CAPSTONE REPORT

ICT30010
e-forensic fundamentals

Yashvi Chaudhary
103174005
Lab: Thu, 6:30PM

INTRODUCTION

In October, 2010, a warrant was executed on the residence of Imanuel Leet-Hacker, after the police received numerous reports of hacking activities tracing back to his IP address.

I have been asked to investigate these attacks and locate any relevant evidences. The police had created a forensic image (*ImaHacker.E01*) of the seized computer.
On *Friday, 20 May 2022*, around *10:00 AM*, I was provided with the download link to access that forensic image along with which, the Police also provided me with 2 exhibits that they had obtained:

a) Exhibit 1 (Exhibit1.jpg): Screenshot of the Hackable's webserver after compromise
b) Exhibit 2 (Exhibit2.jpg): Image placed on "Somepoor Victim's Facebook page

My colleague Troy, who had reviewed the forensic image emailed me with the "*Timescanner Super Timeline*" (detailed timeline generated by him) which contained the operating system artefacts and internet history.

ALLEGED ATTACKS

The following are the attacks to be investigated:

- Hacking of the company "Hackable" (hackable.com.au) on 4th May, 2010
- Similar website attack on 4th March, 2009, at 2:22AM.
- Unauthorised access of the Facebook account of *Somepoor Victim* on 6th August, 2010
- Involvement of a collaborator who is believed to use a website named *hidemyass.com* as email dropbox

In this report, I have carefully documented the steps taken while conducting this forensic investigation on my SIFT Workstation and collected evidences relevant to each alleged attack. I concluded my investigation on 27 May 2022.
The forensic image provided was "*ImaHacker.E01*" which is a compressed Expert Witness Format disk image (EWF/ EnCase format or E01).

First, I checked the information contained in the file other that the disk image usinf ewf tool (ewfinfo) and found:

Sector size(bytes per sector) of the image	Media size (the size of the disk)	Acquisition Date	System Date	Operating System Used
512 bytes	20 Gigabytes	Thu May 26 12:58:54 2011	Thu May 26 12:58:54 2011	Windows 7

Then I verified the hash contained within the E01 file using the *ewf* tool (ewfverify) and it was successful.

Then, I identified the partitions of the disk in order to see what areas of the disk have been allocated for use (using mmls command line tool).

Partition Type	Start Sector	End Sector	Total Sector	Total Size
NTFS	63	0041913584	0041913522	20465.58 MB

MOUNTING THE PARTITION

Then I mounted the partition contained within the raw disk image in the E01 file in the directory: */mnt/windows_mount* so that it is easily accessible from GUI and in read only manner so that we do not override any information on the disk while performing our investigation.

Then I viewed the list of all the files in that directory to ensure that the partition was mounted successfully.

EXAMINING THE REGISTRY SETTINGS

Then I examined the Windows Registry settings using the *RegRipper* tool (rip.pl command - extracts pre-defined registry keys and generates a report) to find and verify that I have the correct time zone.
The current Standard Time Zone was: *AUS Eastern Standard Time*

EXTRACTING THE EMAILS

Since, the alleged attacks involve the use of emails, I installed undbx-0.21 in order to process the databases considering that the suspect might be using Outlook Express, as suggested by my colleague Troy.

So, I used command line tools to search for any files named *.pst or *.dbx (as Microsoft Outlook uses “PST” files and Outlook Express uses “DBX” files) I found ***8 outlook express databases*** in the following location:

./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/

Then I used undbx tool to extract the contents and stored those emails in a new folder at a different location in my workstation. Then I located those emails at via GUI and opened and examined them one by one.

HACKABLE ATTACK

For investigating the 1st alleged attack on the company “*Hackable*” (hackable.com.au) I used the Autopsy Forensic Browser (Autopsy is a Graphical interface where I created an autopsy case for the ImaHacker and the ImaHacker.E01 forensic image file)

I used the file analysis tab and the file search option to locate any files relating to the website “*hackable.com.au*”. So firstly, I searched for the website itself and found the following entry for which I generated the Autopsy ASCII report and examined it:

File Name	Last Accessed	Last Changed	Created	Path
server.hackable.com.au.xml	2010-05-04 22:46:44 (AEST)	2010-05-04 22:46:44 (AEST)	2010-05-04 22:46:44 (AEST)	C:/Program Files/Nmap/server.hackable.com.au.xml

The report revealed that server.hackable.com.au was scanned, open ports were discovered and when the host was up, ports 21 and 80 were configured for FTP(file transfer protocol) and http service (for deploying web pages). Nmap tool was used to discover the open ports and further establish a connection. The *http_title* was *PAWNED!*

