

Rootkit

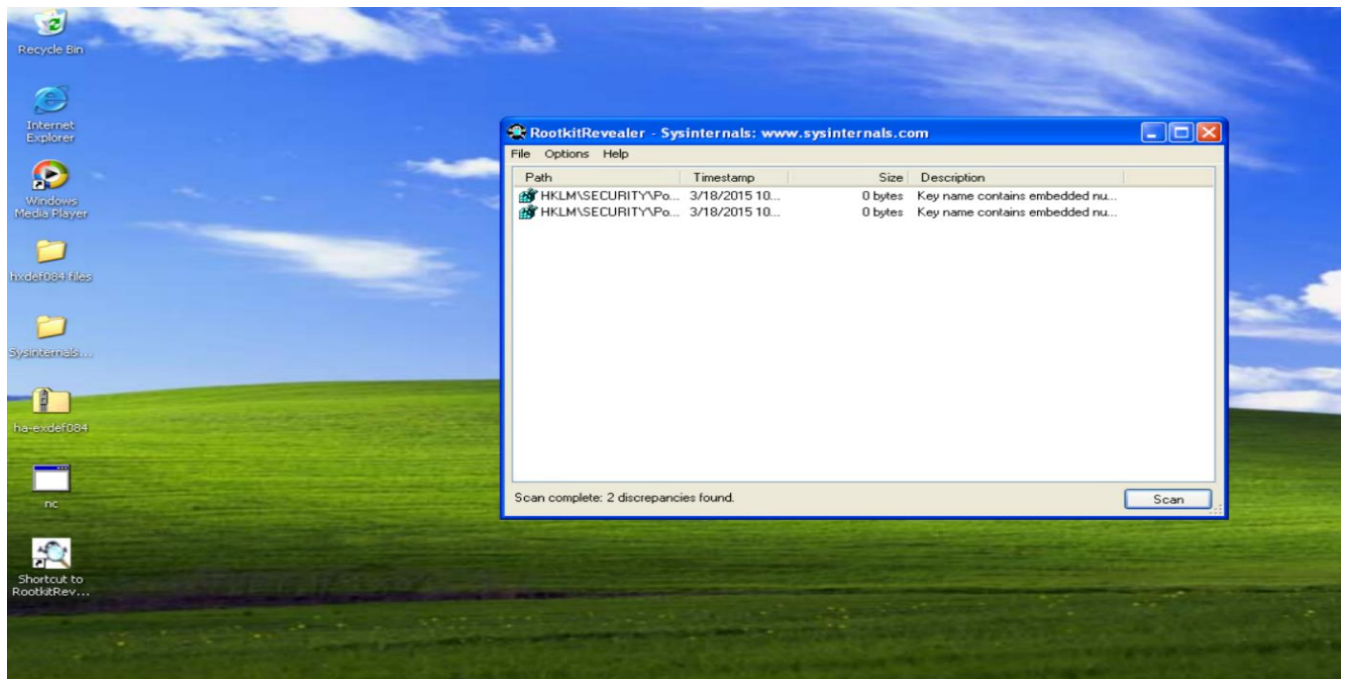


Figure 5.1

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.

