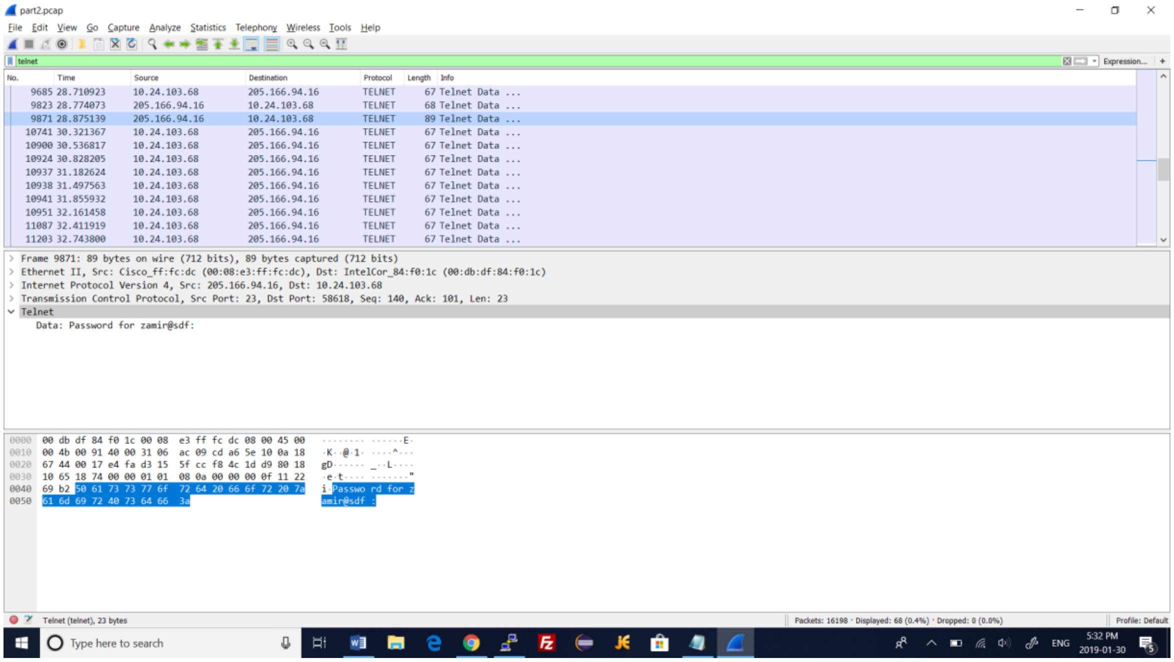
EECS 3482
Lab 2

Zamir Lalji

212779997
Professor: Khalil Abuosba

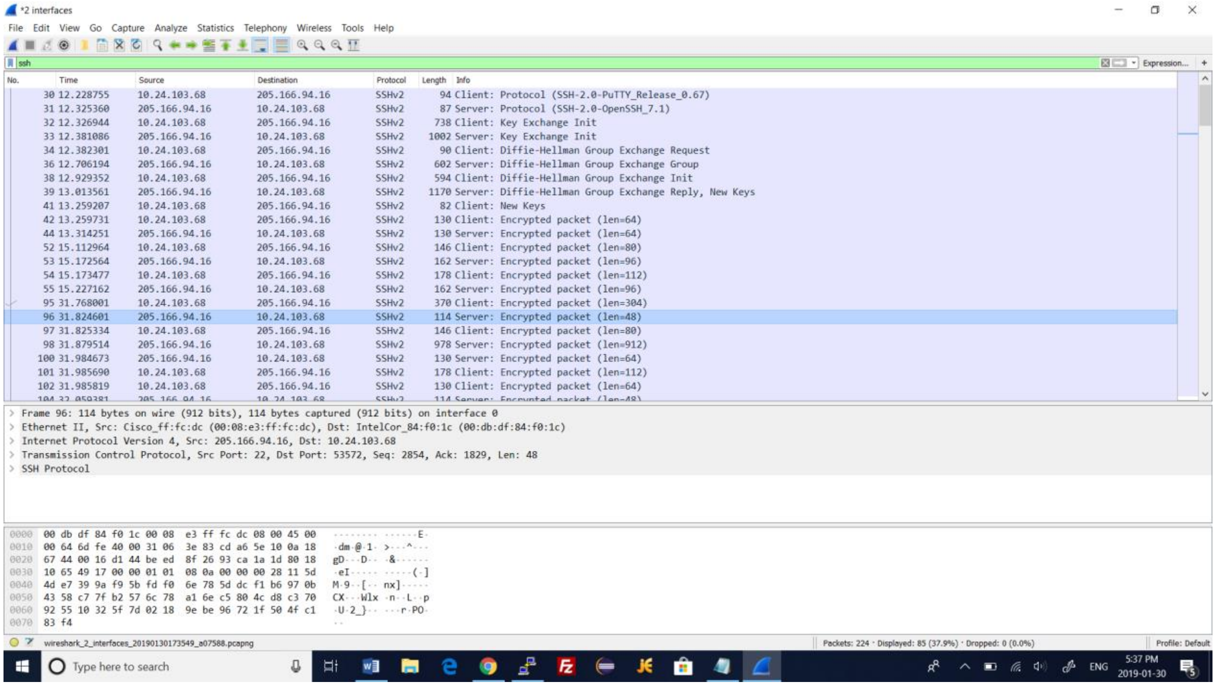
Question 1:

Part 1: Telnet and ssh connections analysis:


part2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
Expression...
Type here to search
ENG
5:32 PM
2019-01-30

```
No.   Time        Source          Destination     Protocol Length Info
 9685 28.710923   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
 9823 28.774073   205.166.94.16   10.24.103.68    TELNET   68 Telnet Data ...
 9871 28.875139   205.166.94.16   10.24.103.68    TELNET   89 Telnet Data ...
10741 30.321367   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
10900 30.536817   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
10924 30.828205   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
10937 31.182624   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
10938 31.497563   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
10941 31.855932   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
10951 32.161458   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
11087 32.411919   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...
11203 32.743800   10.24.103.68    205.166.94.16   TELNET   67 Telnet Data ...

> Frame 9871: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Ethernet II, Src: Cisco_ff:fc:dc (00:08:e3:ff:fc:dc), Dst: IntelCor_84:f0:1c (00:db:df:84:f0:1c)
> Internet Protocol Version 4, Src: 205.166.94.16, Dst: 10.24.103.68
> Transmission Control Protocol, Src Port: 23, Dst Port: 58618, Seq: 140, Ack: 101, Len: 23
v Telnet
    Data: Password for zamir@sdf:

0000  00 db df 84 f0 1c 00 08  e3 ff fc dc 08 00 45 00   ········ ······E·
0010  00 4b 00 91 40 00 31 06  ac 09 cd a6 5e 10 0a 18   ·K··@·1· ····^···
0020  67 44 00 17 e4 fa d3 15  5f cc f8 4c 1d d9 80 18   gD······ _··L····
0030  10 65 18 74 00 00 01 01  08 0a 00 00 00 0f 11 22   ·e·t···· ·······"
0040  69 b2 50 61 73 73 77 6f  72 64 20 66 6f 72 20 7a   i·Passwo rd for z
0050  61 6d 69 72 40 73 64 66  3a                        amir@sdf :

Telnet (telnet), 23 bytes    Packets: 16198 · Displayed: 68 (0.4%) · Dropped: 0 (0.0%)    Profile: Default
```

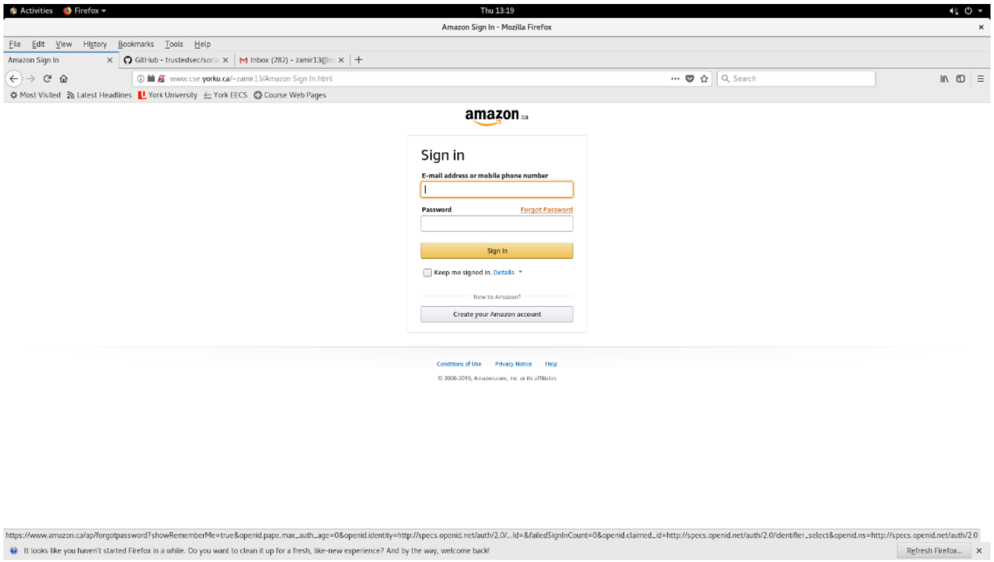
When using telnet password is seen in the next 17 packets and it is displayed.


*2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh
Expression...
Type here to search
ENG
5:37 PM
2019-01-30

```
No.  Time        Source          Destination     Protocol Length Info
  30 12.228755   10.24.103.68    205.166.94.16   SSHv2    94 Client: Protocol (SSH-2.0-PuTTY_Release_0.67)
  31 12.325360   205.166.94.16   10.24.103.68    SSHv2    87 Server: Protocol (SSH-2.0-OpenSSH_7.1)
  32 12.326944   10.24.103.68    205.166.94.16   SSHv2   738 Client: Key Exchange Init
  33 12.381086   205.166.94.16   10.24.103.68    SSHv2  1002 Server: Key Exchange Init
  34 12.382301   10.24.103.68    205.166.94.16   SSHv2    90 Client: Diffie-Hellman Group Exchange Request
  36 12.706194   205.166.94.16   10.24.103.68    SSHv2   602 Server: Diffie-Hellman Group Exchange Group
  38 12.929352   10.24.103.68    205.166.94.16   SSHv2   594 Client: Diffie-Hellman Group Exchange Init
  39 13.013561   205.166.94.16   10.24.103.68    SSHv2  1170 Server: Diffie-Hellman Group Exchange Reply, New Keys
  41 13.259207   10.24.103.68    205.166.94.16   SSHv2    82 Client: New Keys
  42 13.259731   10.24.103.68    205.166.94.16   SSHv2   130 Client: Encrypted packet (len=64)
  44 13.314251   205.166.94.16   10.24.103.68    SSHv2   130 Server: Encrypted packet (len=64)
  52 15.112964   10.24.103.68    205.166.94.16   SSHv2   146 Client: Encrypted packet (len=80)
  53 15.172564   205.166.94.16   10.24.103.68    SSHv2   162 Server: Encrypted packet (len=96)
  54 15.173477   10.24.103.68    205.166.94.16   SSHv2   178 Client: Encrypted packet (len=112)
  55 15.227162   205.166.94.16   10.24.103.68    SSHv2   162 Server: Encrypted packet (len=96)
  95 31.768001   10.24.103.68    205.166.94.16   SSHv2   370 Client: Encrypted packet (len=304)
  96 31.824601   205.166.94.16   10.24.103.68    SSHv2   114 Server: Encrypted packet (len=48)
  97 31.825334   10.24.103.68    205.166.94.16   SSHv2   146 Client: Encrypted packet (len=80)
  98 31.879514   205.166.94.16   10.24.103.68    SSHv2   978 Server: Encrypted packet (len=912)
 100 31.984673   205.166.94.16   10.24.103.68    SSHv2   130 Server: Encrypted packet (len=64)
 101 31.985690   10.24.103.68    205.166.94.16   SSHv2   178 Client: Encrypted packet (len=112)
 102 31.985819   10.24.103.68    205.166.94.16   SSHv2   130 Client: Encrypted packet (len=64)
 104 32.059381   205.166.94.16   10.24.103.68    SSHv2   114 Server: Encrypted packet (len=48)

> Frame 96: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: Cisco_ff:fc:dc (00:08:e3:ff:fc:dc), Dst: IntelCor_84:f0:1c (00:db:df:84:f0:1c)
> Internet Protocol Version 4, Src: 205.166.94.16, Dst: 10.24.103.68
> Transmission Control Protocol, Src Port: 22, Dst Port: 53572, Seq: 2854, Ack: 1829, Len: 48
> SSH Protocol

0000  00 db df 84 f0 1c 00 08  e3 ff fc dc 08 00 45 00   ········ ······E·
0010  00 64 6d fe 40 00 31 06  3e 83 cd a6 5e 10 0a 18   ·dm·@·1· >···^···
0020  67 44 00 16 d1 44 be ed  8f 26 93 ca 1a 1d 80 18   gD···D·· ·&······
0030  10 65 49 17 00 00 01 01  08 0a 00 00 00 28 11 5d   ·eI····· ·····(·]
0040  4d e7 39 9a f9 5b fd f0  6e 78 5d dc f1 b6 97 0b   M·9··[·· nx]·····
0050  43 58 c7 7f b2 57 6c 78  a1 6e c5 80 4c d8 c3 70   CX···Wlx ·n··L··p
0060  92 55 10 32 5f 7d 02 18  9e be 96 72 1f 50 4f c1   ·U·2_}·· ···r·PO·
0070  83 f4                                              ··

wireshark_2_interfaces_20190130173549_a07588.pcapng    Packets: 224 · Displayed: 85 (37.9%) · Dropped: 0 (0.0%)    Profile: Default
```

You cant see your username and password in ssh because the data is encrypted.

Q2: link for the web site was obtained by using the EECS computers, creating a folder called “www” and then clicking on the link for the amazon website from the lab instructions and saving the page then using the url I was able to display the page and load it. URL is

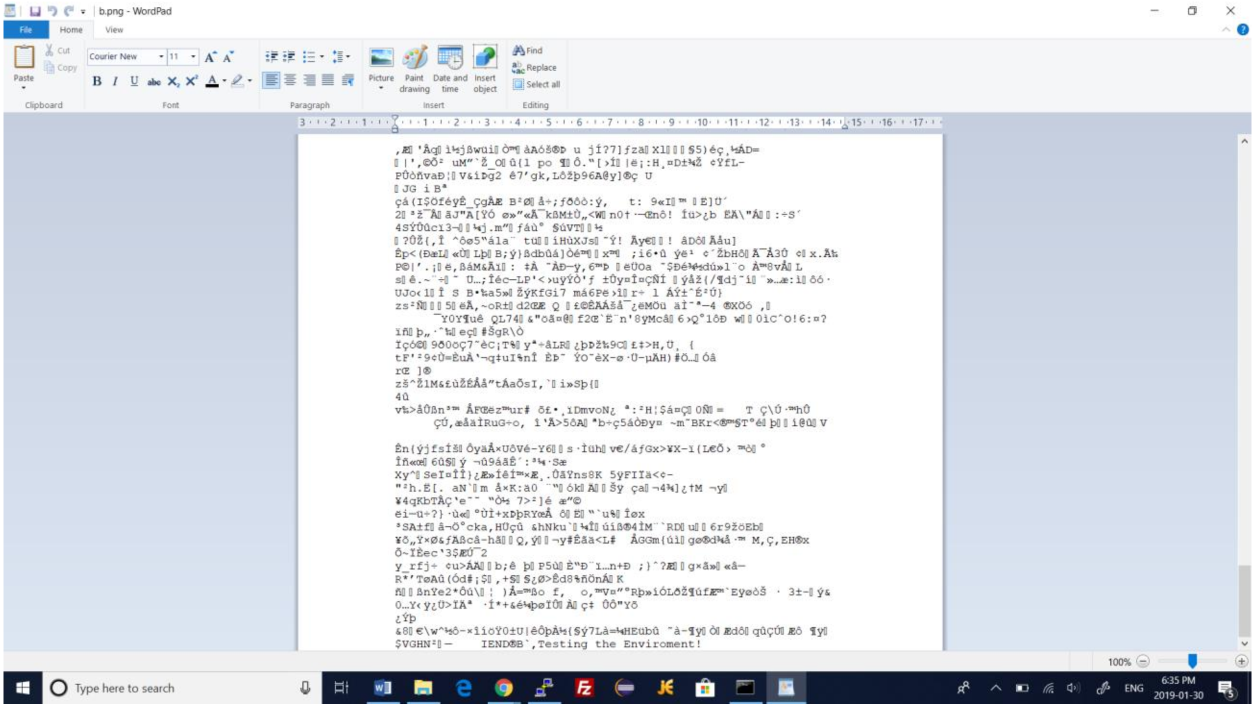


www.cse.yorku.ca/~zamir13/Amazon Sign In.html

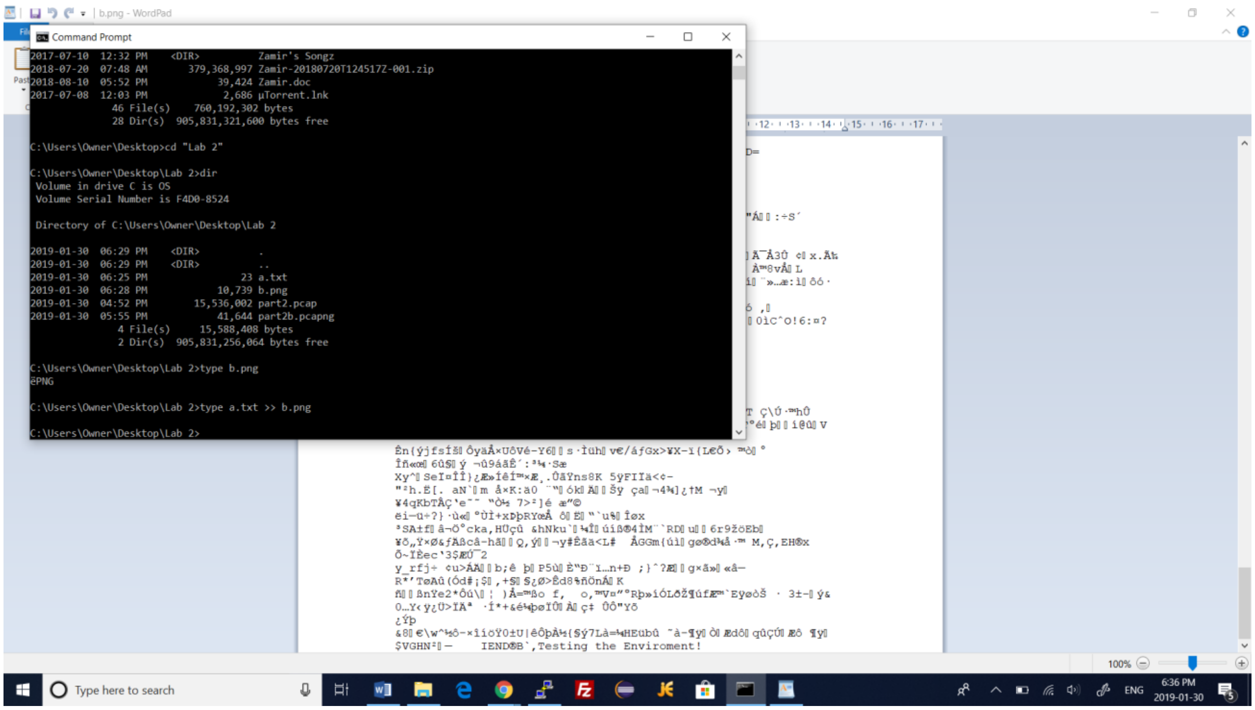
https://www.amazon.ca/ap/forgotpassword?showRememberMe=true&openid.pape.max_auth_age=0&openid.identity=http://specs.openid.net/auth/2.0/...Id=&failedSignInCount=0&openid.claimed_id=http://specs.openid.net/auth/2.0/identifier_select&openid.ns=http://specs.openid.net/auth/2.0

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Q3 part1: 1-8:



```
[illegible]
ëi—ü÷?}·ù«▯ °ÙÌ+xÐþRYœÅ ô▯ E▯ "`u%▯ Îøx
³SA±f▯ â¬Ö°cka,HÜçû &hNku`▯¼Î▯ úíß®4ÌM¨`RD▯ u▯▯ 6r9žöEb▯
¥ō„Ÿ×Ø&fÄßcâ-hã▯▯Q,ý▯▯¬y#Êãä<L#  ÅGGm{úi▯ gø®d¾å·™ M,Ç,EH®x
Õ~ÏÈec'3$ÆÚ¯2
y_rfj÷ ¢u>ÁA▯▯b;ê þ▯ P5ù▯ È"Ð¨ı…n+Ð ;}ˆ?Æ▯▯g×ã»▯ «â—
R*'TøAû(Ód#¡$▯,+§▯ §¿Ø>Êd8‰ñÖnÁ▯ K
ñ▯▯ßnŸe2*Ôú\▯¦ )Å=™ßo f,  o,™V¤"°Rþ»íÓLõŽ¶úfÆ™`EÿøòŠ · 3±—▯ ý&
0…Y‹ÿ¿Ü>ÏÄª ·Í*+&é¼þøÏÛ▯ À▯ ç‡ ÛÔ"Yõ
¿Ýþ
&8▯ €\w^½ô-×îíöŸ0±U|êÔþÀ½{$ý7Là=¼HEübû ˜à-¶y▯ Ò▯ Ædô▯ qûÇÚ▯ Æô ¶y▯
$VGHN²▯—    IEND®B`,Testing the Enviroment!
```

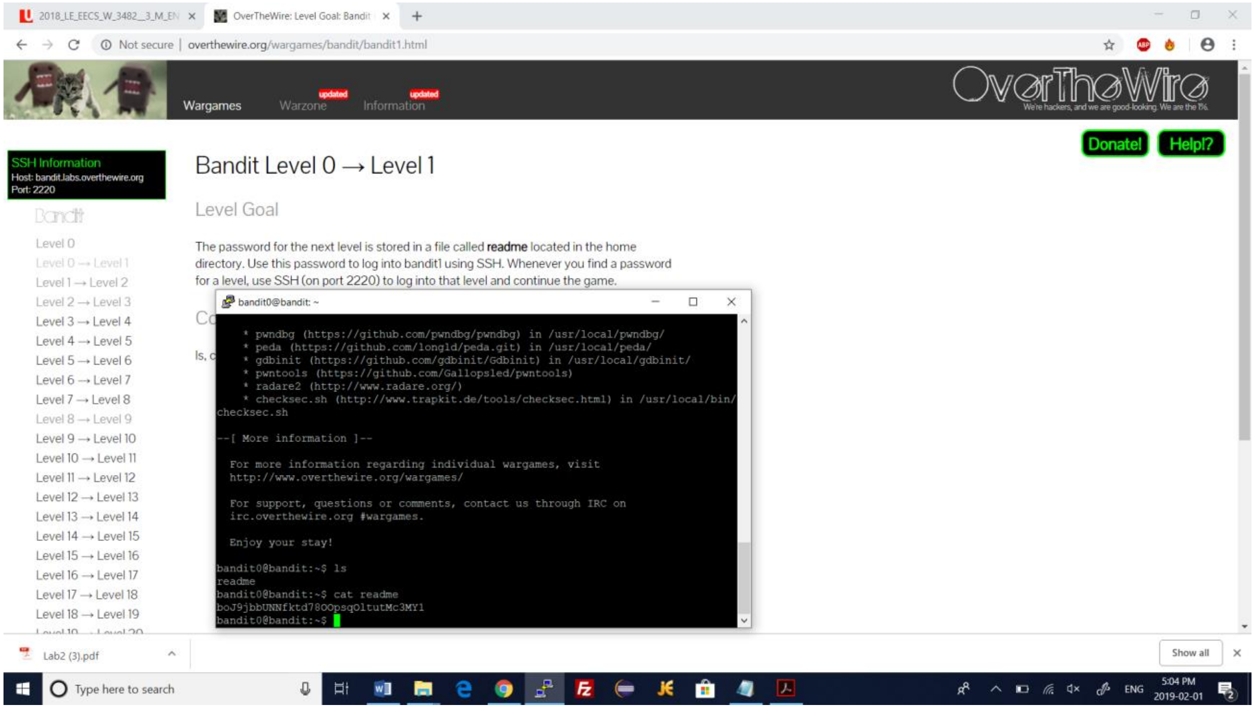


```
2017-07-10  12:32 PM    <DIR>          Zamir's Songz
2018-07-20  07:48 AM       379,368,997 Zamir-20180720T124517Z-001.zip
2018-08-10  05:52 PM            39,424 Zamir.doc
2017-07-08  12:03 PM             2,686 µTorrent.lnk
              46 File(s)    760,192,302 bytes
              28 Dir(s)  905,831,321,600 bytes free

C:\Users\Owner\Desktop>cd "Lab 2"

C:\Users\Owner\Desktop\Lab 2>dir
 Volume in drive C is OS
 Volume Serial Number is F4D0-8524

 Directory of C:\Users\Owner\Desktop\Lab 2

2019-01-30  06:29 PM    <DIR>          .
2019-01-30  06:29 PM    <DIR>          ..
2019-01-30  06:25 PM                23 a.txt
2019-01-30  06:28 PM            10,739 b.png
2019-01-30  04:52 PM        15,536,002 part2.pcap
2019-01-30  05:55 PM            41,644 part2b.pcapng
               4 File(s)     15,588,408 bytes
               2 Dir(s)  905,831,256,064 bytes free

C:\Users\Owner\Desktop\Lab 2>type b.png
ëPNG

C:\Users\Owner\Desktop\Lab 2>type a.txt >> b.png

C:\Users\Owner\Desktop\Lab 2>
```

```
IEND®B`,Testing the Enviroment!
```

As seen from the screen shots I was able to hide a text in between a pic and it shows from the screen shots above

Q4: As seen from he screenshots that I took for the game each password is displayed and showed in the screenshot.



