Lab 5: Ciphers and Crypto Fundamentals

Bill, Richard, Charley

Aim:

The aim of this lab is to give an introduction to ciphers, basic encoding/decoding techniques and frequency analysis, as to provide some fundamental understanding. Activities include decoding a range of ciphers and simple calculations.

Time to Complete:

4 hours (two supervised hours in the lab, and two additional unsupervised hours).

Activities:

- **Complete Lab 5:** Ciphers and Crypto Fundamentals

Learning activities:

At the end of this lab, you should understand:

- How to decode a range of ciphers.
- How to recognise certain encodings, such as base64, Hex, and Binary.
- How to write a bash script to crack PFX certificates.
- How to perform bitwise calculations.
- How to perform frequency analysis.

Reflective statements (end-of-exercise):

- Reflect on the real world use of these fundamental ciphers. Where can they be used? Are they secure on their own?

- See if you can write a more complete script than the one provided to crack passwords on PFX digital certificates. For example, why not have the script read through a text file containing a list of possible passwords?

Lab 5: Ciphers and Crypto Fundamentals

We will allocate you a Cloud instance in the forthcoming labs.

A Introduction

No	Description	Result
1	Go to: **http://asecuritysite.com/Challenges** Click on the "Start Challenge" button, and see if you can score over 30 points.	Your score:
2	Using: http://asecuritysite.com/Encryption/testprime Test for the following prime numbers:	91: [Yes] [No] 421: [Yes] [No] 1449: [Yes] [No]
3	Using: http://asecuritysite.com/Encryption/gcd Determine the GCD for the following:	88, 46: 105, 35:
4	Using: http://asecuritysite.com/coding/ascii Determine the Base 64 and Hex values for the following strings:	Hello: hello: HELLO:
5	Using: http://asecuritysite.com/coding/ascii Determine the following ASCII strings for these encoded formats:	bGxveWRz 6E6170696572 01000001 01101110 01101011 01101100 01100101 00110001 00110010 00110011
6	Using: http://asecuritysite.com/Coding/exor Determine the EX-OR of "hello" ex-ORed with the letter 't'	Hex: Base 64: Is the result printable in ASCII? [Yes][No]

7	What is the result of 53,431 mod 453?	
8	Generate a random number from: http://asecuritysite.com/Encryption/js01	How many hex characters does the result have?
9	Try and crack some certificates from: http://asecuritysite.com/Encryption/certcrack What are the passwords for 'bill09.pfx', 'bill18.pfx', and 'country04.pfx'?	bill09.pfx: bill18.pfx: country04.pfx:

10	We can also create a short **bash script** to try to crack the same certificates.
	
	Boot up your Kali VM, and download the following archive:
	https://dl.dropboxusercontent.com/u/40355863/certs.rar
	
	Select the **Places>Home Folder** menu, navigate to Downloads folder and Unpack the rar file, and use Right click>move to home to move the unpacked folder to the home directory (for the root user)
	
	Open a Terminal Window and you should see the **certs folder** (in /root)
	
	Use **ls certs/** to check the contents
	
	Copy **the fredpfx.pfx** file to the /root folder.
	
	Use openssl to try a password:
	`openssl pkcs12 -nokeys -in fredpfx.pfx -passin pass:charley`
	
	Now script a bash one-liner to try a range of passwords:
	(**Hint**: openssl returns "MAC verified OK" for a valid password):
	`for i in coconut mango apples oranges; do echo "[*] Trying password $i..."; openssl pkcs12 -nokeys -in fredpfx.pfx -passin pass:$i | grep "OK"; done`
		Did you manage to run the script? What password was correct for fredpfx.pfx?
		
		See if you can adapt this script to crack some of the other certificates contained in the archive you have downloaded.

B Frequency Analysis

Now see if you can crack the **five minute cracking challenge** for:

http://asecuritysite.com/challenges/scramb

C Character mapping

Complete the following table for each of the characters:

Char	Decimal	Binary	Hex	Oct	HTML
(Space)					
a					
}					
Ã					
ÿ					

D Test

1. Crack some Caesar codes at: http://asecuritysite.com/tests/tests?sortBy=caesar
2. Determine some hex conversions at: http://asecuritysite.com/tests/tests?sortBy=hex01
3. Determine some Base64 conversions: http://asecuritysite.com/tests/tests?sortBy=ascii01
4 Now complete the test at: http://asecuritysite.com/tests/tests?sortBy=crypto01

E Advanced Challenges

At Edinburgh Napier University, we enjoy cipher cracking competitions. In fact, the University came first in last year's national competition organised by the Cyber Challenge UK. See if you can understand the process or even crack some of the ciphers that were given out from:

http://www.asecuritysite.com/subjects/chapter56

http://www.asecuritysite.com/subjects/chapter49

Bash Scripting
Can you write a script to use one of Kali's built in wordlist files? (try `locate wordlist`)
And stop the script if it cracks the cert?