Analysis Report

by

Team 6 (Dhivya Govindarajan, Sushant Murdeshwar, Ashish Pandit)

This report is the analysis report of **Team 8** malware (Nitish Ganesan; Pradeepkumar Duvvur; Nandakumar Gunalan). The malware identified is the Keylogger which captures the keystrokes and sends it through the server using a TCP connection. The following section provides the detailed analysis performed to detect the malware.

1. We started with the system's CPU usage in the task manager. We saw the usage spiked almost upto 100. This seemed unusual for the system to spike 100% when none of the applications were open.

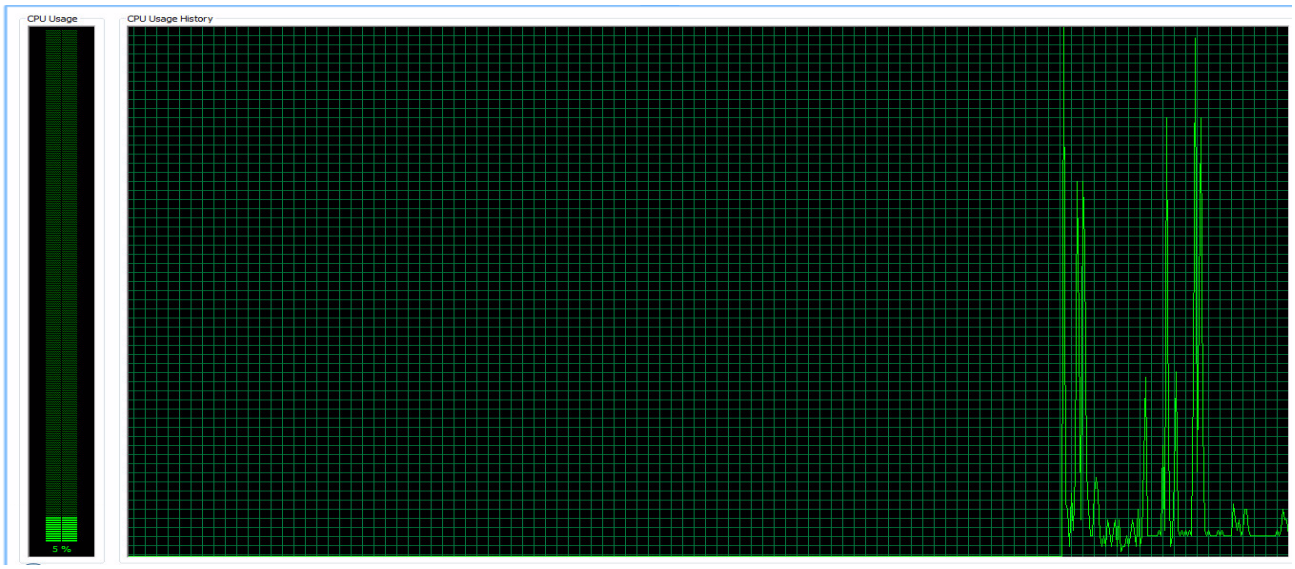

Figure 1 : CPU usage of the system

2. Observing the spikes, we looked at the Processes section to identify what processes were open and running. We observed that two processes backdoor1.exe and explorer.exe were consuming significant amount of resources, as shown in the Fig 2. On analysing, we found that the explorer.exe is the process of the windows system for the user interface functions and it was not the malware. So, we focussed on the backdoor1.exe

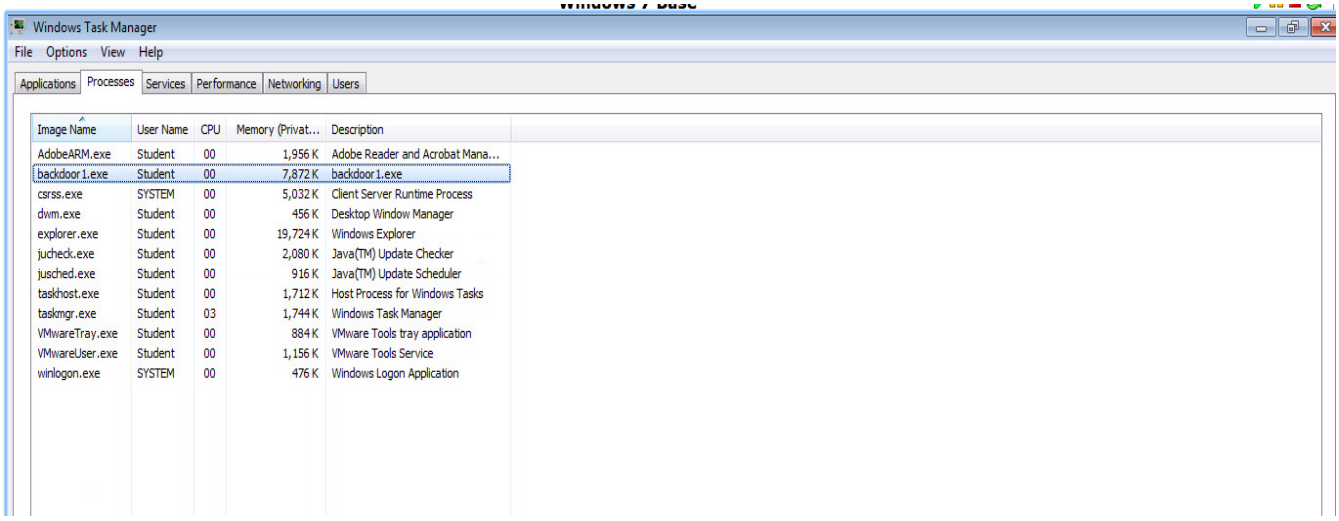

Figure 2 : Identified the active Processes in the Task Manager

3 . Although we doubted that backdoor1.exe was malicious, we were unable to find what exactly the .exe was doing. To explore more on it, we used the process hacker tool. The tool gives the detailed information of the system's activity. We found that the backdoor1.exe was consuming significant resources.

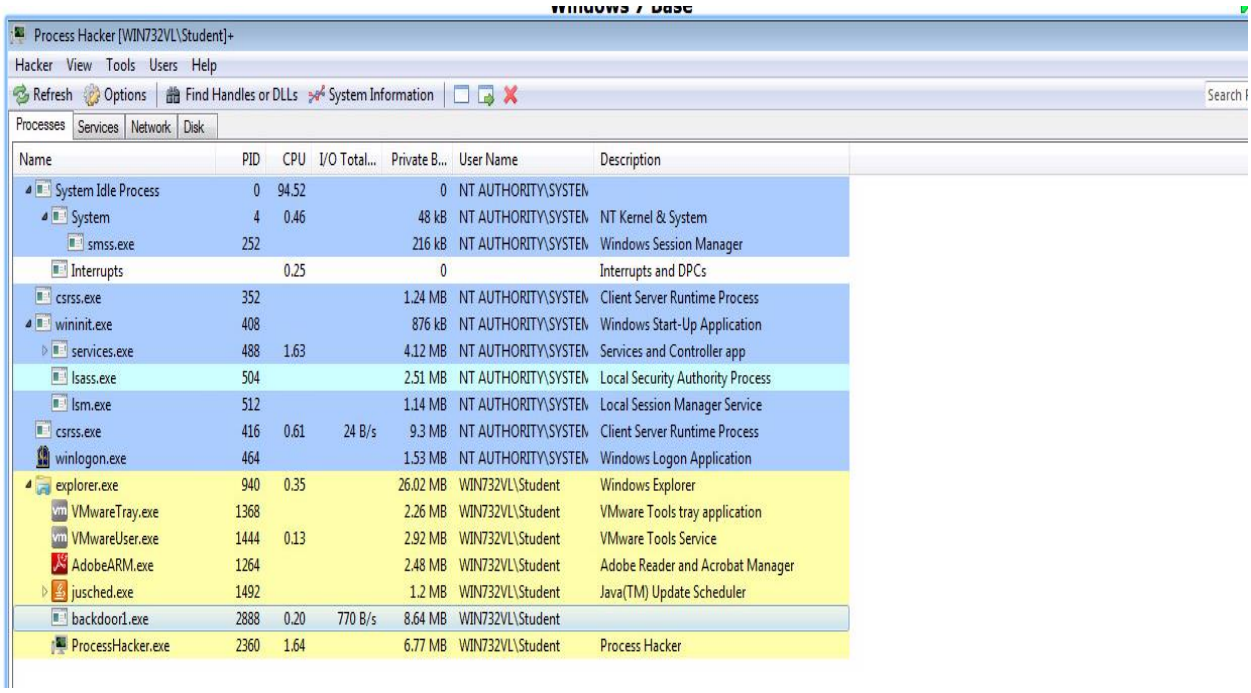

Figure 3 : Identified backdoor1.exe using the Process Hacker Tool

4. Analysing the possibilities, we found in the Network section of the Process Hacker that the backdoor1.exe established a TCP connection and kept listening all the time as shown in the Fig 4. We also verified all the other connections established and we confirmed that the other .exe files are the Windows processes.

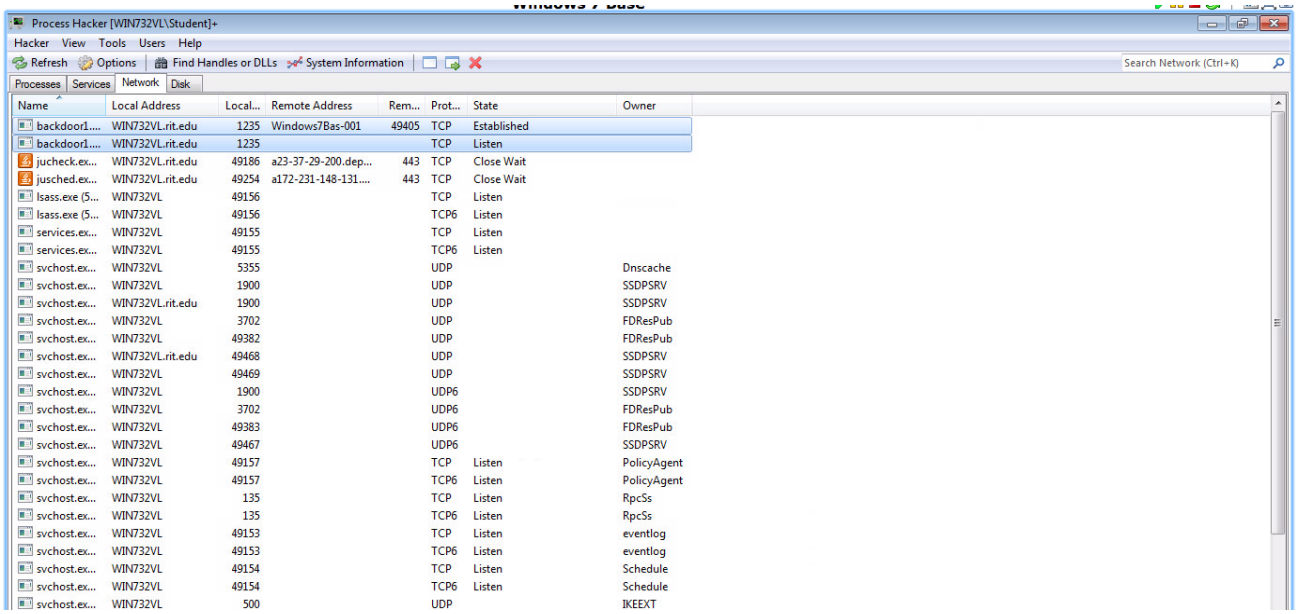

Figure 4 : Network connection established by the backdoor1.exe

5. Tracking the backdoor1.exe file, we also found the backdoor1.exe.log file. We had to change the folder options to unhide the files as all of these files were hidden. The log file contained information about the source file backdoor.pyw written in python, the network connection using socket and the socket's source file socket.pyc