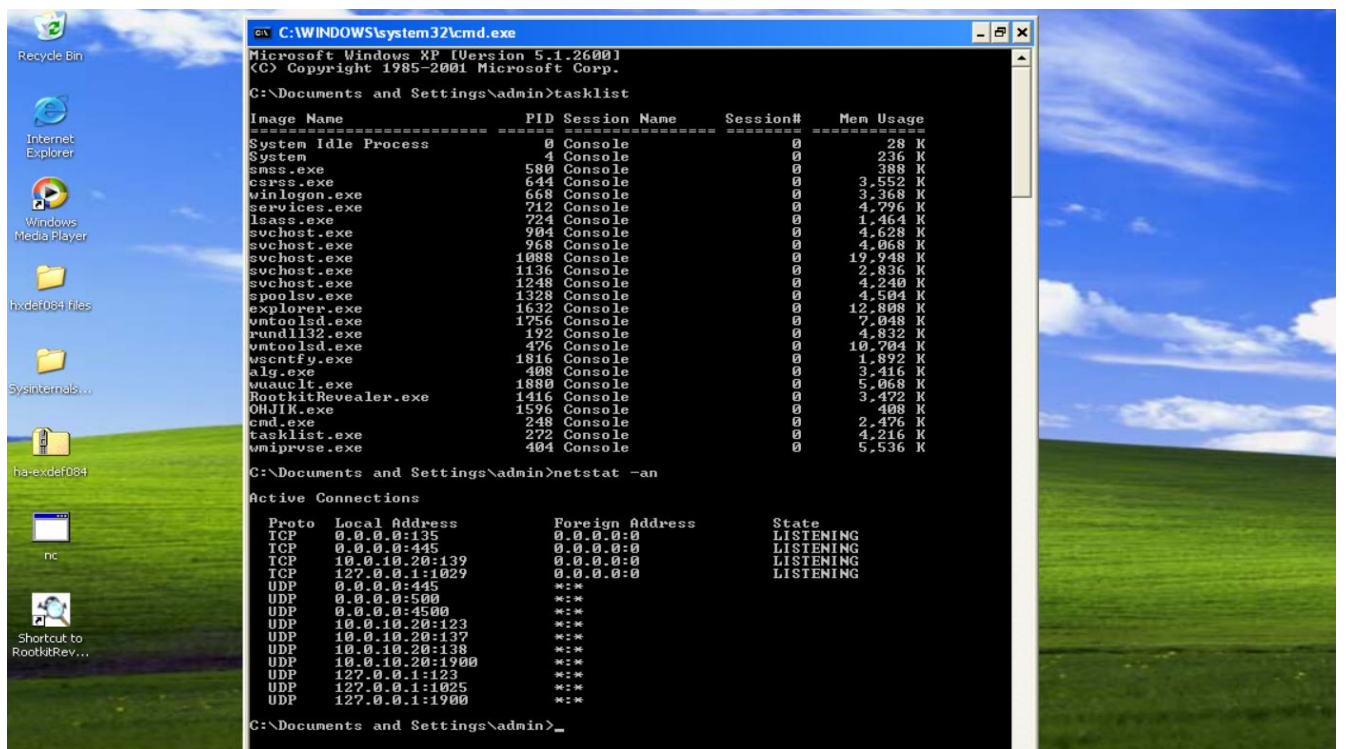


Figure 5.2

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

The screenshot shows a Windows XP desktop environment. The desktop background is the standard Windows XP blue and green wallpaper. Several icons are visible on the desktop: Recycle Bin, Internet Explorer, Windows Media Player, a folder named 'hxddef084 files', and a file named 'ha-exdef084'. A Windows XP taskbar is visible at the bottom of the screen. A Windows XP command prompt window is open, displaying the following commands and output:

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\admin>cd "Desktop\hxddef084 files"

C:\Documents and Settings\admin\Desktop\hxddef084 files>dir
Volume in drive C has no label.
Volume Serial Number is FCB9-D2B3

Directory of C:\Documents and Settings\admin\Desktop\hxddef084 files

04/08/2015  02:41 AM    <DIR>          .
04/08/2015  02:41 AM    <DIR>          ..
04/08/2015  02:25 AM             26,624 hcdli084.exe
04/08/2015  02:26 AM             3,695 hxddef084.2.ini
04/08/2015  02:26 AM            70,144 hxddef084.exe
04/08/2015  02:26 AM             3,872 hxddef084.ini
04/08/2015  02:26 AM            49,152 rdrbs084.exe
10/23/2003  11:23 AM            34,639 readnec2.txt
10/23/2003  11:23 AM            35,174 readneen.txt
               7 File(s)          223,300 bytes
               2 Dir(s)  39,927,484,416 bytes free

C:\Documents and Settings\admin\Desktop\hxddef084 files>rename hxddef084.exe aig.e
xe
C:\Documents and Settings\admin\Desktop\hxddef084 files>rename hxddef084.ini aig.i
ni
C:\Documents and Settings\admin\Desktop\hxddef084 files>dir
Volume in drive C has no label.
Volume Serial Number is FCB9-D2B3

Directory of C:\Documents and Settings\admin\Desktop\hxddef084 files

10/28/2021  12:46 AM    <DIR>          .
10/28/2021  12:46 AM    <DIR>          ..
04/08/2015  02:26 AM             70,144 aig.exe
04/08/2015  02:26 AM             3,872 aig.ini
04/08/2015  02:25 AM            26,624 bcdli084.exe
04/08/2015  02:26 AM             3,695 hxddef084.2.ini
04/08/2015  02:26 AM            49,152 rdrbs084.exe
10/23/2003  11:23 AM            34,639 readnec2.txt
10/23/2003  11:23 AM            35,174 readneen.txt
               7 File(s)          223,300 bytes
               2 Dir(s)  39,927,484,416 bytes free

C:\Documents and Settings\admin\Desktop\hxddef084 files>_
```

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



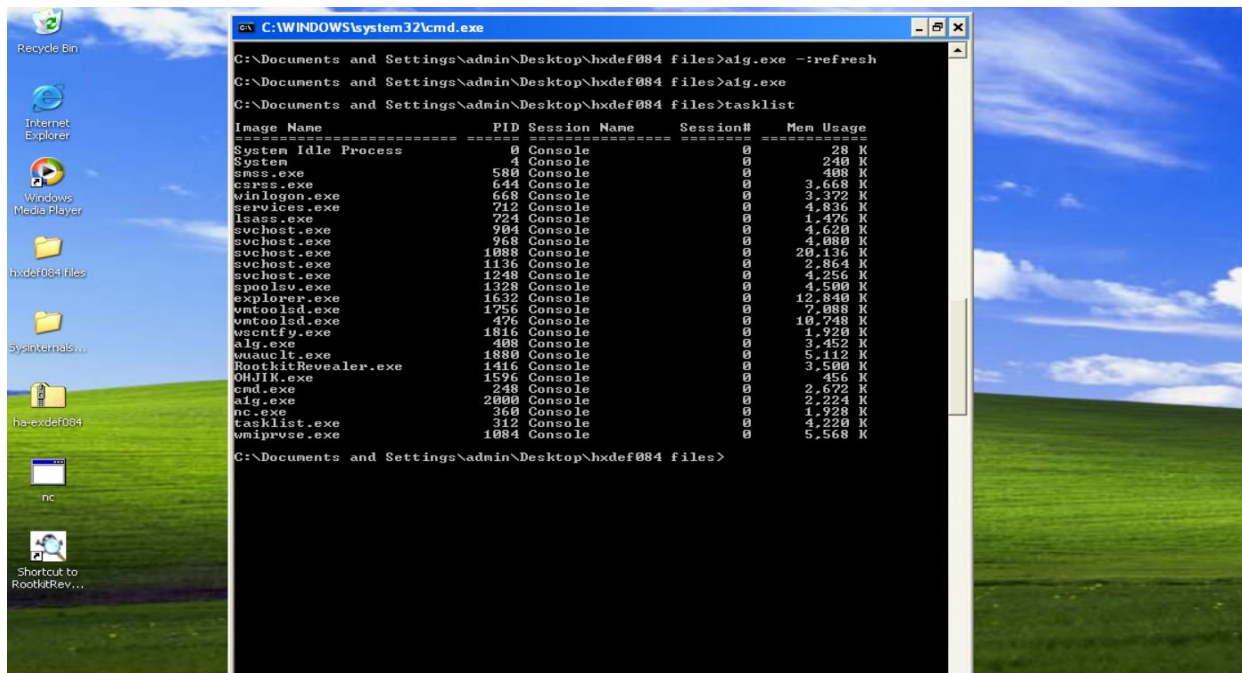


Figure 5.5

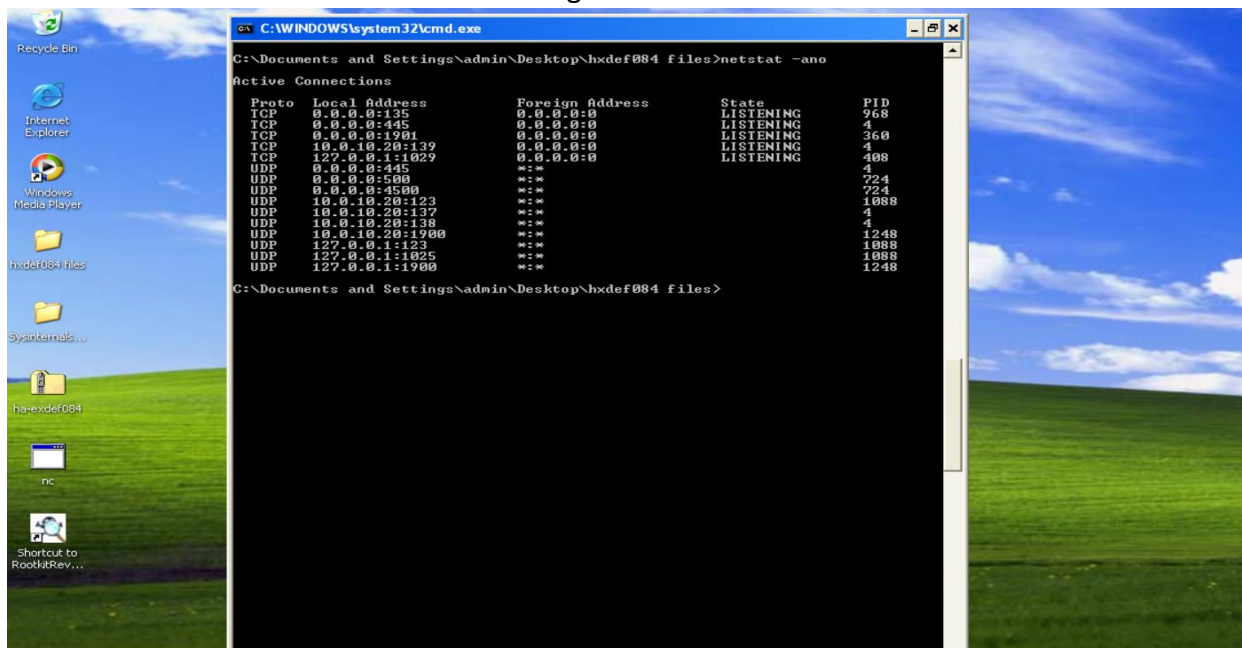


Figure 5.6

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: **aig.exe -:refresh**. The command **aig.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.

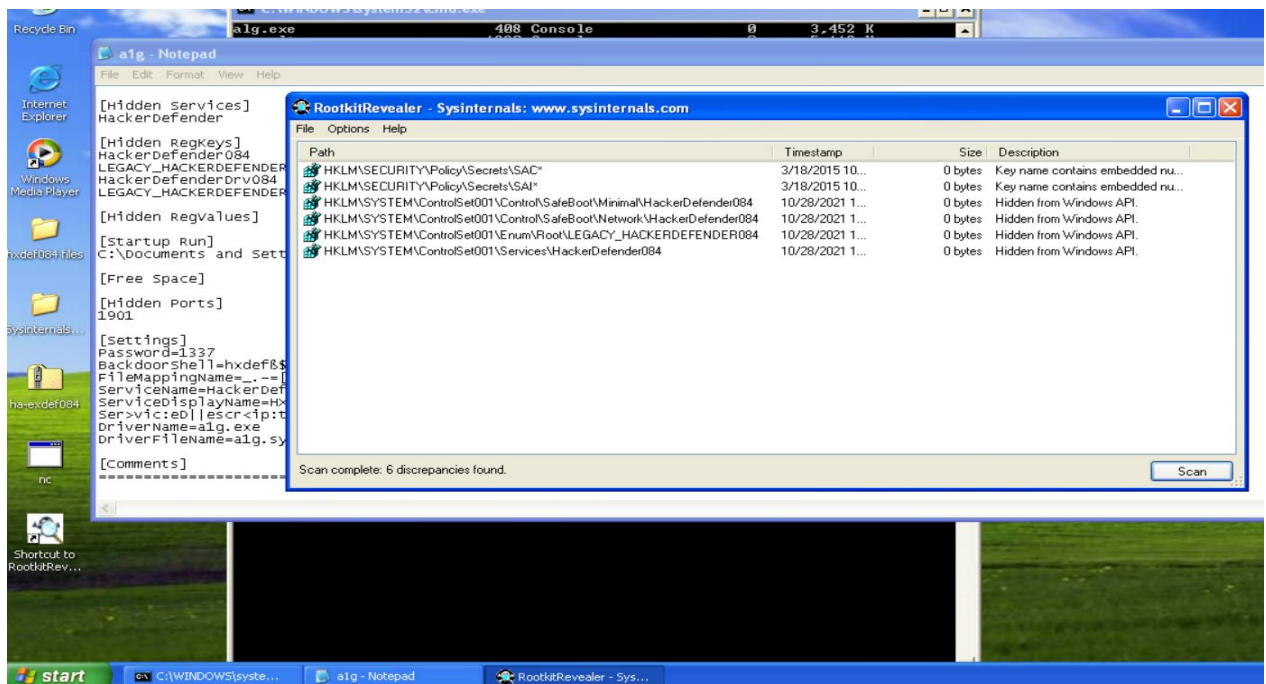


Figure 5.7

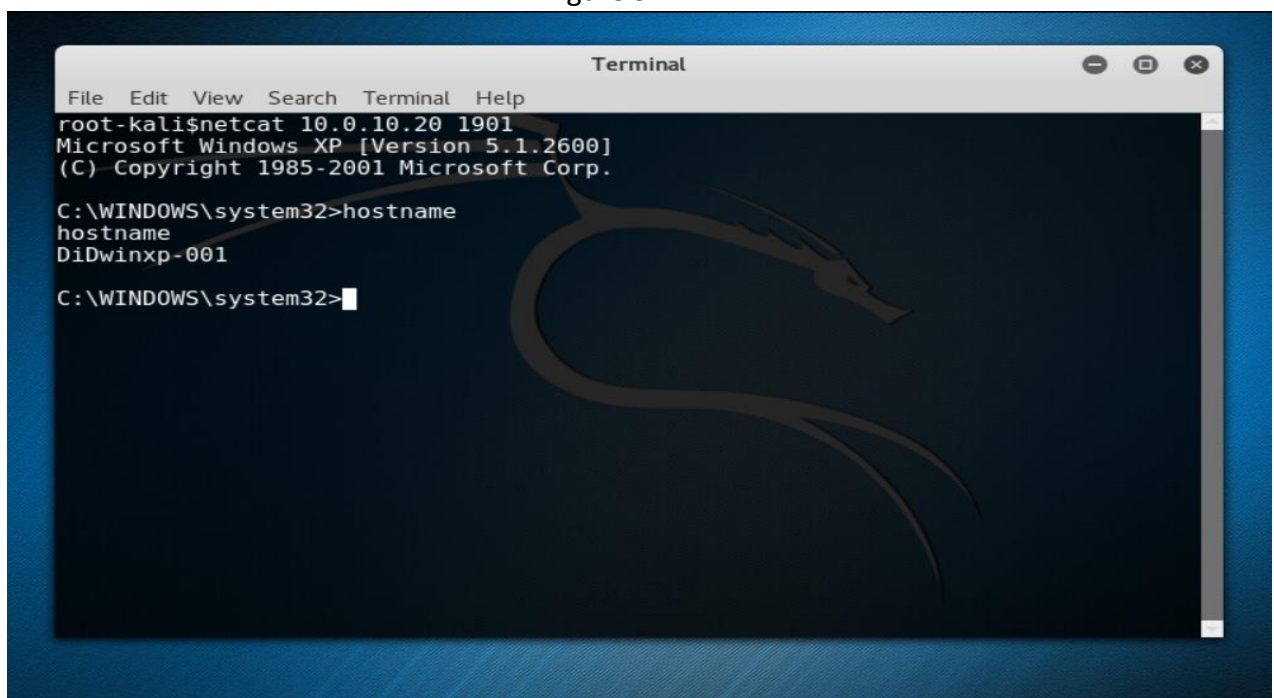


Figure 5.8

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.

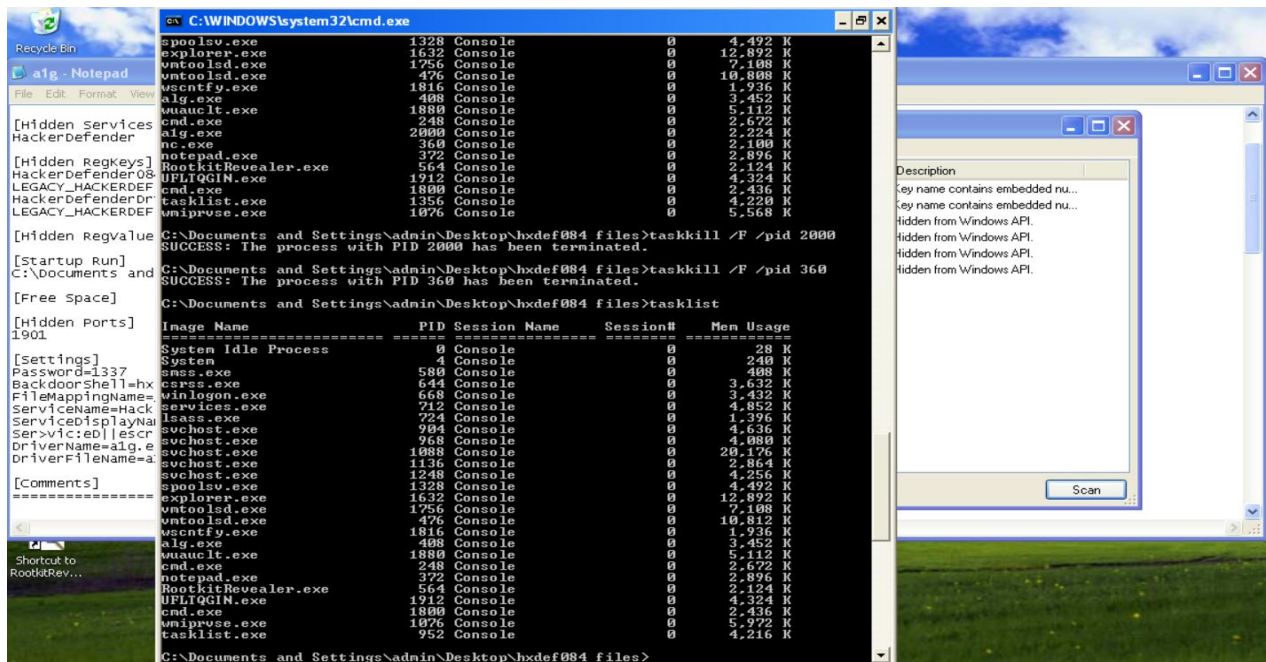


Figure 5.9

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

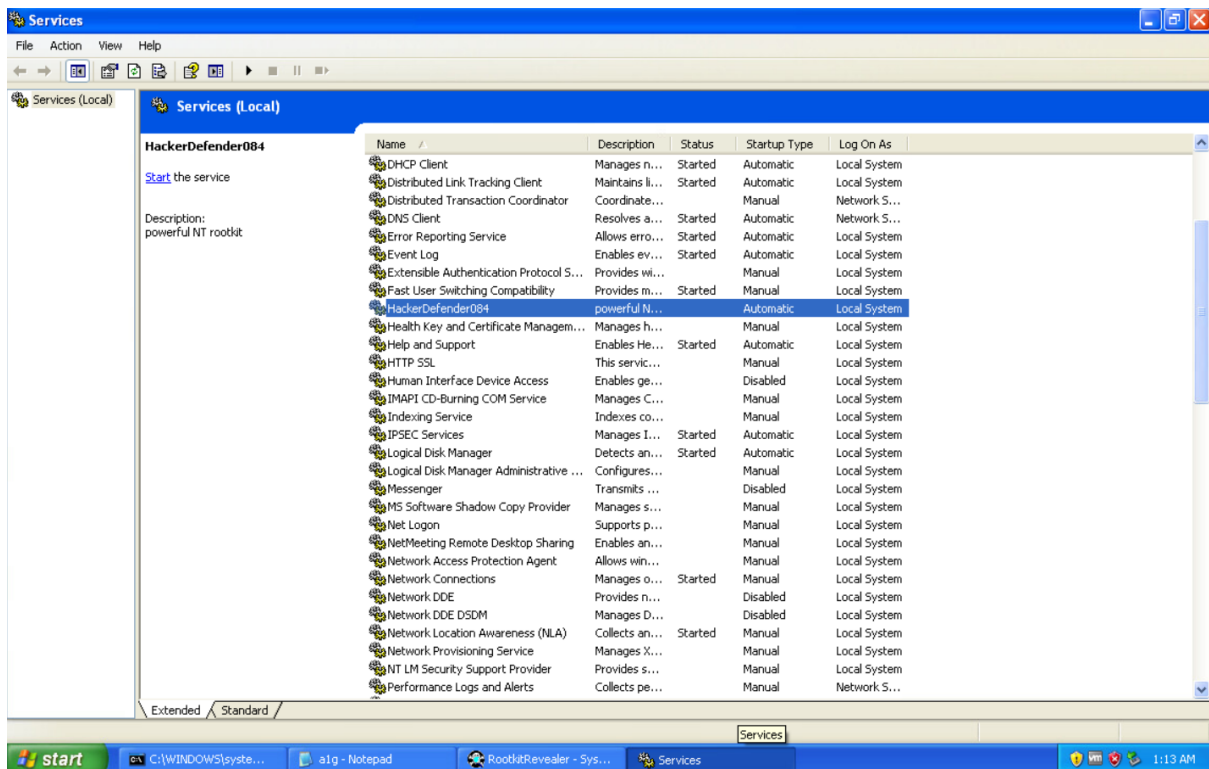


Figure 5.10

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

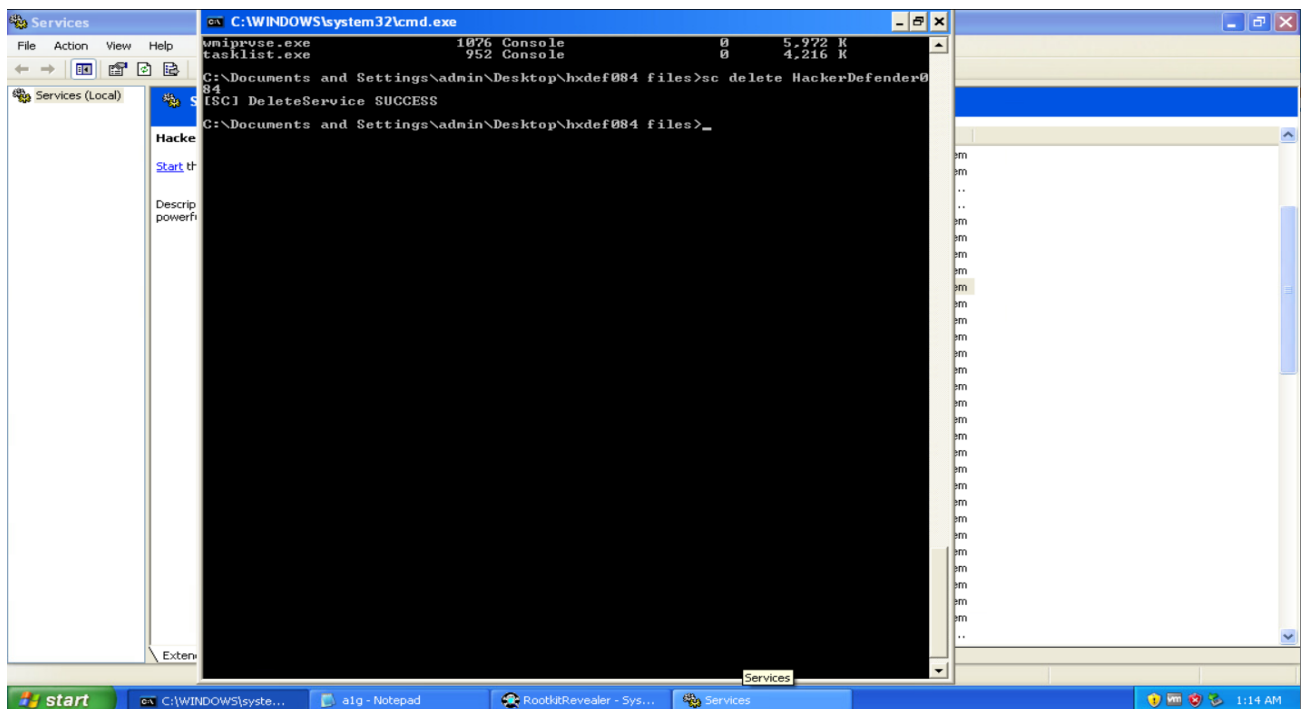


Figure 5.11

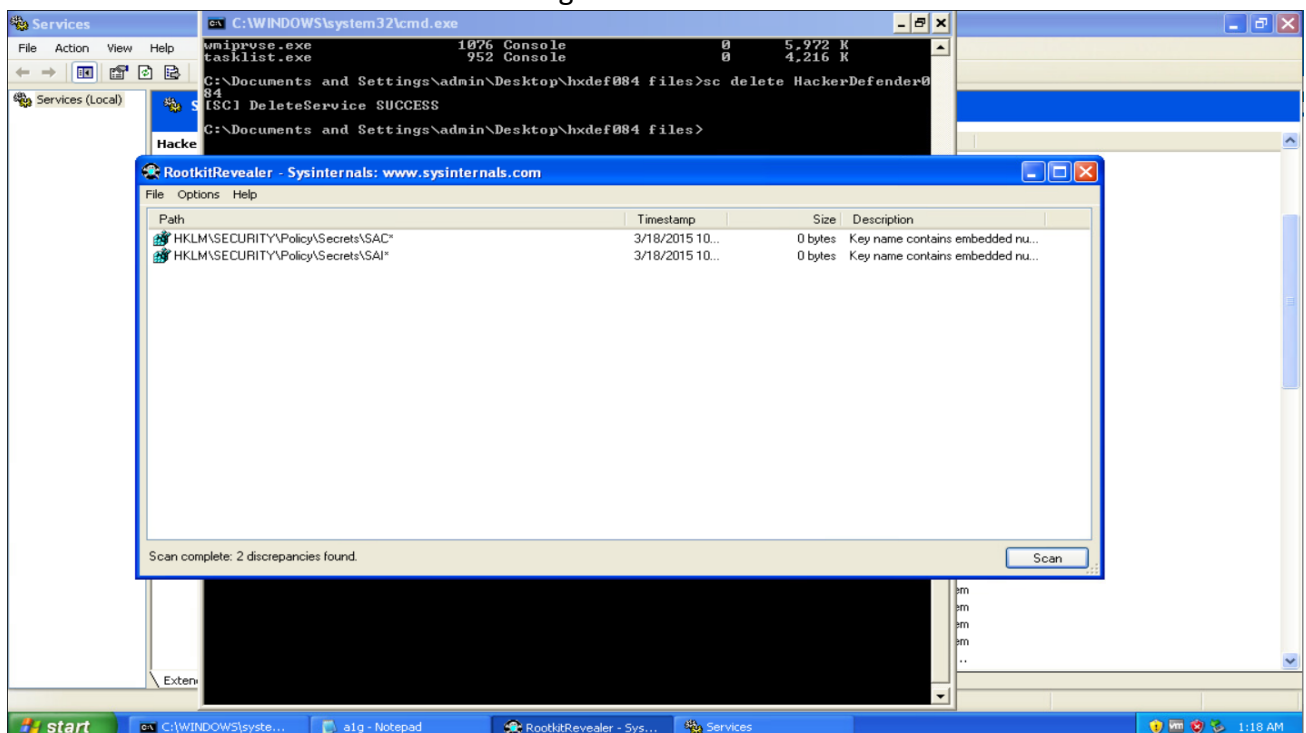


Figure 5.12

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.