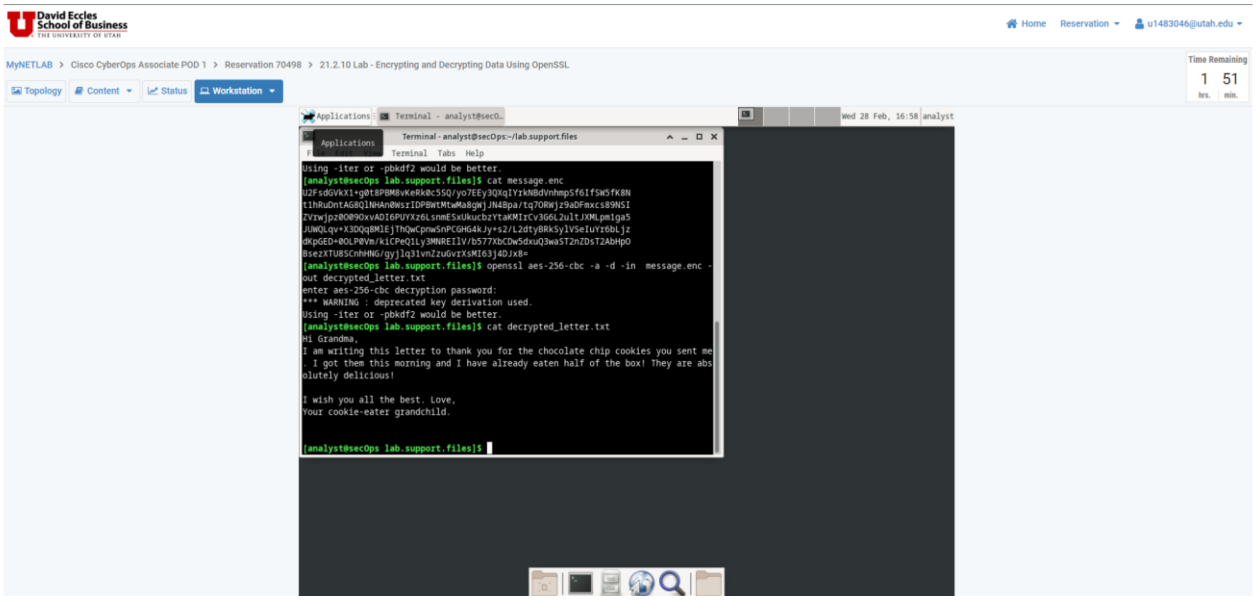
Vu Nguyen

UID: u1483046

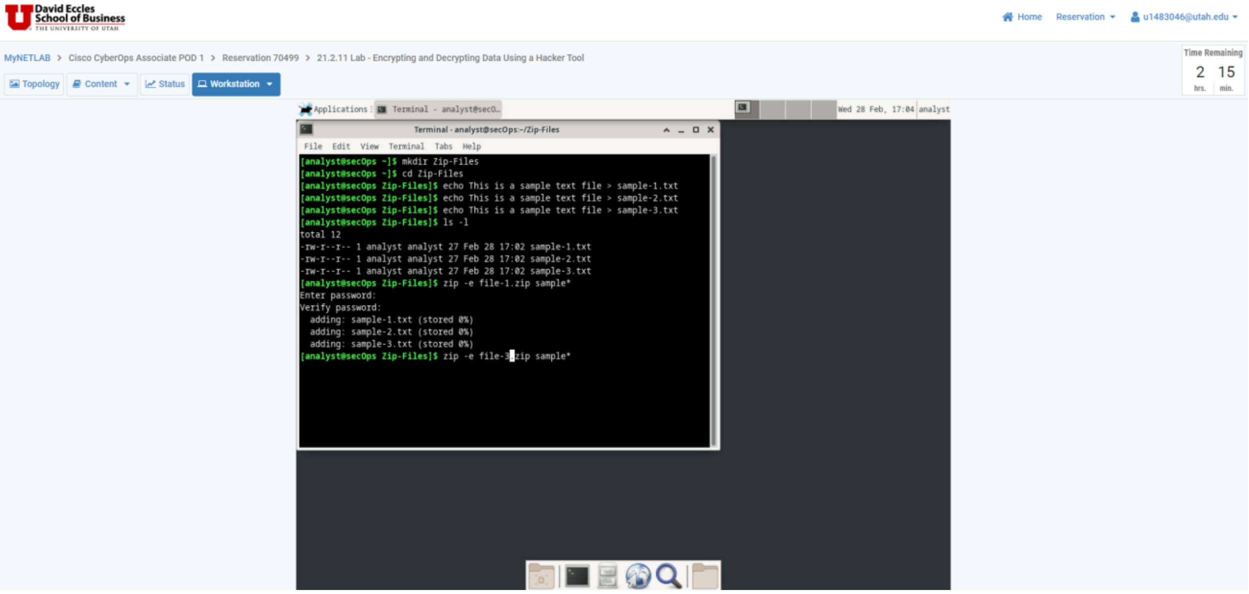
Assignment 25 - Encryption and Decryption (Lab and Quiz)

