entered /bank-transfer
4. Simulated a successful hack by transferring funds between accounts.

To begin, type the following command into the terminal to find potentially hidden pages on FakeBank's website using [Gobuster](#) (a command-line security application).

```
gobuster -u http://fakebank.thm -w wordlist.txt dir
```

The command will run and show you an output similar to this:



```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.thm -w wordlist.txt dir

=====
Gobuster v2.0.1           OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://fakebank.thm/
[+] Threads       : 10
[+] Wordlist        : wordlist.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Timeout        : 10s
=====
2024/05/21 10:04:38 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/05/21 10:04:44 Finished
=====
```

In the command above, `-u` is used to state the website we're scanning, `-w` takes a list of words to iterate through to find hidden pages.

You will see that Gobuster scans the website with each word in the list, finding pages that exist on the site. Gobuster will have told you the pages in the list of page/directory names (indicated by Status: 200).

```
=====
Gobuster v2.0.1                                OJ Reeves (@TheColonial)
=====
[+] Mode          : dir
[+] Url/Domain    : http://fakebank.thm/
[+] Threads      : 10
[+] Wordlist      : wordlist.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Timeout      : 10s
=====
2024/05/21 10:04:38 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200) ←
=====
2024/05/21 10:04:44 Finished
=====
```

Step 3. Hack The Bank

You should have found a secret bank transfer page that allows you to transfer money between bank accounts (`/bank-transfer`). Type the hidden page into the FakeBank website using the browser's address bar.