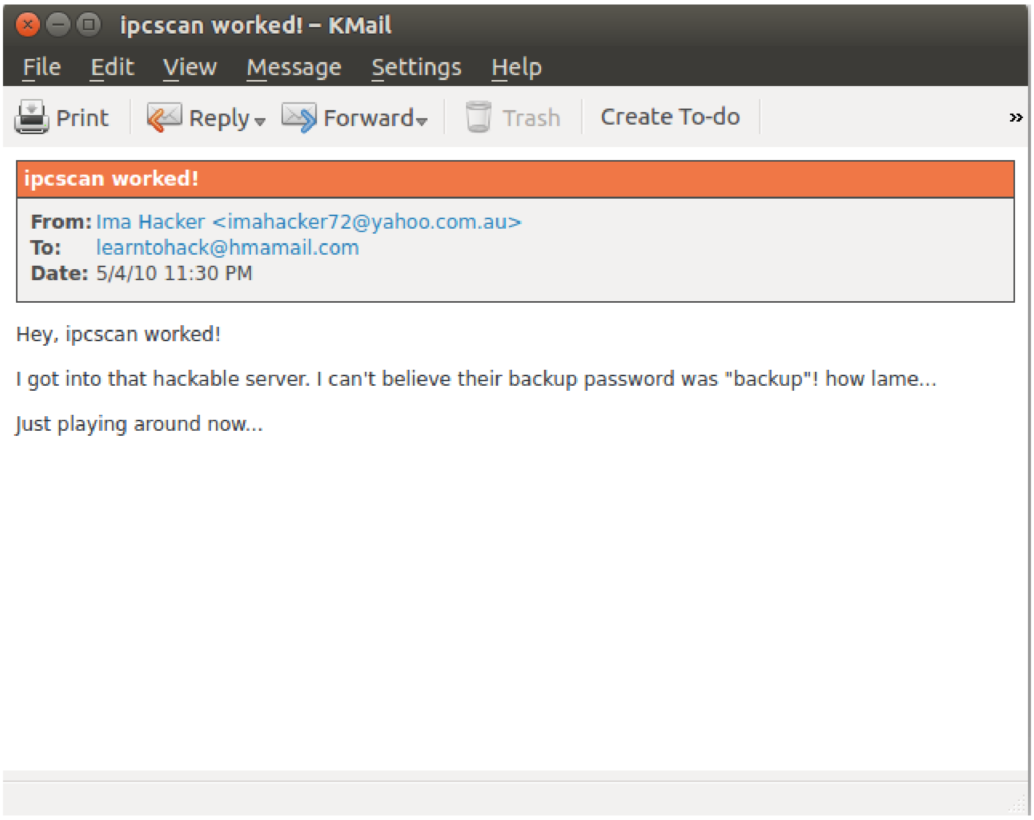
From this, I tried searching for "*server.hackable*" and found the following entries inside server.hackable directory:

File name	Last Accessed	Last Modified	Created	Location
PAWNED, again! .htm	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:36 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/
win2000.gif (inside PAWNED, again!_files directory)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /server.hackablePAWNED, again!_files/
users.txt	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/

Then I viewed these files via GUI using the obtained path and inferred the following:

i. **PAWNED, again!.htm** is exactly the same as the Exhibit 1 provided by the Police.
ii. **win2000.gif** is the gif that is part of the htm page which matched the exhibit 1 of the police
iii. **users.txt** was opened in LibreOfficeCalc and it contained the data related to the different users, their SSIDs, Last logon times, active status, etc.

While examining the emails, I found the following email in the "Sent Items" folder sent by Ima Hacker *imahacker72@yahoo.com.au* to *learntohack@hmamail.com*


ipcscan worked! – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do

ipcscan worked!

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 5/4/10 11:30 PM

Hey, ipcscan worked!

I got into that hackable server. I can't believe their backup password was "backup"! how lame...

Just playing around now...

Fig1. screenshot evidence of the extracted email present in Sent Items folder

In this email, he talks about successful ipscan and getting into the hackable server. Using the autopsy browser, I looked for "prefetch files" (prefetch files are temporary files that store the log of the applications run in the system folder) and found the following entry which was present in:

File Name	Last Accessed	Last Modified	Created	Directory
IPCSCAN-GUI.EXE-1C4F985C.pf	2010-05-04 23:24:27 (AEST)	2010-05-04 23:24:27 (AEST)	2010-05-04 23:24:27 (AEST)	C:/ /WINDOWS/ /Prefetch/

The accessed and modified date is just before he sent that email, the same date when the attack occurred. This means ***ipscan tool*** was actually run as stated by ImaHacker in his email.

Thus, these evidences support the alleged "Hackable" attack.

SECOND WEBSITE ATTACK

For investigating the 2nd alleged website attack which occurred on *4th March, 2009 at 2:22AM*, since Ima Hacker had stated that he was out shopping at a 24-hour convenience store and has no knowledge of the attack, I decided to view the timeline provided as it contains the operating system artefacts and internet history and we can infer what he was doing on his computer before and after the attack.

Examining the Super Timeline

In the timeline, I found that there was no entry between *2:20:18 AM* and *2:29:22 AM* which means that he was not on his system during that time.

Before 2:22 AM, he was surfing the internet as cached files from various websites including *google, trulocal, facebook, traktr news, Microsoft*, etc can be observed including searching google maps for *Tottenham Cellars West Footscray* according to the cached files around the time 2:13:18AM *(line 1919, timeline.csv).*

From 2:29AM, some windows events occur and there are many cached files from numerous websites which means he was back using the system.

Verification via Filesystem Timeline

This was also verified by creating a *filesystem timeline* using the autopsy and viewing the timeline starting March 4, 2009, that there were no logs between *2:20:18 AM* and *2:29:22 AM.*

In conclusion, the timeline logs support the ImaHacker's claim and does not provide any strong evidence to support the alleged attack from his activities.

FACEBOOK ACCOUNT TAKEOVER

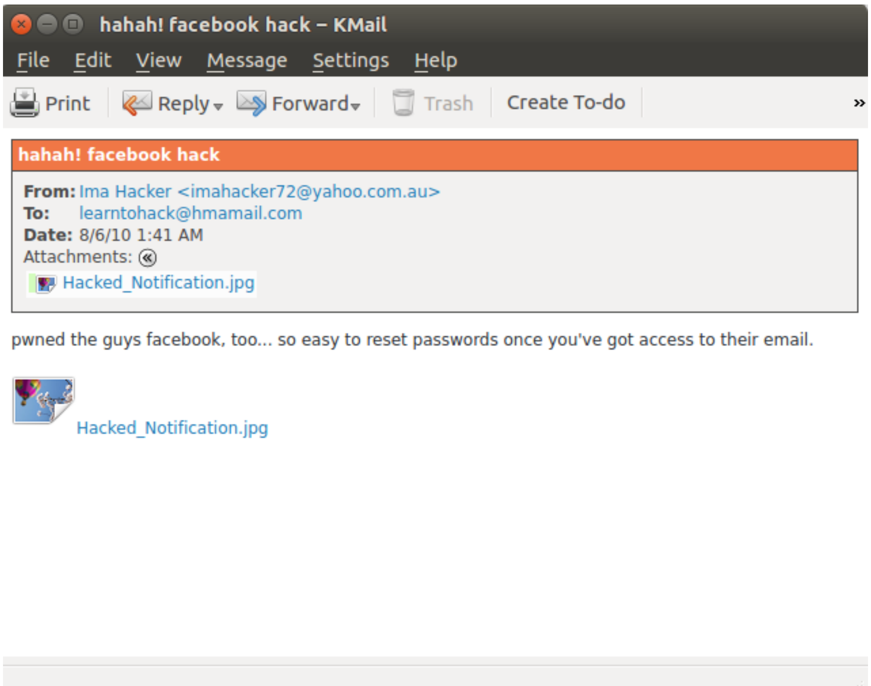
Moving on the investigating the alleged Facebook account takeover on *6th August, 2010* which was traced to a hotel in Brisbane. Somepoor Victim's Facebook account ID was provided – *100002369565636.*

Examining the email

While examining the extracted emails, the email in the folder "sent items" sent by Ima Hacker <imahacker72@yahoo.com.au> to learntohack@hmamail.com on *8/6/2010 at 1:41 AM.*

This contained these text *"pwned the guys facebook, too... so easy to reset passwords once you've =   got access to their email."*

It also contained a .jpg file named *Hacked_Notification.jpg* which is exactly the same as the Exhibit 2 provided by the police


hahah! facebook hack – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do »

hahah! facebook hack

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 8/6/10 1:41 AM
Attachments:
Hacked_Notification.jpg

pwned the guys facebook, too... so easy to reset passwords once you've got access to their email.

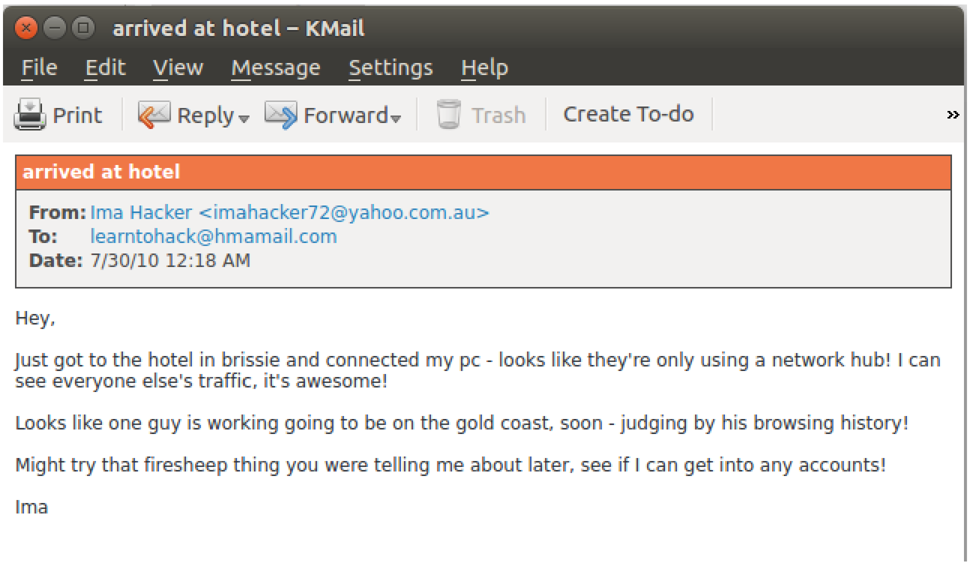
Hacked_Notification.jpg

Fig2. screenshot evidence of one of the extracted emails present in Sent Items folder

I located this image via GUI and it was present on the Desktop folder of Ima Hacker.

Examining the Prefetch Files

The following email talks about him observing everyone's traffic from their devices (connected to the network hub) ImaHacker's intention to try firesheep to get access to the accounts, hence I looked for any prefetch file for his attempt to run this tool.
Firesheep uses packet sniffers to hijack unencrypted session cookies across websites like Facebook.


arrived at hotel – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do

arrived at hotel

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 7/30/10 12:18 AM

Hey,

Just got to the hotel in brissie and connected my pc - looks like they're only using a network hub! I can see everyone else's traffic, it's awesome!

Looks like one guy is working going to be on the gold coast, soon - judging by his browsing history!

Might try that firesheep thing you were telling me about later, see if I can get into any accounts!

Ima

Fig3. screenshot evidence of one of the extracted emails present in Sent Items folder

Using the autopsy browser, I looked for "*prefetch files*" and found the following entry which was present in:

File Name	Last Accessed	Last Modified	Created	Directory
FIRESHEEP-BACKEND.EXE-3A5BA61B.pf	2010-08-06 01:07:25 (AEST)	2010-08-06 01:07:25 (AEST)	2010-08-06 00:58:48 (AEST)	C:/ /WINDOWS/ /Prefetch/

This proves that he ran the firesheep tool inorder to get into their accounts on the same day at around 1:07 AM, though it didn't work as stated by him in another email (fig4).

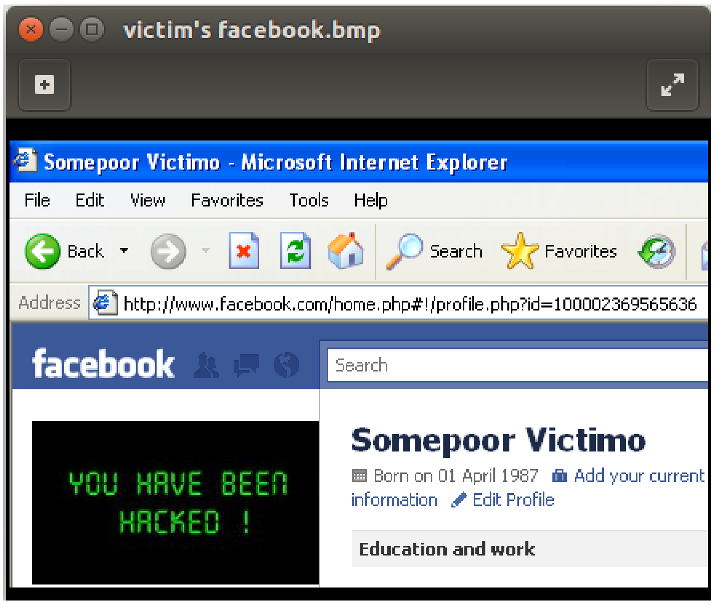
Examining Wireshark

My colleague had suggested that the hacker seemed to like Wireshark and therefore, might have captured some of his attacks in *.pcap* files. In order to examine those files, I used the Autoposy again, and browsed for any pcap files.