1. Lab 21.2.10, Part 2, Step 1c:


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70498 > 21.2.10 Lab - Encrypting and Decrypting Data Using OpenSSL
Time Remaining
1 hrs. 51 min.
Topology
Content
Status
Workstation
Applications
Terminal - analyst@secO…
Wed 28 Feb, 16:58
analyst
Terminal - analyst@secOps:~/lab.support.files
Applications
File Edit View Terminal Tabs Help

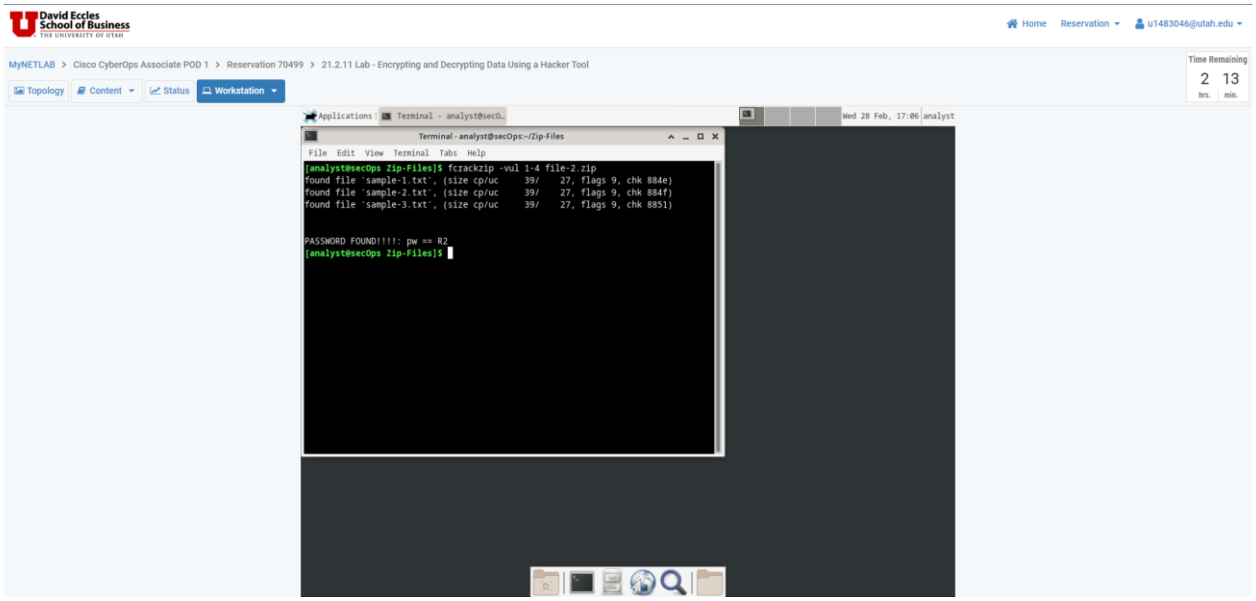
```
Using -iter or -pbkdf2 would be better.
[analyst@secOps lab.support.files]$ cat message.enc
U2FsdGVkX1+g0t8PBM8vKeRk0c5SQ/yo7EEy3QXqIYrkNBdVnhmpSf6IfSW5fK8N
t1hRuDntAG8QlNHAn0WsrIDPBWtMtwMa8gWjJN4Bpa/tq7ORWjz9aDFmxcs89NSI
ZVrwjpz0O09OxvADI6PUYXz6LsnmESxUkucbzYtaKMIrCv3G6L2ultJXMLpm1ga5
JUWQLqv+X3DQq8MlEjThQwCpnwSnPCGHG4kJy+s2/L2dtyBRkSylVSeIuYr6bLjz
dKpGED+0OLP0Vm/kiCPeQ1Ly3MNREIlV/b577XbCDw5dxuQ3waST2nZDsT2AbHpO
BsezXTU8SCnhHNG/gyjlq31vnZzuGvrXsMI63j4DJx8=
[analyst@secOps lab.support.files]$ openssl aes-256-cbc -a -d -in  message.enc -
out decrypted_letter.txt
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[analyst@secOps lab.support.files]$ cat decrypted_letter.txt
Hi Grandma,
I am writing this letter to thank you for the chocolate chip cookies you sent me
. I got them this morning and I have already eaten half of the box! They are abs
olutely delicious!

I wish you all the best. Love,
Your cookie-eater grandchild.


[analyst@secOps lab.support.files]$
```

2. Lab 21.2.11, Part 1, Step 2b:


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70499 > 21.2.11 Lab - Encrypting and Decrypting Data Using a Hacker Tool
Time Remaining
2 hrs.
15 min.
Topology
Content
Status
Workstation
Applications
Terminal - analyst@secO...
Wed 28 Feb, 17:04
analyst
Terminal - analyst@secOps:~/Zip-Files
File
Edit
View
Terminal
Tabs
Help

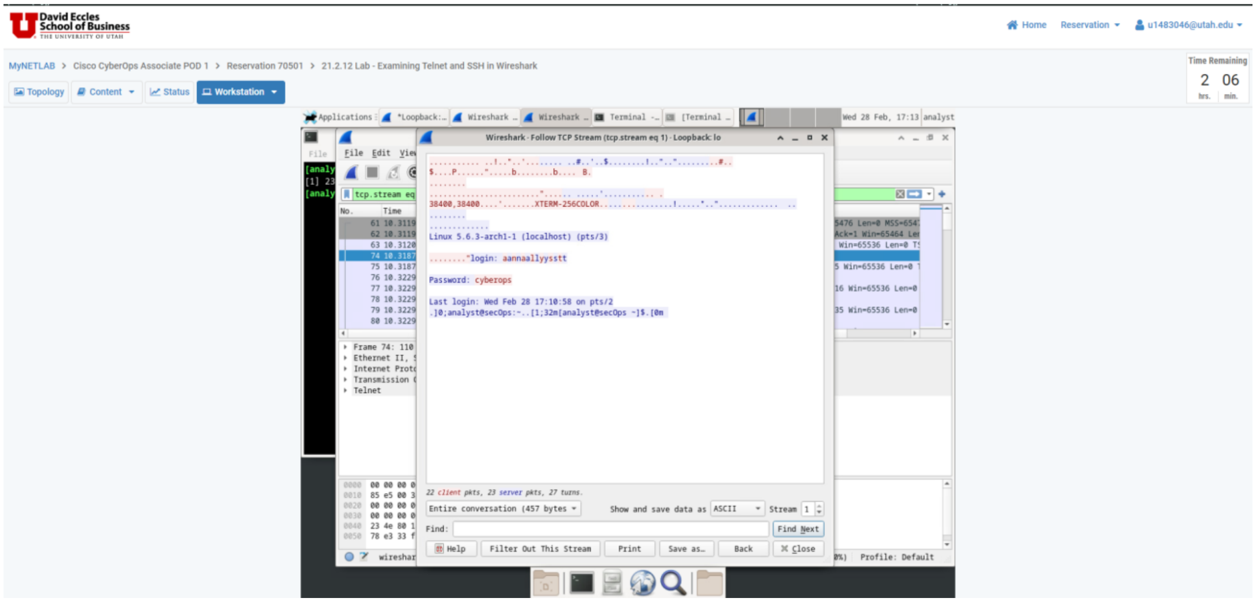
```
[analyst@secOps ~]$ mkdir Zip-Files
[analyst@secOps ~]$ cd Zip-Files
[analyst@secOps Zip-Files]$ echo This is a sample text file > sample-1.txt
[analyst@secOps Zip-Files]$ echo This is a sample text file > sample-2.txt
[analyst@secOps Zip-Files]$ echo This is a sample text file > sample-3.txt
[analyst@secOps Zip-Files]$ ls -l
total 12
-rw-r--r-- 1 analyst analyst 27 Feb 28 17:02 sample-1.txt
-rw-r--r-- 1 analyst analyst 27 Feb 28 17:02 sample-2.txt
-rw-r--r-- 1 analyst analyst 27 Feb 28 17:02 sample-3.txt
[analyst@secOps Zip-Files]$ zip -e file-1.zip sample*
Enter password:
Verify password:
  adding: sample-1.txt (stored 0%)
  adding: sample-2.txt (stored 0%)
  adding: sample-3.txt (stored 0%)
[analyst@secOps Zip-Files]$ zip -e file-3.zip sample*
```

3. Lab 21.2.11, Part 2, Step 2b (your password does not need to match mine):


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70499 > 21.2.11 Lab - Encrypting and Decrypting Data Using a Hacker Tool
Time Remaining
2 hrs.
13 min.
Topology
Content
Status
Workstation
Applications
Terminal - analyst@secO...
Wed 28 Feb, 17:06
analyst
Terminal - analyst@secOps:~/Zip-Files
File
Edit
View
Terminal
Tabs
Help

```
[analyst@secOps Zip-Files]$ fcrackzip -vul 1-4 file-2.zip
found file 'sample-1.txt', (size cp/uc     39/    27, flags 9, chk 884e)
found file 'sample-2.txt', (size cp/uc     39/    27, flags 9, chk 884f)
found file 'sample-3.txt', (size cp/uc     39/    27, flags 9, chk 8851)


PASSWORD FOUND!!!!: pw == R2
[analyst@secOps Zip-Files]$
```

4. Lab 21.2.12, Part 1, Step 2c:


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70501 > 21.2.12 Lab - Examining Telnet and SSH in Wireshark
Topology
Content
Status
Workstation
Time Remaining
2 06
hrs. min.
Applications
Wed 28 Feb, 17:13
analyst
Wireshark · Follow TCP Stream (tcp.stream eq 1) · Loopback: lo

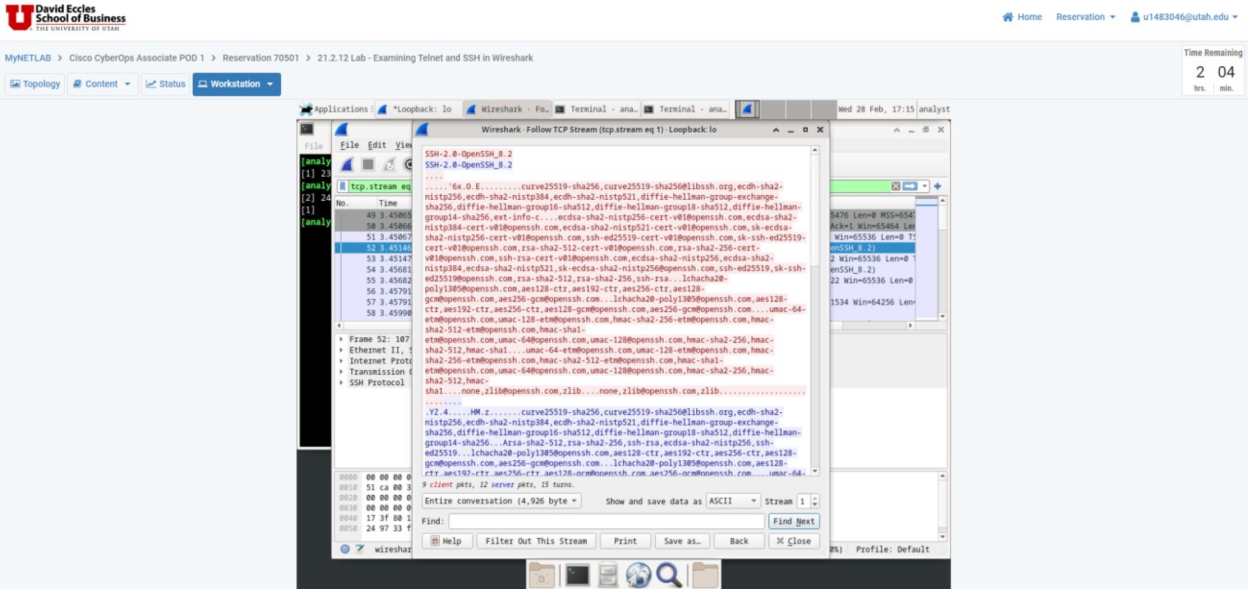
```
........... ..!..."..'........ ..#..'..$........!.."..".........#..
$....P......"......b........b.... B.
........
.......................".......  .....'........... .
38400,38400....'.......XTERM-256COLOR..........!......"..".............  ..
........
.............
Linux 5.6.3-arch1-1 (localhost) (pts/3)

........"login: aannaallyysstt

Password: cyberops

Last login: Wed Feb 28 17:10:58 on pts/2
.]0;analyst@secOps:~..[1;32m[analyst@secOps ~]$.[0m
```

22 client pkts, 23 server pkts, 27 turns.

Entire conversation (457 bytes) Show and save data as ASCII Stream 1

Find:

5. Lab 21.2.12, Part 2, Step 1f:


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70501 > 21.2.12 Lab - Examining Telnet and SSH in Wireshark
Topology
Content
Status
Workstation
Time Remaining
2 04
hrs. min.
Applications
Wed 28 Feb, 17:15
analyst
Wireshark · Follow TCP Stream (tcp.stream eq 1) · Loopback: lo

```
SSH-2.0-OpenSSH_8.2
SSH-2.0-OpenSSH_8.2
....
.....'6x.O.E.........curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-
group14-sha256,ext-info-c....ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-
nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ecdsa-
sha2-nistp256-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,sk-ssh-ed25519-
cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-
v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256@openssh.com,ssh-ed25519,sk-ssh-
ed25519@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa...lchacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com...lchacha20-poly1305@openssh.com,aes128-
ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com....umac-64-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-
sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-
sha2-512,hmac-sha1....umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-
sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-
sha2-512,hmac-
sha1....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib..................
........
.YZ.4.....HM.z.......curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-
group14-sha256...Arsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-
ed25519...lchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com...lchacha20-poly1305@openssh.com,aes128-
ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com....umac-64-
```

9 client pkts, 12 server pkts, 15 turns.

Entire conversation (4,926 byte Show and save data as ASCII Stream 1

Find: