Name: S M Ragib Rezwan
ID: 103172423
Course name: eForensic Fundamentals

Assesment2-Lab 6 Report:

- On 21St April 2022 (Thursday), at 7:10pm a client named Mr ImaVictim contacted me to investigate a potential malware attack.

- So, at 7:11pm, I arrived at his home where his computer was still running with Wireshark capturing data. That time, I spoke with the client who detailed about the following sequence of events that took place:
    1) He had been browsing the web when he downloaded a program called "server.exe"
    2) Then he ran the "server.exe" which in turned caused a weird message to pop up, but nothing else seemed out of place.
    3) A few moment after this, his internet browser opened spontaneously, without any interaction from him (ie. the client hadn't clicked anything to cause browser to open)

  Seeing this, the client suspected that his activities have been monitored by a third party and had been concerned about the fact that the sensitive business proposal he had been writing at that time may have been leaked to that third party individual or group. Thus he called me in to help him locate evidence on the matter so that he can take it to the police to identify and prosecute the third party.

- Thus, after hearing all of this, at 7:12pm, I began my investigation by performing a live forensic triage of my client's computer where I used a forensic tool to note down detailed information regarding his computer. I had noted down those information in the tables below for ease of view:

Time details:

System Date	**04/21/2022**
System Time	**19:12:11.15**
System Timezone	**Canberra, Melbourne, Sydney (GMT+10:00)**
Current Date	**04/21/2022**
Current Time	**7:12:11PM**
Time Variation (between system and current)	**0**

Name: S M Ragib Rezwan
ID: 103172423
Course name: eForensic Fundamentals

Operating System Details:

OS Name	**Microsoft Windows XP Professional**
OS Version	**5.1.2600 Service Pack 3 build 2600**
System Uptime	**31 mins, 16 secs**

User Account Details:

Logon Time	**6:45:15PM**
Logged on User	**Lab6-VICTIM\ImaVictim**

IP Address Details:

IP Address	**192.168.23.2**
Subnet Mask	**255.255.255.0**
MAC Address	**00-0C-29-AA-96-88**

- Later on, at 7:20pm, I opened the task manager on my client's computer to check if there are any suspicious processes. During that process, I had located a process with the name "server.exe" which had the same name as the file my client had downloaded from the web. So I noted the PID of the process in the table below as a suspicious process:

PID of "server.exe"	**1400**

- Then, at 7:25pm, I used a forensic tool to see which processes running on client's computer had open network connections at that point in time. This was done to check whether or not the suspicious process was indeed the malware.

  At that time, I had noticed a foreign address entry on the computer with the same PID as that of the suspicious process noted before. So, I noted the entry details down in the table below:

Foreign Address	**192.168.23.1:1604**
State	**ESTABLISHED**
PID	**1400**

- After that, at 7:30pm, I utilized all the information stated before and another forensic tool to locate the malware on my client's computer. Then I recorded the details about the malware in the table below:

Name: S M Ragib Rezwan
ID: 103172423
Course name: eForensic Fundamentals

File Name	server.exe
Path	C:\Documents and Settings\cisco_lab\Desktop\server.exe
Size	774144 bytes
Created	April 21,2022 6:58:18PM
Modified	April 21,2022 7:02:54PM
Accessed	April 21,2022 7:02:54PM

- At 7:35pm, I decided to find the evidence needed to determine a timeline of the events. Thus, I utilized the Wireshark (which had been running in the background since the time the "server.exe" file had downloaded) in my client's computer for this task.

  By utilizing this forensic tool, I had been able to go through the internet traffic that had occurred in the past and find the initial HTTP request that had caused the malware to be downloaded. So I promptly noted those details in the table below:

Time Malware had been downloaded	18:50:20.657709
Full Request URI for the website	http://192.168.23.1/server.exe

  Then I copied the summary details of the packet as an CSV and pasted it in a notepad *(see at the very end of the report)*

- After this, at 7:40pm, I used the same forensic tool to locate the HTTP reply packet which had the data from the malware and copied it. This had been done so that we would have a copy of the malware which can be used later on to find the offender (as their computer would have the exact same file). Furthermore, I also noted the size of the file during this time:

Server.exe File Size	78 bytes

- Later on, at 7:45pm, I used the same forensic tool to locate the HTTP request that was generated by Firefox when the culprit had remotely accessed and controlled my client's computer. The details of the event are noted down in the table below:

Time webpage had been opened	19:09:03.885386
Full Request URI for the webpage	http://192.168.23.1/index.html

  Then I copied the CSV summary of this packet too in the same notepad as the one stated before *(see at the very end of the report)*

- After this, at 7:50pm, I realized that the culprit had been on the same local network as my client (as they shared a similar IP address) and used the same forensic tool to locate the culprit's MAC address, before noting it in the table below:

MAC Address of the culprit	**00:0C:29:D2:66:24**

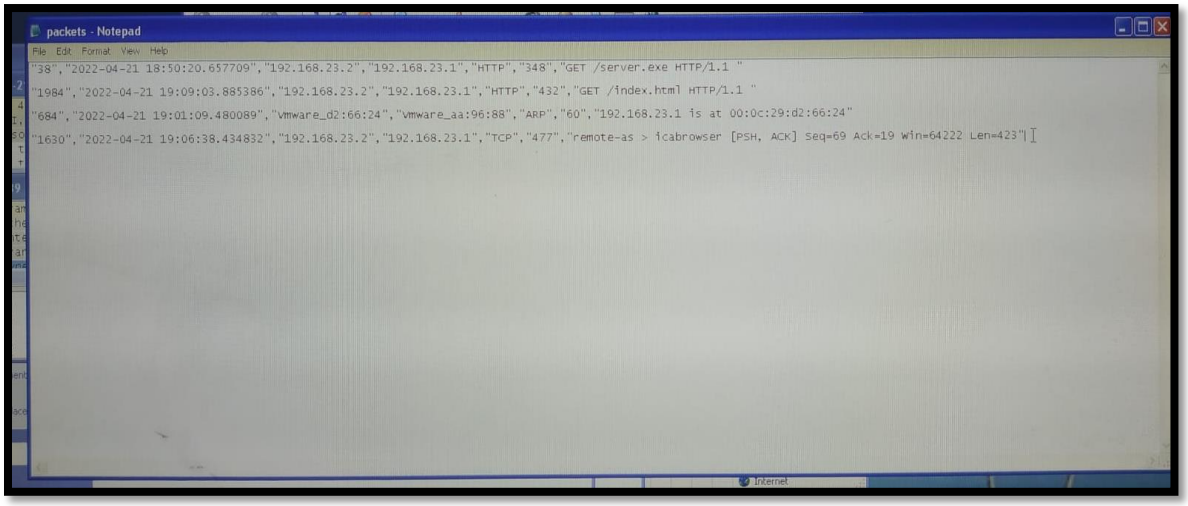
Then I copied the CSV summary of this packet too in the same notepad as the one stated before *(see at the very end of the report).*

So we now had the information we needed to find the physical location of our culprit's computer.

- Later on, at 7:55pm, I used the same forensic tool to filter through the traffic and identified the packet which showed that my client's sensitive business proposal had been recorded by a third party via keylogging and had been sent over to the culprit. Thus I noted the time of the packet (that sent the keylogging data to the culprit) down in the table below:

Time Key logged data was sent	**19:06:38.434832**

After that I also copied the CSV summary of this packet into the same notepad as the one stated before *(see at the very end of the report)* and finally saved it as "packets.csv". Then I moved it to my own computer to submit it along my report to the police. The contents of the file (ie all the CSV summary of the relevant packets) can be seen in the picture pasted below:



Name: S M Ragib Rezwan
ID: 103172423
Course name: eForensic Fundamentals

Overall, I concluded my investigation on 21St April 2022 (Thursday), at around 8:00 pm. From the information I had obtained, my client, Mr ImaVictim has indeed been infected by a program named “server.exe”. This had been downloaded and executed by my client and had caused his sensitive business proposal to have been recorded by the perpetrator. Not only had I found and terminated the program afterwards, but I had also been able to locate the physical location of the culprit’s computer (ie his MAC address). So now I will hand over the report to the police to help my client with the prosecution of the culprit.