The search showed couple of .pcap files out of which "hotel dump including email and "***facebook.pcap***" and "***hotel dump.pcap***" belonged to some folder named Brisbane 2010 and hence, I examined them further.

File Name	Last Accessed	Last Modified	Created	Location
hotel dump including email and facebook.pcap	2010-10-14 02:44:40 (AEDT)	2010-10-14 02:44:42 (AEDT)	2010-08-06 01:24:08 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /Brisbane 2010/
hotel dump.pcap	2010-10-14 03:09:55 (AEDT)	2010-10-14 03:09:55 (AEDT)	2010-07-30 00:19:05 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /Brisbane 2010/

I viewed the Brisbane 2010 folder via GUI and found another file (bitmap image file) named “***victim’s facebook.bpm***”, a part of which matched the Exhibit 2 provided by the police.



Address http://www.facebook.com/home.php#!/profile.php?id=100002369565636

Somepoor Victimo

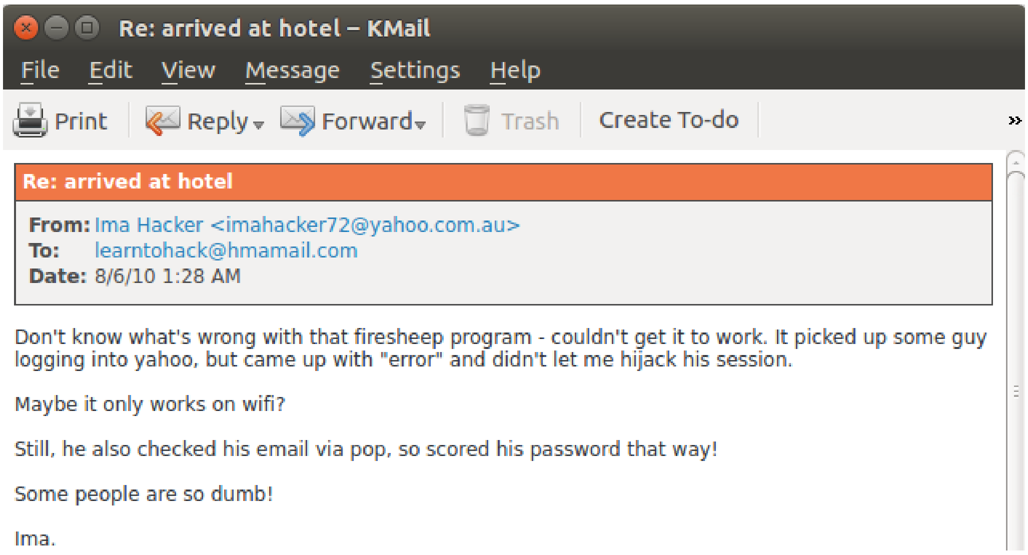
Born on 01 April 1987

Fig. victim’s facebook.bmp

File name	Last Accessed	Last Modified	Created	Location
victim's facebook.bmp	Thu, Oct 14 2010 02:44:32	Fri, Aug 6 2010 01:40:05	2010-08-06 01:40:05 (AEST)	C:/ /Documents and Settings/Ima Hacker/My Documents/Brisbane 2010

This bitmap image file also contained the Facebook ID in the address bar on top which matched the Facebook ID of Somepoor Victim as provided by him to the police.

Further examining the .pcap files discovered earlier, since in the email present in the "Sent Items" folder sent by Ima Hacker to learntohack@hmamail.com on *8/6/10* at *1:28AM* he mentioned checking the email via pop, I filtered the wireshark packets in "*hotel dump including email and facebook.pcap*" file using the word pop.


Re: arrived at hotel – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do

Re: arrived at hotel

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 8/6/10 1:28 AM

Don't know what's wrong with that firesheep program - couldn't get it to work. It picked up some guy logging into yahoo, but came up with "error" and didn't let me hijack his session.

Maybe it only works on wifi?

Still, he also checked his email via pop, so scored his password that way!

Some people are so dumb!

Ima.

Fig4. screenshot evidence of one of the extracted emails present in Sent Items folder

There were numerous packets using pop protocol captured by wireshark around *1:20 AM* on *August 6, 2010*. They revealed that there was a sign in into the account with id: *somepoorvictim@yahoo.com.au* and password *8WXyk5W8*

On carefully observing the Data fragments, I found one of the fragment having Arrival time: Aug6, 2010 01:20:14.06062900 AEST
containing the following text *" Hi Somepoor ,…. You recently asked to reset your Facebook password…" .*
Following this was another data fragment which contained text from Facebook team: "*If you did not request a new password let us know at:…"*

which seems to be an email from facebook sent as the password was being changed. This means that the hacker accessed the victim's email via pop and then used it to change the facebook password in order to hack that account.

Examining the Super Timeline

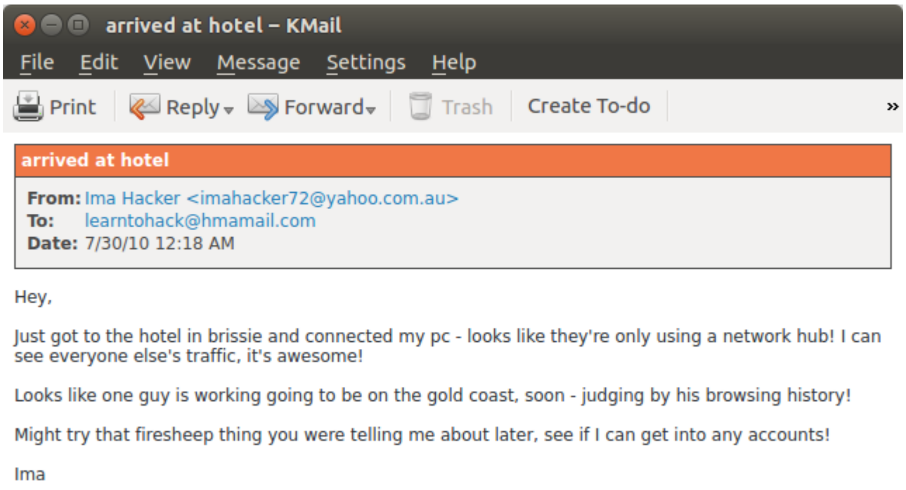
Further, I searched the super timeline using the given facebook ID for any cached files from Facebook. I found numerous Facebook cache entries including the entry at 1:37:58 AM for profile picture upload.It is the same as the exihibit 2 provided by the police. Before this cache entries of logging into Yahoo account can be seen followed by logging into the Facebook account.

These evidences support that Ima Hacker was behind this alleged attack.

COLLABORATOR

The collaborator is believed to use *hidemyass.com.au* as email dropbox, where friends/other hackers communicate with him. Observing the emails extracted earlier, Ima Hacker can be seen communicating with only one person with the email *learntohack@hmamail.com* , to whom he informs his every move and the attacks he performed. Hidemyass is the provider for *hmamail* that the collaborator uses.

The following are the email communications between Ima Hacker and the collaborator:


arrived at hotel – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do »

arrived at hotel

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 7/30/10 12:18 AM

Hey,

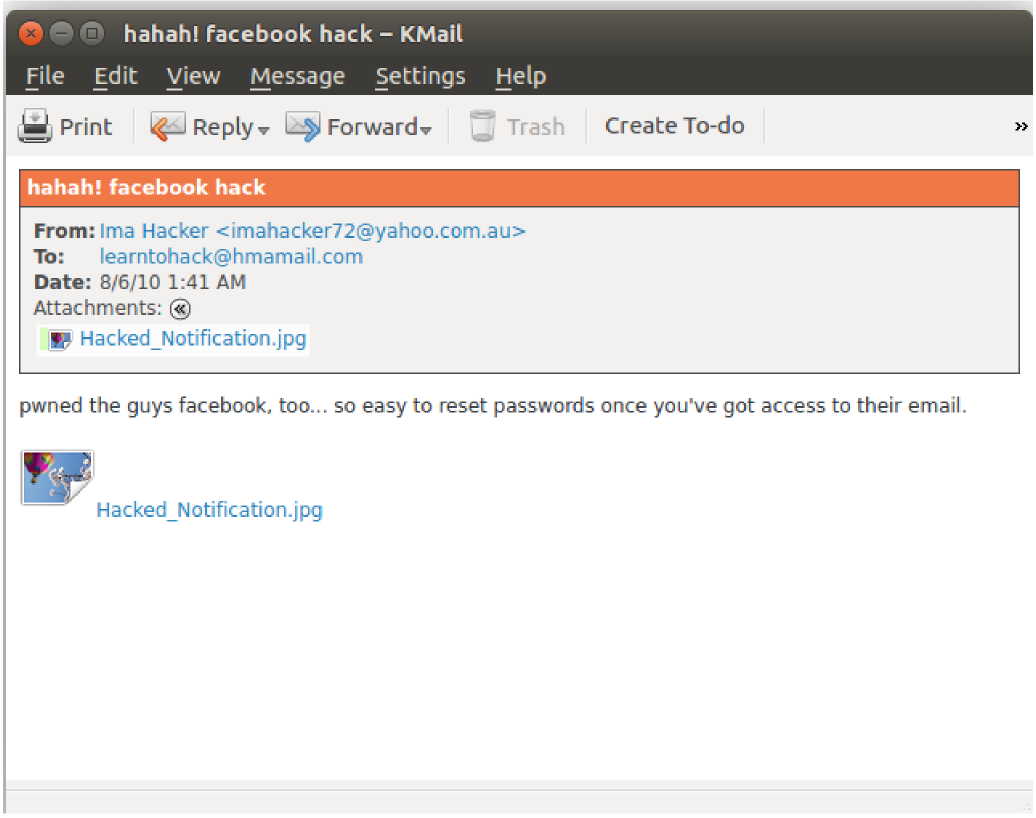
Just got to the hotel in brissie and connected my pc - looks like they're only using a network hub! I can see everyone else's traffic, it's awesome!

