2021-HS1-ICT30010/ICT70006-E-FORENSIC FUNDAMENTALS

LAB 6 REPORT

STUDENT NAME: JOSHUA BARBIERI

STUDNENT NUMBER: 102581445

PLEASE NOTE THAT THERE WILL BE DIFFERENT TIMES TO THE ONES EXPECTED. THIS IS BECAUSE I WAS NOT ABLE TO FINISH THE LAB IN THE FIRST SESSION AND WAS UNABLE TO COME TO THE SECOND SESSION. BECAUSE OF THIS I DOWNLOADED THE REQUIRED DOCUMENTS TO A USB SO I COULD FINISH THE LAB AT HOME. THIS RESULTED IN DIFFERENT TIMES TO WHAT WOULD BE SEEN IN THE LAB. EG 2:30PM INSTEAD OF 6:30PM

INTRODUCTION:

My client Mr ImaVictim has contacted me regarding a potential malware attack. I arrive at Mr ImaVictim home finding his computer running with Wireshark capturing data. Upon talking to Mr ImaVictim in more detail I discover that he has browsed the web and come upon a program called "server.exe". Mr ImaVictim saved and ran "server.exe" and upon doing so a message immediately appeared on his screen however nothing seemed different following this bizarre message.

Approximately 5 or so minutes have passed while conversing before an internet browser window opens without anyone touching the computer. Mr ImaVictim indicates that he is concerned that a sensitive business proposal he was writing at the time might be in the hands of a third party and wants me to locate any evidence that might indicate a malicious third party at work so he can take said evidence to the authorities.

INVESTIGATION:

- I arrive at Mr ImaVictim' s home at approximately 2:30pm, mon, 26th of April. Upon arrival we discuss the exact nature of the issue he is dealing with, what his worries are, what he has done before and after the suspicious activity occurred. I am informed that Mr ImaVictim has been using Wireshark to monitor his network activity and is capturing data.

- At approximately 2:44 pm I use a forensic tool in the command prompt to note down key details regarding the client's computer. As this is a live investigation to aid in my investigation I collect as much information about the running system as I can. This is done by noting down key details for Mr ImaVictim computer. I take down the time details, OS details, User account details and IP address details.

  The details can be seen in the tables below:

TIME DETAILS:

System Date:	**Mon 04/26/2021**
System Time:	**02:44pm**
System Time zone:	**AUS eastern standard time**
Current Date:	**Mon 04/26/2021**
Current Time:	**02:44pm**
Time Variation (+/-):	**GMT+10:00**

OS DETAILS:

OS Name:	**Microsoft Windows XP professional**
OS Version:	**5.1.2600 service pack 3 build 2600**
System Uptime:	**26mins 52 seconds**

USER ACCOUNT DETAILS:	
Logon time:	**4/26/2021 2:23:02 PM**
Logged on user:	**LAB6-VICTIM\ImaVictim**

IP ADDRESS DETAILS:	
IP Address:	**192.168.55.2**
Subnet Mask:	**255.255.255.0**
MAC Address:	**00-0C-29-EA-4E-1B**

- At approximately 2:55 pm to determine if there are any suspicious processes that can be recognized on Mr ImaVictim's computer I access the task manager. Having gone through the task manager I am able to locate a suspicious process called server.exe. I immediately note down the PID of this suspicious process.

  The PID of server.exe is 1052.

- At approximately 3:00 pm To confirm that this suspicious process is in fact malware I use a forensic tool to identify open connections on the client's computer. I find that there is a foreign address entry on the client's computer with the same PID of 1052 as the suspicious process server.exe, the details for this are seen below:

Foreign Address:	**192.168.55.1**
State:	**SYN_SENT**
PID:	**1052**

- At approximately 3:10 pm, having found the information above using a forensic tool I am able to locate the malware on Mr ImaVictim's computer and record the following information seen below:

File Name:	**Server.EXE-12650A48.pf**
Path:	**C:\WINDOWS\Prefetch**
Size:	**19.9KB**
Created:	**Today, April 26, 2021, 2:26:31pm**
Modified:	**Today, April 26, 2021, 2:26:31pm**
Accessed:	**Today, April 26, 2021, 2:26:31pm**

TIMELINE OF INFECTION:

- At approximately 3:30 pm Mr ImaVictim had Wireshark running in the background, as such I have used this forensic tool to trace the exact time when the infection first occurred. I locate the initial HTTP request that prompted the malware download using Wireshark to examine the internet traffic that occurred on Mr ImaVictim's computer. Finding the initial packet allowed me to find the reply which contained the malware. A copy of the malware has been downloaded so that when we investigate any suspects, we can examine their computer to locate the same file. The findings are seen below:

Time of download:	**Apr 26, 2021 14:26:04**
Full request URI for malware:	**http://192.168.55.1/server.exe**
Server.exe File Size:	**19.9KB**

- At approximately 3:40 pm continuing to examine the packets and internet traffic information I was able to locate the HTTP request generated when the alleged hacker remotely accessed and controlled Mr ImaVictim's computer. We were able to determine when the webpage was open and the full request URI the details for which can be seen below:

Time webpage opened:	**Apr 26, 2021 14:36:45**
Full request URI for Webpage:	**http://192.168.55.1/index.html**

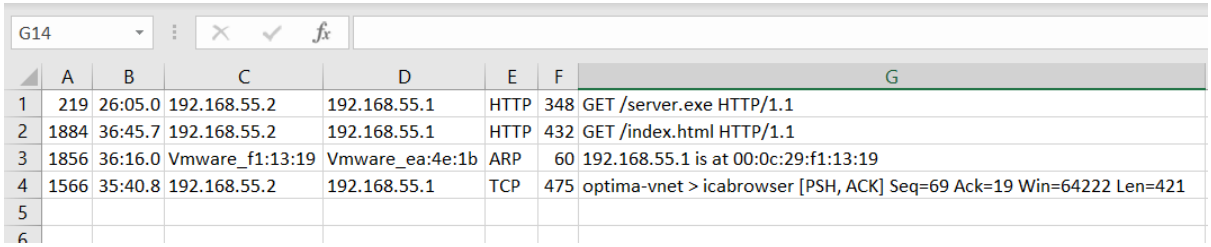
- At approximately 3:50 pm having identified earlier that the alleged attacker was on a local network I was able to use a forensic tool to identify the MAC address of the alleged attacker. This will allow us to know the physical location of our attacker's computer. The details for these findings are seen below:

MAC address of attacker:	**00:0c:29:f1:13:19**

- At approximately 4:00 pm I identified the packet containing sensitive information regarding Mr ImaVictim's business proposal that has been recorded via keylogging by the alleged attacker. This was done using Wireshark to filter and monitor internet traffic. We were able to determine exactly what time the data was logged by the attacker. The results for this can be seen below:

Keylogging time:	**Apr 26, 2021 14:35:40**

- At approximately 4:05 pm I compiled all the evidence in a CSV format gathered from Mr ImaVictim's computer to a text file called "packets.csv". I then moved this file onto my computer to submit along with my report to the authorities. The contents of this file can be seen below:



G14

	A	B	C	D	E	F	G
1	219	26:05.0	192.168.55.2	192.168.55.1	HTTP	348	GET /server.exe HTTP/1.1
2	1884	36:45.7	192.168.55.2	192.168.55.1	HTTP	432	GET /index.html HTTP/1.1
3	1856	36:16.0	Vmware_f1:13:19	Vmware_ea:4e:1b	ARP	60	192.168.55.1 is at 00:0c:29:f1:13:19
4	1566	35:40.8	192.168.55.2	192.168.55.1	TCP	475	optima-vnet > icabrowser [PSH, ACK] Seq=69 Ack=19 Win=64222 Len=421
5							
6							

CONCLUSION:

At approximately 4:10 pm, Monday the 26th of April 2021, I concluded my investigation into the alleged attack on Mr ImaVictim. From the findings that I have collected via my investigation I have confirmed that Mr ImaVictim was infected with a malicious program named "server.exe". This program was downloaded and executed by Mr ImaVictim and consequently his activities including the aforementioned sensitive business proposal have been recorded by the attacker. We have been able to find the malicious program and terminate it and have also been able to pinpoint the location of the attacker. This report will be handed over to the authorities to aid in prosecution.