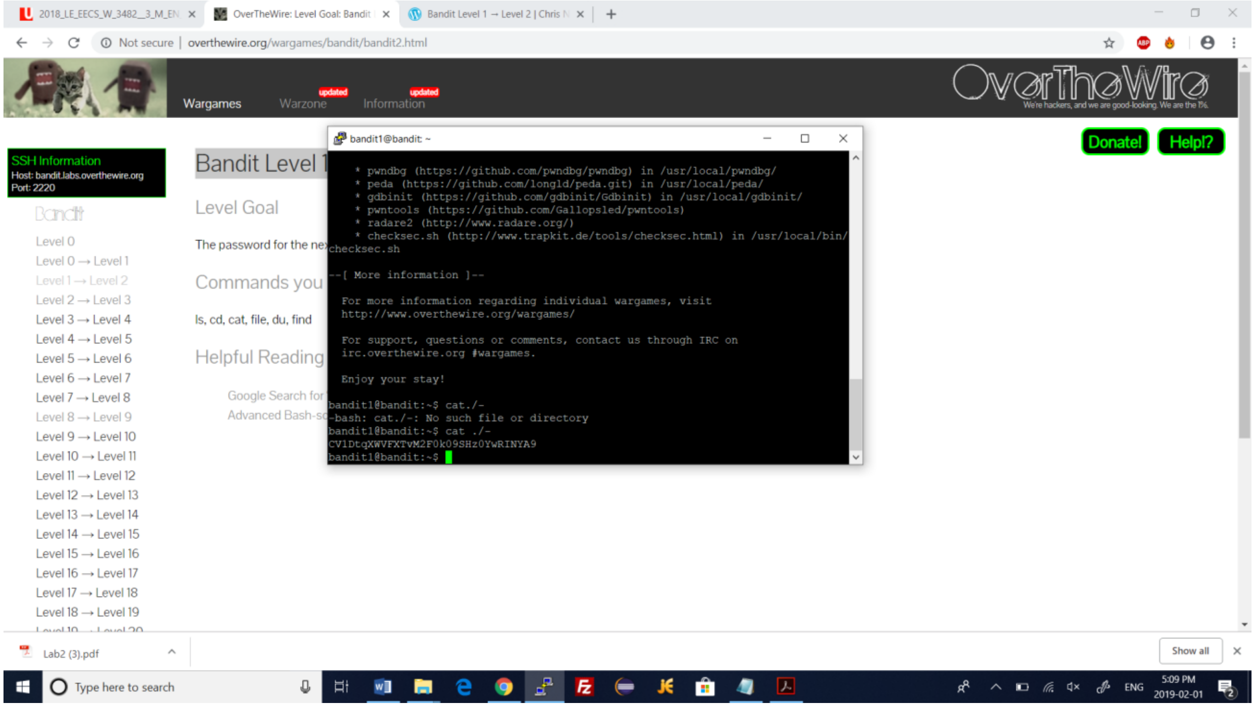
Bandit Level 0 → Level 1

Level Goal

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

```
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

Password for level 0: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

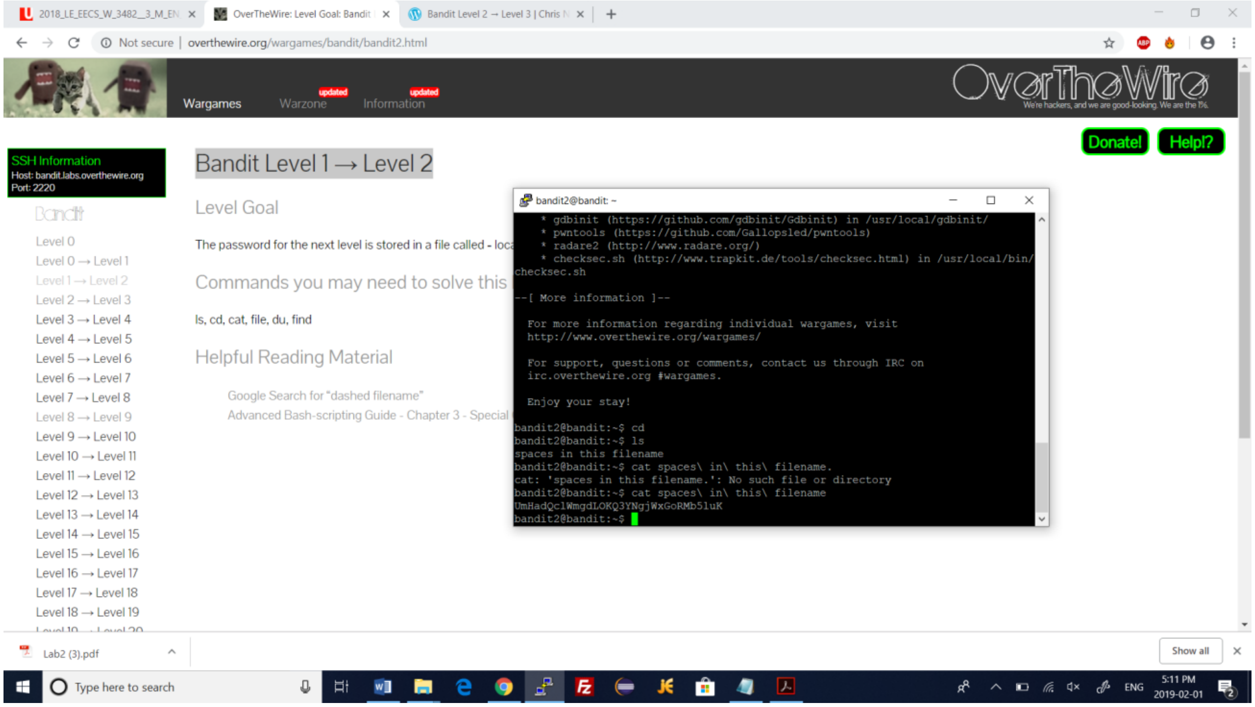


The password for the ne

ls, cd, cat, file, du, find

```
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit1@bandit:~$ cat./-
-bash: cat./-: No such file or directory
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ 
```

Password for level 1: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

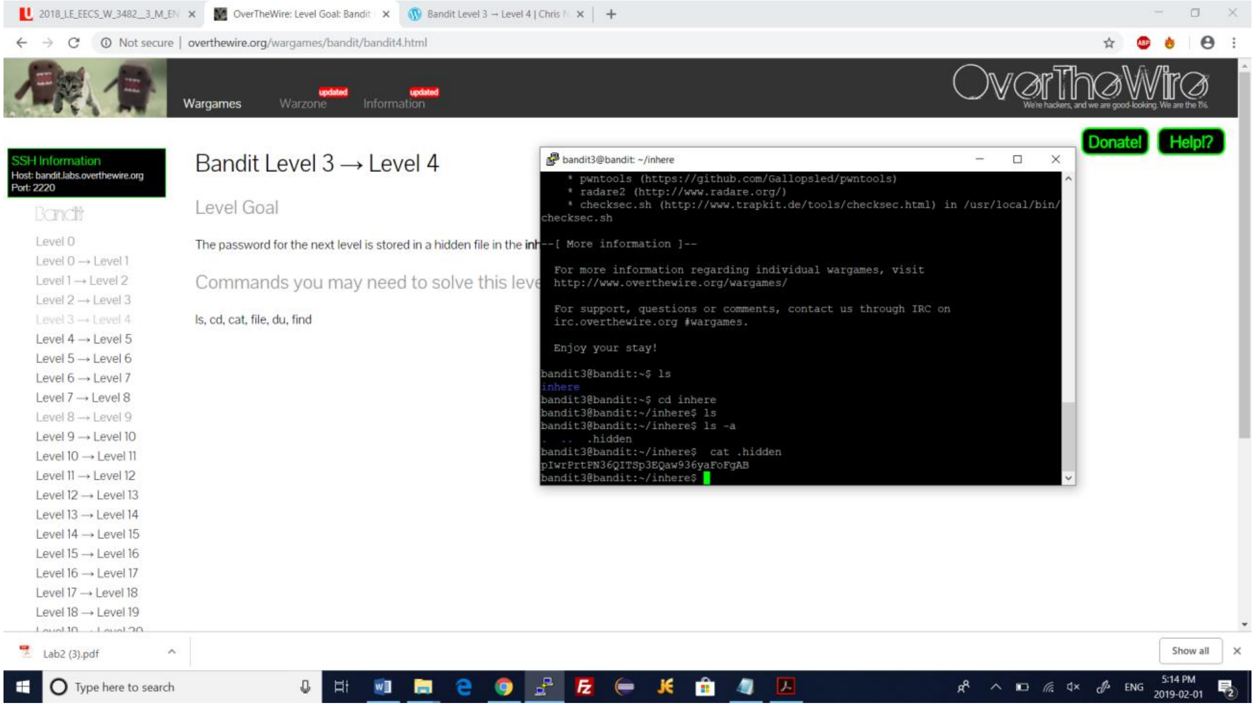


The password for the next level is stored in a file called - loca

ls, cd, cat, file, du, find