Looks like one guy is working going to be on the gold coast, soon - judging by his browsing history!

Might try that firesheep thing you were telling me about later, see if I can get into any accounts!

Ima

Fig. screenshot evidence of one of the extracted email present in Sent Items folder


hahah! facebook hack – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do

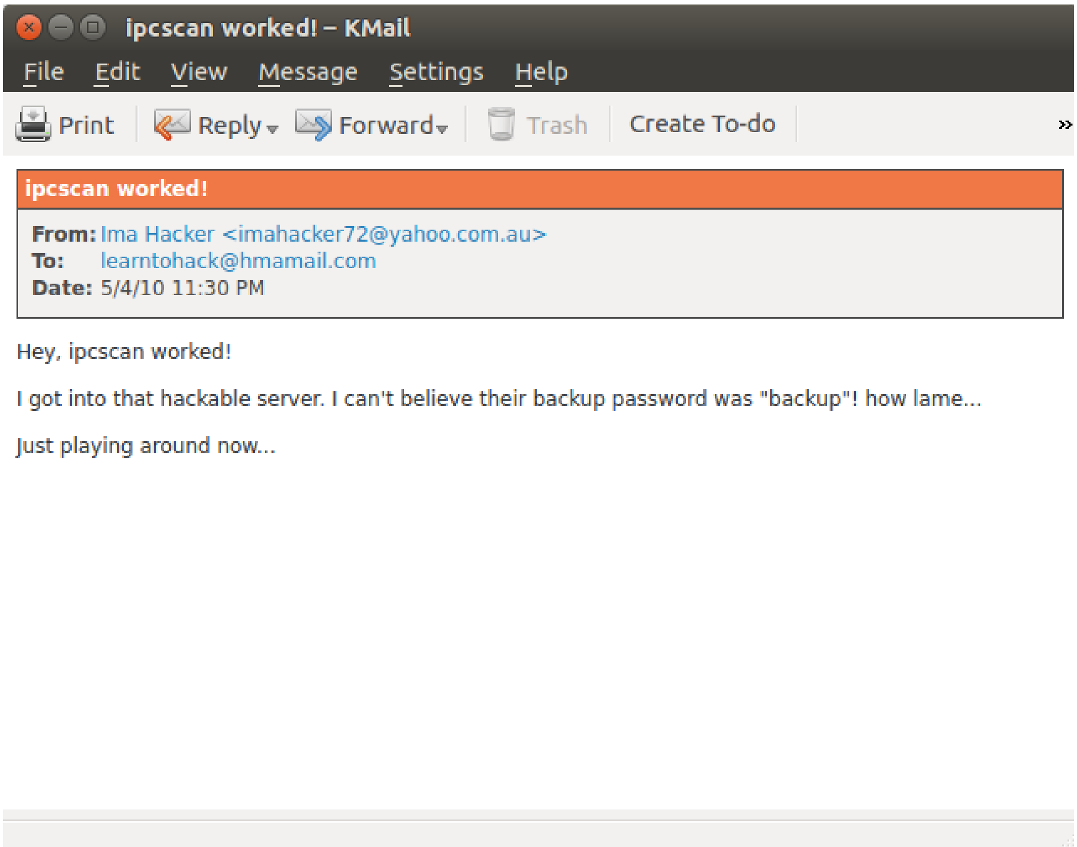
hahah! facebook hack

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 8/6/10 1:41 AM
Attachments:
Hacked_Notification.jpg

pwned the guys facebook, too... so easy to reset passwords once you've got access to their email.

Hacked_Notification.jpg

Fig. screenshot evidence of one of the extracted email present in Sent Items folder


ipcscan worked! – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do

ipcscan worked!

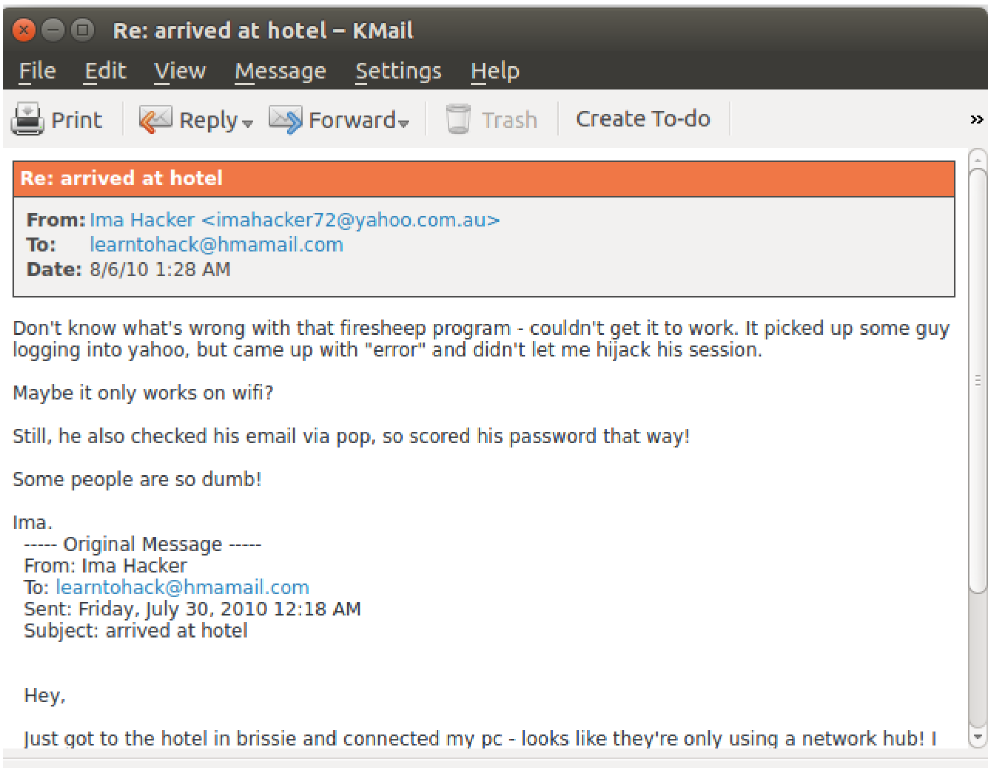
From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 5/4/10 11:30 PM

Hey, ipcscan worked!

I got into that hackable server. I can't believe their backup password was "backup"! how lame...

Just playing around now...

Fig. screenshot evidence of one of the extracted email present in Sent Items folder


Re: arrived at hotel – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do

Re: arrived at hotel

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 8/6/10 1:28 AM

Don't know what's wrong with that firesheep program - couldn't get it to work. It picked up some guy logging into yahoo, but came up with "error" and didn't let me hijack his session.

Maybe it only works on wifi?

Still, he also checked his email via pop, so scored his password that way!

Some people are so dumb!

Ima.
----- Original Message -----
From: Ima Hacker
To: learntohack@hmamail.com
Sent: Friday, July 30, 2010 12:18 AM
Subject: arrived at hotel

Hey,

Just got to the hotel in brissie and connected my pc - looks like they're only using a network hub! I

Fig. screenshot evidence of one of the extracted email present in Sent Items folder

I also examined the "*hotel dump.pcap*" file and found an IMF packet capture that had the info that it was an email sent by Ima Hacker with the subject arrived at hotel, which was sent to *learntohack@hmamail.com.au* as seen in the emails before.

Thus, these evidences support the presence of a collaborator and explain their communication method.

CONCLUSION

I concuded my investigation by verifying the hash of the provided image using ewf tool and there was a match, the verification was successful.

Evidences supporting and relevant to all the alleged attacks were found and documented in detail in this report except for the second attack on 4th March 2009 for which no supporting evidence could be found. The collaborator with whom ImaHacker was communicating the whole time was identified and the relevance of Hidemyass was also stated.