**SIT703-Advanced Digital Forensics**

**Assignment 2**

Student’s Name

Institution

**Introduction**

Rapid growth of information technology has developed several challenges related to cyber crime. Globally, the rate of cyber crime targeting financial institution, learning institution, government and even personal information are high. A study conducted by Appudurai (2007), concluded that the rate of cyber crime has increased due to advanced technology and interest of people to access information both for personal and political gain. It is also stated that most hackers or other cyber crimes activities targeted government and financial institution to leak information to the public and for financial gain. A survey conducted by the Massachusetts Institutes of technology pointed that the increased cyber crime related activities are driven by intense to cause financial and political harm to institutions and government (Shinder & Michael, 2015). It is therefore, evident that 90% of cyber crime related activities target institution. This paper therefore, represent an investigate result of a cyber crime which occur at university where an account was created on one of the employees with her consent. It report procedure of investigation, tools or equipment used to conduct the analysis or investigation of the cyber attack, and how the problem was addressed. It also illustrates the detailed findings, and review and reflection of the finding.

**Overview of computer crime case**

Computer crime case is referred as illegal activities which are perpetrated through the use of a computer. The activities include hacking, attacks, denial of service and unauthorized access and use of services and cyber vandalism. In this case, a staff computer was accessed and an account created without her consent. Amy an employee with a University called their IT administrator to inform him that her suspicious account has been created in her laptop without her consent. The IT administrator is also not allowed to transfer any file from Amy computer because of the top secret information Amy is working on for the government and therefore, the policy does not allow Arif the IT administrator to transfer any file registry from her computer. It is also established that Arif requested Amy to export the Window file registry and copy few windows log files of her laptop from the directory. It is therefore, important to scan the computers including the investigator computer to ensure that they are safe from any spy programs before conducting the analysis and investigation of the attack.

**Resources of forensic investigation**

In order to ensure that the investigator computers are safe, several tools were used to scan the computer. Appudurai (2007) pointed out that it is important to ensure that a computer intended to be used for forensic analysis is secure and there is no rootkit installed. Rootkit is regarded as the computer program installed in a computer to provide privilege access to a computer while in hiding. Therefore, BitDefender Rootkit Remover was used to scanner computer being used by the investigators. The computer was scanned completely to ensure that there is not any application running in the background which can compromise the investigation of the cyber crime activity.

Besides BitDefender Rootkit Remover and window defender other resources which were used to conduct the investigation of the cyber crime activities to protect Amy files and computer are SANS SIFT, ProDiscover Forensic, Computer Aided Investigation Environment (CAINE), Xplico, X-Wys forensic and the sleauth kit. In this case, after the scanning of the investigator computer, procedures were followed to back up the files. It is pointed that before backing up of file, the window registry files were exported. The window registry files are exported to make sure that files can be access later when the investigation is done. This ensure the data are secure from any access from unauthorized perform. According Tron (2015), it is the first procedures necessary to be taken when any violation or hacking is detected.

Computer Aided Investigation Environment (CAINE) was used to analyze all the files in the hard disk and windows registry for any unauthorized access (Rosenberger, 2018). Since the investigator computer had been scanned and free from any attack, the desktop zip file was unzip and the windows log file was analyzed and repaired. The analysis of the log files indicates that Amy computer was accessed and account created without her knowledge. Hacking can be done to create an account without the knowledge of the computer users and mostly can be used to monitor the activities of an individual and transfer files as well.

**Description of information stored in the log files**

There are four log files backed up for investigation of what occurred. The log files are AppEvent, SecEvent, Internet and SysEvent.

**AppEvent log file**

Analysis of the AppEvent log file indicates a unique trend with several warnings, and errors originated from different applications which attempted to access or were used in the computer (Michael, 2015). There is also evident of attempted data corruption which occurred several occasions. The AppEvent indicates that ESENT error occurred several times randomly. Most errors are originated from the disks and ESENT. But errors from the disks performed no tasks which mean that these are normal errors generated by the computer. However, the error occurred from ESENT performed data corruption. As show in the diagram 1 (one), below, there were several errors encountered from AppEvent.



***Diagram 1: AppEvent View***



***Diagram 2: AppEvnt overview Summary***

**Internet log file**

The analysis of the internet log files indicates there are several errors originated from account WUSA and information. It is established that WUSA access the computer on May 26, 2019 at 2:15:53 PM, and no task was done. Internet log file could not be viewed on the event view, it indicates error consistent.



***Diagram 3: Event View of Internet log file***



***Diagram 4: Event property of WUSA***

There is evident of warning all Events in SysEvent, AppEvent, Internet and secEvent. The errors activities are also reported originated from different sources. Most errors are warning occurred between the period of May 23, 2019 and August 29, 2019. This can indicate the period, which Amy’s computer was accessed by a third party.

The analysis established that WUSA is the accounted which was created without the consent of Amy, and therefore, Arif, IT Administrator should look for WUSA account with Event ID 2. This will help the Arif to troubleshoot and solve the problem related to security related issues. The diagram 5 below indicates some of the activities which occurred using the account WUSA.



One of the staffs called Amy who worked for University complaint to the IT administrator that a suspicious account has been created on her laptop. Suspicious account is WUSA was created accessed mostly doc.

TASK 6:

The bogus account was used to log into Amy’s computer at 2:15:53PM on May 26, 2019. The account was logged thrice at different rimes. The computer can therefore, be protected using window defender and an anti-virus to protect any future entry.

**Task 7**

The information obtained from the system indicates that bogus account was used to access doc document. The analysis indicates WUSA accessed several information and more so performance data corruption. In this case, it means there was an attempt to obtained data from the computer several times. The attempt was made between 2:15:53 PM to 4:14:23PM and then logged off.



**Diagram 6: logged time**

**Task 8**

The events on Amy account lasted for days. After the creation of bogus account, the user access Amy’s computer three times and visited used several applications and files. First, the account was used to conduct data corruption and also to access information from the hard disk several times. It therefore, can be concluded that the bogus account was used to access and files from the computer.

**Task 9**

The analysis indicates that several activities took place in the system. It is identified that the installation of application occurred from the device manager. It is more likely that the installed application was used to access the files and other documents from the computer. However, other events identified are Event ID 47, Event ID 10024, Event 6005, 6006, and Event 7003 as some of the events which will be visible.



**Analysis of finding**

The investigation revealed that Amy’s computer was accessed several times between 2:25:53 PM on May 23. Amy computer was accessed and other account created used to access and transfer information from the laptop. Though there is no proof of any file transferred, the account created in the name of WUSA was used to access data file. There was evident of data corruption and several attempts and logged in which violated the privacy of information Amy is working. The attack was done through installation of an application which made it easily to create and access the laptop remotely. Moreover, it is important to point that CAINE was used to investigate the attack but before the investigation started Arif computer was scanned to ensure that any attack is avoided from the system or log files to be analyzed. Therefore, the result obtained result what happened.

**Reflection of findings**

The findings indicate that Amy computer was hacked and account created. The creation of an account gave unauthorized person the right to access Amy’s computer and make some changes and copy data from the hard disk. The investigation revealed that there are several errors originated from the hard disk of the laptop. The error could be as a result of access to the hard disk from the account created.

**Recommendation**

It is necessary to take strict action to avoid the repeat of what happened to Amy and to secure all the files and information of the company. Therefore, it would be important to install and update windows defender in all the computers being used in the university. It would also be advisable to installed anti-virus and keep updating its database to ensure that it remains updated to scan system continuously. The network of the university should also be protected from the backbone of the structure to prevent any attack to the system. It is evident that the attacked managed to log into the system and access the information. Without strong protection from the backbone, it would be difficult for any hacker to access the system or any computers on the network.

# References

Appudurai, J. (2007). Computer Crimes: A Case Study of What Malaysia Can Learn from Others? *Journal of Digital Forensics, Security and Law* *, 2* (2), 2-15.

Shinder, L., & Michael, C. (2015). Understanding E-mail and Internet Crimes. *https://www.sciencedirect.com/topics/computer-science/cybercrime-case* , 2-15.

Tron, M. (2015). Computer Forensics: An Inseparable Part of Criminal Investigations. *Journal of forensic Analysis* , 2-15.