Capture the Flag (CTF) Unplugged

- Overview -

What is CTF?

The phrase "**Capture the Flag**" (abbreviated CTF) refers to any type of game in which two or more teams compete for a flag (or other marker) as an indication of victory.

In terms of cybersecurity, Capture the Flag contests are typically designed as educational exercises. These competitions give participants the opportunity to gain experience in securing a machine, conducting research, and reacting to the sorts of cyber attacks that can be found in the real world.

Mission 000: Reconnaissance

Introduction:

Recently, CEROC has been working closely with the FBI to track down a notorious hacker (pseudonym Hax0r) who is skilled in removing all traces of cyber attacks that he has completed. However, Hax0r has become overconfident and has begun leaving clues for the FBI to demoralize the investigative team and demonstrate his/her superiority. The investigative team is hoping to capitalize on Hax0r's narcissism by cracking these clues and uncovering his or her true identity.

Activity 1: Research Your Target (Physical Clues)

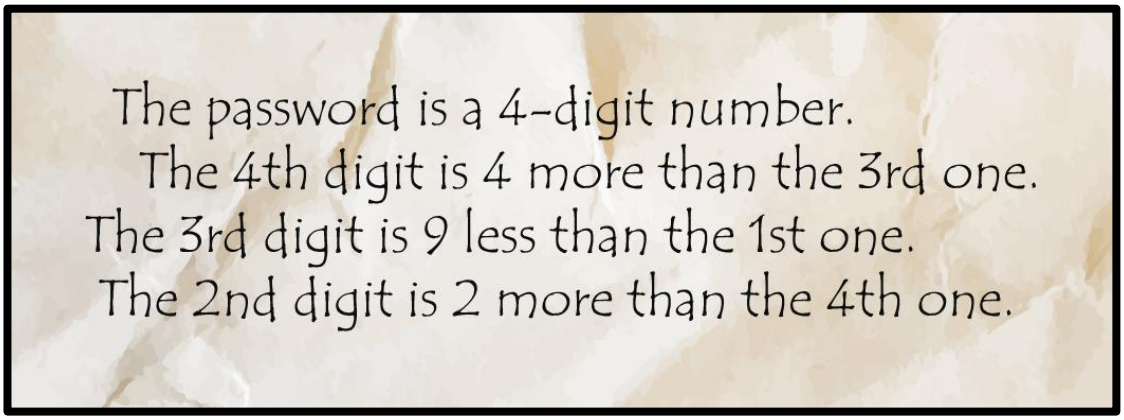
Cybersecurity *reconnaissance* (a.k.a. information or open source intelligence gathering) is the preliminary process of surveying of a person or system using publicly available resources, such as search engines (Google), social networks, friends lists, visual observations, direct contacts, and network analysis. For example, before a hacker tries to get into your email account, he/she may try to send you phishing emails (using prior knowledge about you from social networks and publicly available information in a search engine) in an attempt to make you respond with sensitive information like your credit card number, full name, social security number, or home address.

The FBI agent working with CEROC mentioned that Hax0r stayed in Cookeville for a few days to use computing resources at Tennessee Tech. CEROC will be assisting the FBI by searching for clues in this area.

Tasks at Hand:

[Task 1] Hax0r has a known accomplice who goes under pseudonym Lis@. Although the FBI managed to discover the location of their next meeting, they were too late to intercept them. Thankfully, we managed to find a piece of paper in a nearby trash can that appears to have been written by our suspects. Can you figure out the password?

(5 pts) **Solution (1) :** _____



Activity 2: ASCII table

ASCII stands for “American Standard Code for Information Exchange”. Every symbol in this table is linked with a certain number that a computer can understand. Given a number, the computer knows what symbol to show to a user. For example, if a program tells the computer to show a symbol corresponding to number 80_{10} (or 50_{16}), the computer will display ‘P’ on the screen.

Remove The Back Page For An Easy To Access Copy Of This Table

ASCII Table								
ASCII Code		Symbol	ASCII Code		Symbol	ASCII Code		Symbol
Dec	Hex		Dec	Hex		Dec	Hex	
32	20	Space	64	40	@	96	60	`
33	21	!	65	41	A	97	61	a
34	22	"	66	42	B	98	62	b
35	23	#	67	43	C	99	63	c
36	24	$	68	44	D	100	64	d
37	25	%	69	45	E	101	65	e
38	26	&	70	46	F	102	66	f
39	27		71	47	G	103	67	g
40	28	(	72	48	H	104	68	h
41	29	)	73	49	I	105	69	i
42	2A	*	74	4A	J	106	6A	j
43	2B	+	75	4B	K	107	6B	k
44	2C	,	76	4C	L	108	6C	l
45	2D	-	77	4D	M	109	6D	m
46	2E	.	78	4E	N	110	6E	n
47	2F	/	79	4F	O	111	6F	o
48	30	0	80	50	P	112	70	p
49	31	1	81	51	Q	113	71	q
50	32	2	82	52	R	114	72	r
51	33	3	83	53	S	115	73	s
52	34	4	84	54	T	116	74	t
53	35	5	85	55	U	117	75	u
54	36	6	86	56	V	118	76	v
55	37	7	87	57	W	119	77	w
56	38	8	88	58	X	120	78	x
57	39	9	89	59	Y	121	79	y
58	3A	:	90	5A	Z	122	7A	z
59	3B	;	91	5B	[	123	7B	{
60	3C	<	92	5C	\	124	7C	|
61	3D	=	93	5D	]	125	7D	}
62	3E	>	94	5E	^	126	7E	~
63	3F	?	95	5F	_	127	7F	Delete

As you can see, every symbol has a corresponding 2-digit hexadecimal (hex) number. Now, let's make use of hex in transmitting messages to your friend! Suppose that you want to say 'hi'

to your friend and send it over a communication channel in a chat. Do you know what happens behind the scenes? First, it converts the symbols you typed into the corresponding ASCII code and then sends it via the Internet to your friend. End of the day, all of the data is translated to 0's and 1' which can be easily transferred as electrical signals! Hexadecimal system also has a bigger range of numbers than the decimal system! Just think about it, FF in hex is 255 in dec (why?!), therefore we represented a 3-digit decimal number with just 2 digits in hex.

To encode a message with the ASCII character set,, convert it to hex. 'h' corresponds to 68 and 'i' - to 69 (remember, capitalization matters in ASCII table). So, the resulting string of numbers that will get sent to your friend will be 6869_{16} which your computer would translate in signals to send over the communication medium.

Tasks at hand:

1) What is an ASCII decimal code of 'A'?

(2 pts) **Solution (2) :** _____

2) What symbol does 95_{10} correspond to in the ASCII table?

(2 pts) **Solution (3) :** _____

3) What message is encoded in hex: 77 65 5F 6A 75 73 74 5F 68 65 78 61 6C 69 6E 5F 68 65 78 61 6C 69 6E?

(5 pts) **Solution (4) :** _____

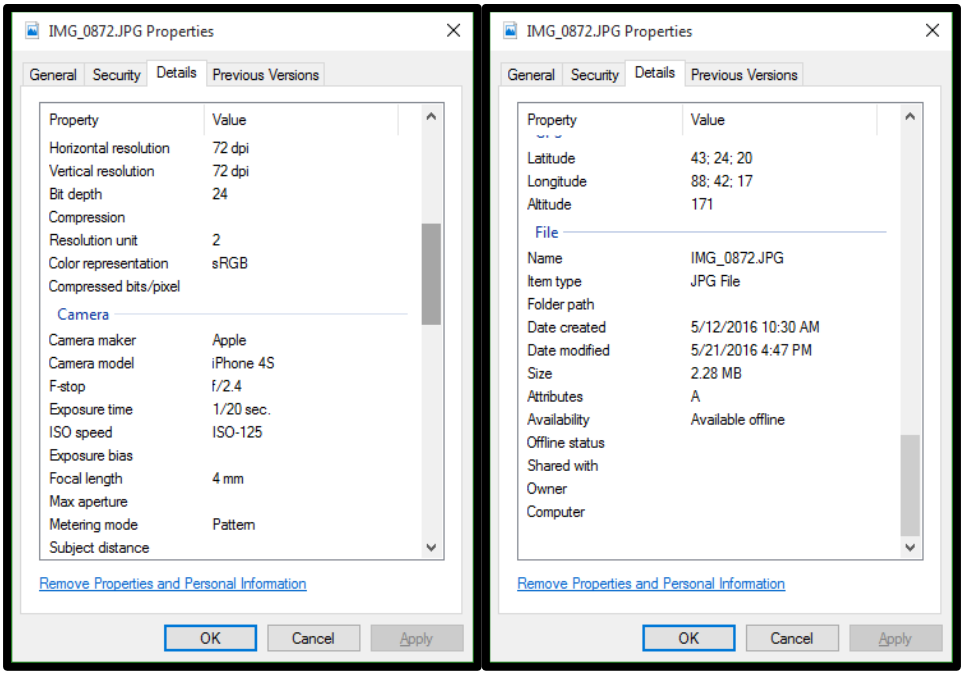
Mission 001: Forensics

Forensics is a set of techniques that are applied on a data set or system to investigate what has happened on that system following a significant event (e.g. a system compromise). This work is performed by extracting data from corrupted hard drives and analyzing the resulting files to make sense of their contents and develop intrusion scenarios.

Activity 1: GPS Spy

For the past two days, CEROC has been analyzing a data dump from a computer containing sensitive information about our university's employees, which Hax0r compromised. The computer was found in one of the buildings that Hax0r visited. The FBI recovered an image from that computer and provided you its *metadata* (i.e. properties, or "data to describe other data").

Name	SSN	E-mail
Alf A. Romeo	235-78-4487	aromeo@ssn.edu
Anna Prentice	456-98-1145	aprentice@ssn.edu
Anna Sasin	778-69-3689	asasin@ssn.edu
Anne Teak	445-87-1121	ateak@ssn.edu
Annette Curtain	446-99-5487	acurtain@ssn.edu
Armand Hammer	759-67-1211	ahammer@ssn.edu
Barry Cade	969-86-9893	acade@ssn.edu
Bill Loney	183-46-7877	aloney@ssn.edu
Billy Rubin	489-56-5687	arubin@ssn.edu
Bob Apple	567-48-2532	aapple@ssn.edu
Brock Lee	878-46-7789	alee@ssn.edu
Cam Payne	158-54-7619	apayne@ssn.edu
Cara Van	658-98-2210	avan@ssn.edu
Casey Macy	507-96-1680	amacy@ssn.edu
Chip Munk	665-78-5059	amunk@ssn.edu
Chuck Waggon	127-89-4897	awaggon@ssn.edu
Claire Annette Reed	568-20-4596	areed@ssn.edu



It is amazing how much time and geographic information can be obtained from a single digital picture. By using metadata, you can track an individual's location within a precision of several meters. Think about that next time you post a selfie on Facebook…

Tasks At Hand:

Your mission is to figure out where Hax0r took that picture, particularly you need to know 2 things:

`[Task 5]` In what state was the picture taken?

`[Task 6]` In what city was the picture taken?

We need this information ASAP because it may give us a clue where Hax0r's home town is.

(5 pts) **Solution (5) :** _____

(5 pts) Solution (6) : _____

Activity 2: Pass the Word

Using the TnTech employees' information, Hax0r managed to break into several bank accounts. However, thanks to your help in identifying the hacker's location, the FBI were able to track down the computer he/she used to perform the attack. On this computer, they found a collection of music and email files; the dump of one of the email files contained the following string: "Lis@, the mission is complete. We have access to the necessary data. Now we can transfer money to the offshore account. You will find a flash drive under the carpet in front of the door. There is a password-protected file on it. The password is a word from a song we listened to on the radio when we drove to Washington, DC."

I See Fire
By Ed Sheeran

Oh, misty eye of the mountain below
Keep careful watch of my brothers' souls
And should the sky be filled with fire and smoke
Keep watching over Durin's son

If this is to end in fire
Then we should all burn together
Watch the flames climb high into the night
Calling out for the rope, sent by and we will
Watch the flames burn on and on the mountainside hey

And if we should die tonight
Then we should all die together
Raise a glass of wine for the last time
Calling out for the rope
Prepare as we will
Watch the flames burn on and on the mountainside
Desolation comes upon the sky

Now I see fire, inside the mountain
I see fire, burning the trees
And I see fire, hollowing souls
And I see fire, blood in the breeze
And I hope that you'll remember me

Oh, should my people fall
Then surely I'll do the same
Confined in mountain halls
We got too close to the flame
Calling out father hold fast and we will
We got too close to the flame
Calling out father hold fast and we will

Watch the flames burn on and on the mountainside
Desolation comes upon the sky

Now I see fire, inside the mountain
I see fire, burning the trees
And I see fire, hollowing souls
And I see fire, blood in the breeze
And I hope that you'll remember me
And if the night is burning
I will cover my eyes

For if the dark returns then
My brothers will die
And as the sky's falling down
It crashed into this lonely town
And with that shadow upon the ground
I hear my people screaming out

Now I see fire, inside the mountain
I see fire, burning the trees
And I see fire, hollowing souls
And I see fire, blood in the breeze

I see fire, oh you know I saw a city burning (fire)
And I see fire, feel the heat upon my skin (fire)
And I see fire (fire)
And I see fire (burn on and on and mountainside)

Tasks at Hand:

[Task 7] On the same computer, we found a music file with the name "I See Fire, Ed" and an image file containing a list of ordered triplets. Can you figure out the password the hacker used to encrypt the file?

Hint: (3, 2, 4) = t

(3, 2, 4), (4, 6, 5), (1, 1, 1), (6, 1, 1), (1, 1, 1), (6, 1, 1), (15, 1, 1), (24, 4, 1), (28, 5, 2), (45, 4, 1), (7, 1, 4), (4, 3, 2), (11, 6, 1), (11, 6, 1), (25, 5, 6), (4, 6, 3), (39, 3, 3), (45, 4, 1)

(8 pts) **Solution (7) :** _____

Activity 3: The *Italic* Job

The password worked, but the folder it opened was empty. Although initially disheartened, we found another odd-looking message on Hax0r's desktop. This message apparently describes how Hax0r broke into the bank.

`Tasks at Hand:`

`[Task 8]` This message holds a clue of how Hax0r compromised the bank (HINT: the numbers denote the order of the "special" words).

(9 pts) **Solution (8) :** _____

6 Do you know how I got *inside* the network of the bank? I positioned myself near the bank for a few
5 hours early in the morning, giving away CD disks with my new "music" and asked people
2 to check it out. Some of these people were employees of the bank and a few of them actually put
4 the CD into their laptop! My CD installed a virus on the laptop and captured their email password.
3 From there, I asked bank's IT department to restore the password to the accounting system
1 using that employee's email! The game was over. I was in.

Mission 010: Cryptography

Activity 1: Decimal gibberish

The FBI found some evidence of Lis@ meeting Hax0r in one of the Los Angeles hotels. In that hotel room they found a paper with random numbers. They asked CEROC for help to decrypt it and see what that message is all about.

The easiest way to encrypt text is to transform it to numbers and work directly with those numbers because it is simpler to apply mathematical functions to numbers than letters. HINT: Do you recall seeing similar numbers in previous challenges?

Tasks at Hand:

`[Task 9]` Decode the following cipher:

(5 pts) **Solution (9) :** _____

(77,101,101,116,32,109,101,32,97,116,32,49,58,51,48,32,112,109)

Activity 2: Hail, Caesar!

Hax0r's message indicates that he/she has an insider working with the bank. One of our agents has just completed a dumpster diving exercise on the property and found what might be our next clue. It is a wad of paper tucked inside a discarded Caesar salad bowl. The piece of paper is a crumpled check from the bank in question. Other than the number of the check (007) and a series of jumbled letters, all other printed information has been destroyed. The letters on the check are as follows:

Note:

In *cryptography* (which is a method for secure communication via data hiding), we use ciphers to keep messages hidden from unauthorized viewers. A *cipher* is an algorithm (or a series of steps) that you have to follow in order to encrypt (make normal text look like gibberish) or decrypt (convert gibberish back to the normal text) information. A Caesar cipher is a *substitution cipher* that replaces every letter in a message with another letter obtained by shifting the original alphabet X places (or letters) to the right.
For example, take a look at the image below:

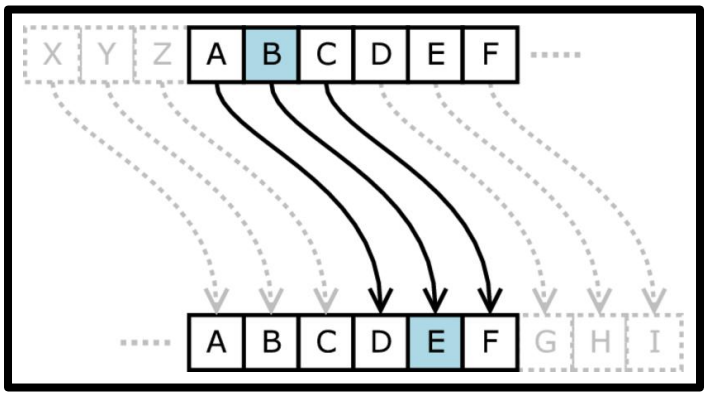
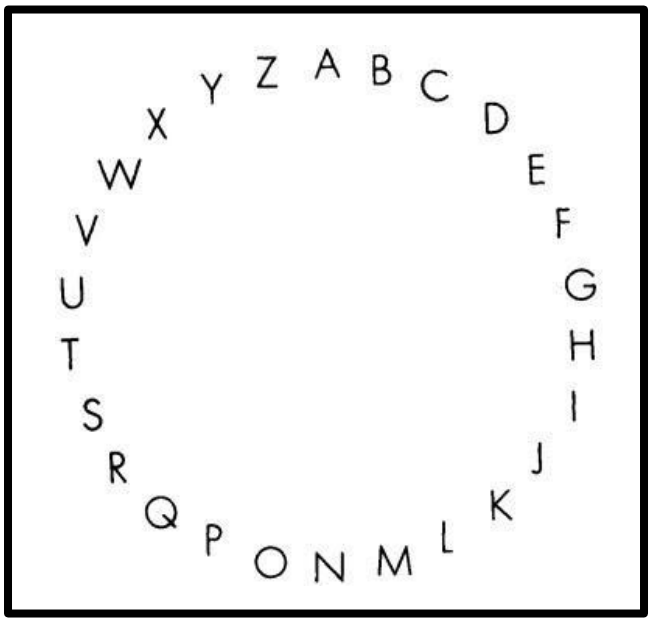


Image source: https://upload.wikimedia.org/wikipedia/en/7/75/Caesar3.png

As illustrated above, letter A becomes letter D, letter B becomes letter E, and so forth, resulting in a message that is unreadable to anyone without the key. Notice a pattern? We replace every letter with the letter X places down the alphabet, where is X our key. For example, if our original message is “HELLO” and the key is three, then the ciphertext becomes “KHOOR”. Keep in mind that the key to a Caesar cipher can be almost any number, as long as that number can eventually be reduced by division to a number between 1 and 26.

(H → K; E → H; L → O; O → R).

If encrypting a Caesar cipher means moving each letter X spaces down the alphabet, where X is your key, how might one *decrypt* a Caesar cipher? An alphabet wheel (shown below) has been provided:



Yhkzhm mh fxgmbhg max ietvx Ptmxk Zkbee

Tasks at Hand:

[Task 10] What is the message?

(8 pts) **Solution (10) :** _____

Activity 3: Morse code

The FBI and CEROC went to the water grill at 2 pm, and it was already too late, Hax0r and Lis@ had left the restaurant. The restaurant had cameras installed so the FBI asked the manager to pull the videos off the data center and let us use those videos in our investigation. We found the perpetrators on one of the videos but they both were wearing anonymous masks (yes, it was October 31st). However, after zooming into their table conversation, we noticed this code that was written on a napkin:

Tasks at Hand:

[Task 11] Decrypt the following morse code:

(5 pts) **Solution (11) :** _____

```
---  ..-  .-.       -.  .  -..-  -       -  .-  .-.  --.  .  -
..  ...       -...  .-  -.  -.-       ---  ..-.       .-  --
.  .-.  ..  -.-.  .-
```

A •–	B –•••	C –•–•	D –••
E •	F ••–•	G ––•	H ••••
I ••	J •–––	K –•–	L •–••
M ––	N –•	O –––	P •––•
Q ––•–	R •–•	S •••	T –
U ••–	V •••–	W •––	X –••–
Y –•––	Z ––••	0 –––––	1 •––––
2 ••–––	3 •••––	4 ••••–	5 •••••
6 –••••	7 ––•••	8 –––••	9 ––––•

Mission 011: Reverse Engineering

Reverse engineering is the art of learning how something is constructed when given only the finished product. For example, you might decide to take apart a phone or a toaster in order to see how the product works. Working backwards from a given solution to better understand a process - be it in math, manufacturing, computer science, or anything else - is what reverse engineering is all about.

In computer science, specifically information security, reverse engineering helps you find out how programs work when all you have is the executable machine code, rather than the easier-to-understand program file. This can be a tedious but productive task, especially if we want to learn how a specific piece of *malware* (**mal**icious soft**ware**, such as computer viruses) works in order to prevent any future malware infection.

Activity 1: The Good, the Bad, and the Password

It seems that Hax0r is in the game again. At our university, we gained access to an executable program that Hax0r used for generating the passwords to protect files. Our specialists extracted the code and converted it into a format that can be read by humans.

Tasks at hand:

[Task 12] Can you figure out the password used by Hax0r?

(10 pts) **Solution (12) :** _____

```
C = 69       // Assign 69 to the variable C.
B = 99       // Assign 99 to the variable B.
pass = ""    // Assign pass to be an empty string.
step = 1     // Assign 1 to the variable step.

Repeat until step is equal to 3:
{  // Start the loop.

      // Insert a letter to pass from the variable C by converting it to ASCII.
      pass.insert( convertDecimalToASCII(C) )
      // Insert a letter to pass from the variable B by converting it to ASCII.
      pass.insert( convertDecimalToASCII(B) )

      C = B + 5        // Assign the result of (B + 5) to the variable C.
      B = C - 56       // Assign the result of (C - 56) to the variable B.

      step = step + 1 // Increase step by 1.
}  // End the loop.
```

Activity 2: What If?

The FBI managed to catch Hax0r at his rendezvous location, but his accomplice, Lis@, remains at large. During an interrogation session, Hax0r gave us access to one of his servers. However, everything on the server is encrypted. Using a tool called "Volatility," we are able to read the memory of the computer and extract all procedures that Hax0r performed to log in to the server.

Tasks at Hand:

[Task 13] If we can reverse-engineer this section of code, we will uncover the password to a file containing the GPS location of Lis@.

(10 pts) **Solution (13) :** _____

```
B = 89          // Assign 89 to the variable B
pass = ""       // Assign pass to be an empty string.
step = 1        // Assign 1 to the variable step.

Repeat until step is equal to 5:
{  // Start the loop.

      if B < 90 then do:
      { // Enter this block only if B is less than 90
            // Insert a letter to pass from B by converting it to ASCII.
            pass.insert( convertDecimalToASCII(B) );
            // Assign the result of (B + 5) to the variable B.
            B = B + 5;
            //If you've gotten here, skip the next else
      } // Finish the first block

      Else B >= 90 then do:
        { // Enter this block only if B is greater than or equal to 90 and if
          // you didn't enter the first loop
            // Assign the result of (B - 15) to the variable B.
            B = B - 15;
      } // Finish the second block

      step = step + 1 // Increase step by 1.
      }  // End the loop.
```

Mission 100: Steganography

Steganography is a method of hiding information inside of an unassuming file, such as an image. To any random viewer, the file will appear completely normal. However, someone who knows that the information exists (and knows how it was hidden) can easily extract it. For example, you can append additional text to the end of image data (recall that everything stored on a computer is technically encoded in binary: just 1's and 0's). You will still see an image because the computer thinks that it is an image with random data at the end, but if you know that something is hidden there, you can uncover what it is.

Activity 1: Selfie Steganography

Using the GPS data extracted from Hax0r's files, the FBI managed to locate and arrest Lis@. Now, the only remaining mystery is where Hax0r and Lis@ hid their stolen money. One of the files on Lis@'s personal computer appears to contain hidden information, possibly relating to the bank's name or location.

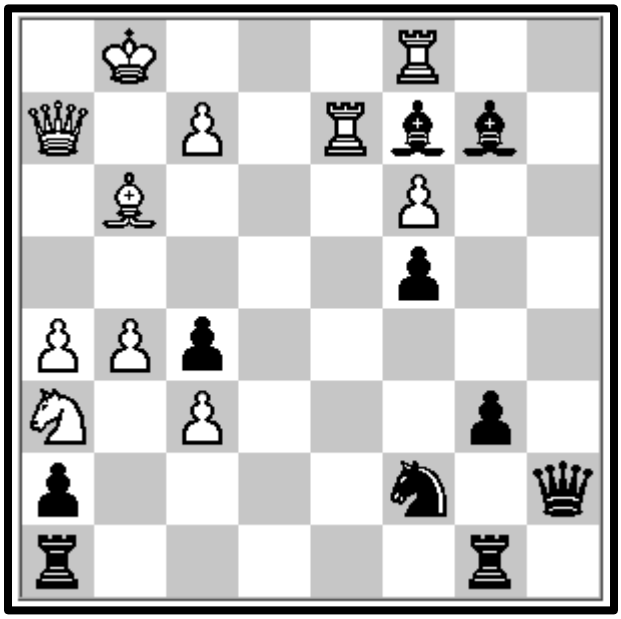
Tasks at Hand:

[Task 14] Given the image found on Lis@'s computer, can you determine the name of the offshore-bank in which they have hidden their money?

(8 pts) **Solution (14) :** _____

Activity 2: To Check or Not to Check?

Having determined the name of the bank, the FBI's last step is to find Hax0r's personal account. Strangely, when confronted with this question during interrogation, Hax0r agreed to tell us - but only if we played him in a game of chess. The FBI agreed, but when we got to the position on the board as shown below, Hax0r exclaimed, "You got it!" Can you figure it out what Hax0r meant?



Tasks at hand:

[Task 15] What is Hax0r's account name in the offshore bank?

(8 pts) **Solution (15) :** _____

Mission 101: Social Engineering

Activity 1: Coffee Talk

It seems that Hax0r took a break from his normal crime spree to drink some coffee at a local coffee shop. We know this, because several people who were visiting the shop at the same time have had their Facebook pages broken into. These compromised accounts have been asking their friends and family if they can borrow some money. It seems that Hax0r was able to guess people's passwords by just talking to them. Below is a conversation that we found in the background of a video of a couple visiting the shop at the same time. Unfortunately, Hax0r was not in the frame. However, we could hear his voice. Below is a transcribed copy of their conversation.

1. Hax0r: Oh excuse me miss, I just saw the sticker of a pug you have on your laptop and wanted to let you know that I thought it was cool.

2. Nancy: Why thank you. I really love pugs.

3. Hax0r: Me too. I have one named Stumpy at home. Do you have a pug?

4. Nancy: Not anymore, I just think they are so cute. Now I only have a cat.

5. Hax0r: Oh wow, really? My first pet was a cat but he was kind of mean. Is he your first pet?

6. Nancy: Oh, no. My first pet was a hamster, named Fred. I got him when I was 9.

7. Hax0r: My favorite teacher in high school had a hamster in his classroom. I loved math class.

8. Nancy: Oh, I hated math, but I loved english my teacher. He was always interesting when he taught.

9. Hax0r: Did you go to high school around here?

10. Nancy: Yep, just down the road from here.

11. Hax0r: Did you have Mr.Hicks for english like I did, or did he already retire before you got there?

12. Nancy: No my teacher was Mr.Wilks.

13. Hax0r: Well I .....(Audio recording ends. It seems that Hax0r got Nancy's name later in the conversation.)

Tasks at hand:

[Task 16] Can you determine where in the conversation that Nancy revealed sensitive information. The solution will be the combination of the line numbers, in order, that reveal sensitive information (example: line 1, line 2, and line 3 would be '123').

Hint: security questions

(5 pts) **Solution (16) :** _____

Points to Ponder

Capture The Flag

- Security is full of puzzles, some are harder than others too!
- Our adversary used all of these puzzles to ensure his Confidentiality.
- Cryptographic functions can be used to hide information.
- Keeping things simple can really confuse an attacker, like the last puzzle.
- Defense in Depth leads to layers of puzzles, much like what you just solved.

Relationship with GenCyber Cybersecurity Concepts

Cyber threats show themselves in all sorts of ways, and oftentimes the very way we secure our own information can be used against us. In CTF there are two teams that must secure information against one another in some form or fashion, and we have to think like an adversary in order to find what we want.

Defense in Depth is one of the biggest parts of a secure system. It took awhile to solve some of these puzzles for a reason. Imagine if they had all been steganography puzzles, or if they were all breaking a Caesar cipher. It wouldn't be nearly as secure, as you could use the same method or tool to break through.

Resource Links

- CTF Intro - introduction to CTF concepts (https://trailofbits.github.io/ctf/)
- Open CTF - How to participate in CTF (http://www.openctf.com/html/firstctf.html)
- Captf - list of online CTF competitions (http://captf.com/practice-ctf/)
- Ctf365 - Capture the flag practice site (https://ctf365.com/)
- Ctftime - CTF competitions near me (https://ctftime.org/event/oldlist/upcoming)

Remove This Off For Easy Access

ASCII Table								
ASCII Code		Symbol	ASCII Code		Symbol	ASCII Code		Symbol
Dec	Hex		Dec	Hex		Dec	Hex	
32	20	Space	64	40	@	96	60	`
33	21	!	65	41	A	97	61	a
34	22	"	66	42	B	98	62	b
35	23	#	67	43	C	99	63	c
36	24	$	68	44	D	100	64	d
37	25	%	69	45	E	101	65	e
38	26	&	70	46	F	102	66	f
39	27		71	47	G	103	67	g
40	28	(	72	48	H	104	68	h
41	29	)	73	49	I	105	69	i
42	2A	*	74	4A	J	106	6A	j
43	2B	+	75	4B	K	107	6B	k
44	2C	,	76	4C	L	108	6C	l
45	2D	-	77	4D	M	109	6D	m
46	2E	.	78	4E	N	110	6E	n
47	2F	/	79	4F	O	111	6F	o
48	30	0	80	50	P	112	70	p
49	31	1	81	51	Q	113	71	q
50	32	2	82	52	R	114	72	r
51	33	3	83	53	S	115	73	s
52	34	4	84	54	T	116	74	t
53	35	5	85	55	U	117	75	u
54	36	6	86	56	V	118	76	v
55	37	7	87	57	W	119	77	w
56	38	8	88	58	X	120	78	x
57	39	9	89	59	Y	121	79	y
58	3A	:	90	5A	Z	122	7A	z
59	3B	;	91	5B	[	123	7B	{
60	3C	<	92	5C	\	124	7C	|
61	3D	=	93	5D	]	125	7D	}
62	3E	>	94	5E	^	126	7E	~
63	3F	?	95	5F	_	127	7F	Delete