Homework 8 - Forensics Investigation Report

Steven Englehardt (ste), Steven Goldfeder (stevenag), Mihai Roman (mihair)

Overview

We have completed our investigation of the provided image and will summarize our findings in the following sections. Our exhaustive search has allowed us to answer the set of investigation questions from our higher-ups and provide some interpretation of what we believed happened. We will give a brief overview of our investigation before diving into the details. We discovered and reverse engineered the laptop's self-destruct method (via Puppy Linux). In order to directly access files without altering the state of the disk we mounted the file systems directly and explored them with tools ranging from off the shelf linux utilities to specialized forensics tools. We were able to find evidence that the suspect was researching nerf weapons and password cracking tools, and we have evidence of an accomplice. We found that the murder was indeed pre-meditated as the suspect has a highly-detailed depiction of the scene, and have found further evidence by examining a remote machine defaced by the suspect.

Investigation Procedure

Throughout our investigation we used Ubuntu as our host OS for to explore, mount, and virtualize the provided image. To facilitate our investigation, we used VirtualBox's clonehd tool to convert the VDI to a RAW image. After that, we were able to mount the file system and peruse through it from the command line. In order to avoid altering the filesystem while doing this, we were sure to use the mount options -ro,noload (read only and no load, as recommended by the mount man page). We used grep and find to look for strings, files, and folders of interests.

We also used The Sleuth Kit(TSK) and Autopsy, a GUI for The Sleuth Kit, to facilitate our investigation. We used the following tools from TSK/Autopsy:

- grouping the disk by File type
- finding deleted files
- searching the disk for keywords
- obtaining details about the image(e.g. which file system was being used in the different partitions

Additionally, we facilitated our search by using Google to find out where different log files are stored. This technique led us to the Firefox History, which proved to be very valuable to our investigation.

We used John the Ripper to break into passwords.zip(more details in Question 5). Once we

cracked the passwords, we were able to log into Nefarious's machine and eventually a remote server. To recover deleted files, we used extundelete and the data recovery features of TSK.

Investigation Questions

Throughout the investigation report we will reference external evidence files that we have also included in the evidence subdirectory. These files are all pulled from the suspect's machine or remote machines included in the investigation. The format we use for this is: <evidence: Question #.Item #>. If evidence is referenced outside of the question it was discovered in, it will retain the original number.

1. What specific behaviors make booting into the suspects machine and using it normally a bad idea?

The provided .vdi disk image was mounted using VirtualBox on an Ubuntu host machine. If the machine is allowed to boot normally it begins the startup procedure for Puppy Linux. The system gives an error message about a theft being detected and begins to delete the contents of the disk, this is explored further in the Investigation Appendix. On future reboots the machine fails to find a bootable device. If, instead of booting into Puppy Linux, we enter the grub boot menu by pressing ESC, we are able to boot into Ubuntu.

Booting the suspects device is a bad idea because we are unclear what alterations we are making to the device by doing so. Booting through the recovery menu fixes some disk errors, and once we are on the login screen any number of processes may be running that could alter the original state of the disk. Since we don't have a password to login anyway, we decided to use a fresh disk image and mount the filesystem directly.

2. What operating system and file system does the suspect use?

The suspect's computer has two distinct operating systems installed on two different partitions. On the boot partition, the suspect installed Puppy Linux 4.31 with an ext2 file system. This OS does not appear to be intended for use but is rather set up as a kill switch, as explained in the Investigation Appendix. The suspect also has Ubuntu 9.04, kernel 2.6.28 installed with an ext3 file system. This can be confirmed by the grub boot menu (also stored on the ext3 partition) and by inspecting the OS files directly. This appears to be the primary system used by the suspect and is the source of most of our evidence. As such all directory paths given for evidence is assumed to be located on the Ubuntu partition unless otherwise noted. Additionally, the suspect has a swap partition used by Ubuntu.

The filesystem was determined by running Autopsy/The Sleuth Kit(TSK) and looking at the "Image Details".

3. *What is the username of the account typically used by the suspect?*

The suspect typically uses the username nefarious. We saw as his home folder in Ubuntu and were able to log into the OS using the password 'supersecret' (the recovery of which is discussed in Question 5). This is further confirmed in IRC chat logs located in '/home/nefarious/irclogs/freenode/' and through the XChat IRC program(which we accessed when we logged onto Nefarious's machine).

