**QUESTION 1**

An attacker left a CD in the trash at your company that contained a single file called plans.  Click on the link below to download the file: [plans](https://blackboard.iit.edu/bbcswebdav/pid-386227-dt-content-rid-2168581_1/xid-2168581_1)

Either download it from Kali or move to file to your Kali VM.

On the outside of the CD the word wheaton was written.  That word may be important in this exercise.  You looked at the content of the file and it looks to be base64 encoded.

Decrypt & decode the file.

(Hint: You will need to use the openssl command to decrypt this file and will need to determine the correct cipher that was used.  This will take some trial and error.  You will need to figure out the correct arguments to the openssl command to:

1.  Specify the correct cipher (this will be trial and error)  You can see the Cipher commands at the bottom if you just enter openssl help

2.  Decrypt the file

3.  Base64 decode the file

4.  Choose the plans file as input to the command

Answer this question by entering the decrypted plaintext sentence.

[Extra Credit - 5 points: Create a script that accepts a key and an input file and then will use openssl to try all of the cipher types and output each result.  If the result contains "bad decrypt" or "openssl:Error" then move on to the next cipher type. If "bad magic number" is returned, then try adding the base64 decode argument.  Else, once the correct cipher type is chosen, output the decrypted message to standard output or to a file.]

**QUESTION 2**

The following is cyphertext of a caesarian shift type of cipher.    Znk gtyckx oy ixevzu

 Answer this question by entering the decrypted plaintext.

**QUESTION 3**

Below is cipher text from a keyed vigenere cipher.  You have been told the key length is between 1 and 10 characters long.  You need to figure out what key was used and then decrypt the below plaintext using CrypTool.

Vyc ttunv fpl zcebtw.  Fggcpm, hjv cpzzg yyh eopucs. Mvkj gh t ggtptm agjqpzs.  Qeat rcw ucrkmrk rwbg ovqhtug, dyzx gwic ih spkcg tzn fd iawu gjpbbvvvibbvf rwx pnrazuccib fnsukgdg ou ncae ou kft dsa zl dkrgi rd tbuncg bh efpgxqvcw.

Answer this question by providing the decrypted plaintext as well as the key used to encrypt/decrypt it.  (Hint: you learned a way to crack this cipher without knowing the key in class.)

**QUESTION 4**

Individual Project:

You should have your service installed, functioning and understand its default options already.

You now need to be able to demonstrate methods you have uncovered that can be used to attack your service.  Please write and upload a report that answers the following three questions and include screenshots for each:

1.  What ports does your service cause to be open?  (Use nmap or zenmap before and after installation or you can possibly just use netstat after installation.)

2.  What default configuration options are dangerous by default and how would you attack them?  (Can an attacker view or download data they shouldn't be able to access, access a configuration menu through a web server gui, use the service to attack another system, does the service use default passwords that should be changed, etc.)

3.  Are there any other attacks you can perform against your service that aren't related to default configuration options?