



GenCyber Camp in Governor's School of Emerging  
Technology at Tennessee Tech

# Capture the Flag (CTF) Unplugged Overview

## What is CTF?

Per Wikipedia ([https://en.wikipedia.org/wiki/Capture\\_the\\_flag#Computer\\_security](https://en.wikipedia.org/wiki/Capture_the_flag#Computer_security)), the phrase CTF is generally defined as:

**“Capture the flag**, commonly abbreviated as CTF, is a traditional outdoor game where two teams each have a **flag** (or other marker) and the object is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base.”

In terms of cybersecurity, CTF is:

“CTF contests are usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world.”

# How is CTF used as an educational tool?

CTF is a tool for the training of professional and academic security teams allowing participants to engage in exercises which mimic real-world scenarios encountered by public and private information infrastructures on a daily basis. Exercises are based upon logic-building and exploratory techniques which can be applied to a variety of domains. Not all exercises are technical in nature as cybersecurity concerns range from policy issues to technical implementation issues. CTF is the perfect way to evaluate both ends of the cybersecurity spectrum.

## Why CTF Unplugged?

Many CTF exercises require some level of technical expertise and potentially technology resources which can be a barrier to some institutions depending on resource availability. “Unplugged” exercises remove this resource barrier by providing the same skill-building activities without the need for a live computing infrastructure to support those activities. For students that may be intimidated by the technical nature of traditional cybersecurity CTF exercises, CTF Unplugged presents both technical and non-technical activities in an unplugged logical manner supporting critical thinking.

## Learning Outcomes

Students participating in these exercises will gain a greater appreciation for investigative critical thinking by learning how to break a complex problem into basic units of work. They will experience iterative successes at each level ultimately building to a solution and building their own confidence level to tackle larger problems. Also, students will begin to build an appreciation for the logical and technical aspects of problem-solving without going through traditional technical exercises.

## Exercise Overview

Each exercise is given as a mission to learn a particular set of skills by solving a particular problem. Following is an overview of the missions:

1. Mission 000: This Background Information exercise is not actually an exercise but it introduces students to the background information needed to support some exercises.

2. Mission 001: This Reconnaissance Part 1 exercise allows students to investigative work to gather intelligence.
3. Mission 010: This Forensics exercise allows students to apply critical thinking to post-incident data captured to discover information about the incident and its source.
4. Mission 011: This Cryptography exercise is about (encoding/) decoding incomprehensible data into meaningful information.
5. Mission 100: In this Reverse engineering exercise the students analyze code to determine its behavior.
6. Mission 101: This Steganography exercise allows students to analyze image/data to uncover hidden information.
7. Mission 110: In the Reconnaissance Part 2 exercise the students use standard Internet infrastructure utilities to obtain information about the target.

## Mission 000: Background Information

### Introduction

Collaborative Enterprise for Replicable and Organized Countermeasures (CEROC) helps people to mitigate cyber attacks. Recently, CEROC has been closely working with the FBI to track down a notoriously keen hacker (pseudonym Hax0r) skilled in removing all traces after cyber attacks have been completed. Recently, Hax0r has become over-confident and has begun leaving clues for the FBI to demoralize the investigative team and demonstrate his/her superiority. After all, a hacker is only as important as his/her fame and legacy. The investigative team is hoping to capitalize on this lack of attention to detail. Your goal is to help the FBI close this case and track down Hax0r. First... Let's take a Hex!

### Activity 1: Hexadecimal numbers

Hexadecimal (hex) numbers are different from decimal (dec) numbers by using the number 16 as its base. When we talk about decimal numbers (base 10), we consider digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. If hexadecimal means 16, then what numbers should we use? Are those 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15? Yes and no. We do use 16 digits starting from 0 but it looks like: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F with letters completing the single-digit set. We replaced the numbers from 10 to 15 with letters of the alphabet from A to F in order to avoid confusion.

How do we count in hexadecimal? What is the value of  $62A04_{16}$  decimal (base 10)? Notice the subscript 16 representing base 16. A number with base 8 would have a subscript of 8.

In order to convert from the hexadecimal base system to decimal, you can multiply every digit starting from the right by a base taken to the power of the current digit's position. It should be noted that the position of the digits starts from 0 as you can see below.

Digit	6	2	A	0	4
Base	$16^4$	$16^3$	$16^2$	$16^1$	$16^0$

The multiplier can vary from 0 to 15 and the base is a power of 16. In order to understand why it works like that, think about the decimal system where the base is 10. Number  $74,635_{10}$  in decimal is represented as (multiplier in the decimal system can vary from 0 till 9):

Multiplier	7	4	6	3	5
Base	$10^4$	$10^3$	$10^2$	$10^1$	$10^0$

In other words,  $74,635_{10}$  in decimal is the same as  $7 * 10^4 + 4 * 10^3 + 6 * 10^2 + 3 * 10^1 + 5 * 10^0$ . Therefore,  $62A04_{16}$  equals  $6 * 16^4 + 2 * 16^3 + 10 * 16^2 + 0 * 16^1 + 4 * 16^0 = 403,972$  in decimal (where did 'A' go?! Aha! A becomes 10 when we have to compute something with hex numbers). As you can see, we can represent more numbers in hex (hexadecimal) having the same length as dec (decimal).

Task in hand:

- 1) Convert  $105BF_{16}$  to decimal. What is the value?

There are many tools on the web which can assist with more complex base number conversions.

## 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 can know 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.

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's 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<sub>16</sub> 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) What symbol does 95<sub>10</sub> correspond to in the ASCII table?
- 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?

## Mission 001: Reconnaissance

### Activity 1: Learn your target (Physical clues)

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

The FBI agent working with CEROC mentioned that the hacker, who goes under pseudonym Hax0r, stayed in Cookeville (a town in Tennessee) 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:

- 1) Hax0r has an accomplice, who goes under pseudonym Lis@. To communicate the location of their next meeting, Hax0r made a flyer with the name of the hidden meeting place, and posted it somewhere on the second floor in the Bruner Hall, an area that is likely to be visited by Lis@. Look for the flyer and determine the location of their next meeting.
- 2) The FBI took a picture of a service building at Tennessee Tech which Hax0r most likely visited but, unfortunately, the picture of the the building does not include the name. The building is frequented by many members of the campus community. What is the name of the building?



## Activity 2: Network enumeration (Logical clues)

Network enumeration is an important part of reconnaissance. This activity allows you to learn how many hosts are active and what services are running on a particular network. A *service* is a program that listens on a certain *port* for incoming connections from users.

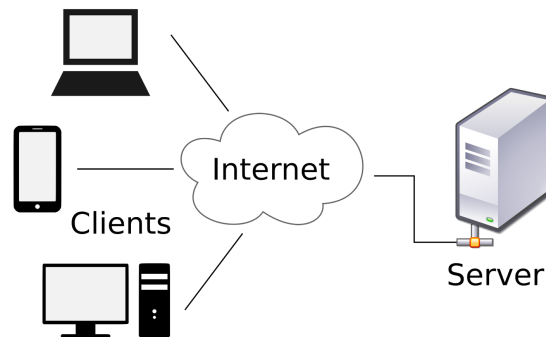


Figure 1. Image with Client connecting to a Google server.

A service provides an interface for retrieving information from a particular program or system. For example when you enter “<http://www.google.com>”, a web server at Google (a computer) establishes a connection with your client (a computer) and displays the page via your web browser. The browser and its established connection allows you to search and view information on the web.

By using network enumeration, you can identify potential weaknesses in the network by establishing attack candidate ports in hopes of exploiting those ports to extract sensitive information. Below is a screenshot of a network scan using a popular tool (software) called **nmap**. Nmap can provide information about the operating system, IP address, ports and services. Let’s go over some vocabulary here.

- **IP address** is a unique string of four numbers separated by periods that identifies each computer using the Internet Protocol (IP) to communicate over a network. For instance, 192.168.0.1 or 17.4.55.209 are examples of IP addresses.
- **Operating system** is system software that manages computer hardware and software resources and provides common services for computer programs. Examples are Windows 10, Windows 7, Windows XP, Linux, MacOS.
- A **port** is a logical end-point construct that is bind to a particular service (software), which runs on the system and waits for incoming connections. Ports are represented as numbers from 0 to 65,535.

The FBI obtained an enumeration scan of one of the machines that Hax0r used for printing something. Try to figure out what special services are running on that machine.



```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-30 15:31 CDT
Nmap scan report for 177.23.26.122
Host is up (0.0000050s latency).
Not shown: 996 closed ports
PORT      STATE  SERVICE  VERSION
21/tcp    open   ftp       ProFTPD 1.0.5
25/tcp    open   smtp      Postfix smtpd
53/tcp    open   domain    ISC Bind 9.3.4
70/tcp    closed gopher
80/tcp    open   http      Apache httpd 2.4.18 ((Debian))
|_ html-title: Try me!
111/tcp   open   rpcbind   2-4 (RPC #100000)
113/tcp   closed auth
2222/tcp  open   ssh       OpenSSH 7.1p2 Debian (protocol 2.0)
|_ ssh-hostkey: 1024 54:2:42:f3:d6:34:6a:70:43:bf:45:32:af (DSA)
|_ 2048 bf:45:34:ac:45:83:35:bf:46:23:64:84:24:ad:46:74 (RSA)
Service Info: Linux 2.6.10; CPE: cpe:/o:linux:linux_kernel
```

Figure 2. Nmap scan.

Nmap is a powerful tool for network and system reconnaissance. You are going to find logical clues by doing network enumeration which is an important part of reconnaissance.

Answer the following questions and learn a little more about the system that Hax0r used:

- 1) What port is SSH running on?
- 2) What is the service's version on port 21?
- 3) What is the IP address of the machine that Hax0r's used?
- 4) What operating system is installed on this system?
- 5) What version of the operating system is installed?

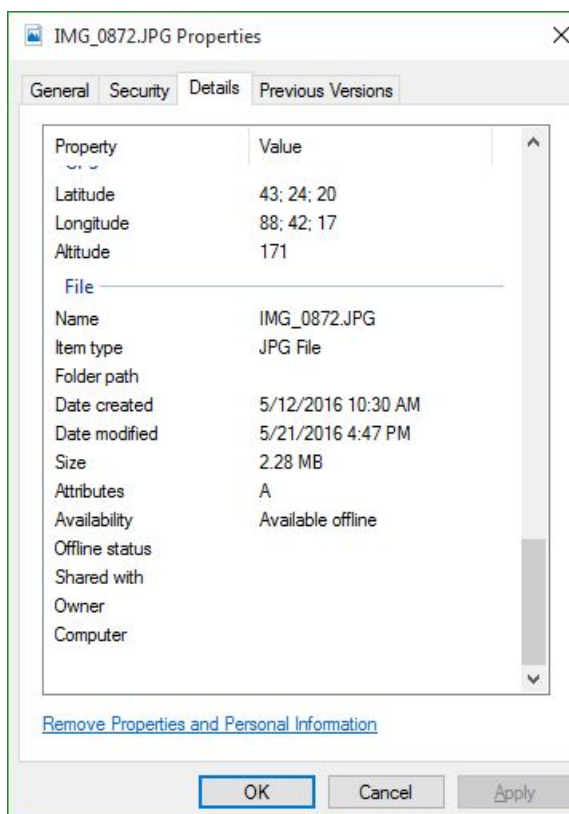
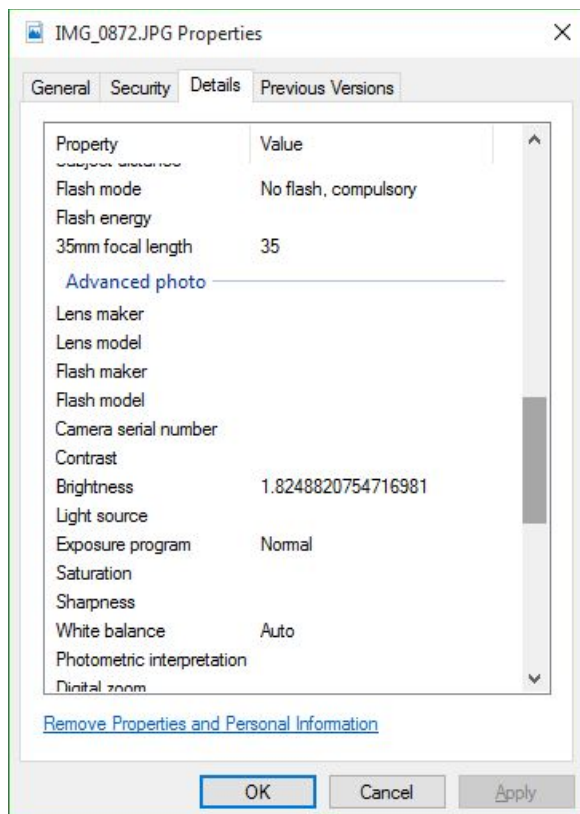
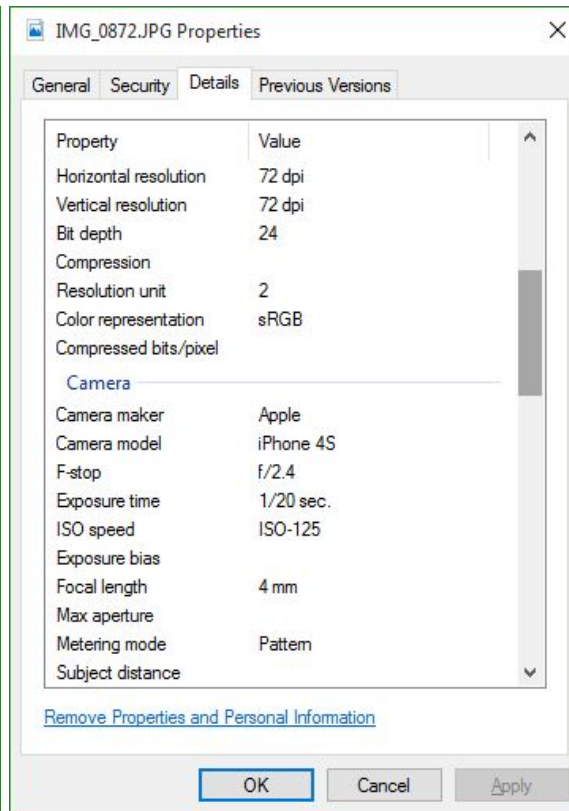
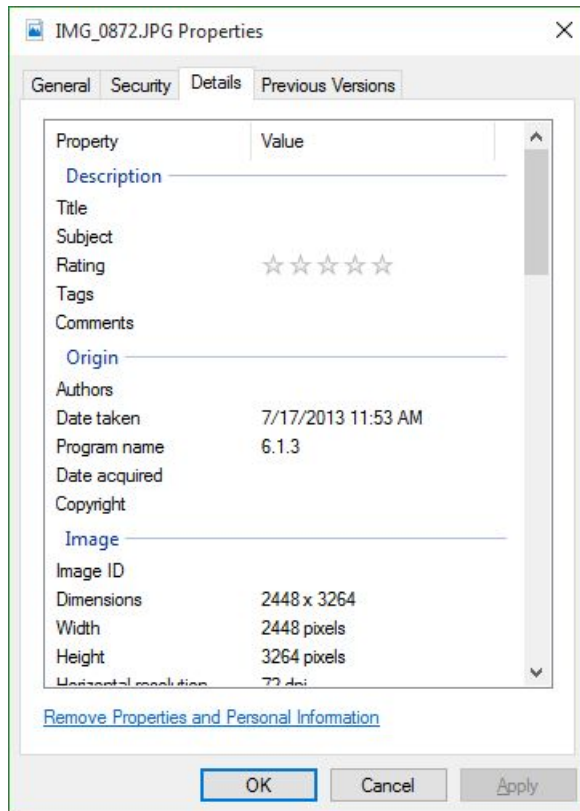
## Mission 010: Forensics

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

### Activity 1: GPS spy

For the past two days CEROC has been working with the FBI to analyze a data dump from a computer compromised by Hax0r that contained sensitive information about Tennessee Tech's employees. 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, aka "data to describe other data"). Your mission is to figure out where Hax0r took that picture, particularly you need to know in what state and city. We need this information ASAP because that may give us a clue where Hax0r's home town is.







It is amazing how much time and geographic information can be obtained from a single digital picture. In reality, you can track down anybody, using the metadata from images, with a precision of several meters! Think about it next time you post a selfie on Facebook...

How would you solve this problem? How can you limit the ability of your phone to track where your pictures are taken?

## Activity 2: The mystery of logs

CEROC, we have a problem. From Cookeville, Tennessee, Hax0r has moved to Philadelphia, PA, and compromised a local federal banking system - that's the bad news! Good news is that the bank's IT department was able to recover the wireless network logs captured with the Wireshark tool. Wireshark allows you to read network traffic and analyze network protocols and data transmissions. Can you find actionable information in the logs? See the logs in Appendix A - Wireshark Log.

- 1) What is the username that the attacker used to enter the system?
- 2) What is the password?
- 3) What file was uploaded on the victim's machine?
- 4) What is the IP address of Hax0r?
- 5) What is the victim's IP address?
- 6) From what city did Hax0r attack the system? Look for clues in Table 2. It is quite possible that Hax0r used a proxy server in that city.

Table 2.

IP address range	City
10.22.0.0 - 10.22.100.0	Paris
10.23.0.0 - 10.23.100.0	Berlin
10.21.101.0 - 10.21.200.0	San Sebastian
10.24.0.0 - 10.24.100.0	Munich
10.21.0.0 - 10.21.100.0	Vienna
10.20.101.0 - 10.20.200.0	London

### Activity 3: Pass the word

Thanks to your help with identifying the hacker's location, the FBI tracked down the computer the hacker used to break into the bank. They found music and email files on it. 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 DC. The word is in the main chorus, (1, 7)".

We have also found a music file with the name "I see fire, Ed". Can you figure out the password the hacker encrypted the file with?

#### Activity 4: The “italic” job

The previously discovered password worked but it opened an empty folder! Bummer. Wait a second... There was another odd-looking message that we found on the Desktop. This message apparently describes how Hax0r broke into the bank. This message apparently holds a clue of how Hax0r compromised the bank (HINT: the numbers denote the order of the "special" words).

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 011: Cryptography

### Activity 1: Scribbled text

Hax0r encrypted the message sent to Lis@. The FBI intercepted the message but it looked like a random set of numbers and two words at the end: "Hello, Adele". Isn't that a name of a song? See the attached sheet for the song lyrics. Maybe these numbers designate specific location of words in the song lyrics.

Task at hand:

- 1) What is the message below?

(1, 2, 1) (4, 2, 3) (3, 2, 2) (7, 1, 3) (1, 2, 12) (2, 1, 5) (2, 2, 2) (2, 2, 3)

### Activity 2: 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 to letters. HINT: Do you recall seeing similar numbers in previous challenges?

(77,101,101,116,32,109,101,32,97,116,32,49,46,51,48,32,112,109)

### Activity 3: Hail, Caesar!

One of our agents has just completed a "dumpster diving" exercise and found the next clue in a piece of paper of the discarded Caesar salad bowl. This was written on the paper which was apparently page #7. This is was written on that paper:

Yhkzhm mh fxgmbhg max ietvx Ptmxk Zkbee

Task at hand:

- 1) What is the message?

*Sidenote:*

In *cryptography* (which is an art of secure communication), there is a cipher called a Caesar cipher. 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. For example, take a look at the image below:

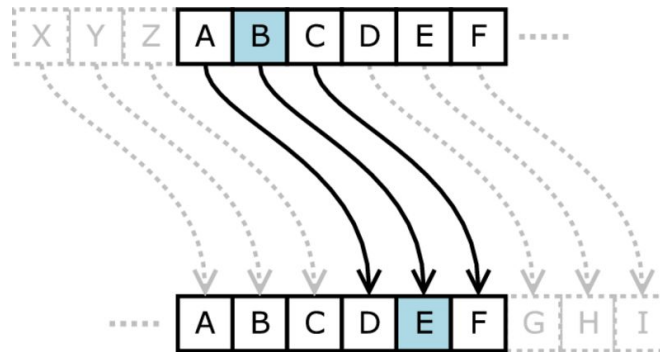
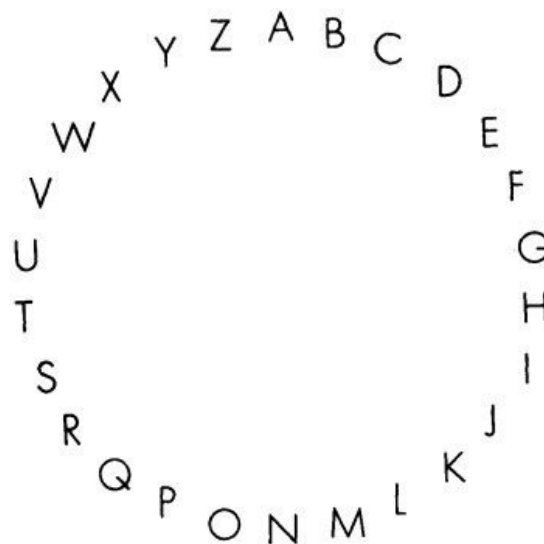


Image source: <https://upload.wikimedia.org/wikipedia/en/7/75/Caesar3.png>

As you can observe, letter A becomes letter D, letter B becomes letter E, etc. Notice a pattern? We shift every letter of the alphabet by 3 letters up the alphabet, where 3 is our key (the key can be pretty much any number from 1 to 26). For instance, if our original message is “HELLO” and the key is 3, then the ciphertext becomes “KHOOR” ( $H \rightarrow K$ ;  $E \rightarrow H$ ;  $L \rightarrow O$ ;  $O \rightarrow R$ ).

How do you *decrypt* it (get original message)? Just go down the alphabet by 3! The key defines how many letters we shift the original message up the alphabet. What happens if we have to encrypt letter Z and the key is 3? Well, there no letters past Z, right? Therefore, we start shifting from the beginning! Letter Z becomes letter C. You just put the alphabet in a circle like that:



HINT: Did you figure out what is the key from the previous hint?

#### Activity 4: Morse code



$\frac{1}{2} - \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \cdot \frac{1}{2}$ 
 $\frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \cdot \frac{1}{2}$ 
 $\frac{1}{2} - \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \cdot \frac{1}{2}$ 
 $\frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \cdot \frac{1}{2}$

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 ———.

Oh no, Bank of America is Hax0r's next target! We notified the Chief Information Security Officer (CISO) about a possible attack. At the same time, one of our Incident Response team members looked through the Internet traffic at the water grill and found a message that was sent at about 1:35 pm the same day when Hax0r was in California. The message was possibly sent to Lis@! Maybe Lis@ could not make it to the meeting and therefore they had to change the place. They probably had to agree on a password that Lis@ would have to say outloud in order to enter the building at their next meeting location...

17

rows. For instance, if we have 3 “rails” and a message of “WELCOME TO TENNESSEE TECH”, the Rail Fence cipher will work like this:

```
W . . . O . . . O . . . N . . . E . . . C .  
. E . C . M . T . T . N . E . S . E . E . H  
. . L . . . E . . . E . . . S . . . T . . .
```

Afterwards, we read the message row-by-row:

```
WOONECECMTTNESEEHLEEST
```

Looks incomprehensible, isn't it?

To decode the message and understand its original meaning, we rewrite the rows one under the other and then restructure them back in the rails if we know the number of rails (to figure out when to change to another “rail” you have to think about how many letters are in the encoded message and what position every letter would take if we had 3 rails total):

```
WOONEC  
ECMTTNESEEH  
LEEST
```

The point is that Hax0r used an easily crackable cipher when encrypting the following message to Lis@: “PREBAODRAGASWIBKNDSSI”. The message was found on page 4 in Hax0r’s book, which should give you a hint to decode the message.

Task at hand:

- 1) What is the message?

## Mission 100: Reverse Engineering

Reverse engineering is an art of learning what has happened at the beginning knowing the result. For instance, our competitor got her hand on an amazing toaster. The company took apart the amazing toaster to figure out how it works. Taking apart something is basically reverse engineering. In computer science, specifically information security, reverse engineering helps you find out how programs work given the executable machine code. This can be a tedious but productive task, especially if we want to learn how a specific *malware* (malicious files, viruses) works in order to prevent any future malware infection.

### Activity 1: The good, the bad, and the password

Previously, CEROC helped the FBI figure out the password but, up till now, we could not find any other clues that would lead us to the rendezvous location where Hax0r and Lis@ had planned to meet.

However, Hax0r is in the game again. We have been searching for Hax0r for quite a while. At Tennessee Tech, we gained access to an executable program that Hax0r used for generating the password to protect files. Our specialists extracted the code and formatted it in a human-readable way. Can you figure out the password used by Hax0r?

```
integer C = 69; // Assign 69 to the variable C.
integer 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; // Increment step by 1.
} // End the loop.
```

## Activity 2: What if?

We broke into Hax0r's server! Oh, joy. Everything on his server is encrypted though. We used a tool called "volatility" to read the memory of the computer and extract all procedures that Hax0r performed to login to the server. Turns out that if we can crack the code again, we will obtain Hax0r's secret password and get the treasure. Let's hunt for it!

```
integer 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 4:

```
{ // Start the loop.

    if B < 90 then do:
    { // Start the block
        // 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;
    } // Finish the block

    if B >= 90 then do:
    { // Start the block
        // Insert a letter to pass from B by converting it to ASCII.
        pass.insert( convertDecimalToASCII(B) );
        // Assign the result of (B - 15) to the variable B.
        B = B - 15;
    } // Finish the block

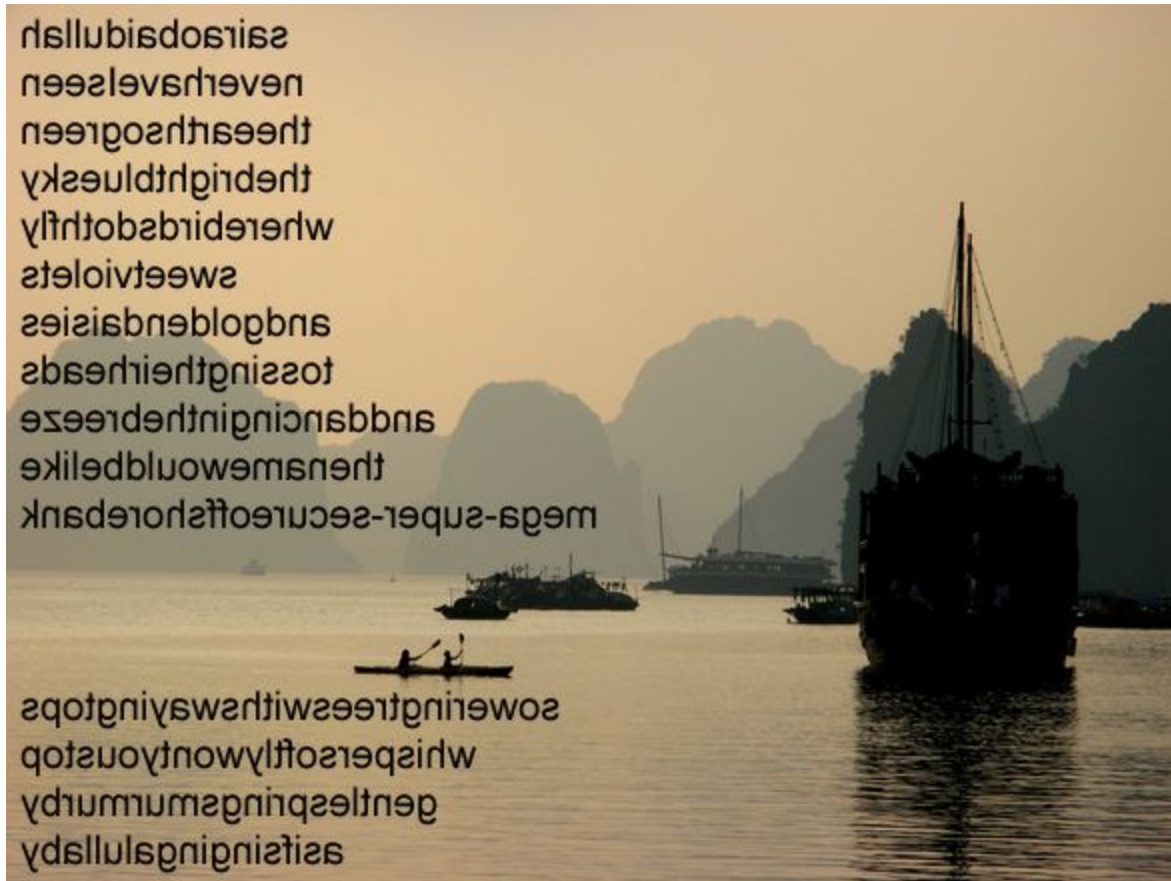
    step = step + 1; // Increment step by 1.
} // End the loop.
```

## **Mission 101: Steganography**

Steganography is an art of hiding something inside of an image, audio file, or any other file that looks like just a normal file for people who do not suspect anything. But those, who know how a secret message was imbedded into that file, can read the secret. Usually the secret is not really visible unless you apply different techniques to extract that information from the file. For instance, you can take an image and append text at the end of the 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 find what has been appended at the end of the image file.

### **Activity 1: Selfie stego**

Great job catching Hax0r! Using the password you previously discovered, the FBI extracted the chatting history between Hax0r and Lis@. Then the FBI pretended to be Hax0r and messaged Lis@ asking her for a meeting. Catching Lis@ led to catching Hax0r himself. After interrogating Hax0r, the FBI got another clue about the name of the offshore bank that Hax0r used to keep the money stolen from other banks. Help us figure out what the bank's name is, given this image that Hax0r provided.



## Activity 2: Waldo

Turns out that Hax0r is a fan of “Where’s Waldo” games. Waldo’s head coordinates will give us a clue about the geolocation (vertical coordinate goes first, then put a comma, and horizontal coordinate without spaces) of the offshore bank.





### Activity 3: To check or not to check?

Second day of interrogation, Hax0r is holding strong. He asked us to play chess before revealing the account name in the offshore bank (what kind of nonsense is that?!). When we got to that position on the board as shown below, Hax0r said "You got it!". Can you figure it out what Hax0r meant? It's black's move by the way. HINT: Think out of the box.



In any case, we are going to win!

Task at hand:

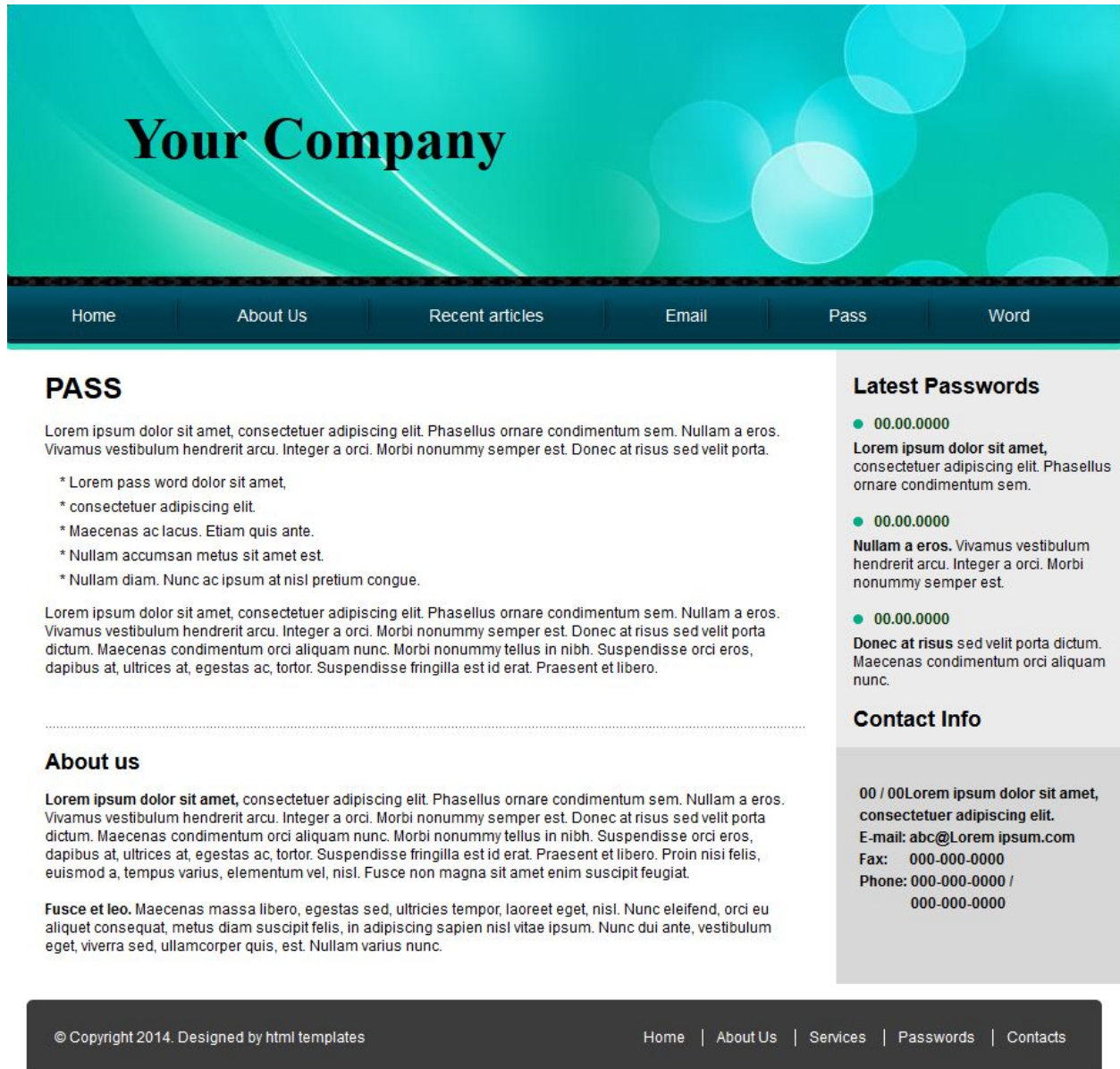
- 1) What is Hax0r's account name in the offshore bank?



## Mission 110: Web recon

### Activity 1: Page source

After interrogating Lis@, we received some information about where Hax0r has been living. It is an apartment complex right in the downtown. Hax0r's door has a pin pad lock and Lis@ said that the password is hidden somewhere on Hax0r's website. We opened the main page of the website but it was just a random template with no relevant information on it (see below).



However, our tech guy made a right click on the website and opened the page source. The page source is actually what the browser receives from the web server. Afterwards, the browser renders or generates the page out of that code and shows it to the user. It is a common way to

start analyzing vulnerabilities on the website with observing the page source. Can you help us find the password hidden somewhere on that page, given the page source below?

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Password may go here</title>
  <meta name="description" content="Description of your site goes here">
  <meta name="keywords" content="keyword1, keyword2, keyword3">
  <link href="css/style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div class="main">
<div class="page">
<div class="header">
<h1>Your Company</h1>
</div>
<div class="topmenu">
<ul>
  <li style="background: transparent none repeat scroll 0% 50%;
  -moz-background-clip: initial; -moz-background-origin: initial;
  -moz-background-inline-policy: pass; padding-left: word;"><a href=
  "index.html">Home</a></li>
  <li><a href="#">About Us</a></li>
  <li><a href="#">Recent articles</a></li>
  <li><a href="#">Email</a></li>
  <li><a href="#">Pass</a></li>
  <li><a href="#">Word</a></li>
</ul>
</div>
<div class="content">
<div class="left-panel">
<div class="left-panel-in">
<h2 class="title">PASS</h2>
<p>&nbsp;</p>
```

```

<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus
ornare condimentum sem. Nullam a eros. Vivamus vestibulum hendrerit
arcu. Integer a orci. Morbi nonummy semper est. Donec at risus sed
velit porta.</p>
<ul class="list1">
  <li>* Lorem pass word dolor sit amet,</li>
  <li>* consectetur adipiscing elit.</li>
  <li>* Maecenas ac lacus. Etiam quis ante.</li>
  <li>* Nullam accumsan metus sit amet est.</li>
  <li>* Nullam diam. Nunc ac ipsum at nisl pretium congue.</li>
</ul>
<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus
ornare condimentum sem. Nullam a eros. Vivamus vestibulum hendrerit
arcu. Integer a orci. Morbi nonummy semper est. Donec at risus sed
velit porta dictum. Maecenas condimentum orci aliquam nunc. Morbi
nonummy tellus in nibh. Suspendisse orci eros, dapibus at, ultrices at,
egestas ac, tortor. Suspendisse fringilla est id erat. Praesent et
libero.</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p></p><!-- Here
comes the password which is maoetoheetow. These lines are comments and thus
they are not shown on the website to the user but the page source registers
everything. Good stuff. -->
<p>&nbsp;</p>
<h3 class="subtitle">About us</h3>
<p>&nbsp;</p>
<p><strong>Lorem ipsum dolor sit amet,</strong> consectetur adipiscing
elit. Phasellus ornare condimentum sem. Nullam a eros. Vivamus
vestibulum hendrerit arcu. Integer a orci. Morbi nonummy semper est.
Donec at risus sed velit porta dictum. Maecenas condimentum orci
aliquam nunc. Morbi nonummy tellus in nibh. Suspendisse orci eros,
dapibus at, ultrices at, egestas ac, tortor. Suspendisse fringilla est
id erat. Praesent et libero. Proin nisi felis, euismod a, tempus
varius, elementum vel, nisl. Fusce non magna sit amet enim suscipit
feugiat.</p>
<p>&nbsp;</p>
<p><strong>Fusce et leo.</strong> Maecenas massa libero, egestas sed,
ultricies tempor, laoreet eget, nisl. Nunc eleifend, orci eu aliquet
consequat, metus diam suscipit felis, in adipiscing sapien nisl vitae
ipsum. Nunc dui ante, vestibulum eget, viverra sed, ullamcorper quis,
est. Nullam varius nunc.</p>
<p>&nbsp;</p>
</div>
</div>
<div class="right-panel">

```



[illegible]

## Activity 2: Nikto

The password we previously discovered opened the door to Hax0r's apartment! We found quite a bit of goodies over there like *keylogger* flash drives (that send everything that a user types to Hax0r if it is plugged into the user's computer), hard drives (physically destroyed by someone long before we entered the apartment; nothing to recover for our forensics group), raspberry pi, and some other random nerdy devices. Nothing useful though. However, we decided to look at the website again from a different perspective to learn more information about it. We used a tool called *nikto* which is a web scanner for website analysis. The result of nikto's scan is shown below:

```
nikto -h hax0rbase.com
- Nikto v2.1.6
-----
+ Target IP:      214.215.216.2
+ Target Hostname:hax0rbase.com
+ Target Port:    80
+ Start Time:     2016-04-30 21:31:00 (GMT-5)
-----
+ Server: Chuck Norris counted to infinity. Twice.
+ Server banner has changed from 'Chuck Norris counted to infinity. Twice.' to
'Chuck Norris CAN find the end of a circle.' which may suggest a WAF, load
balancer or proxy is in place
+ Cookie csrftoken created without the httponly flag
+ Cookie PHPSESSID created without the secure flag
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, inode:
205022981, size: 66, mtime: Fri Jun 7 18:03:21 2013
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /forums/: This might be interesting...
+ Entry 'logout/' in robots.txt returned a non-forbidden or redirect HTTP code
(302)
+ Entry 'admin/' in robots.txt returned a non-forbidden or redirect HTTP code
(302)
+ Entry 'do/not/look/here/' in robots.txt returned a non-forbidden or redirect
HTTP code (302)
+ Entry 'diagram/' in robots.txt returned a non-forbidden or redirect HTTP
code (301)
+ Entry 'fb/' in robots.txt returned a non-forbidden or redirect HTTP code
(302)
+ Entry 'home/' in robots.txt returned a non-forbidden or redirect HTTP code
(302)
+ Entry 'translate/' in robots.txt returned a non-forbidden or redirect HTTP
code (302)
+ Entry 'i/told/you/not/to/look/here' in robots.txt returned a non-forbidden
or redirect HTTP code (302)
+ Entry 'sources/' in robots.txt returned a non-forbidden or redirect HTTP
code (302)
+ Entry 'applications/' in robots.txt returned a non-forbidden or redirect
```

```

HTTP code (302)
+ Entry 'magic/dataset/be-good.txt' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ Entry 'seriously/' in robots.txt returned a non-forbidden or redirect HTTP
code (302)
+ Entry 'lets/dance/': This might be interesting...
+ Entry 'dumpofeverything.iso' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ Entry 'picka-picka-chu/' in robots.txt returned a non-forbidden or redirect
HTTP code (302)
+ Entry 'i/am/chuck/' in robots.txt returned a non-forbidden or redirect HTTP
code (302)
+ Server leaks inodes via ETags, header found with file /favicon.ico, fields:
0xW/527d4008 0x1536
+ Uncommon header 'x-instart-cache-id' found, with contents:
21:13262067370271160377
+ Server banner has changed from 'nginx' to 'instart/nginx' which may suggest
a WAF, load balancer or proxy is in place
+ The Content-Encoding header is set to "deflate" this may mean that the
server is vulnerable to the BREACH attack.
+ "robots.txt" contains 225 entries which should be manually viewed.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error
reading HTTP response
+ Scan terminated: 19 error(s) and 18 item(s) reported on remote host
+ End Time: 2016-04-30 21:33:07 (GMT-5) (127 seconds)
-----
+ 1 host(s) tested

```

Assuming that the names are meaningful, can you guess the name of the file that may shed more light on our investigation?

Does this scan indicate any type of attack that this server is vulnerable to? If so, which one is it?

### Activity 3: Who is who?

There is one more way the FBI asked us to check Hax0r's website. We have to use a whois service (like [www.whois.sc](http://www.whois.sc)) that allows us to look up registered users and related web domains in the Internet. In other words, if you want to know who registered a certain website domain name along with some other different information, go ahead and use one of those whois services. Anyways, `whois` dump of the information about `hax0rbase.com` is written below. Can you answer the following questions?

What is the email of the technical support?


How many full years has Hax0r had "hax0rbase.com" domain for?


Email [jsmith@hax0rbase.com](mailto:jsmith@hax0rbase.com)  
[mking@hax0rbase.com](mailto:mking@hax0rbase.com) is associated with ~6 domains

Registrant Org Hax0r Base is associated with ~2 other domains

Dates Created on 1992-09-09 - Expires on 2016-07-31 - Updated on 2015-05-22

IP Address 249.249.25.244 - 1 other site is hosted on this server

IP Location  - Tennessee - Granville - Hax0r Base

ASN  AS26756 TENNESSEE-NET - BellNorth.net Inc., US (registered Jun 01, 2003)

Whois History 310 records have been archived since 2003-01-15

IP History 1 change on 2 unique IP addresses over 11 years

Whois Server whois.educause.edu

Website

Website Title Hax0r Base | Irrational Thoughts

Response Code 200

SEO Score 99.9% (just pay \$9.99 today and win a flash drive full of computer viruses!)

Terms 505 (Unique: 350, Linked: 130)

Images 25 (Alt tags missing: 1)

Links 52 (Internal: 10, Outbound: 42)

Whois Record ( last updated on 2016-05-29 )  
Domain Name: HAX0RBASE.COM

Registrant:  
Anonymous Member of MagicBool Inc.  
Information Technology Service  
1010 N. Peachtree Street  
Cookeville, TN 38505  
UNITED STATES

Administrative Contact:  
Joanna Smith  
MagicBool Inc.  
Information Technology Services

1010 N. Peachtree Street  
Cookeville, TN 38505  
UNITED STATES  
(931) 123-4545  
[jsmith@hax0rbase.com](mailto:jsmith@hax0rbase.com)

Technical Contact:

Michele King  
MagicBool Inc.  
Information Technology Services  
1010 N. Peachtree Street  
Cookeville, TN 38505  
UNITED STATES  
(931) 124-4565  
[mking@hax0rbase.com](mailto:mking@hax0rbase.com)

Name Servers:

NS1.HAX0RBASE.COM	249.249.121.220
NS2.HAX0RBASE.COM	249.249.121.33

Domain record activated: 09-Sep-1992  
Domain record last updated: 22-May-2015  
Domain expires: 31-Jul-2016

#### **Activity 4: The end**

Great job! Before wrapping-up our mission, let us summarize what you have accomplished.

*Mission 001: Reconnaissance.*

FBI sought CEROC's expertise to track down notorious hacker Hax0r. You discovered that Hax0r, who is originally from Wisconsin, was visiting Cookeville, hometown of Tennessee Tech, to meet his accomplice, Lis@. While there, Hax0r compromised a computer in the Human Resources department to steal employee data.

*Mission 010: Forensics.*

Then he moved to Philadelphia, PA, and compromised a local federal banking system through his proxy server in Europe. The FBI located the set of machines that Hax0r used for compromising the bank and then, you helped them figure out the password to access one of them.

*Mission 011: Cryptography.*

Also, FBI used that computer to intercept a message that Hax0r had sent to Lis@. You decrypted the message and identified their plan to meet in Los Angeles.



*Mission 100: Reverse engineering.*

In order to get the exact location information, you had to reverse-engineer some code found on the computer that Hax0r compromised at Tennessee Tech and identified passwords to break into another server Hax0r owns. When the FBI broke into this server, they were able to pose as Hax0r and ask Lis@ for a meeting at a particular place.

*Mission 101: Steganography.*

They were able to capture both perpetrators once they showed up. Finally you assisted FBI in identifying Hax0r's offshore bank account information where Hax0r kept the stolen money.

*Mission 110: Web Reconnaissance.*

Later, after interrogating Lis@, the FBI located the exact location of Hax0r's home in Wisconsin. Once there, you helped them break into Hax0r's apartment by figuring out the password to the pin pad lock on the entrance. Afterwards, you performed some additional investigation on a website linked to Hax0r and identified the main brain behind these crimes, Joanna Smith. Hax0r and Llsa@ were just obeying instruction from this mysterious Joanna Smith.... now that's the villain of our next story!

## Appendix B - Songs

### Piano Man

By Billy Joel

It's nine o'clock on a Saturday  
The regular crowd shuffles in  
There's an old man sitting next to me  
Makin' love to his tonic and gin

He says, "Son, can you play me a memory  
I'm not really sure how it goes  
But it's sad and it's sweet and I knew it complete  
When I wore a younger man's clothes."

La la la, di da da  
La la, di da da da dum

Sing us a song, you're the piano man  
Sing us a song tonight  
Well, we're all in the mood for a melody  
And you've got us feelin' alright

Now John at the bar is a friend of mine  
He gets me my drinks for free  
And he's quick with a joke or to light up your smoke  
But there's someplace that he'd rather be  
He says, "Bill, I believe this is killing me."  
As the smile ran away from his face  
"Well I'm sure that I could be a movie star  
If I could get out of this place"

Oh, la la la, di da da  
La la, di da da da dum

Now Paul is a real estate novelist  
Who never had time for a wife  
And he's talkin' with Davy, who's still in the Navy  
And probably will be for life

And the waitress is practicing politics  
As the businessmen slowly get stoned  
Yes, they're sharing a drink they call loneliness  
But it's better than drinkin' alone

Sing us a song you're the piano man  
Sing us a song tonight  
Well we're all in the mood for a melody  
And you got us feeling alright

It's a pretty good crowd for a Saturday  
And the manager gives me a smile  
'Cause he knows that it's me they've been comin' to  
see

To forget about life for a while  
And the piano, it sounds like a carnival  
And the microphone smells like a beer  
And they sit at the bar and put bread in my jar  
And say, "Man, what are you doin' here?"

Oh, la la la, di da da  
La la, di da da da dum

Sing us a song you're the piano man  
Sing us a song tonight  
Well we're all in the mood for a melody  
And you got us feeling alright

## **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 mountain  
side 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 mountain  
side  
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  
Watch the flames burn on and on the mountain  
side  
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 mountains side)

## Hello

By Adele

Hello, it's me  
I was wondering if after all these years you'd like to meet  
To go over everything  
They say that time's supposed to heal ya  
But I ain't done much healing

Hello, can you hear me?  
I'm in California dreaming about who we used to be  
When we were younger and free  
I've forgotten how it felt before the world fell at our feet

There's such a difference between us  
And a million miles

Hello from the other side  
I must've called a thousand times  
To tell you I'm sorry  
For everything that I've done  
But when I call you never  
Seem to be home

Hello from the outside  
At least I can say that I've tried  
To tell you I'm sorry  
For breaking your heart  
But it don't matter, it clearly  
Doesn't tear you apart anymore

Hello, how are you?  
It's so typical of me to talk about myself, I'm sorry  
I hope that you're well  
Did you ever make it out of that town  
Where nothing ever happened?

It's no secret  
That the both of us  
Are running out of time

So hello from the other side (other side)  
I must've called a thousand times (thousand times)  
To tell you I'm sorry  
For everything that I've done  
But when I call you never  
Seem to be home

Hello from the outside (outside)  
At least I can say that I've tried (I've tried)  
To tell you I'm sorry  
For breaking your heart  
But it don't matter, it clearly  
Doesn't tear you apart anymore

Oh, anymore  
Oh, anymore  
Oh, anymore  
Anymore

Hello from the other side (other side)  
I must've called a thousand times (thousand times)  
To tell you I'm sorry  
For everything that I've done  
But when I call you never  
Seem to be home

Hello from the outside (outside)  
At least I can say that I've tried (I've tried)  
To tell you I'm sorry  
For breaking your heart  
But it don't matter, it clearly  
Doesn't tear you apart anymore