4. *Do you have any evidence that the suspect had an accomplice who was physically present on the night of the crime?*

We found IRC logs located on the ext3 partition, under /home/nefarious/irclogs/freenode/#planning.log <evidence: 4.1> that provide evidence of an accomplice on the night of the crime. They speak about the murder taking place at 3:15 am near a "Dow" building and imply that accomplice is a getaway driver.

It is worth noting that both connect from the host 'swolchokhost.eecs.umich.edu', and the accomplice uses that id as his login. This handle seems to correspond to a handle used by http://scott.wolchok.org/ (on github: https://github.com/swolchok), a former PhD student at UMass working under Alex Halderman. We recommend bringing him in for questioning.

5. *Were there any suspicious-looking encrypted files on the machine?*

We found a passworded zip file located at /home/nefarious/passwords.zip <evidence: 5.1>. The file was password protected using WinZip 2.0 (pkzip) encryption. We used a combination of John the Ripper and AccentZPR (to provide CUDA acceleration), bruteforcing ^[a-z0-9]*$ up to length 9. We did not manage to properly configure John for a dictionary attack -- we suspect cracking would have taken much less time. With this setup, we were able to recover the password overnight, and extract the contents, 5 txt files <evidence: 5.2 - 5.6>. The contents are summarized here:

- password is: "soelite"
- contents:
    - password1.txt: "enigma"
    - password2.txt: "love"
    - password3.txt: "supersecret"
    - password4.txt: "KERMIT"
    - password5.txt: "eeMeisei700x"

The password "supersecret" turned out to be the password to log on to Nefarious's machine, and the password "eeMeisei700x" was the password for the remote server that we accessed (more on the remote server in Questions 8-12).

(It should be noted that after we cracked the password, we also found that the contents of the 5 password files were in <evidence: 7.4>.)

6. *What evidence do you have that the suspect owned or was researching weapons of the kind involved in the murder? Please attach the specific evidence and a brief explanation.*

We found lots of evidence in which the suspect was searching for nerf guns and watching a video about how to modify nerf guns to make it more powerful. Below is a summary of the evidence we found with references to the included supporting documents:

- We recovered the firefox history which was in /3/home/nefarious/.mozilla/firefox/4vda6zgy.default/places.sqlite. <evidence 6.1> The database was corrupted, and when viewed in an sqlite database browser, much of the information within it did not show up. However, when we examined the contents of the files, we found many interesting and incriminating links about nerf guns. The following sites were all in the file indicating that they were visited by the suspect:

Browsing Hasbro's website for Nerf	http://www.hasbro.com/nerf/en-us/
Searching Google for "nerf guns"	http://www.google.com/search?q=nerf+guns&ie=utf-8&oe=utf-8&aq=t&rls=com.ubuntu:en-US:unofficial&client=firefox-a8
Searching Google for "best nerf gun"	http://www.google.com/search?hl=en&client=firefox-a&rls=com.ubuntu:en-US:unofficial&hs=TmR&q=best+nerf+guns&start=10&sa=N
video on how to modify a nerf gun to give it more fire power	http://www.metacafe.com/watch/766831/easy_nerf_gun_hack/
amazon search for nerf guns	http://www.amazon.com/s/ref=nb_ss?url=search-alias%3Daps&field-keywords=nerf+guns&x=0&y=0
Viewed this specific nerf gun on amazon	http://www.amazon.com/Stuff-Blasters-Motorized-Tommy-Blaster/dp/B000F5YYMU/ref=sr_1_23?ie=UTF8&s=toys-and-games&qid=1259033274&sr=8-23xW
Link is not active or corrupted, but url shows intent of searching for nerf guns	http://www.amazon.com/BuzzBee-Stuff-Blasters-Double-Blaster/dp/B000I
eHow page on choosing the best Nerf gun to	http://www.ehow.com/how_4765156_choose-

