CSCI-6637-01, Introduction to Cyber Forensic Science

**Forensics Final Challenge**

**Final Report**

December 16, 2022

TC

Table

Description automatically generated

Table of Contents

[**1    Executive Summary** 4](#_Toc122116811)

[**2    Apparatus** 6](#_Toc122116812)

[**3    Methodology** 8](#_Toc122116813)

[**3.1 Procedure** 8](#_Toc122116814)

[**Step 1:** 8](#_Toc122116815)

[**Step 2:** 8](#_Toc122116816)

[**Step 3:** 8](#_Toc122116817)

[**Step 4**: 8](#_Toc122116818)

[**Step 5**: 9](#_Toc122116819)

[**Step 6**: 9](#_Toc122116820)

[**Step 7**: 10](#_Toc122116821)

[**Step 8**: 10](#_Toc122116822)

[**Step 9:** 10](#_Toc122116823)

[**4    Problem solving and troubleshooting** 11](#_Toc122116824)

[**Problem 1** 11](#_Toc122116825)

[**Problem 2:** 11](#_Toc122116826)

[**Problem 3** 12](#_Toc122116827)

[**Problem 4** 12](#_Toc122116828)

[**Problem 5** 12](#_Toc122116829)

[**5    Conclusion and Final Remarks** 13](#_Toc122116830)

[**6    References** 14](#_Toc122116831)

[**Acquisition Computer 1** 15](#_Toc122116832)

[**Acquisition Computer 2** 16](#_Toc122116833)

[**Windows 10 VM** 17](#_Toc122116834)

[**Autopsy Screenshots Computer1/2 & VMU 18**](#_Toc122116835)

[Graphical user interface, text, application

Description automatically generated 18](#_Toc122116836)

[**Hashes Recovered from SAM** 21](#_Toc122116837)

[**Hash Cracking using hashcat/John The Ripper/ Mimikatz** 21](#_Toc122116838)

[**NMAP Output** 23](#_Toc122116839)

[**Suspicious Files** 23](#_Toc122116840)

[**Exfiltrated File Statistics** 24](#_Toc122116841)

[**Computer Specifications** 24](#_Toc122116842)

[**Password Table** 24](#_Toc122116843)

[**Web History** 24](#_Toc122116844)

[**Crazywickedawesome Credentials** 25](#_Toc122116845)

[**WireShark PCAP Analysis** 25](#_Toc122116846)

# **1    Executive Summary**

Due to the recent evidence recovered from the HiTek corporation after a data breach a forensic responder has successfully created 2 forensic images. Tasked with analyzing the findings from the previous forensic specialist we will begin to analyze the files and disk images present in the case. Following a series of forensic tools will be used to investigate Computer 1 and 2, tools such as autopsy, wire shark, and NetworkMiner will be used to assist. Our personal computer running investigative software tools will be known as Computer 3 for future reference in the report.

Analysis of computer 1 revealed Windows User accounts that had been stored in the System registry files, these accounts contained private data of account usernames and passwords. Account user profiles contained: Carlson, Jonathan, and tester. Virtual kali Linux machine was able to extract passwords for all three user accounts (See “APPENDIX SCREENSHOT #”). Strange activity with the user Johnathon never logging into the machine although the Carlson user was found in the Users folder (“C:\Users”). A kali Linux virtual machine was found on computer 1 with a suite of cyber forensics penetration tools which would give evidence to support computer 1 was used to gain access to the webmasters account on computer 2.

Analysis of computer 2 revealed the computer to be a webserver using the Apache web server using the name web-srv-02 for reference to the server. Further investigation showed this was HiTek’s website server which contained credentials of users. Using the list of users 3 were found and led to viewing the contents of the /var/www folder to find traces of exfiltration techniques. After further analysis the webmaster account was recovered and utilized to access the following files “Secrets.zip” and “BusinessStrategy.zip”. Analysis of the PCAP showed this user copying files off machine, file permissions change, and deleting the files. Leading to the conclusions there was a data exfiltration present and a breach in the network should be found.

# **2    Apparatus**

|  |  |  |
| --- | --- | --- |
| Hardware Used | | |
| Type Of Hardware | Version | Usage |
| Desktop-PC | Windows 10 Home Version 21H2 | Operating system that runs forensic analysis tools such as autopsy, wire shark, and NetworkMiner. Used to download associated case files. |
| Acer Laptop | Windows 10 Home Version 21H2 | Used to load and examine files in forensic lab |
| Iphone 13 | IOS 16 | Used to take pictures of the incriminating evidence |
|  |  |  |
| Software | | |
| Software Used | Version | Usage/Description |
| NetworkMiner | 2.7.3(2022-04-04) | Used in PCAP network log analysis to attain artifact data pointing to metadata log files |
| Medusa | Stable (1.4) | Used to decrypt passwords on computer 1 and 2 (Use in Kali Linux VM) |
| Kali Linux | Stable (2.4) | Operating system used in forensic analysis and required for password cracking and packet sniffing tools |
| Virtual Box | Stable (6.1.26) | Virtual machine tool to create a VM of kali linux, and to execute forensics operations in fail safe environment that is designed for forensic work |
| Pwdump8 | Stable (8.2) | Used to extract hashes from shadow files systems on ubuntu software |
| Hashcat | Stable (6.2.5) | Used to create a keyword list to be used in the medusa password cracker to crack computer 1 and 2 |
| John the Ripper jumbo | Stable (1.9.0-jumbo) | This is another tool that is used to crack the hashes just like hash cat, but john the ripper has the jumbo version which allows for many different ways to decrypt with netntlm, SunMD5 etc... |
| Wireshark | Stable (4.0.1) | Used to analyze TCP traffic, download "traffic files" for further analysis in a hex viewer tool. Allows for tracing of Ip routes and transfers of information, allowing to detect where the malware entered the system how, when, and from swhat Ip |
| Virus Total | Web Tool | Used in analysis of potentially malicious files to detect if they are a threat or not |

# **3    Methodology**

# **3.1 Procedure**

Using the following process to investigate the evidence found and verify the results and findings of the previous investigator

***Step by Step Breakdown:***

# **Step 1:**

* Load virtual box to ensure safety of parsing through data associated with the investigation. Utilize windows 10 professional to ensure computer integrity is not compromised.
* Create a forensic window 10 VM for forensic tools and other analysis software
* The virtual machine being used will be known as VMW10 (Virtual Machine Windows 10) using the IP address of 10.0.2.15

# **Step 2:**

* First load each of the forensic images associate with computer 1 and 2 into a disk image analyzer for further analysis. Using Windows Registry Viewer, Email Parser, and Regenerating the user directory structure were included methods used in autopsy.
* \*REMINDER\* Images contain vital metadata that can reveal geo location, user information, or time and date.

# **Step 3:**

* After parsing through the data and images generated by the previous investigator, we must look through these files and container folders to find any useful information pertaining to proving there was a data exfiltration. Operating system (OS) and IP addressing was obtained…
  + Computer 1 Breakdown:
    - OS: Windows 10 Professional (DESKTOP-A8BOTBH)
    - IP: 192.168.0.6
  + Computer 2 Breakdown:
    - OS: Ubuntu 12.04.4 Operating System (User: web-srv-02)
    - IP: 192.168.0.8

# **Step 4**:

* After analysis of Computers 1 & 2, autopsy was run on the windows 10 VM to recreate the active hard drives on computers 1 & 2 and to generate user log files which indicate programs ran and files opened and manipulated. This allowed for in depth analysis revealing an embedded Virtual Machine within the hard drive.
* Allowing for further analysis for alternate hypervisor 2 systems on the machine. The Ubuntu OS was found within the Users/tester/Documents folder on Computer 1. Attempts to activate the machine proved no effect due to the files being separated after loaded into autopsy (version 4.19.3)
* Resolving this error using VDiskManager, mismatched files were combined to create the virtual environment for inspection \*Note: This Ubuntu Virtual Machine will be called VMU (Virtual Machine Ubuntu)
* VMU IP: 192.168.0.7
* Code Used
  + Run the following command to ensure the file recontrsuction for the virtual machine
    - “vmware-vdiskmanager.exe – r “Virtual Disk.vmdk” -t 0 CombinedVM.vmdk”

# **Step 5**:

* Further investigation in autopsy revealed the search history of computer 1 and the VMU pointing towards suspicious activity within the network packets of the machines.
* Due to the VM being used on computer 1 we can trace the IP route taken by the VM through the host computers internet protocol address.
* Recovered Accounts:
  + Gmail: [csmith.hitek@gmail.com](mailto:csmith.hitek@gmail.com)
  + Browsing History: Further examination showed mounted hard disk drive (HDD) H: Within this drive passwords.txt was retrieved pointing to useful information for the case.
  + Within the VMU examination revealed software that could be used for penetration testing or unethical hacking. File found was Metasploit a known toil that penetration testers use, or a hacker could use to detect open vulnerabilities to be executed on.
  + Metasploit was found to be configured to have multiple execute tasks going at once.
  + A zip file named “a.zip” was found on this drive and contained only a’s indefinitely repeating this potentially could be labeled a ZIP bomb which leads the operating system or software attempting to open the file to crash due to the contents being more than the system/software can handle.
    - Mainly used against antivirus software’s to disable them to get a vulnerability against a target.

# **Step 6**:

* Further inspection revealed computer 1 to be a primary suspect for the illegal extraction of data. The registry files were then extracted from autopsy and imported to the security account manager (SAM) file. The Security account manager (SAM) files were then extracted from the registry of the windows computer.
* This revealed multiple system accounts and passwords after further inspection
  + System Accounts: Administrator, Guest, Default Account
  + Local Users Accounts: tester [1001], Carlson [1002], Johnathan [1003] (This account was never used which added to suspicion)
* Once user accounts were located the passwords would follow utilizing the tool hashcat/johntheripper the passwords could be cracked.
  + First the utilization of the command “pwdump8.exe -s SAM SYSTEM”, used for extraction of the MD5/SHA256 hashes
  + Pwdump8 is used due to its support of AES-128 encrypted hash which works with windows 10 v1607 and later.
* Hashcat/johntheripper tool would be next in line to crack the hashes extracted from the SAM registry file into a text document to be inspected (See appendix 7.?) For the above user Jonathon who had not logged in there was “no password”

# **Step 7**:

* To retrieve an ubuntu password the method approached used the user lookup /etc/passwd which led to the etc/shadow folder being used to locate the password hashes. Following it was loaded into hashcat to crack the user passwords.
* Recovered information:
  + VMU User account: tester
  + VMU User pass: tester

# **Step 8**:

* Once user passwords and files were recovered it was time to take a deeper look into the files and their metadata to gain any relevant data to point in the direction of time of attack, what day it happened, and if there was any premediated planning with malicious files and encoded and encrypted data.
* Computer 1:
  + Contained the file “crazywickedawesome.com” which was deemed suspicious as it was discovered through hidden text within image files.
  + Two files located on computer 1 “locked” and “network-architecture” located in “/users/Carson/Documents” and “/users/tester/documents”
  + Signs point to these recovered files being veracrypt files as it was used multiple times in the user logs (recovered from previous step)
* Virtual Machine Ubuntu (VMU)
  + “tester” user account had multiple files located within the /home/tester/Desktop path. These were identified to be nmap files
  + Nmap is a networker utility to detect open ports, open vulnerabilities, and many more features.

# **Step 9:**

* After acquiring the veracrypt files and confirming through the user logs that these files have been encrypted the decryption process starts. Multiple passwords were used to gain decryption access to the files
* The process discovered to be used was utilizing a method of encryption using the first 512 bits of a image file that needed to be transferred into the .vc format with the first 512 bits only being used.
* Once the container folder had been extracted it was on to figure out what was in it the following command was used “dd if=locked of=locked-out.vc bs=512 count=1”
* Hashcat and a word list was then used to crack the hashes located in the veracrypt files
  + Hashcat -a 0 -w 3 -m 13721 -0 locked-padd.txt locked-out.cv /usr/share/wordlists/rockyou.txt
  + After running this command, the locked file was now renamed to “qwerty” and network-architecture was renamed “12345678”
  + The cracked passwords were used to decrypt the veracrypt encrypted files to reveal the following
    - File: “locked”
    - Items Found: BTCFC.gif, BusinessStrategy.zip, passwords.txt, and secrets.zip.
    - File: “network-architecture”
    - Items Found: IP Addresses.txt

# **4    Problem solving and troubleshooting**

# **Problem 1**

*Description:*

* There was a problem with Computer1.E01 where it appeared that some data was missing.

**Solution 1**

*Process:*

* Verified by removing most of the ingestion presets, and instead analyzed for what was needed speeding up time and also increase chances of not crashing autopsy.

# **Problem 2:**

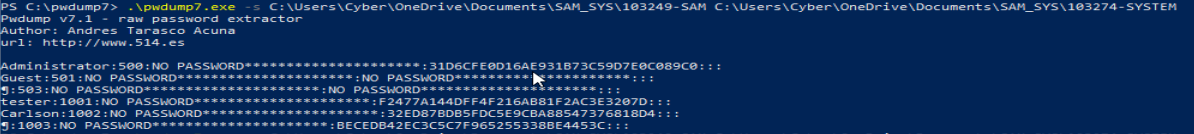
*Text

Description automatically generated*

*Description:*

* There was a error with the Hive Key when using pwdump7

**Solution 2:**

**

*Process:*

* This required extensive research on my part with learning the SAM and the SYSTEM registry file and where they are located how they are stored how the hive key is accessed and only after going back to autopsy and extracted the files again and then having it point to a different file path it worked

# **Problem 3**

*Description:*

* There was an issue with mounting the E01 files as a virtual machine.

**Solution 3**

*Process:*

* After looking through the autopsy scan of the files and data there was a few that were strewn about the computer and its software and not understanding how to put together these files to create the VM

*Alternative Solution:*

* Installing VDiskManager this was able to take the split files of the virtual machine found on autopsy and combine them in the correct order.

# **Problem 4**

*Description:*

* Problem cracking passwords for Secrets.zip and BusinessStrategy.zip. Error message indicated that the End of Content could not be found.

**Solution 4**

*Alternative Solution*:

* File has been being corrupted or otherwise incomplete. Attempted to use a workaround. Attempted to use jar command, but this was unsuccessful.
* Attempted to use quick jar command. This was unsuccessful with BusinessStrategy.zip but resulted in small output for Secrets.zip. The output was "Ick! 0x6f4a2023."

# **Problem 5**

*Description:*

* The problem was simply lack of hardware and lack of time for myself working alone it was quite difficult to get these challenges done and I had to make use of a lot of solutions and connections

*Solution:*

* For my solution I used my resources and found examples and other references online to solve this problem and solving the problem for running and scanning these files I create a Windows 10 environment to handle it all for me and run in the background while other things could be processed
* For the solution to hacking the passwords and VeraCrypt. I had to rely on the small bit of help I had from my group before working alone and thus using their images for two of the items.

# **5    Conclusion and Final Remarks**

Due to the recovery of the “Business Strategy.zip” and “secrets.zip” we can conclude the hacking attempts and efforts were successful in the exfiltration of two import HiTek business documents.

Piecing together the time frame the first-time stamp found was dated 10/21/2015, this was retrieved from the install date of the virtual machine running ubuntu was installed (VMU). Only after a month of the initial setup and installation of the proper exfiltration tools such as Metasploit, which was used to hack SAM registry files and their associated hashes for user accounts on the database. Located on 11/20/15 computer 1 contained a decompression bomb or “zip bomb” within users/Carson/Documents, this was most likely used to disable the antivirus software on the system and allow for the msvenom from Metasploit to begin the exploit the computer.

The attacks were planned accordingly to Thanksgiving Day 11/28/15 which would be an ideal time to strike as most of the company will be off for holiday. Analysis within the FTP logs showed the two exfiltrated files from computer 2 were now being downloaded to computer 1, therefore allowing the hacker to utilize the fact the Virtual machine is attached to the host computer to pretend as though it was another computer within the HiTek company. These files were encrypted utilizing the open-source tool veracrypt which would make sense due to the fact of anonymity of not leaving any suspicious file traces on the computer 1 host machine. These files were located within the users/Carson/Documents titled “locked” and “passowrds.txt” most useful information pertaining to the three passwords found within the text document. After understanding that the VMU was the culprit NMAP was run to identify IP addresses, open ports, and any other vulnerabilities that may have been used to exfiltrate this data from computer 1 and 2.

Concluding on this, the attack was planned and executed meticulously and to cover as many tracks as possible. The delay of the attack on computer 1 would signify the hacker wanted complete anonymity and why the attack between the instillation of the virtual machine and the actual exploitation tools was delayed. Due to the bios machine virtualization setting needing to be switched to enable or the computer needed to be reset to complete the instillation of the virtual machine. More likely VMware would need a reboot as stated in the documentation on their website. Working on the location of the hacker it would be hard to pinpoint it but more likely than not it is a US resident who understand the traditions and holidays of the American people, or a highly informed foreign hacker. Pointing more towards an employee at HiTek being the one to breach the security as the NMAP of the network revealed no previous attempt to detect vulnerabilities was used, meaning this could once again be a highly informed foreign hacker or more likely an insider at the company. Someone would have to either know HiTek’s weak points or this could potential be an attempt of a penetration tester which could explain the tools used as they are widely acclaimed tools for forensic investigations and commonly are found within a penetration testers software library. This could also be the reason the ubuntu VM had the username of “tester” as making sure this it is known that this is a penetration tester. The main suspect would be Carson user along with the user tester on the VMU.

Nothing particularly points to one conclusion clearly, but from the evidence acquired there is a high probability that it could be two things.

1. The hacker was a previous employee or an employee who was on their way out and wanted to create backlash for him leaving. Explaining the fact there was no Nmap run in the first place to find weaknesses, the knowledge that the company would restart the computer to finish the installation of the VMU, and finally explain why he had access enough to get a virtual machine on computer 1.
2. This was a penetration tester doing their job, one explaining the “tester” user on the VMU, relating to “tester” being a penetration tester profile, also explaining the fact Nmap was not used to detect weaknesses as the company may have told the penetration tester to see how vulnerable this weak point was however another alternative is the Nmap scan but the incognito version where the sync ack is sent and then the termination signal is sent instead of the proper response to complete the transmission.

# **6    References**

“What Is a Sam File & How to Back It up?” *What Is a SAM File?*, https://www.lsoft.net/posts/what-is-a-sam-file/#:~:text=The%20Security%20Account%20Manager%20.

“Windows PWDUMP Tools.” *Openwall*, <https://www.openwall.com/passwords/windows-pwdump#:~:text=pwdump8%20supports%20AES%2D128%20encrypted,support%20for%20domain%20cached%20>.

Openwall. “Openwall/John: John the Ripper Jumbo - Advanced Offline Password Cracker, Which Supports Hundreds of Hash and Cipher Types, and Runs on Many Operating Systems, Cpus, Gpus, and Even Some Fpgas.” *GitHub*, https://github.com/openwall/john.

“John the Ripper Password Cracker.” *Openwall*, https://www.openwall.com/john/.

**7    Appendices**

# **Acquisition Computer 1**

Text

Description automatically generated with low confidence

# **Acquisition Computer 2**

Text

Description automatically generated

# **Windows 10 VM**

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

# Autopsy Screenshot Computer1/2 & VMU

# **Graphical user interface, text, application Description automatically generated**

Download history on computer 1 with the user tester downloading VMware player.

Graphical user interface, text, application, Word

Description automatically generated

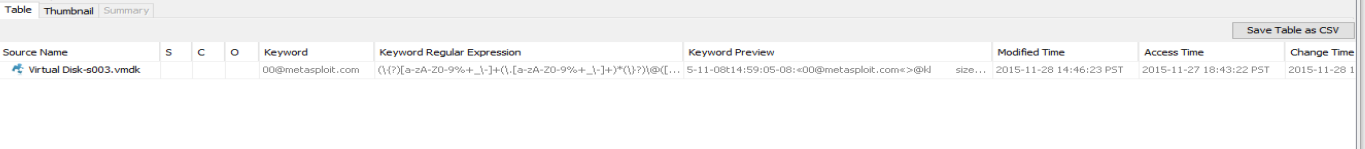
Graphical user interface, text, application, email

Description automatically generated

System specifications of DESKTOP-A8BOTBH and the tester user on the C:\ drive.

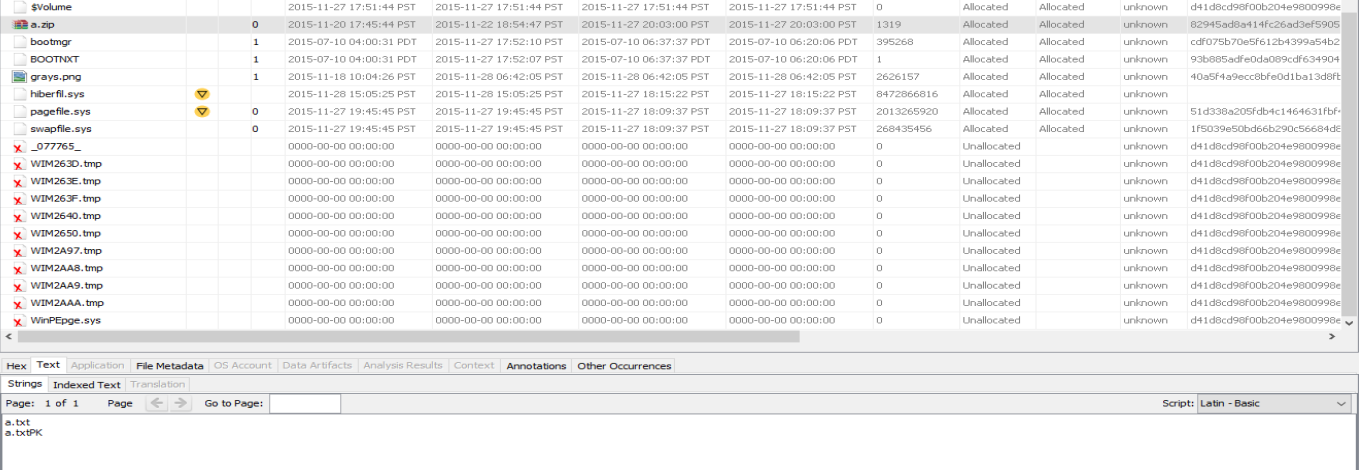


User with the name tester location of the Ubuntu virtual machine on 11/28/15.

 ****

Proof of veracrpyt software on computer 1

Proof of Metasploit on Virtual Machine (VMU)



a.zip potential decompression bomb.

Computer 2 Web server FTP Logs proof of file exfiltration

Graphical user interface, text, application, email

Description automatically generated

# **Hashes Recovered from SAM**

# **Hash Cracking using hashcat/John The Ripper/ Mimikatz**

Text, table

Description automatically generated

Using .\pwdump7.exe to run as elevated privilege and shown cracking the SAM and SYSTEM registry files and using the >> computer1dump.txt to create a text file for the hashes.



Due to my jobs interference with the pathing and root systems on my desktop I received errors I could not resolve not being able to crack it for some reason I reached out for some extra help these images below are not mine however everything besides these two images is my own.

Graphical user interface, text, application

Description automatically generated

Example of john the ripper cracking the above hash extraction for computer 1

Text

Description automatically generated

Example of John the ripper successfully cracking the hashes pictured above for computer 2

# **NMAP Output**

Text

Description automatically generated

# **Suspicious Files**

Table

Description automatically generated

# **Exfiltrated File Statistics**

Table

Description automatically generated

# **Computer Specifications**

Table

Description automatically generated

# **Password Table**

# **Web History**

Computer 1

Table

Description automatically generated

## **Crazywickedawesome Credentials**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

# **WireShark PCAP Analysis**

**Graphical user interface, application, Word

Description automatically generated**

Showing the host of the server as webmaster and scrubbing through FTP transmissions.

Graphical user interface, text, application

Description automatically generated

Following the TCP stream led to the webmasters username and password being discovered.

Table

Description automatically generated

A screenshot of the extraction of the Secrets.zip file

A picture containing table

Description automatically generated

Following the extraction of the BusinessStrategies,zip File

Table

Description automatically generated

The user then deleting the files once again attempting to cover tracks