Rootkit

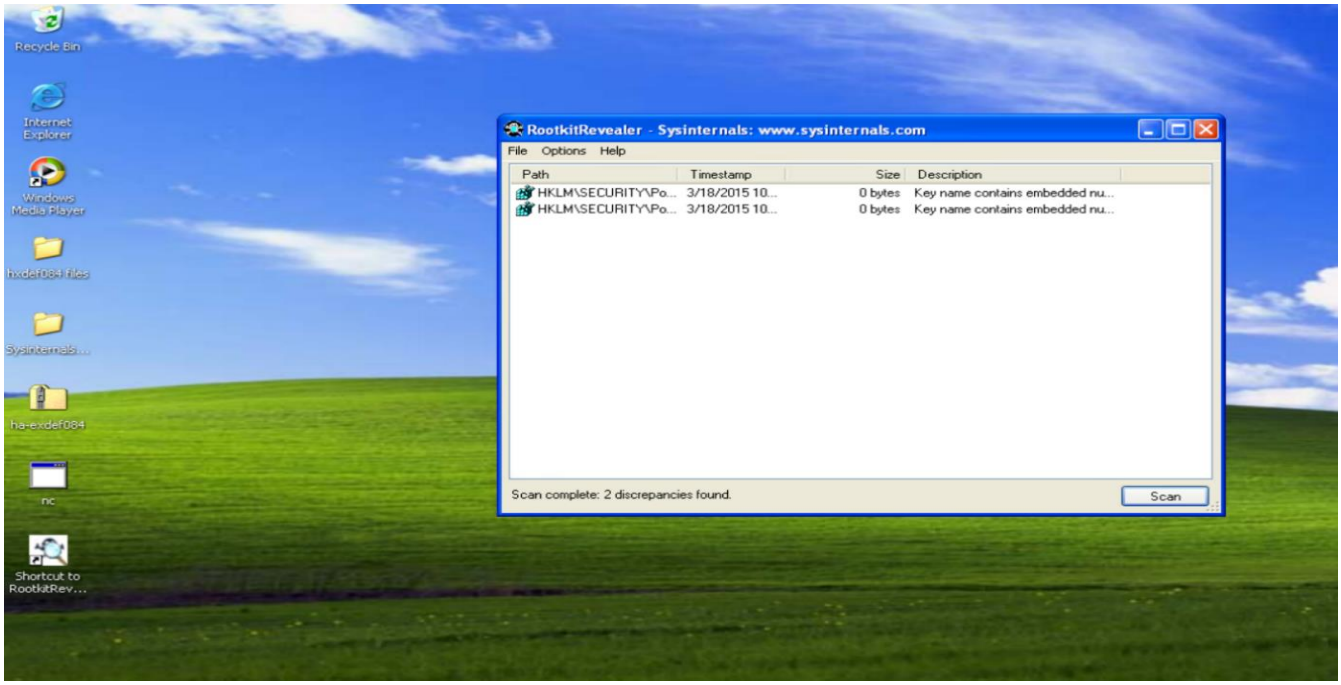

Figure 5.1

The main aim of this lab is to discover Windows rootkit using Rootkit Revealer tool. As seen in figure 5.1, we run the Rootkitrevealer tool and scan the system to check for suspicious activity. It is found that the system is clean.

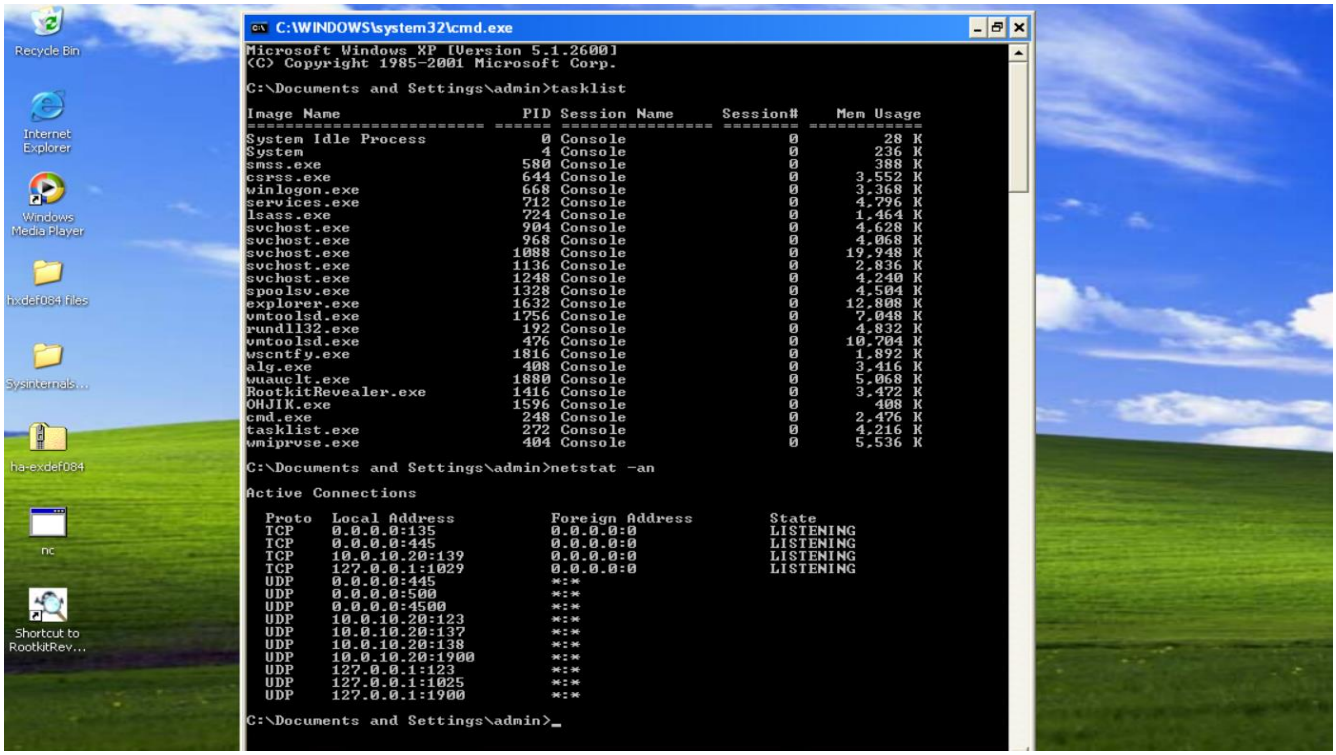

Figure 5.2

The command **tasklist** is used to find what processes are running in the system.

Then we will select a legitimate process to mimic. We aim to name our rootkit implant something that will not raise suspicion. I have chosen **a1g** making it similar to **alg** process.
The command **netstat -an** verifies which ports are currently open. I have chosen port number **1901** for the rootkit implant.

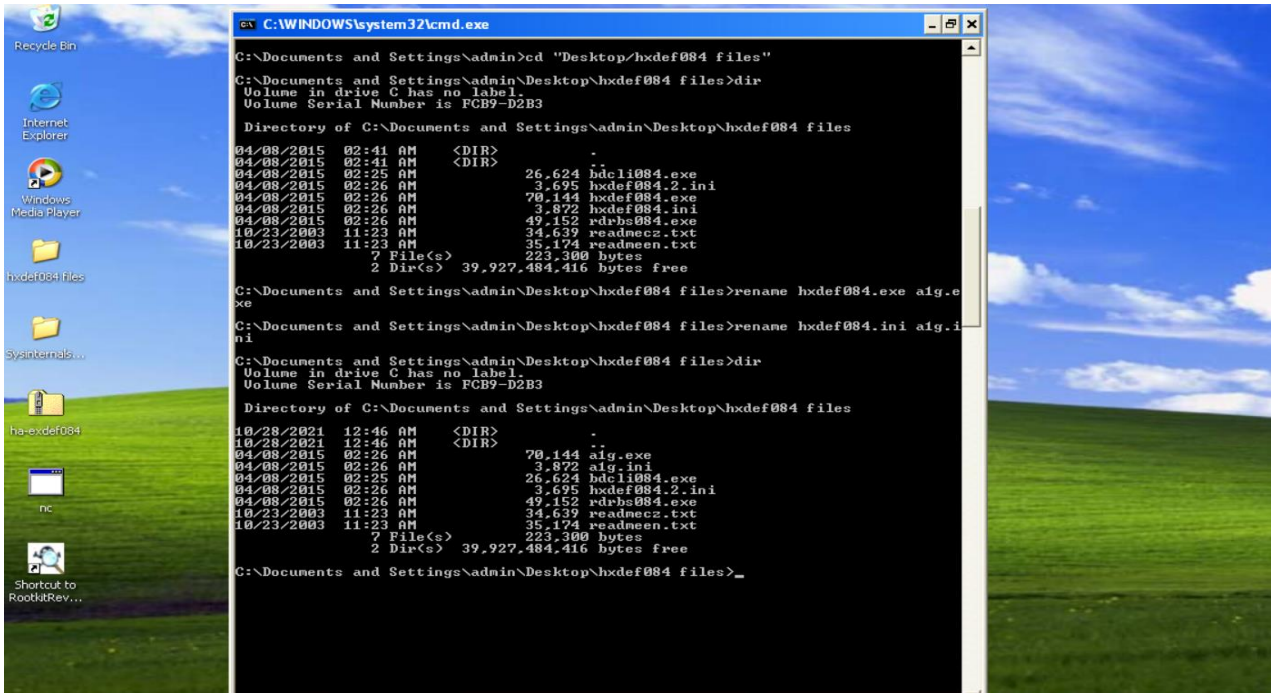

Figure 5.3

We are going to change the directory to:
C:\Documents and Settings\admin\Desktop\hxdef084 files
We need to rename the two files to mimic the process. The commands used are:
rename hxdef084.exe a1g.exe, **rename hxdef084.2.ini a1g.ini**

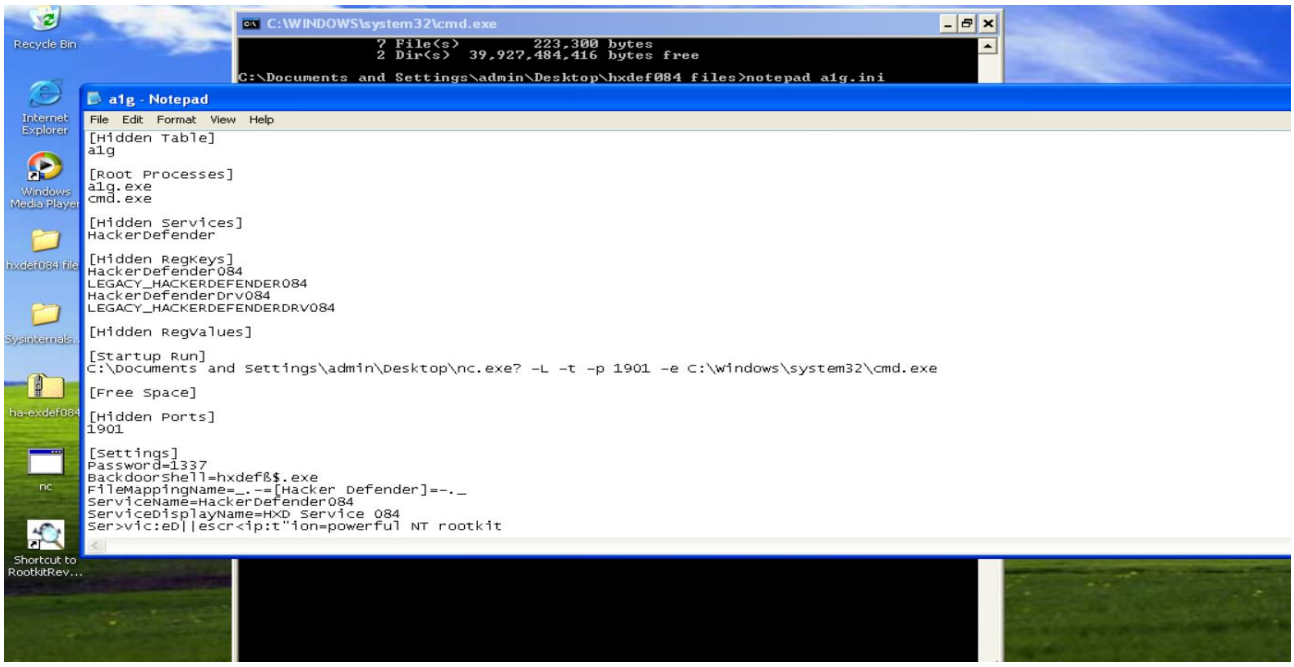

Figure 5.4

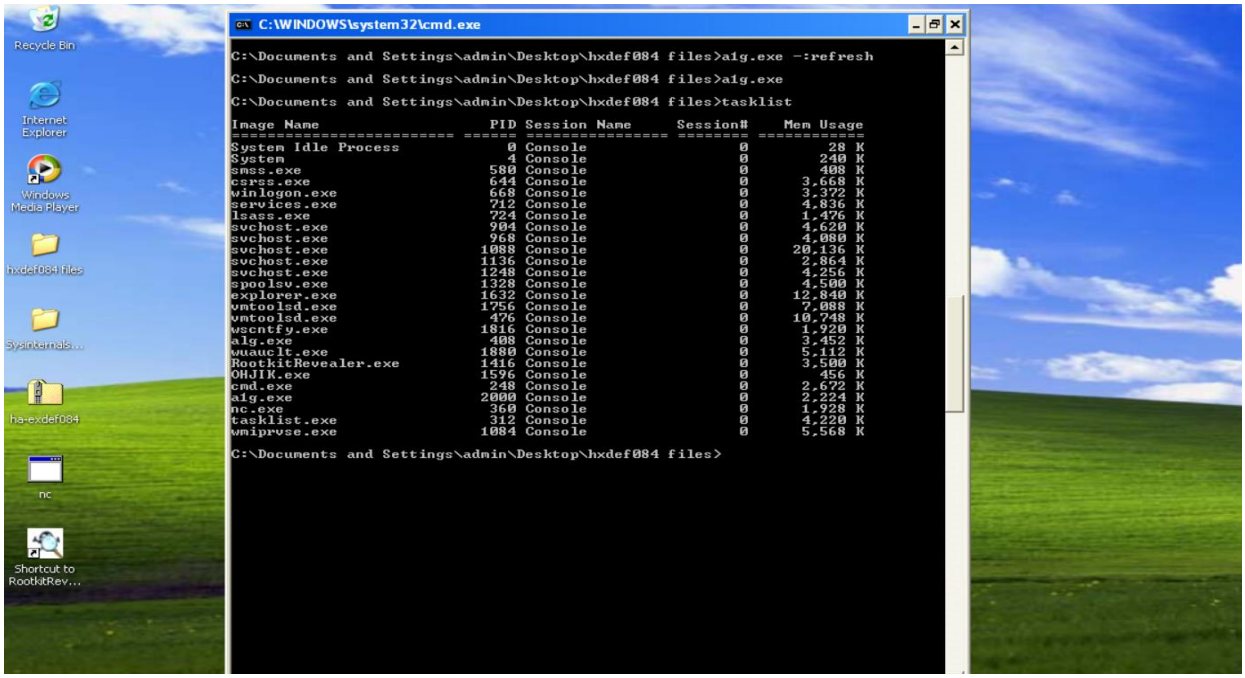

Figure 5.5

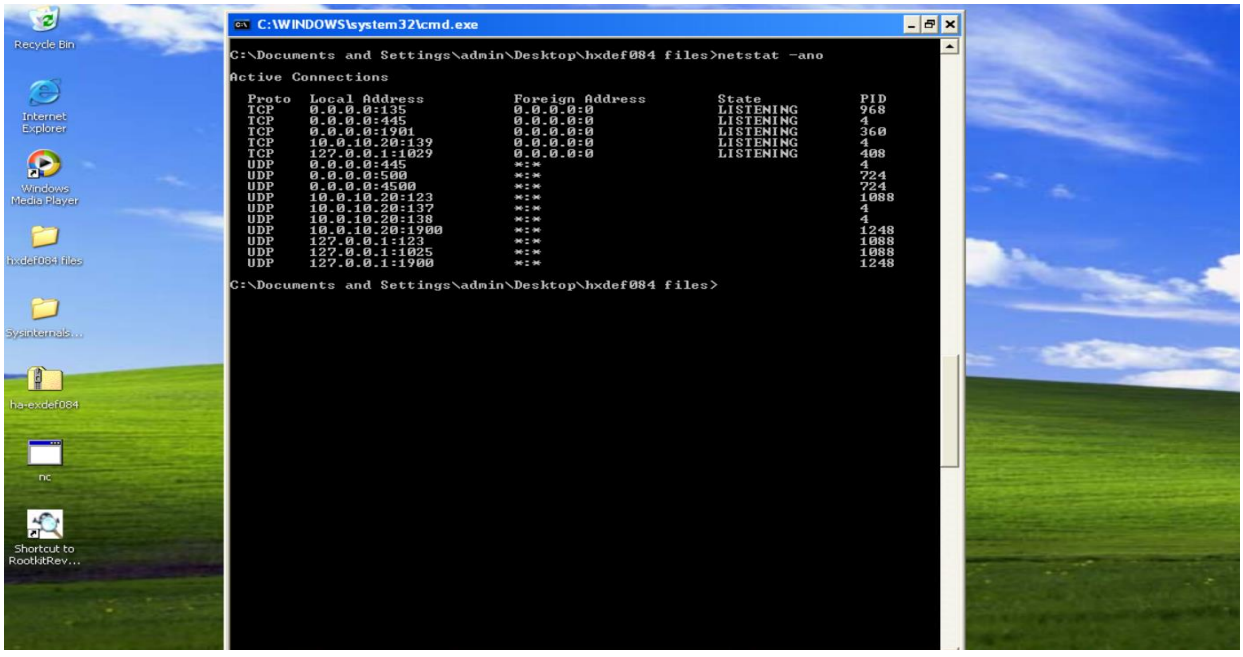

Figure 5.6

As seen in figure 5.4, we open the newly renamed initialization file and modify the name, root process and port. To load the modified initialization file to the memory, the following command is used: **a1g.exe -:refresh**. The command **a1g.exe** is used to run the executable rootkit. To verify that the alg.exe process is running, the tasklist command is used. To verify that the rootkit is listening to port 1901, **netstat -ano** command is used.

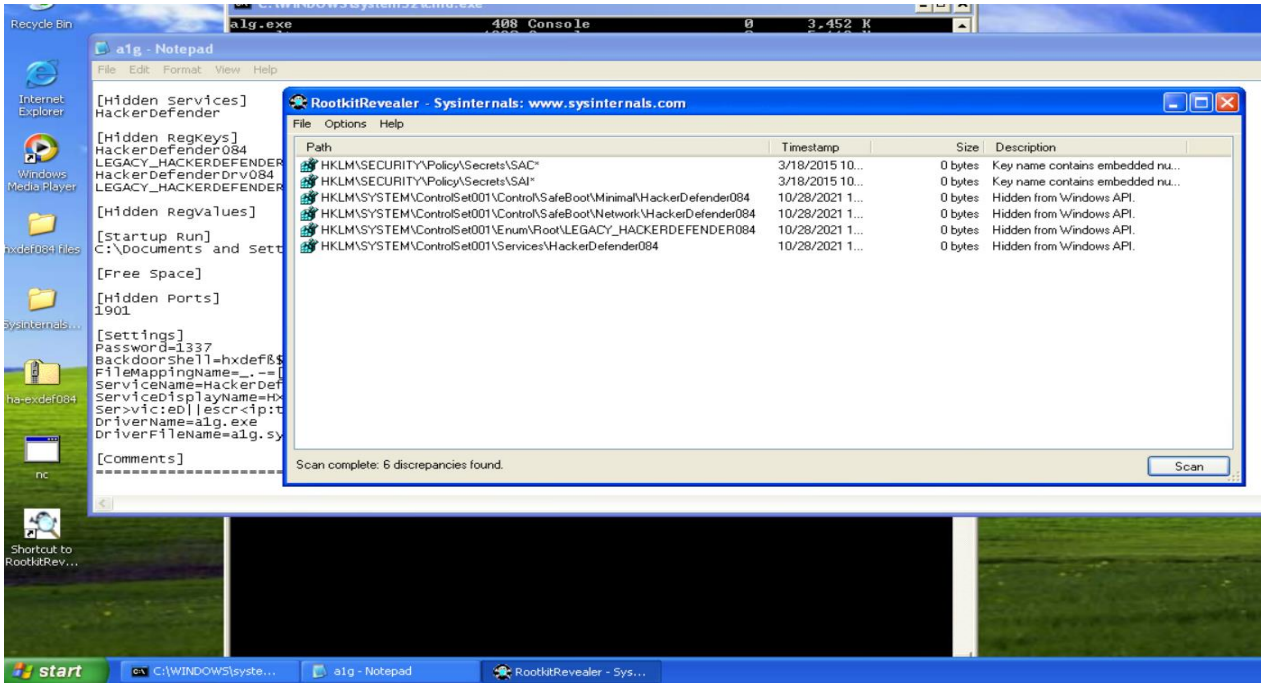

Figure 5.7

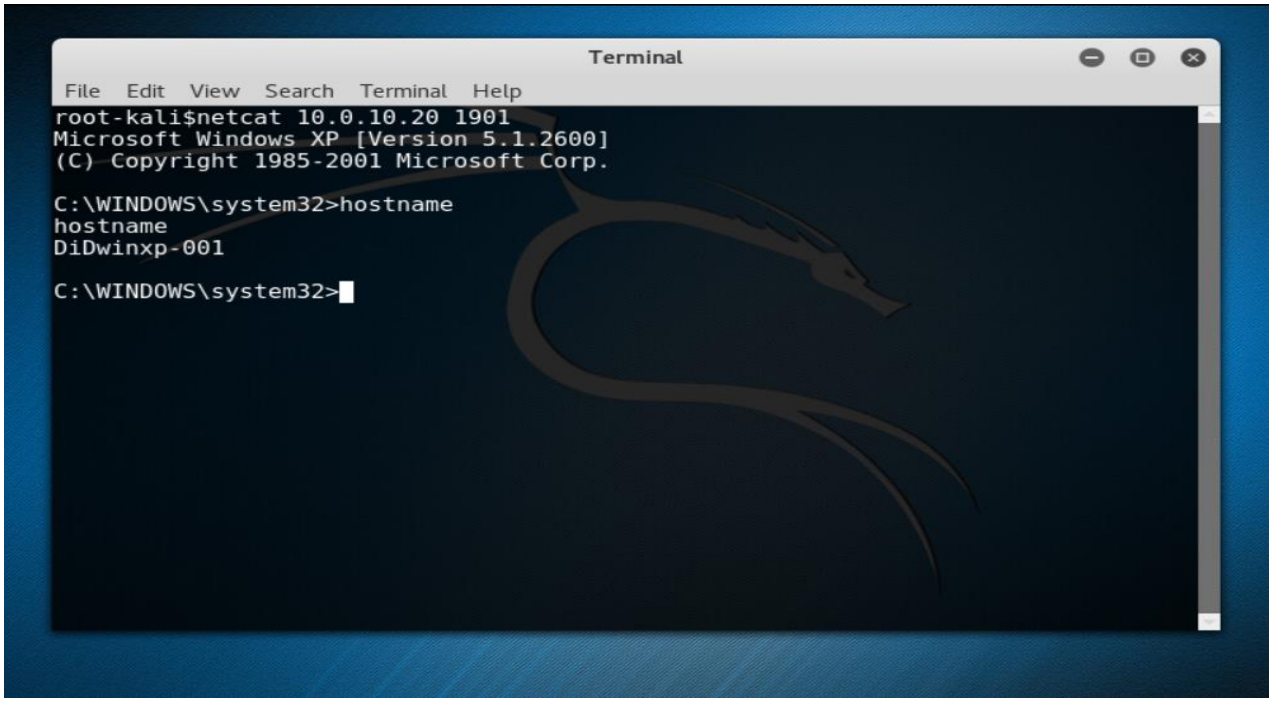

Figure 5.8

Again launching Rootkit Revealer tool and scanning to find the suspicious activity, the **HackerDefender084 Rootkit** is found on the system. Now logging into the kali linux system, we have verified that that rootkit is connected from a possible attack machine through the use of the netcat tool.

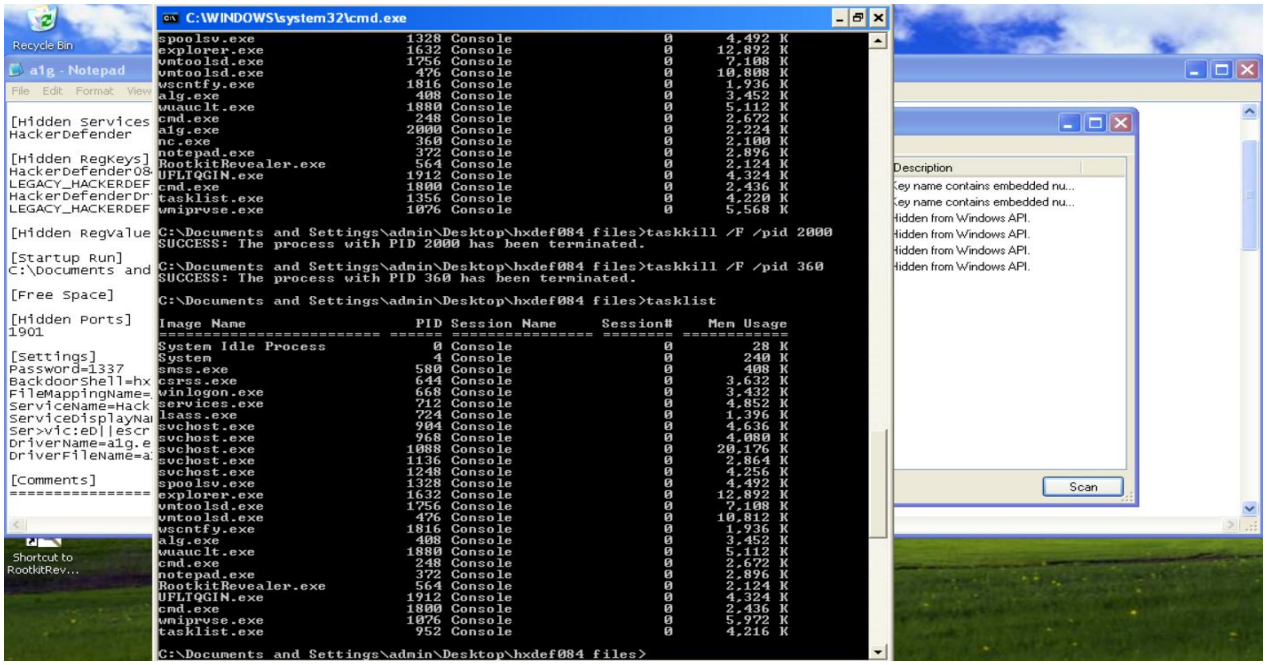

Figure 5.9

Now logging into the Windows machine again, the **tasklist** command is used to find suspicious processes. I have listed nc.exe and a1g.exe as the suspicious process.

To stop the suspicious processes, the following command is used by entering their #PID:

taskkill /F /pid PID#

We have also confirmed that the suspicious processes are stopped by using the command tasklist.

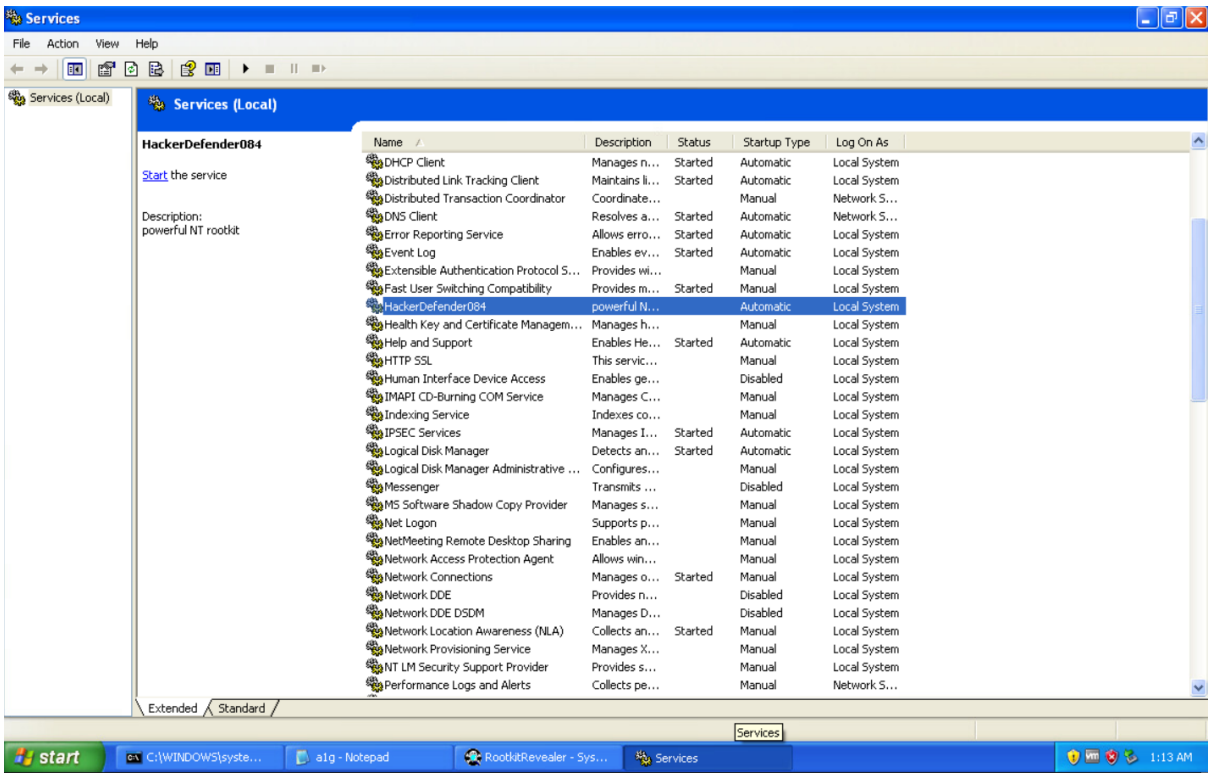

Figure 5.10

To check the HackerDefender084 service is stopped, running the windows service tool and found that the service is stopped.

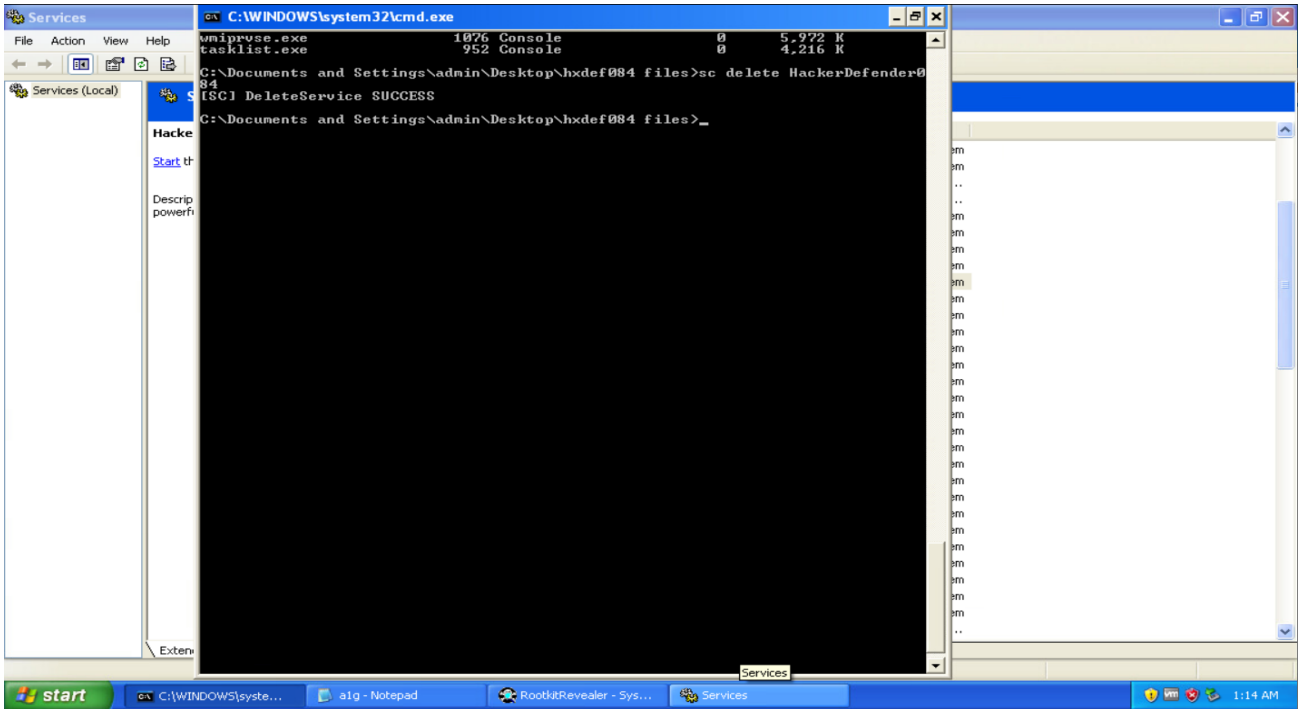

Figure 5.11

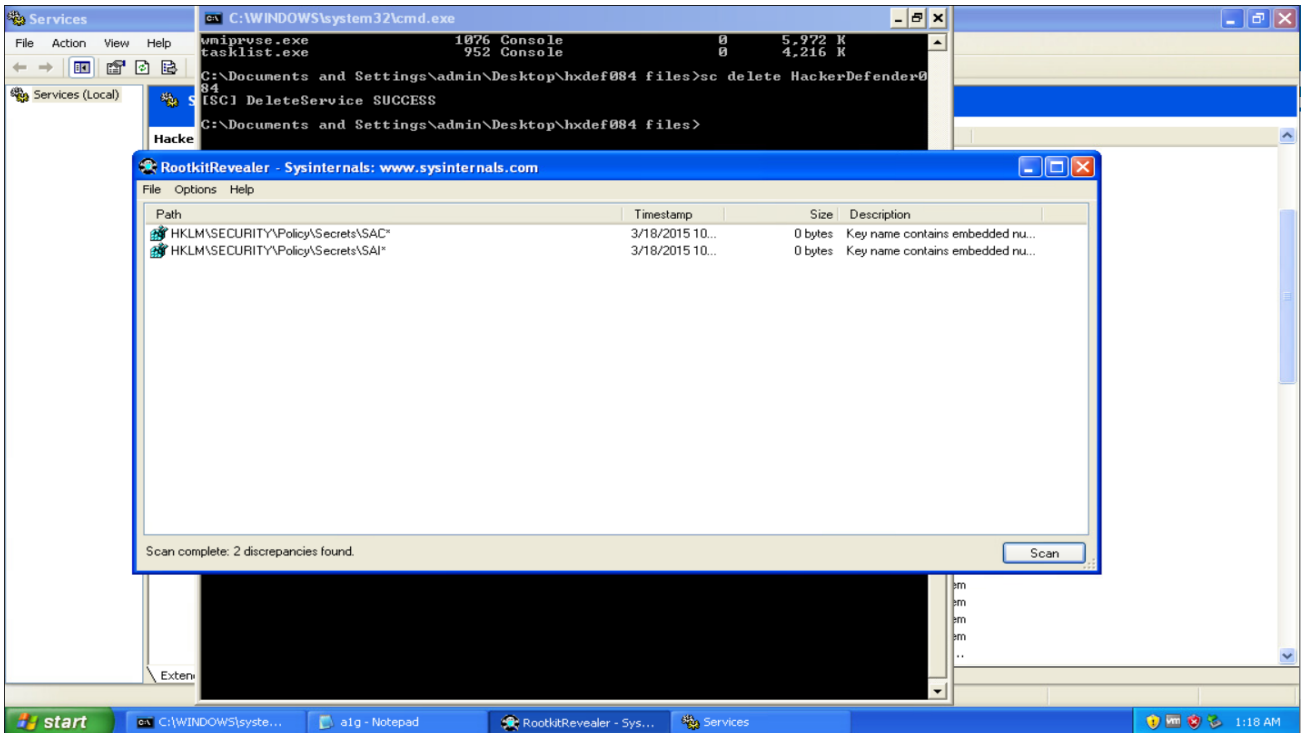

Figure 5.12

To delete the suspicious activity, the following command is used:

sc delete HackerDefender084

Also to check that the process is deleted, I have used the registry editor to check and found that the file is deleted.

As seen in figure 5.12, the scan is completed and the suspicious activity is not found as the system is clean.