win a fight	nerf-gun.html
ebay shopping for nerf guns	http://shop.ebay.com/?_from=R40&_trksid=p3907.m38.l1313&_nkw=nerf+gun&_sacat=See-All-Categories
wiki.Answers.com question/answer about best Nerf gun	http://wiki.answers.com/Q/What_are_best_nerf_guns_to_get
evidence adding an item on amazon to shopping cart. While we don't know what the item was, the only item that we could find browsing history for on amazon was nerf guns	http://www.amazon.com/gp/product/handle-buy-box/ref=dp_start-bbf_1_glance
Doubleclick url. Look at the keywords. They include: **NERF, Toys, Guns, Hack, Mod, Modify, Simple, Easy, Foam, Darts, Shoot, Firepower, Controversial, Weapons,** and **Hacking.**	http://ad.doubleclick.net/adi/mc.watch.f1;age=;gen=;leid=899;dcopt=ist;ord=1259033226;env=prod;campaign=;item=766831;submitter=;cat=how_to;channel=;dcZone=;num=0;kw=NERF;kw=Toys;kw=Guns;kw=Hacks;kw=Mod;kw=Modify;kw=Simple;kw=Easy;kw=Foam;kw=Darts;kw=Air;kw=Shoot;kw=Firepower;kw=Cats;kw=Otto;kw=0prend0107;kw=0prend0107;kw=Controversial;kw=Weapons;kw=Hacking;kw=Tricks;kw=Metacafe;kw=disambiguation;kw=mcPR;kw=ProducerRewardsApproved;pg=;wikified;dur=01:27;dc_ref=http://www.google.com/search?hl=en&client=firefox-a&rls=com.ubuntu:en-US:unofficial&hs=TmR&q=best+nerf+guns&start=10&sa=N;sz=300x250;tile=1;pos=1
Popular Mechanics article on the "Most Powerful Nerf Gun Ever". It is worth quoting the text of the article, which is violent in nature: Like plenty of other toy guns, the Nerf N-Strike Vulcan EBF-25 Blaster ($40, nerf.com) has a pneumatic pump that's used to fire off single rounds. But six D batteries turn the hybrid Blaster into a foam-shooting tommy gun—feeding a 25-dart belt through a fully automatic chamber at more than two shots per second. The result: the fastest, most powerful Nerf gun ever and the one best equipped for mowing down moving targets. To make sure you're the last man standing in a firefight, start by	http://www.popularmechanics.com/technology/upgrade/4263421.html (related: digg.com/odd_stuff/The_Most_Powerful_Nerf_Gun_Ever)

pinning down your prey with suppression fire. "You're not trying to hit them, just make them take cover," says Justice Smith, who fires a similar weapon at hapless competitors on TV's American Gladiators. "Then aim 1 to 2 ft. in front of them and pull the trigger the second they get up. You'll hit them on the first shot nine times out of 10."	

Firefox Form History (terms typed into the search bar) <evidence: 6.2>. The database is corrupted, but the search terms can be extracted by examining the file in a text editor such as vim. The terms of interest to this question are listed here:

- searchbar-history: best nerf guns
- searchbar-history: nerf

7. *Did the suspect try to delete any files before his arrest?*

Yes, there is evidence that the suspect deleted files before the disk was apprehended. The suspect's .bash_history <evidence: 7.1> (located /home/nefarious/.bash_history), shows the following deletions:

- rm /home/nefarious/.bash_history
- rm evil_plan.bmp

The original evil_plan.bmp <evidence: 7.2> was recovered from /home/nefarious/Documents/evil_plan.bmp by first mounting that partition of the disk image and using the tool extundelete. The two following commands will recover all files from that partition:

- sudo losetup -f <disk image>.raw -o <block_offset*512>
- sudo extundelete --restore-all /dev/loop0

It should be noted that we used a second copy of the raw image and did not mount it as readonly. This is due to the fact that extundelete warns that all files may not be recovered unless the image has its disk errors fixed with fsck, which we did.

evil_plan.bmp shows a depiction of the murder with what appears to be a nerf gun. We also found a thumbnail of this image <evidence: 7.3> located at: /home/nefarious/.thumbnails/normal/22d0c19de013e5009a681dd92e965fbd.png.

The original .bash_history file <evidence: 7.4> was recovered using keyword search in Autopsy/TSK. We searched for the string "**141.212.111.42"**. This was the original IP of the server that we had evidence that Nefarious logged in to(see later for more details on this server) . Searching for this address turned up the bash history in which Nefarious was attempting to access the server. This file contains a wealth of incriminating information, and is discussed further in Question 8.

8. *Is there anything else suspicious about the machine?*

There is evidence that the suspect was researching and using tools that allow him to crack passwords and penetration test over the network. The three main topics that we have found supporting evidence for are password lists, Metaspolit, and Hydra.

As in Question 6, the Firefox form history database <evidence: 6.2> and page history database <evidence: 6.1> both provide additional supporting evidence that the suspect was researching password lists and exploit tools

- Relevant terms from the form history database:
    - password list
    - searchbar-history: common passwords
    - searchbar-history: libssh-0.11
    - searchbar-history: metasploit ubuntu
    - searchbar-history: metasploit

- Relevant information from places.sqlite regarding password cracking:

Google search for “common passwords”	http://www.google.com/search?q=common+passwords&ie=utf-8&oe=utf-8&aq=t&rls=com
Google search for “password list”	http://www.google.com/search?hl=en&client=firefox-a&rls=com.ubuntu:en-US:unofficial&hs=sRN&q=password+list&start=10&
Description taken off the webpage “There has been three instances that I know of where a significant number of hacked account passwords have been publicly released. I have obtained the lists and made a thorough analysis of each of them, including the most common passwords and character frequencies. In total, there were 116782 passwords.”	http://blog.jimmyr.com/Password_analysis_of_databases_that_were_hacked_28_2009.php
A list of common passwords. **This list was saved on Nefarious’s Desktop in a file called “password.lst”**	http://www.openwall.com/passwords/wordlists/
Article about worm stealing iPhone users’ banking credentials	http://arstechnica.com/apple/news/2009/11/malicious-attacks-continue-against-jailbroken-iphone-users.ars
This link appears to be inactive, but the following texts appears alongside the link in	http://tech.yahoo.com/blog/hughes/11844

the file indicating the contents was a common password list “Most Common Passwords : Gina Hughes : Yahoo!” A google search also shows that it was also a password list. See here: http://www.xmarks.com/site/tech.yahoo.com/blogs/hughes/11844/most-common-passwords	
Webpage explaining how people tend to gravitate towards the same passwords. The page contains a list of “The Top 500 Worst Passwords of All Time”	http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

- Relevant information from places.sqlite regarding Metasploit:

Google search for “metasploit”	https://www.google.com/search?q=metasploit&ie=utf-8&oe=utf-8&aq=t&rls=com.ubuntu:en-US:unofficial&client=firefox-a
Google search for “metasploit ubuntu”	http://www.google.com/search?q=metasploit+ubuntu&ie=utf-8&oe=utf-8&aq=t&rls=com.ubuntu:en-US:unofficial&client=firefox-a
Instructions on how to install metasploit	http://www.howtoforge.com/installing-metasploit-3.0-on-ubuntu-7.10
Browsing Metasploit’s website	http://www.metasploit.com/framework/
Browsing Metasploit’s website. This link is inactive, but an internet search shows that it was the link to download the latest stable version of metasploit(see: http://fabienduchene.blogspot.com/2010/02/getting-metasploit-33-to-work-on-mac-os.html)	http://www.metasploit.com/releases/framework-3.3.tar.bz2
Browsing Metasploit’s website	http://www.metasploit.com/redmine/projects/framework/issues?set_filter=1&tracker_id=1

Hydra, “a fast and flexible network logon cracker” , is located in /home/nefarious/hydra-5.4-src and Metasploit, penetration testing software, is located in /home/nefarious/Desktop/msf3 along with a password list also on the desktop. Although just downloading these tools is not

incriminating, the recovered bash_history discussed in Question 7 <evidence: 7.4> shows that the suspect had been actively using Hydra to attack a remote server.

The following excerpts are particularly revealing:

- the suspect launching hydra with a wordlist in an attempt to crack the root password to 141.212.111.42
    - ssh 141.212.111.42
      ./hydra
      ./hydra -l root -P /usr/share/dict/words -f 141.212.111.42 ssh2
      ./hydra -l root -P /usr/share/dict/words -f 141.212.111.42 ssh2 -v
      ./hydra -l root -p test 141.212.111.42 ssh2
      ./hydra -l root -p test 141.212.111.42 ssh2 -v
      ./hydra -l root -P /usr/share/dict/words -f 141.212.111.42 ssh2 -v
- again after downloading it again
    - rm -rf hydra-5.4-src
      tar zxf hydra-5.4-src.tar.gz
      cd hydra-5.4-src/
      ./configure --help
      ./configure
      vi Makefile
      make
      ls ~/lib
      vi Makefile
      make
      ls
      sudo ifconfig eth0 141.212.111.41
      ./hydra -l root -P /usr/share/dict/words -f 141.212.111.42 ssh2 -v
      LD_LIBRARY_PATH=~/lib ./hydra -l root -P /usr/share/dict/words -f 141.212.111.42 ssh2 -v
- and finally, a root login attempt
    - 141.212.111.42 ssh2
      ssh 141.212.111.42
      ssh 141.212.111.42 -l root

ssh's known_hosts file <evidence: 8.1> (located in /home/nefarious/.ssh/known_hosts) also contains the RSA fingerprint for this IP, leading us to believe that the suspect did indeed make a login attempt to the server.

With this new evidence, our team was given the permission to access the remote server. The following four sections are a follow-up to that investigation.

9. *Who owns this machine, according to the files on it?*

To gain access to this server, we needed to try several passwords. We knew that the suspect had likely successfully cracked the root password (as shown in Question 8), so we decided to try the passwords we gathered from passwords.zip (as shown in Question 5). We were able to successfully connect as root using the password: 'eeMeisei700x'. From here, we explored the server a bit.

The remote server is owned by Dr. Academic Researcher. The server has the home directory 'academic'. We also found his name in what appears to be a defaced website, located in /var/www/index.html <evidence: 9.1>.

10. *What does its purpose appear to be?*

The purpose of this server is likely just to host a website. Running 'top' shows that there are several apache2 services running. In addition to this, an index.html page was found <evidence: 9.1>. Aside from this, there seems to be little on the server as the home folder of academic is pretty sparse.

11. *Was the suspect granted access to the machine, or was it compromised? If the suspect was granted access, when? If it was compromised, when and how was it compromised?*

We found evidence that the machine was compromised both on Nefarious's computer as well as on the server itself. On Nefarious's computer, in the recovered bash_history file <evidence: 7.4> there was ample evidence that Nefarious was running hydra on the root user's password (as examined in Question 8).

The remote machines' system logs for login attempts, /var/log/auth.log <evidence: 11.1>, shows that there were many failed login attempts from Nefarious' IP address. Included is a heavily abridged version:

Nov 24 23:25:05 debian sshd[2134]: Invalid user nefarious from 141.212.111.41
Nov 24 23:25:05 debian sshd[2134]: **Failed none for invalid user nefarious from 141.212.111.41** port 49903 ssh2
Nov 24 23:25:11 debian sshd[2137]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh r
…
Nov 24 23:38:53 debian sshd[2238]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=141.212.111.41 user=root
Nov 24 23:38:53 debian sshd[2224]: **Failed password for root from 141.212.111.41** port 41700 ssh2
…
Nov 25 09:45:08 debian sshd[6346]: Failed password for root from 141.212.111.41 port 48284

ssh2
Nov 25 09:45:08 debian sshd[6346]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=141.212.111.41 user=root
Nov 25 09:45:09 debian sshd[6368]: **Accepted password for root from 141.212.111.41** port 48299 ssh2

From Nov. 24th 23:25:11 to Nov. 25th, 9:45:08 there are continual failed connection attempts from the suspects computer, until a password is finally accepted. We believe this is the point when the suspect's tool correctly guesses the root password.

NOTE: We know 141.212.111.41 is Nefarious' IP address. He configures his connection with that IP in the recovered bash_history <evidence: 7.4> (specifically, the following line: *sudo ifconfig eth0 141.212.111.41*). Also, the first few login attempts give errors on the remote server about 'Invalid user nefarious from 141.212.111.41'. This is a common mistake, rising from the fact that ssh uses the local machines' current username when none is specified. Again, the recovered bash_history <evidence: 7.4> shows that Nefarious did indeed type 'ssh 141.212.111.42'.

12. *In either case, it appears as though the suspect has abused his access to the machine. How?*

The .bash_history of the root user <evidence: 12.1> gives some insight into what the suspect did while on the system (located in /root/.bash_history on the remote machine). Specifically, it shows that the user was editing the webpage: "*vi /var/www/index.html*" The new contents of index.html <evidence: 9.1> are:

<html><body><h1>Academic Researcher</h1>
Dr. Academic Researcher is a loser who knows nothing about computer security. <!--The duck flies at midnight! -->
</body></html>

The HTML comment appears to hint towards something happening at midnight on Nov. 26th (since it was posted sometime after the server was broken into around 9:30am Nov. 25th. This coincides with the date/time of the murder of Hapless Victim.

Investigation Appendix: Boot Trap/Self Destruct Mechanism Examination

Although we briefly touched on this in our investigation questions, we wanted to go into a bit more detail about the trap that the suspect has set on boot. If the suspect's computer is allowed to boot normally it will display a message saying that a system theft is detected and begin to write zeros to the disk. We will explain the sophistication of this mechanism.

The Puppy Linux OS was installed on the boot partition and the entire purpose of it seems to be to be to run this “theft detection” trap. We were able to examine the contents of the OS by mounting the raw disk image and finding Puppy Linux’s pupsave.2fs file, which contains all data the may be altered by someone using the OS. We could mount the partition with the command: *mount -t ext2 -o loop /locationof/your/pupfile.2fs /mnt/yourmountpoint*. Once mounted we were able to examine the bash history <evidence: A.1>, which shows edits to two boot files (rc.sysinit and rc.network), as well as two custom shell scripts (tweet_alarm.sh, get_external_ip.sh). The important parts of the files are highlighted here:

- tweet_alarm.sh <evidence: A.2>
    - uses twitter API to auto-post messages to the innocuous_news user
    - https://twitter.com/innocuous_news
        - has urls: http://68.40.49.30/love.html, http://141.212.54.121/love.html
- get_external_ip.sh <evidence: A.3>
    - gets an external site that returns the IP of the current machine
- /mnt/puppy/etc/rc.d/rc.sysinit <evidence: A.4>
    - causes the system to start deleting files
    - Lines 460 - 463:
        - /etc/rc.d/rc.services #run scripts in /etc/rc.d/init.d
        - echo -ne "\nTHEFT DETECTED, ENGAGING SECURITY SYSTEM" > /dev/console
        - dd if=/dev/zero of=/dev/sda
            - this line copies garbage data over disk...
        - #echo -e "\\033[62G\\033[1;33m[backgrounded]\\033[0;39m" >/dev/console #column 62, yellow.
- /mnt/puppy/etc/rc.d/rc.network <evidence: A.5>
    - runs tweet_alarm.sh if it finds a network
    - Lines 650-652:
        - if ["$GOT_ONE" = "yes"]; then
        - /tweet_alarm.sh
        - exit

During a normal boot, rc.sysinit will call rc.network. If a network is found, rc.network runs tweet_alarm.sh, which grabs the machine’s current IP using get_external_ip.sh and tweets it under the user innocuous_news. Then execution will return to rc.sysinit, which runs the code excerpt above. Specifically, notice the line: *dd if=/dev/zero of=/dev/sda*, which copies zeros to the disk. Note this will occur no matter what (there are not conditions surrounding the code excerpt) so the suspect really values his privacy. If the computer was to ever be turned on by an unsuspecting person this would occur and a potentially large amount of data would be lost.

Character

Aside from all of the evidence already listed, we also notices some interesting links that may point to consistencies in Nefarious character with that of a murderer. Firstly, we found that Nefarious had visited this page:http://news.bbc.co.uk/2/hi/health/8374519.stm. On that page is an article suggesting that it is healthier for one to let out their anger and not bottle it up. This could help us understand what Nefarious may have been thinking.

Additionally, we found that Nefarious had visitied this page: http://news.bbc.co.uk/2/hi/8373794.stm. This is an article about the effects of violent video games. While having visited either of these pages is certainly not a criminal offense, it does give us some insight into Nefarious's interest and may prove useful in the big picture analysis and may help a psychologist analyze Nefarious's mental state.

Conclusion

The collected evidence in this forensics investigation definitely provides a better understanding of the murder. Nefarious is a narcissistic (particularly in relation to cryptographic skills), potentially mentally-deranged suspect bent on murdering academics. Nefarious shows an above average care for his security, through his complicated boot trap and attempts to delete evidence from his machine. The lack of secure deletion, extremely poor choice of passwords, and the continual traces of his activity through bash_history logs shows that he actually is not very technically skilled and leads to jealousy as a potential motivator for the murder. We were even able to recover the contents of files he intended to encrypt for safety through a recovered bash history file. We recovered a detailed drawing of him enjoying, even laughing, at the future death of his victim. We have also found him completely overjoyed at the thought of his victim dying while speaking to his accomplice driver in IRC.

The suspect carefully researched nerf weapons and how to upgrade them, as well as tools to break into remote servers. We determined that he broke into Academic Researcher's server and defaced the researcher's homepage with an insult to his security skills. With what little remorse this suspect has shown, we hope that our investigation will help keep this deranged person, and his accomplice, off the streets.