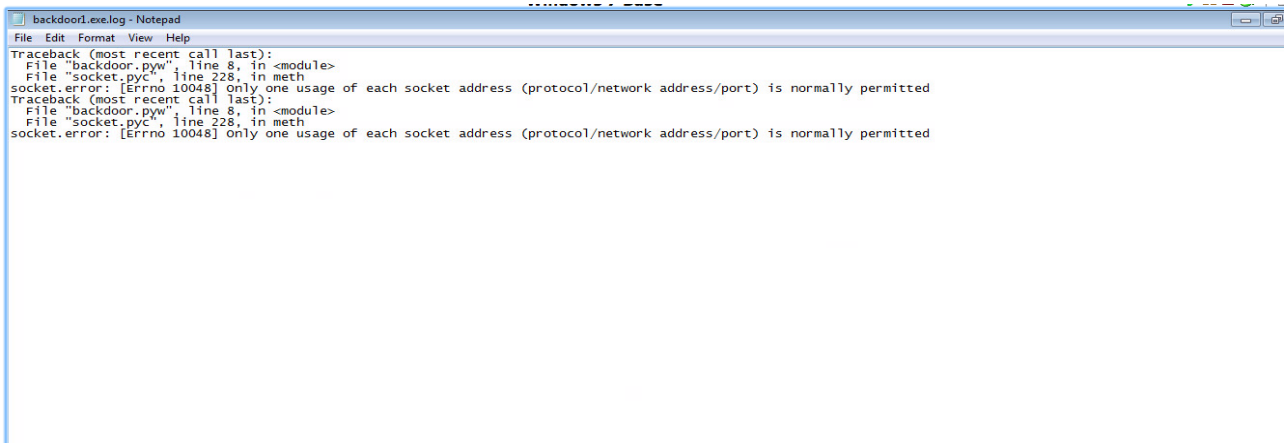

Figure 5 : Identified the malware's Log file

6. We then used the TCPView tool to identify where and how much data is been sent. We found that the backdoor1.exe established a TCP connection and was listening at the local port 1235. We noticed that whenever a key was pressed, the data packets were sent. In the below fig 6, we noticed that 9 bytes of data packets were sent to the address "windows7bas-001".

