ICT30010: Final Capstone Lab

INTRODUCTION

In this lab, we will examine a forensic image taken of a computer that has been seized by Police in the continuing investigation of Imanuel Leet-Hacker.

RESOURCES AND LINKS

- SANS Investigative Forensic Toolkit (SIFT) Workstation
  https://computer-forensics.sans.org/community/downloads
- The Sleuth Kit
  http://www.sleuthkit.org
- RegRipper
  http://regripper.wordpress.com/regripper/
- Windows Registry Hives
  http://msdn.microsoft.com/en-us/library/ms724877%28v=vs.85%29.aspx
- Internet Explorer Index.dat URL Records
  http://www.forensicswiki.org/wiki/Internet_Explorer_History_File_Format
- UnDBX
  https://sourceforge.net/projects/undbx/

LAB OUTLINE

1. Background 2

Exhibit 1: Screenshot of Hackable's Webserver After Compromise 3

Exhibit 2: Image Placed on "Somepoor Victim"'s Facebook Page 3

2. Forensic Examination 4

3. Forensic Report 6

ICT30010: Final Capstone Lab

1. BACKGROUND

In October, 2010, a warrant was executed on the residence of Imanuel Leet-Hacker (aka Ima Hacker), after police received numerous reports of hacking activities tracing back to his IP address. The computer you'll be examining today is believed to be the computer he has used in the majority of his hacking activities.

The police have created a forensic image of the computer that was seized and have outsourced the forensic investigation to you to complete, you will be provided with a download link to access the forensic image for your investigation.

Along with the forensic image, Police have also provided you with two exhibits they have obtained that may be relevant to your investigation.

Your colleague Troy has reviewed the forensic image and has generated a detailed timeline of system events for you to utilise in your investigation in the form of a "Timescanner Super Timeline". The Super Timeline contains operating system artefacts and internet history that may be relevant to your investigation, this will be provided to you via email from your colleague.

The alleged hacking events are as follows:

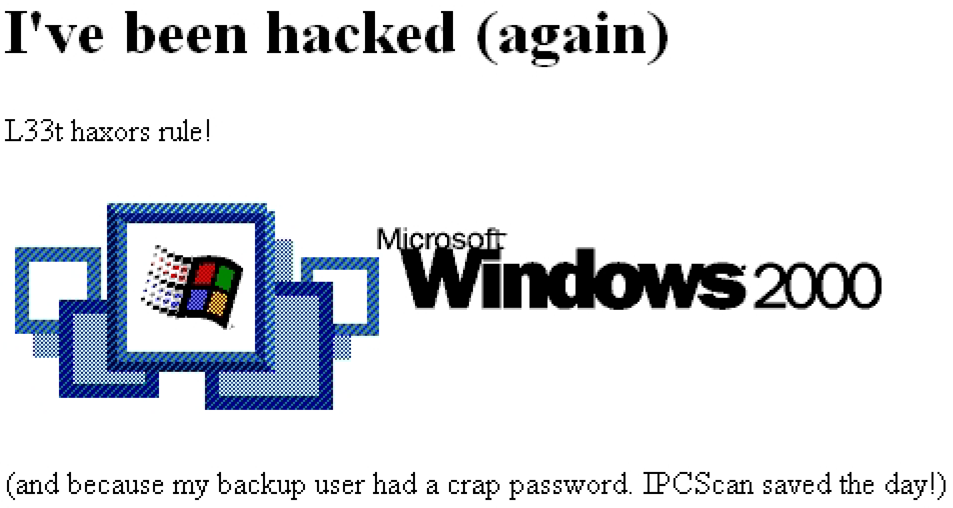
- The company "Hackable" (hackable.com.au) has provided logs to police which suggest their website was hacked on 4th May, 2010. The IP address has traced back to Ima Hacker. It is up to you to find additional evidence to support this charge.

- Another similar website attack occurred on 4th March, 2009 at 2:22am. Ima Hacker has stated that he was out shopping at a local 24-hour convenience store at the time, and has no knowledge of the attack. Can you locate evidence on his computer to support this claim? What was Ima Hacker doing on his computer just before and just after this attack?

- A person named Somepoor Victim (somepoorvictim@yahoo.com.au) has also approached police regarding the unauthorised access of their Facebook account (ID: 100002369565636) on 6th August, 2010. This has been traced to a Hotel in Brisbane, in which Ima Hacker was staying at the time. The hotel was unfortunately unable to provide details of which guest performed the attack. Thus, it is up to you to prove it was Ima Hacker.

- There has also been some suggestion that Ima Hacker may be involved with a collaborator. This collaborator is believed to use the website hidemyass.com as an email dropbox, where friends/other hackers can communicate with him. Locate the email address for Ima Hacker's collaborator, and any email communication you can find.

EXHIBIT 1: SCREENSHOT OF HACKABLE’S WEBSERVER AFTER COMPROMISE



I've been hacked (again)

L33t haxors rule!

(and because my backup user had a crap password. IPCScan saved the day!)

Figure 1. Hackable's Webserver Front Page

EXHIBIT 2: IMAGE PLACED ON “SOMEPOOR VICTIM”’S FACEBOOK PAGE

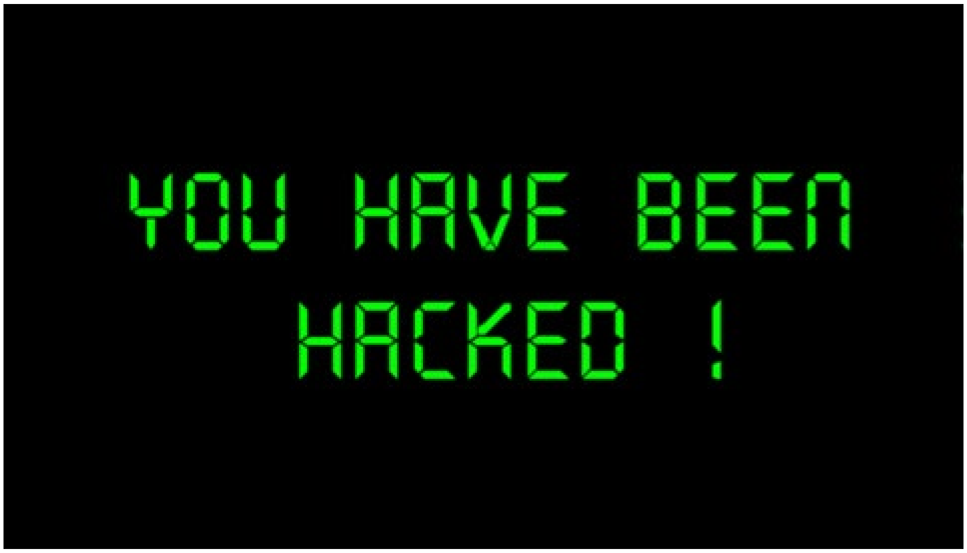


Figure 2. Image file uploaded to Somepoor Victim's Facebook

2. FORENSIC EXAMINATION

For this lab, you'll need:

1. SIFT Workstation
2. Disk image "ImaHacker.E01" – Downloaded from Canvas
3. Timeline of system events "timeline.csv" - Email (MD5: 9574ac771fdeeeb9a95d8dda5ed1749a)

In this lab, you'll be left on your own to locate items of relevance to the investigation. However, Troy has looked through the details provided by police, and has suggested the following:

1. Refer to previous lab sheets if you don't remember how to do something.
2. Since the image is an E01, you'll need to use the ewf tools to verify and open the image (ewfinfo, ewfverify, ewfmount and mmls (try "man *command*" or "*command* –h" if you're unsure of the specific settings to use). Also, don't forget to use sudo for mounting the ewf image!
3. Don't forget to check the registry settings using Regripper (rip.pl).
4. Autopsy (the GUI) should be helpful in locating items of interest without having to rely only on the command line.
5. When opening the provided timeline, you may need to import the file as a CSV. Additionally pay attention to the date/time format and change the formatting if dates/times do not make sense.
6. Some tools or the super timeline may report time in GMT (UTC 0) or UTC -8, so take this into account if you're seeing times that don't make sense, consider converting the times to local time if needed.
7. If the suspect is using Outlook Express (storing mail in DBX files), you may need to install undbx-0.21 to process the databases.

Linux Command Cheat Sheet:

ls	list files in the current directory
ls -al	list all files (including hidden) with additional details
cd *dir*	change directory to *dir*
cd	change to home
pwd	show current directory
mkdir *dir*	create a directory *dir*
rm *file*	delete *file*
rm -r *dir*	delete directory *dir*
cp *file1 file2*	copy *file1* to *file2*
mv *file1 file2*	rename or move *file1* to *file2*
more *file*	output the contents of *file*
head *file*	output the first 10 lines of file
tail *file*	output the last 10 lines of file
touch *file*	create or update the time on *file*
sudo *command*	run *command* as root
date	show the current date and time
man *cmd*	show the manual (help) for *cmd*
ping *host*	ping *host* and output results
ifconfig	show IP and MAC address info
df	show disk usage
fdisk -lu	list all disk partitions (run as root)
hdparm -I /dev/*sda*	show info about disk *sda*

8. Since Ima Hacker uses Yahoo! Mail, he may also check his email online. Keyword searches for the username part of his email address may be helpful in locating these fragments, if they exist. Come up with a list of keywords from the police report. You may also want to add to this list as you discover new things.

9. Your colleague Troy has provided a diagram which may help you navigate the Sleuth Kit commands:

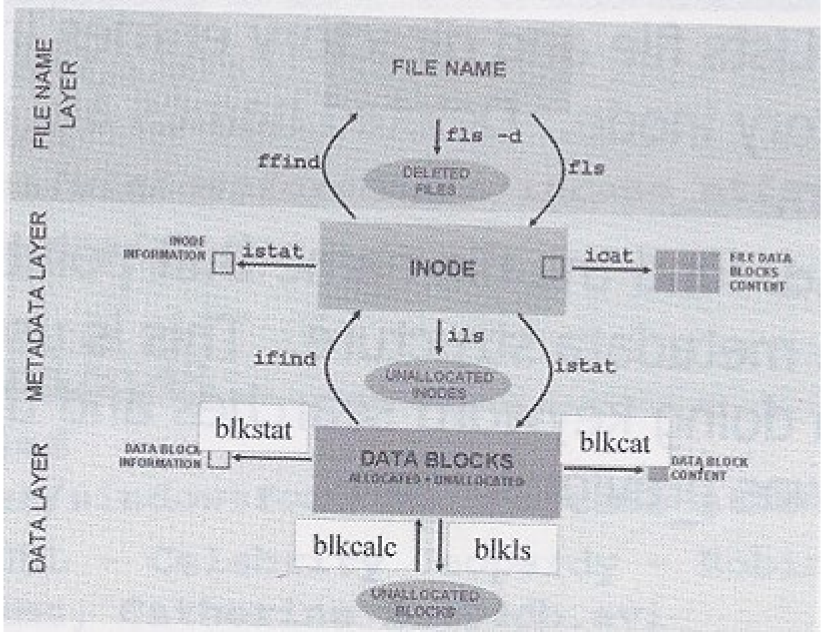


Figure 3. Sleuth Kit Commands

10. Prefetch files may be interesting – particularly if he’s using hacking tools. The prefetch files may tell you when the tools were run. If you see programs you’re not sure about, try googling to see what they are. Timescanner will include these files, as will the timeline analysis in Autopsy.

11. The hacker seems to like Wireshark. He may have captured some of his attacks in pcap files. These could definitely be worth examining.

12. The provided “super timeline” relates predominantly to event and log timelines, consider supplementing this by creating a filesystem timeline within autopsy.

13. You will need to do your own research to understand the evidence items and their relevance to the investigation.

14. Don’t forget to take lots of notes as you’re going, and export/save copies of any files that may contain evidence (e.g. emails, reports from timelining tools, graphic images or HTML files) to include in your report.

15. It may make sense to break the report into smaller logical sections for each scenario. It will be difficult to present the findings in chronological order as your investigation is likely to cross over scenarios.

ICT30010: Final Capstone Lab

3. FORENSIC REPORT

For this final Capstone Lab you need to write a report to the police outlining your findings including how you found the relevant evidence, the report should also include copies of any relevant evidently items.

The report may be used in court if the police believe there is enough evidence to prosecute Ima Hacker. It is important that you explain how the evidence located and is relevance to the investigation.

Your report should be factual, and include enough information for another forensic examiner to replicate your results, but does not need to detail exact settings and commands issued to obtain the information (in other words, "I used a forensic tool to determine the created date of the file" is better than "I ran the command 'istat –o 63 lab3.dd 123'"). The audience for your report will be police, lawyers, judges and other non-technical people.

It is important that opinions and other suppositions are *not* part of your report. Statements like "Ima Hacker saved the file at 12:03pm" is a conclusion not based entirely on the evidence you were provided. A better statement might be "the file had a created date of 12:03pm".

You will be marked on:

1. Your explanation of all the evidence received from the Police, how and when it was received and how you handled continuity (chain of custody) of the digital evidence. (1 *mark*)
2. Your explanation of the item received from your colleague Troy, how and when it was received and how you handled continuity (chain of custody) of the item. (1 mark)
3. Details of the partition contained within the image, and determination of the seized devices time zone (2*marks*)
4. Evidence and explanation for the alleged "Hackable" attack (*5 marks*)
5. Relevant evidence and the explanation of your findings that supports or refutes the hacker's alibi for the alleged "second" website attack (*3 marks*)
6. Evidence and explanation for the alleged Facebook account takeover (*5 marks*)
7. Explanation of the communication method between the hacker and the collaborator including an assessment regarding the use of hidemyass (*1 mark*)
8. The inclusion of relevant evidence from Timescanner super timeline in your findings (1 *mark*)
9. Your ability to stick to the facts, and explain your processes and findings in non-technical (but still accurate!) language (2*marks*) (.5 Reduction for each non-factual statement)
10. Overall presentation of your report (*1 mark*)

While the exact format of the report is up to you, you may consider breaking the report into sections related to each alleged incident. A simple way of presenting the report might be in dot point form, remembering the use of tables makes a report easy to read.

Evidence from one alleged hack may be relevant for other alleged hacks, consider how you will present this evidence in a way that makes sense for each marking criteria.