Lab 3.1: Google Hacks and Link Hiding

Aim:

To provide a foundation in understanding how Google can be used to search for open source documents

Time to complete: Up to 45 minutes.

Leaning Activities:

At the end of these activities, you should understand:

- How to search within certain sites.
- How to search for certain document types.
- How to analyse obfuscated links.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- A fraudster deletes a document from their Web site. What methods would you use to be able to get the document?

- Think about some of the ways that a fraudster would try to trick a user.

Lab 3.1: Google Hacks and Link Hiding

A Details

Aim: To provide a foundation in understanding how Google can be used to search for open source documents

B Viewing HTML

3.1.1 Within a browser you can normally right-click and viewing the HTML content. The following is a phishing attempt:

http://ac-uk-users.bravesites.com

Perform an initial investigation and also right clicking, and examine the HTML code, to determine:

IP address of the site:

What is the address of the registrant:

What happens when you put in a fake name and email address:

By finding the <form> and </form> tags, and find the page in which the details of the user are posted to and also the details that are posted.

Why are there so many `<p> </p>`

C Tracing Information

3.1.2 By trailing the Web, for Elvis Presley, could you determine some key information to reset his credit card:

His date of birth:

His last address:

His mother's maiden name:

The name of his first pet:

His favourite food:

His credit card number (from 1977):

C Google Hacks

3.1.3 For the following using Google hacks to find the information:

Using **filetype:xls site:napier.ac.uk** and **intitle:"2010+salary"**. Find the salary for a Grade 10 member for Napier staff in 2010:

Using **filetype:pdf** and **site:ac.uk** and **intitle:rfid+health**. Outline a paper which was publishing in the ac.uk domain with health and RFID in the title:

Using **filetype:pdf site:rbs.co.uk intitle:closure**. Find a PDF which allows a user to close their account. What is the name of this document:

Using **filetype:pdf site:billatnapier.com Mobile+Agents.** Find the PDF document. Now ask your tutor to delete the access file. Can you now access it?

Now select the cache option on the link. Can you now access it?

Using **filetype:java site:napier.ac.u**k. Find Java files on the Napier Web site. Pick off one of the files. Who is the author:

In using filetype:sql site:napier.ac.uk, the user cs181 comes up. Who is cs181?

Find Charlton Heights Database Sites and passwords.

3.1.4 We can also find sensitive information. Try the following and note what they return:

allintext:username filetype:log

allintext:email OR mail +*gmail.com filetype:txt

3.1.5 We can also return a certain domain from our search. Try the following and note the returns:

site:napier.ac.uk -site:www.napier.ac.uk promotions

site:napier.ac.uk promotions -site:staff.napier.ac.uk promotions

3.1.6 Investigate what the following Google hacks dO;

inurl:8080 -intext 8080 site:ac.uk

intitle:"Index of" passwords modified site:bbc.co.uk

filetype:inc intext:mysql_connect

D Link Obfuscation

The user can be confused with a hexadecimal address. For example www.bbc.co.uk is 212.58.246.95, so we can convert each of these digits to D4.3A.F6.5F.

3.1.7 A malicious link in a page has the following format (Figure 1 for conversion):

http://0x812a2601

Where does this link go:

Which is an obfuscated link for cisco.com:

Which is an obfuscated link for www.napier.ac.uk:

3.1.8 A certain site is blocked for its domain name and associated IP address, but an intruder creates on in the form:

http://0110.0243.04.0241/

Where does this link go:

Which is an obfuscated link in a similar form for apple.com:

Which is an obfuscated link in a similar form for bbc.co.uk:

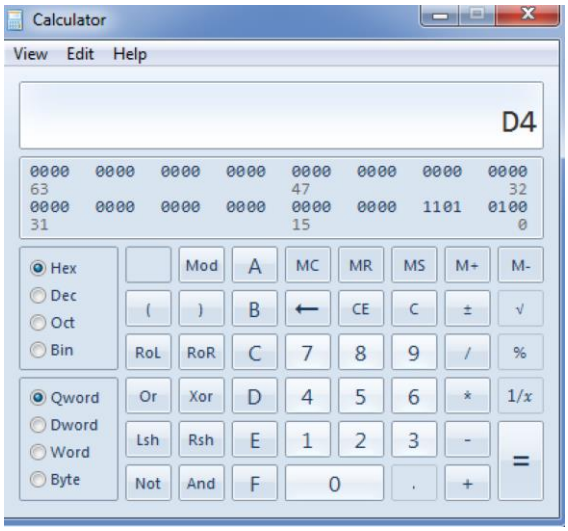

Figure 1: Hex to decimal