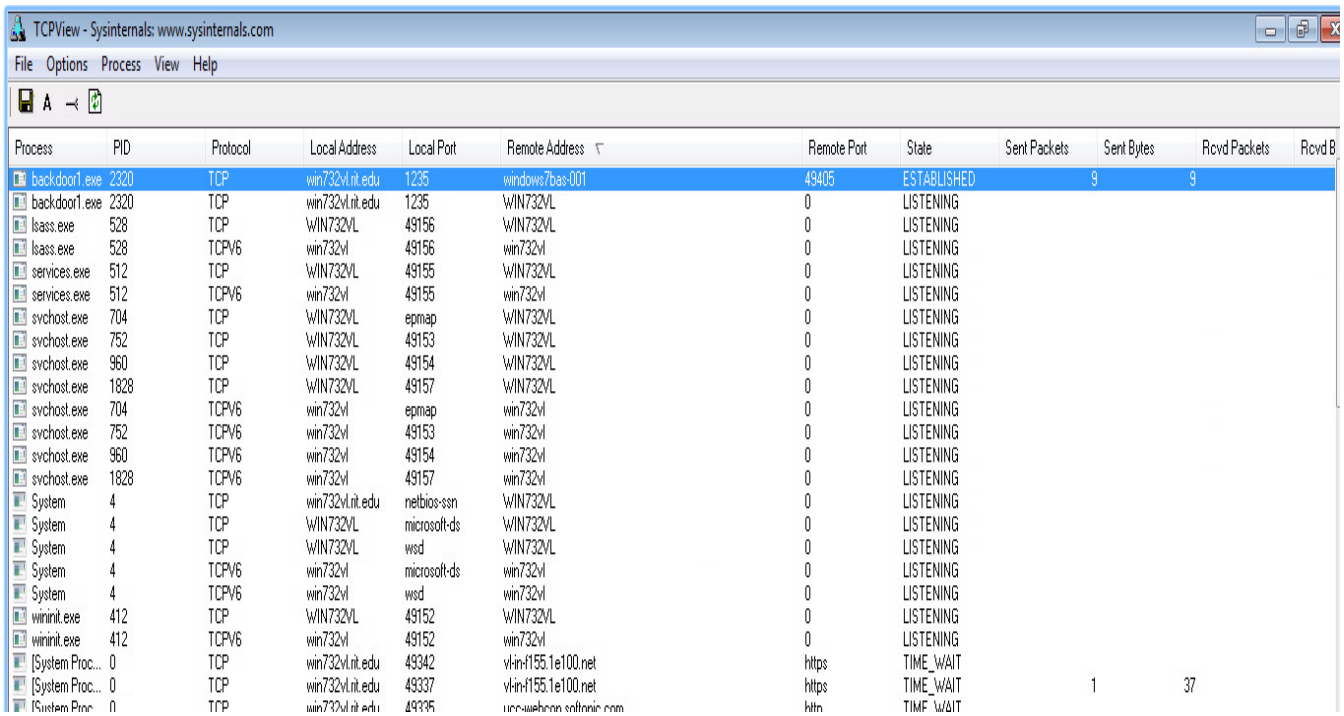

Figure 6 : Observed the Network connection details using TCPView

7. We resolved for the ip address using the TCPview tool and found the ip address as 192.168.206.248 to which the keystrokes are sent as shown in fig 7.

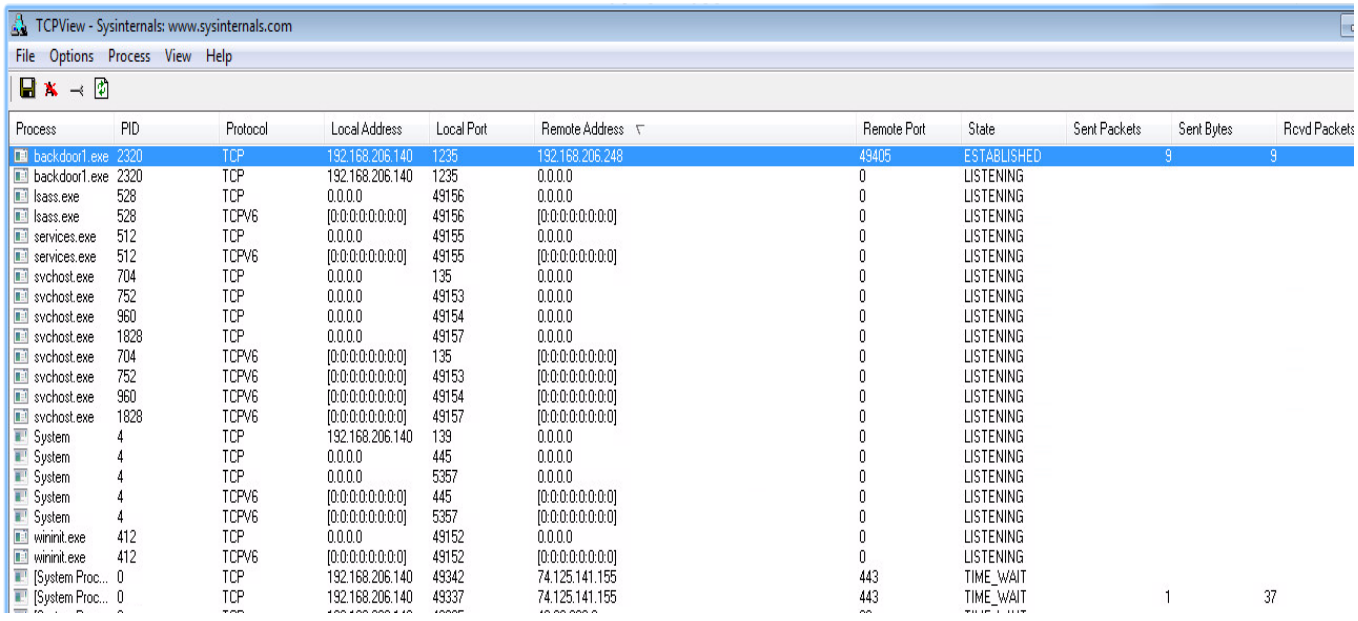

Figure 7 : Resolving the IP address to which the data is sent

We then tried to find the host/server name of the ip address. The ip address of the target machine is 192.168.206.248, which is a private ip address. The ip address of the virtual machine used to scan the target to obtain it's hostname is 192.168.11.128, which is also a

private ip address of the lab network we worked from. Hence when we tried to scan the target using Nmap tool, it scanned the machine which has the target's ip address in the Lab environment and displayed the results; but it didn't connect to the server where the keystrokes were sent as the server was in a separate private network. The test is shown in fig 8. So we were unable to resolve it.

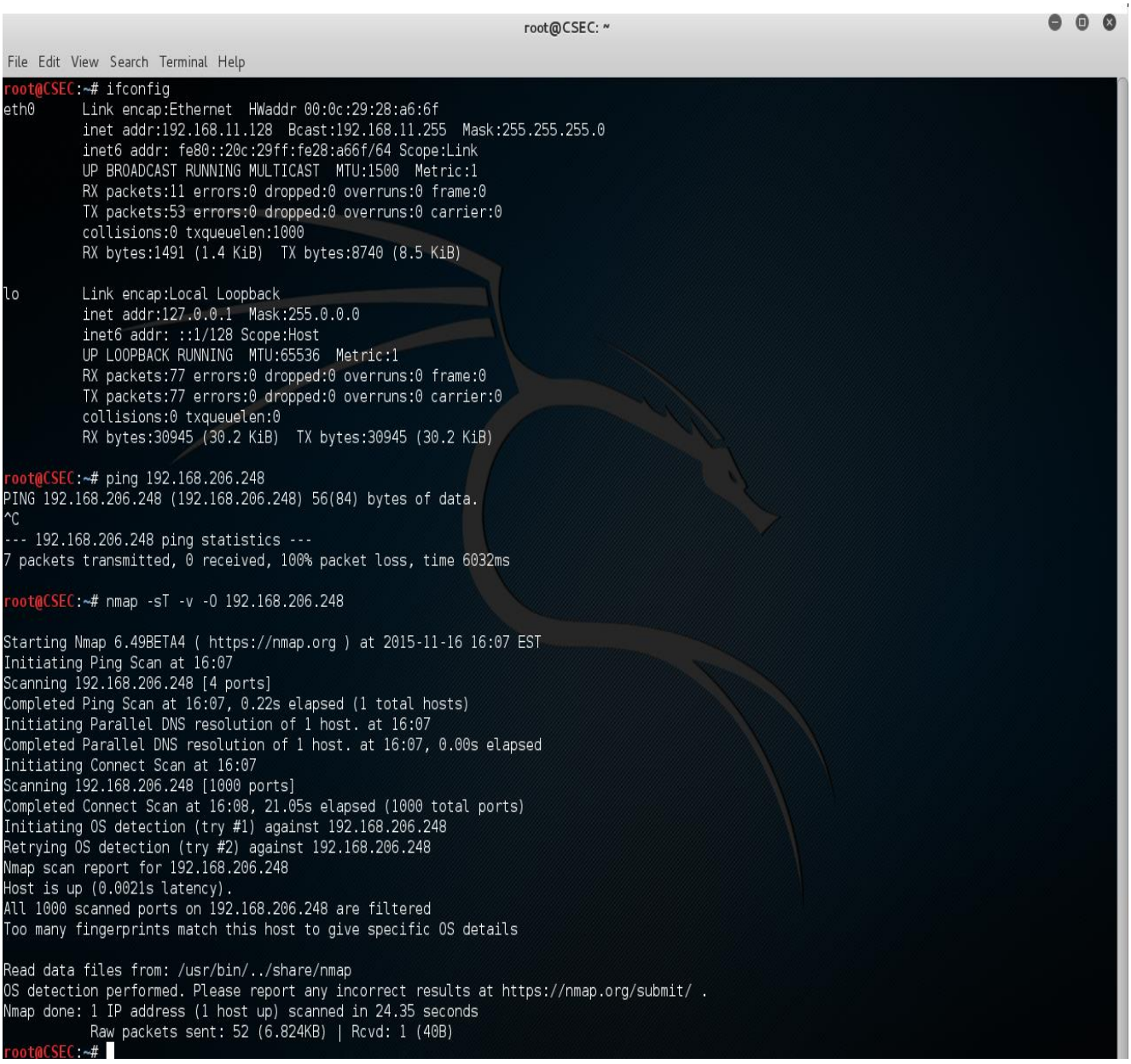

Figure 8: Using Ping and NMap to find the host/server name

Conclusion

Through this investigation phase, we learnt that detecting keyloggers is all about knowing what to look and where to look for.