Intro to Cyber Forensics Lab Grading Sheet

Project: Final Challenge
Member Name: Christopher Bowen
Member Name: George Hendrick
Member Name: Alejandro Marin Arellano
Member Name: Terrence Scott
Member Name: Saehwan Park

Executive Summary _________ / 4 points

+ ✔ -
❑ ❑ ❑ Executive summary is brief and focused to the point of the project ❑ ❑ ❑ The summary clearly illustrates the objectives of the laboratory exercise

Apparatus _________ / 4 points

❑ ❑ ❑ The apparatus are clearly illustrated and documented

Procedures _________ / 12 points

❑ ❑ ❑ Adequate information provided to allow re-creation of work
❑ ❑ ❑ Consistent level of coverage throughout the project – nothing overly detailed or omitted

Problem Solving _________ / 5 points

❑ ❑ ❑ All problems identified
❑ ❑ ❑ Alternative solutions identified
❑ ❑ ❑ Solutions attempted listed
❑ ❑ ❑ Final solution detailed (what fixed the problem and why?)

Conclusions & Recommendations _________ / 5 points

❑ ❑ ❑ Tie back to the learning objectives identified in the executive summary - <u>critical</u>
❑ ❑ ❑ ________ Conclusions stated in a logical fashion
❑ ❑ ❑ Conclusions are viable based on the procedures and results
❑ ❑ ❑ Recommendations practical & relevant

Format & Grammar _________ / 5 points

❑ ❑ ❑ Table of Contents present
❑ ❑ ❑ Report written in past tense
❑ ❑ ❑ Proper voice (no I's, We's, Our's or The group)
❑ ❑ ❑ Paper easy to read (fonts, spacing, etc.)
❑ ❑ ❑ Proper credit given to sources in bibliography (APA style)
❑ ❑ ❑ Paper is cohesive and consistent in tone
_______ Spelling & grammar errors: *minus one half point for each, up to a max deduction of 5 points – at that time, paper is returned for correction and re-submission with a one letter grade penalty.*

Final Score: _______________ / 35

Contents

1 Written Summary

On January 10th, 2023, Investigators receive a cyber forensics challenge to test their abilities on forensic investigations. The investigators received three main sources of evidence: two E01 digital copies of computers, and a network packet capture (Table 1). Investigators also received information pertaining to the hashes of each piece of evidence. The first step taken by investigators was hashing each file and comparing them to the hashes provided to ensure a proper chain of custody. Next, investigators proceeded to create a shared Autopsy Case file of each source of digital forensic evidence. Autopsy took two days to process all modules on the evidence. In the two days of processing, Investigators spent time investigating the network.pcap file.

Investigators first used Wireshark to investigate the pcap for valuable information. While investigating the packet capture, Investigators were able to identify two pieces of data that were transferred within the business. Two files were transferred via vsftp to the /var/www/ root of the webserver in the network (Computer 2): Secrets.zip and BuisnessStrategy.zip (Table 11). These files were encrypted with a password, so investigators resorted to cracking the hash associated with the zip files. To do this, investigators first passed the zips through zip2john to get the password hashes, then investigators used hashcat with seclists' wordlist and rockyou to try and break the hash with the OneRuleToRuleThemAll rule list. Investigators were able to break the hash for the BuisnessStrategy.zip, and the password was found to be crazylongpassword. In this zip file, investigators found a potential motive for the incident that had occurred.

After Investigators were finished with Wireshark, Investigators turned to NetworkMiner to "mine" the pcap for other potential artifacts. In Table 8, the websites that were accessed by computers on the network are listed. Some of the websites are malicious and show that a crime had probably occurred in the network. The last piece of evidence found was the massive amount of SYN packets sent to various ports in the network from 192.168.0.4. This pointed Investigators to believe that a scan of the network had occurred.

When the Autopsy modules finished running on the E01 files of the computers, Investigators were able to begin conducting digital forensics. Investigators began by searching for each system in the evidence sources. In Table 4, the information on each operating system is displayed. While retrieving the OS information, Investigators found a virtual machine folder on machine one and determined that this needed to be further investigated. Next, Investigators began to look for information in logs for an assigned IP addresses at the time of the packet capture and were able to determine each machine's IP (Table 5). The next step of the investigation was to determine the users on each of the machines and their passwords. This process started with computer 1, investigators extracted the SAM and SYSTEM file, where passwords and user information is stored on Windows machines, and used samdump2 to grab the user accounts and NTLM hashes. Note that this resulted in improper evidence that will be discussed in the next section, however, the passwords in Table 6 are correct. The investigators then moved the computer1's Virtual Machine. For extracting user and password hashes on a unix system, the shadow and passwd files are required. Investigators extracted these files, used the unshadow tool and johntheripper to obtain the passwords. The same process was taken on computer2. One of the user's hashes was unable to be broken: jhathaway. Investigators tried to run every possible seclist with multiple rulelist and were unable to break the hash.

Investigators later tried to conduct a dynamic analysis of the computer1 and determined that the passwords from the System and SAM file were not correct when attempting to log in. Investigators tried using the same password of computer1's VM tester account, monkey, and gained access. After gaining access, Investigators used mimikats, a popular pentesting tool, to gain access to the password hashes of the users. After gaining access to the password hashes, Investigators used hashcat to break them.

To create a timeline of each of the three machines, Investigators used logs2timeline to create a complete timeline of all incidents that occurred. Logs2timeline is a popular forensic metadata and log analysis tool to create a complete timeline of a system. This timeline was used numerous times to check for evidence and artifacts. Each time line is 70+mb of information, therefore, they are not linked in this report.

The next step that Investigator took was static manual enumeration of the filesystems to look for artifacts and evidence. In Table 9, a list of suspicious file and programs are listed. One of the most interesting artifacts/programs found on the system was veracrypt, a tool used to encrypt drives on a computer, on computer1, and Metasploit a framework used to pentest/hack into the machine on the VM on computer1 in tester's account. After finding metasploit in Autopsy on the VM, foul play was suspected. Investigators also found payout.docx in vol4 of computer1 and determined that a crime had occurred and a clear motive was defined. Investigators determined that an inside job may have occurred and that the tester account on the Windows machine had been used to steal private information– Corporate Espionage.

The next step Investigators took was investigating the virtual machine. Many issues occurred with static analysis of the virtual disk, so investigators determined that dynamic analysis of the vm would be the next step. Investigators properly documented each step and is as follows. Investigators extracted the virtual machine folder and booted it in VMware 17 pro. Investigators then logged into the tester account with the password monkey. Next investigators noted the text files on the desktop of the tester profile and hashed each of them. Investigators then open each of the text files and determined that each of the text files were output of a nmap scan. Finally investigators opened a terminal and ran the history command to see what commands had potentiall has been run on the vm. In history, investigators found that both nmap and Metasploit had run. Investigators determined that the nmap scan explains the traffic in the pcap. Investigators also could not find commands that were run in Metasploit, therefore, log inspection occurred and Investigators determined that Metasploit pro was run in the web browser. Investigators then ended the dynamic investigation and began the further static investigation in the Autopsy with the original virtual disk.

Investigators found multiple Firefox cache files (Table 8) to support the following theory. The tester user in computer1's VM was used to exploit the computer2 webserver. The tester account was used to run Metasploit pro and gained RCE on the webserver. Investigators followed up in the logs of computer2 and where not able to conclude what was remotely run on computer2. However, Investigators believe this was used to help aid the exfiltration of data from the company

The following is the theory of data exfiltration from the company. A user on computer1 set up a virtual machine under the tester account, which had administrative privileges, to execute nmap to scan for the webserver on the company's network. After finding the webserver (computer2) the user attempted to exploit the server and succeeded. The user enabled access to transfer data via the ftp service (Investigators do not have evidence to back up this part of the claim). This allowed the user to send stolen files that were hidden on the Veracrypt drives (found in logs from computer1). These files were transferred to the webserver where anyone could access them remotely and exfiltrate them. Investigator believe that the individual that stole the information is linked to Professor Michael Robin from Stevenson University because the form filled out for the Metasploit pro account used his information.

2 Time line and Artifacts

Table 1: The time line of events in the case as found by investigators

#	DATE	ACTION
1.	11/28/2015	Attacker sets up VM on host machine
2.	11/28/2015	Attacker scans the company network for the webserver
3.	11/28/2015	Attacker finds the webserver and attempts an exploit
4.	11/28/2015	Attacker connects to web server and downloads Secrets.zip and BusinessStrategy.zip to the VM
5.	11/28/2015	Attacker deletes the zip files from the webserver and disconnects

Table 2: List of items given to investigators to start case

#	FILE	MD5 HASH
1.	Computer1.E01	53ff8a7c786e36824118ccdf5d13cb01
2.	Computer2.E01	762f3742c81aa0d3017674c2083f1e97
3.	network.pcap	8754862e479eb1e93eaa72d79e12e84d

Table 3: Operating System Detected

#	COMPUTER	OPERATING SYSTEM	FILE PATH	MD5 HASH
1.	Computer 1 (E01)	Windows 10 Pro	C:/Windows	b40c6acd32c1e9a41fc55ede67a4848b
2.	Computer 1 (E01) VM	Linux (Ubuntu 15.10)	/Users/tester/Documents/Ubuntu 64-bit 15.10.vmwarevm/Virtual Disk.vmdk	7db0068517ca68ea4d9624fc46228b48
3.	Computer 2 (E02)	Linux (Debian)	/img_Computer2.E01 /vol_vol2 /etc/debian_version	931870fda5e3f942afc004db670b3cae

Table 4: Host Names and IPs

#	HOST NAME	IP ADDRESS	FILE PATH	MD5 HASH
1.	DESKTOP-A8BOTBH	192.168.0.6	/img_Computer1.E01/ vol_vol3/Windows/ System32/config/SYSTEM	b40c6acd32c1e9a41fc55ede67a4848b
2.	ubuntu / unknown.local, UNKNOWN	192.168.0.4	/img_Computer1.E01/ vol_vol3/Users/tester/ Documents/Ubuntu 64-bit 15.10.vmwarevm/Ubuntu 64-bit 15.10.vmx	198e57678d1331f32d3528e3e6dcbd3e
3.	web-srv-02	192.168.0.8	pcap	N/A

Table 5: Windows User Accounts and Passwords (E01)

#	USER ACCOUNT NAME	PASSWORD	PASSWORD HASH	ARTIFACT FOUND
1.	Administrator	’ ’ - no password	31d6ccfe0d16ae931b73c59d7e0c089c0	SAM/SYSTEM
2.	Guest	-DISABLED-	-DISABLED-	SAM/SYSTEM
3.	DefaultAccount	-DISABLED-	-DISABLED-	SAM/SYSTEM
4.	tester	monkey	f2477a144dff4f21ab81f2ac3e33207d	SAM/SYSTEM
5.	Carlson	123456	32ed87bdb5fdc5e9cba88547376818d4	SAM/SYSTEM
6.	Jonathan	letmein	becedb42ec3c5c7f965255338be4453c	SAM/SYSTEM

Table 6: User Accounts and Passwords(E02)

#	USER ACCOUNT NAME	PASSWORD	PASSWORD HASH	ARTIFACT FOUND	MACHINE
1.	webmaster	password	$6$YIvB3TIX$Kp...	/etc/.shadow	E02
2.	cknight	popcorn	$6$n7FU15MvgA8...	/etc/.shadow	E02
3.	jhathoway		375QZ16ZaLVuJAtr $IjThiS3EfP...	/etc/.shadow	E02

Table 7: User Accounts and Passwords(E01 VM) (full hashes can be found in Table 2)

#	USER ACCOUNT NAME	PASSWORD	PASSWORD HASH	ARTIFACT FOUND	MACHINE
1.	tester	monkey	f2477a144dff4f216...	E02:/etc/shadow	E01 and VM
2.	postgres	N/A	N/A	E02:/etc/shadow	E01 and VM
3.	henchman	P@ssw0rd!@#	N/A	Documents/grays.jpg	Website Login
4.	Laslow	FritoLay	N/A	/Windows/MMC.exe	Website Login

Table 8: Websites Visited

#	WEBSITE	MACHINE	DATES	ARTIFACT FOUND	USER
1.	mozilla.org	VM From E01	11/18/2015 18:18 CST	Downloaded firefox installer	tester
2.	rapid7.com	VM From E01	11/18/2015 18:19 CST	download.jsp (metasploit)	tester
3.	downloads. metasploit.com	VM From E01	11/18/2015 18:21 CST	metasploit-latest-linux-x64-installer.run	tester
4.	imdb.com	E01	11/27/2015 22:06 CST	Nothing of interest	tester
5.	bing.com	E01	11/28/2015 2:32 CST	Search: how to get help in windows 10	tester
6.	google.com	E01	11/28/2015 8:25 CST	Downloaded chrome installer	Default
7.	cnn.com	E01	11/28/2015 9:25 CST	Nothing of interest	Default
8.	gmail.google.com	E01	11/28/2015 11:00 CST	Nothing of interest	Default
9.	amazon.com	E01	11/28/2015 16:27 CST	Nothing of interest	Default
10.	google.com	E01	11/28/2015 16:32 CST	Search: star wars	Default
11.	youtube.com	E01	11/28/2015 22:49 CST	Nothing of interest	Default

Table 9: Suspicious Files

#	FILE NAME	MACHINE	PATH
1.	a.zip	E01	/img_Computer1.E01/vol_vol3/a.zip
2.	Report.odt	E01	/img_Computer1.E01/vol_vol3/Users/Carson/Desktop/Report.odt
3.	VeraCrypt Setup 1.16.exe	E01	/img_Computer1.E01/vol_vol3/Users/Carson/Desktop/VeraCrypt Setup 1.16.exe
4.	network-architecture	E01	/img_Computer1.E01/vol_vol3/Users/tester/Documents/network-architecture
5.	locked	E01	/img_Computer1.E01/vol_vol3/Users/Carson/Documents/locked
6.	notes.doc/notes.odt	E01	/img_Computer1.E01/vol_vol3/Users/Carson/Documents/notes.doc(odt)
7.	payout.docx	E01	/img_Computer1.E01/vol_vol4/payout.docx
8.	output.txt	E01 VM	/home/tester/Desktop
9.	output-1.txt	E01 VM	/home/tester/Desktop
10.	output-2.txt	E01 VM	/home/tester/Desktop
11.	output-3.txt	E01 VM	/home/tester/Desktop
12.	output9.txt	E01 VM	/home/tester/Desktop
13.	output.2.txt	E01 VM	/home/tester/.local/share

Table 10: Stolen Credentials

#	USER ACCOUNT NAME	PASSWORD	ARTIFACT FOUND	LOGICAL OFFSET
1.	henchman	P@ssw0rd!@#	Documents/grays.jpg	N/A
2.	Laslow	FritoLay	/Windows/MMC.exe	N/A

Table 11: Stolen Files

#	FILE NAME	MD5 HASH	ARTIFACT FOUND	LOGICAL OFFSET
1.	BusinessStrategy.zip	c05fc707175f4e09201ae80d9c774d1f	/$CarvedFiles/f0270656_BusinessStrategy.zip	N/A
2.	BusinessStrategy.rtf	4376ad7dbfb49d91528292bdf571f160	/$CarvedFiles/f0270656_BusinessStrategy.zip/BusinessStrategy.rtf	N/A
3.	Secrets.zip	1142df97fd45fa8ea57f02cc51b457e9	/$CarvedFiles/f0270648_Secrets.zip	N/A

3 Conclusion

Investigators are of the firm belief that this attack was carried out for the purposes of corporate espionage and monetary benefit. There is no doubt that the perpetrator(s) were aware that HiTek would not recover if this information was leaked, outlined in BusinessStrategy.zip, making malicious intent clear. They also disclosed interest in making monetary profit, outlined in payout.docx. The file displayed potential profits for all of HiTek's assets. In addition, to reiterate from the end of the written summary, investigators have a strong suspicion the perpetrator has some connection to Professor Michael University. This is because the form filled out for the Metasploit Pro account on the VM detailed his information.