```
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit2@bandit:~$ cd
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename.
cat: 'spaces in this filename.': No such file or directory
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ 
```

Password for level 2: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK



Bandit Level 3 → Level 4

Level Goal

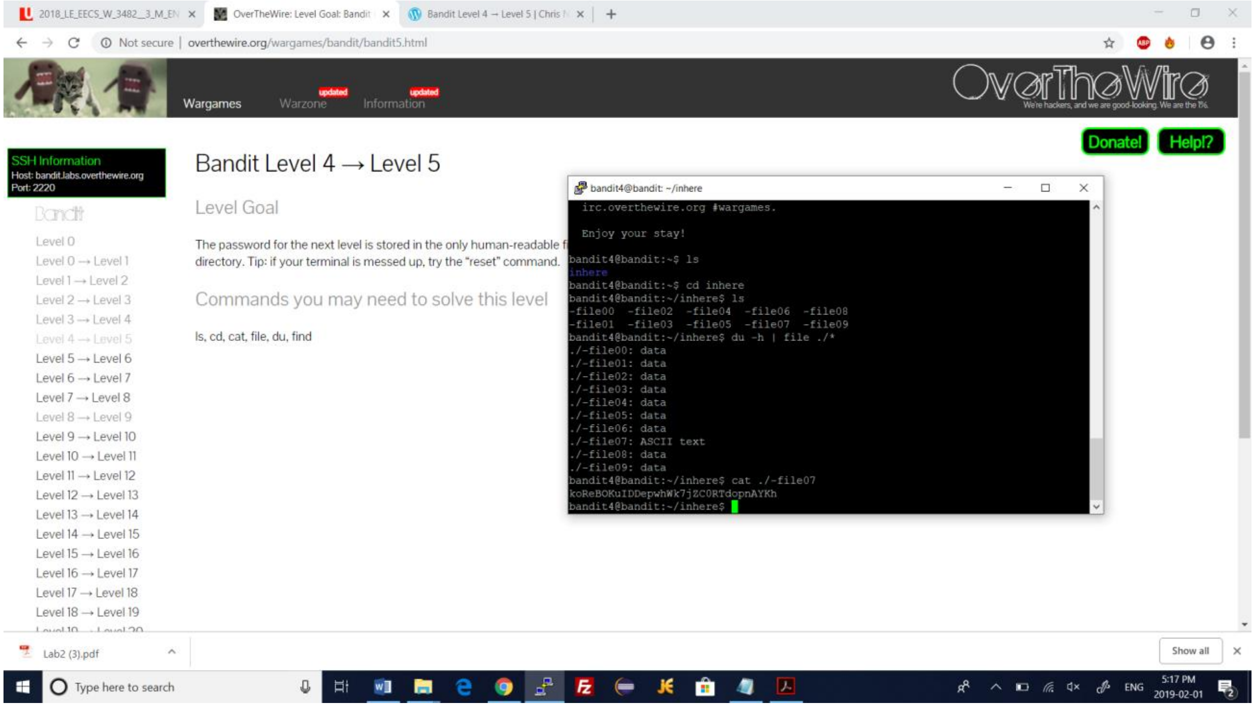
The password for the next level is stored in a hidden file in the inh

Commands you may need to solve this leve

ls, cd, cat, file, du, find

```
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$  cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

Password for level 3: pIwrPrtPN36QITSp3EQaw936yaFoFgAB



Bandit Level 4 → Level 5

Level Goal

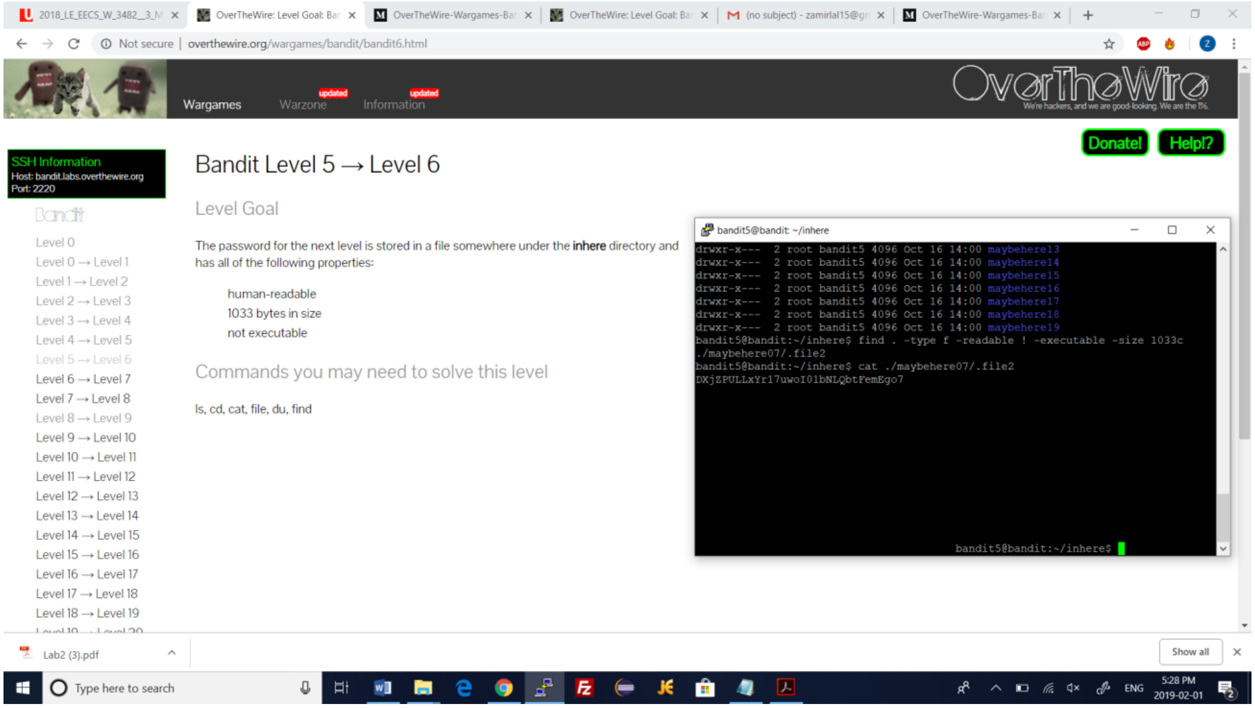
The password for the next level is stored in the only human-readable f directory. Tip: if your terminal is messed up, try the "reset" command.

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ du -h | file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Password for level 4: koReBOKuIDDepwhWk7jZC0RTdopnAYKh



Bandit Level 5 → Level 6

Level Goal

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

human-readable
1033 bytes in size
not executable

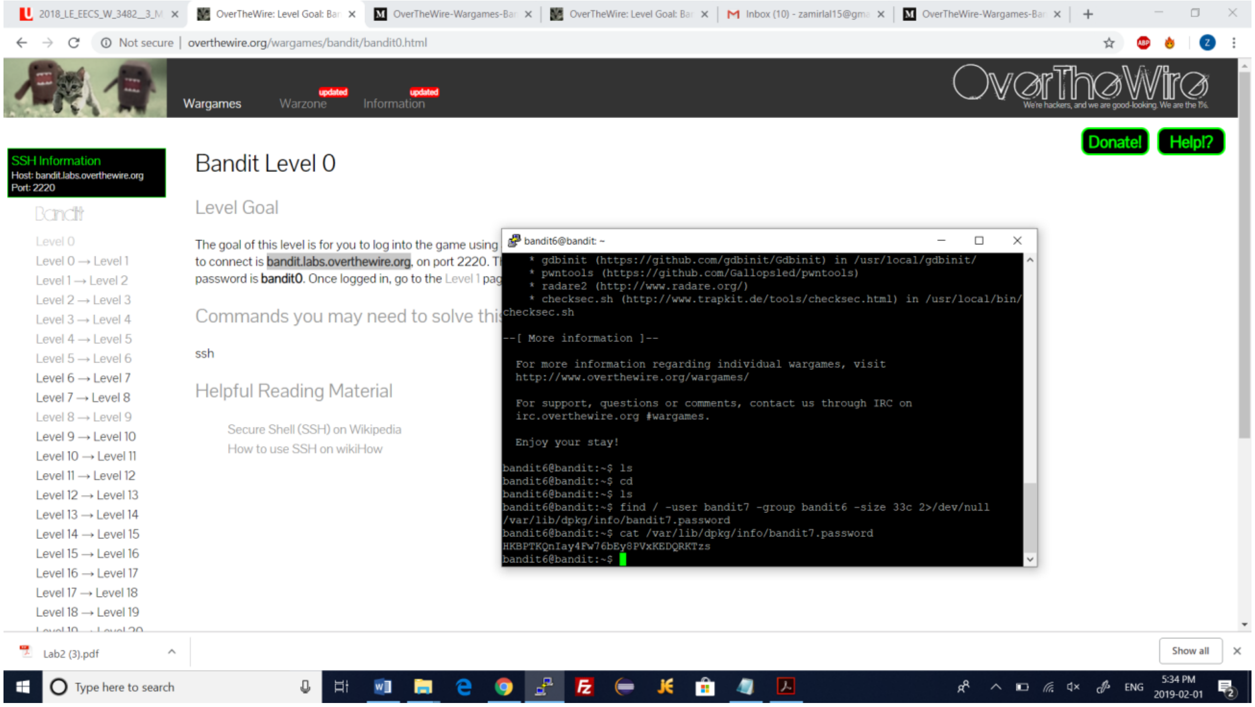
Commands you may need to solve this level

ls, cd, cat, file, du, find

bandit5@bandit: ~/inhere

```
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere13
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere14
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere15
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere16
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere17
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere18
drwxr-x---  2 root bandit5 4096 Oct 16 14:00 maybehere19
bandit5@bandit:~/inhere$ find . -type f -readable ! -executable -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7



                                     bandit5@bandit:~/inhere$
```

Password for level 5: DXjZPULLxYr17uwoI01bNLQbtFemEgo7



Bandit Level 0

Level Goal

The goal of this level is for you to log into the game using
to connect is bandit.labs.overthewire.org, on port 2220. Th
password is **bandit0**. Once logged in, go to the Level 1 pag

Commands you may need to solve thi

ssh

Helpful Reading Material

Secure Shell (SSH) on Wikipedia
How to use SSH on wikiHow

bandit6@bandit: ~

```
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit6@bandit:~$ ls
bandit6@bandit:~$ cd
bandit6@bandit:~$ ls
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Password for level 6: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs