Lab 12: Web and Email Analysis

Aim:

To provide a foundation in understanding of the threats within Web pages and email messages.

Time to complete: Up to 45 minutes.

Activities:

- **Complete Lab 12**: Web and Email Analysis

Leaning Activities:

At the end of these activities, you should understand:

- How to analyse for key threats for Web pages.
- Define traces of evidence from Web accesses.
- How to analyse threats.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- What social engineering methods might a phisher use to gain information from a user?
- Which things would a phisher want to gain information on from a user?
- How might a phisher trick any spam filters?

Lab 12: Web and E-mail

1 Details

Aim: To provide a foundation in understanding how to analyse Web and email content.

2 Web Trace

L1.1 When you access Web sites there is a whole lot of information that a Web site can gain from the access. Go to the following site:

http://asecuritysite.com/IP/details

Determine the following:

Your IP address:

Is this address the same as the one which you are connected to:

What browser type has been identified. Is it correct:

What is the server address:

What is the name of the stored cookie:

What other information is present that could be useful for an investigation:

L1.2 Now start-up your Windows 2003 virtual machine. Once started, access it a few times from your Internet Explorer Web browser on your host with:

http://[Windows 2003 IP]

L1.3 **Next install Firefox,** access the page a few times, again, and now go the Windows 2003 machine, and you will find the logs either in:

C:\windows\system32\logfiles\W3SVC1

Or:

C:\inetpub\logs

Determine the following:

What details of your access has been logged:

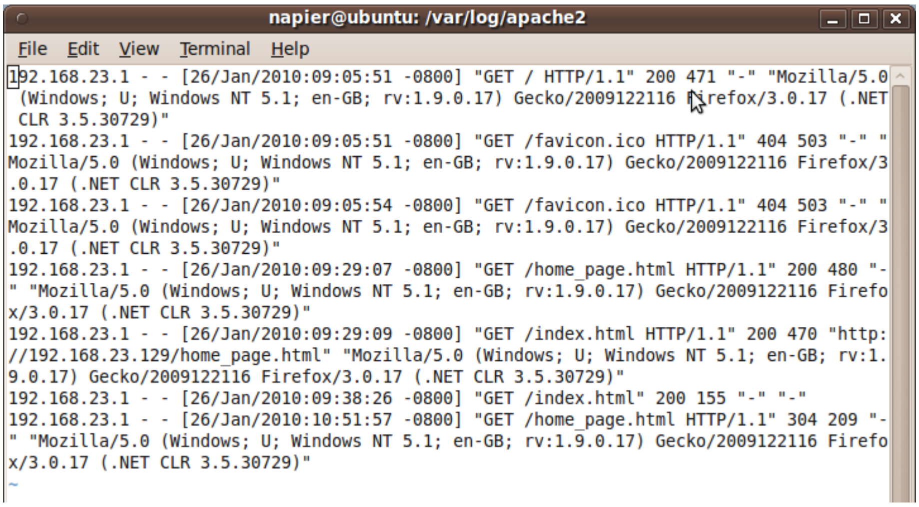
How often are these files created:

How can you determine the most up-to-date log:

L1.4 Now perform the same task for your UBUNTU virtual machine.

On UBUNTU, go to **`/var/log/apache2`**. What are the contents of the folder (Figure 1)?

How do these differ to the Windows 2003 log file:



```
192.168.23.1 - - [26/Jan/2010:09:05:51 -0800] "GET / HTTP/1.1" 200 471 "-" "Mozilla/5.0
 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.17) Gecko/2009122116 Firefox/3.0.17 (.NET
 CLR 3.5.30729)"
192.168.23.1 - - [26/Jan/2010:09:05:51 -0800] "GET /favicon.ico HTTP/1.1" 404 503 "-" "
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.17) Gecko/2009122116 Firefox/3
.0.17 (.NET CLR 3.5.30729)"
192.168.23.1 - - [26/Jan/2010:09:05:54 -0800] "GET /favicon.ico HTTP/1.1" 404 503 "-" "
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.17) Gecko/2009122116 Firefox/3
.0.17 (.NET CLR 3.5.30729)"
192.168.23.1 - - [26/Jan/2010:09:29:07 -0800] "GET /home_page.html HTTP/1.1" 200 480 "-
" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.17) Gecko/2009122116 Firefo
x/3.0.17 (.NET CLR 3.5.30729)"
192.168.23.1 - - [26/Jan/2010:09:29:09 -0800] "GET /index.html HTTP/1.1" 200 470 "http:
//192.168.23.129/home_page.html" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.
9.0.17) Gecko/2009122116 Firefox/3.0.17 (.NET CLR 3.5.30729)"
192.168.23.1 - - [26/Jan/2010:09:38:26 -0800] "GET /index.html" 200 155 "-" "-"
192.168.23.1 - - [26/Jan/2010:10:51:57 -0800] "GET /home_page.html HTTP/1.1" 304 209 "-
" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.17) Gecko/2009122116 Firefo
x/3.0.17 (.NET CLR 3.5.30729)"
~
```

Figure 1 - Apache Web Server Access Log

3 Analysing Email

L1.5 The following is a malicious email:

http://asecuritysite.com/email01.txt

What you determine the subject field and the content of the message:

What type of social engineering is used for this:

What happens when the user clicks on the link in the email:

Draw any graphic files that are used in the email:

Who is the email sender of the email:

Which email gateway(s) were used to send the email?

Is the sender a creditable for this email:

On what day/time was the email received:

Who is the receiver of the email:

Could you make a reasoned guest as to where the email originated from:

Can you view the HTML part of the email in a browser:

L1.6 Analyse the following email:

http://asecuritysite.com/email02.txt

Is it a malicious one:

What is the format of the message and what will happen if the user clicks on the link:

What are the key pieces of evidence that could be used to find the source of the email:

Where do you think the source of the email has originated from:

L1.7 Analyse the following email:

http://asecuritysite.com/email03.txt

Is it a malicious one:

What are the key elements which shows whether is it a valid or an invalid email:

4 A Few Risks

L1.8 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:

The name of a significant teacher

If Elvis had a password, what do you think it would be:

L1.9 View the following Web page, and then right-click to view the source:

http://asecuritysite.com/log/risk01.html

What is/are the malicious elements in this page:

L1.10 Analyse the following:

http://phoenxport.org/kil1.html

Alternative: http://asecuritysite.com/log/malware01.txt

What is/are the malicious elements in this page: