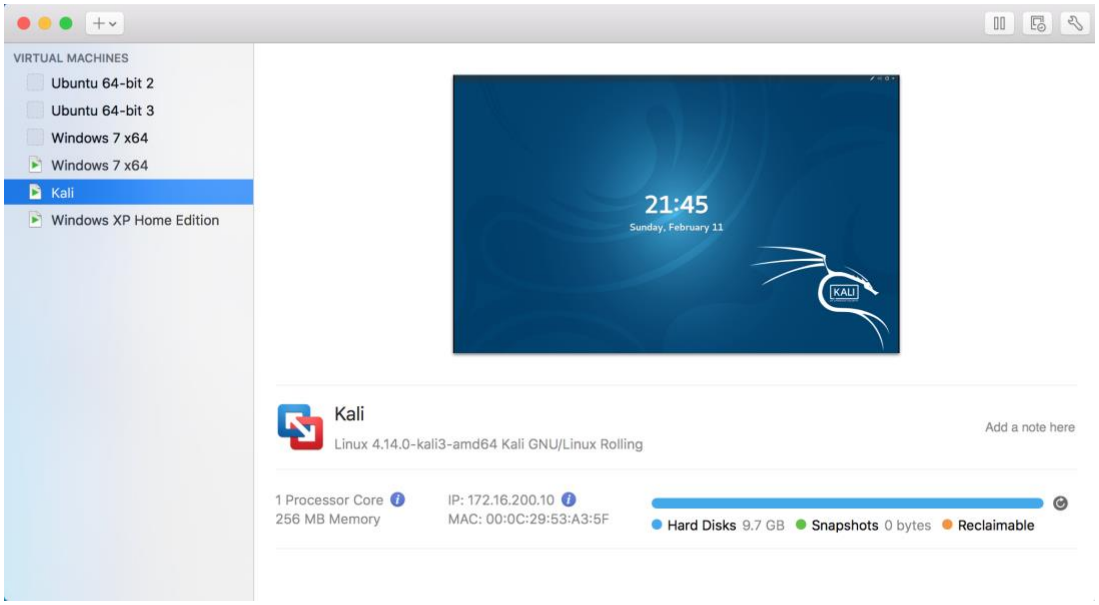
Dynamic Analysis Environment Setup

1) The following are the IP addresses of the virtual machines setup
Windows 7 VM: 172:16:200:131
Kali VM: 172:16:200:10
Host only adapter: 172:16:200:1

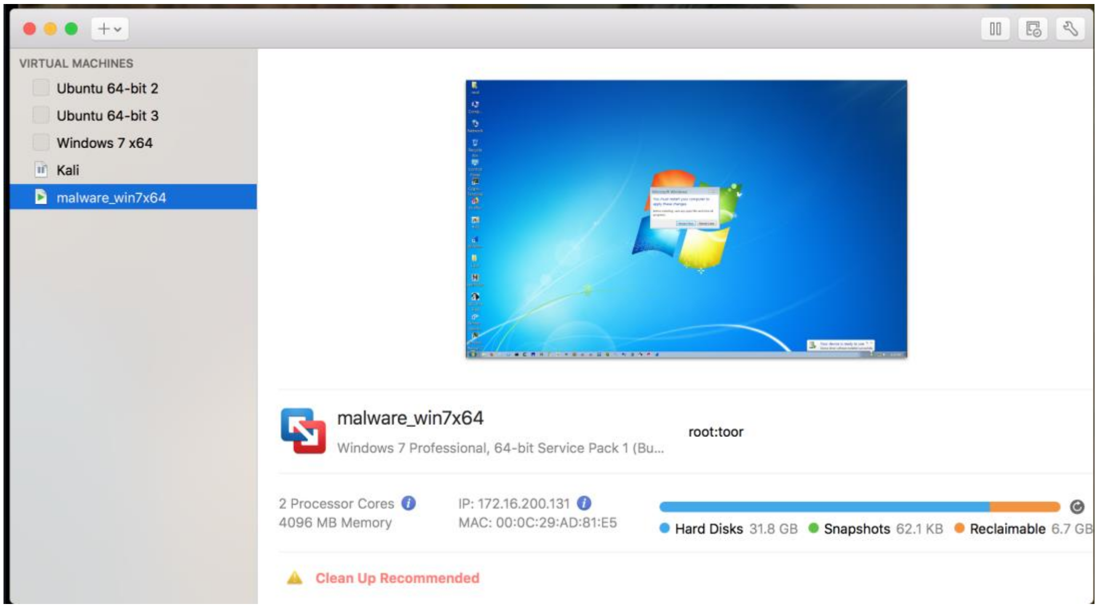


Kali
Linux 4.14.0-kali3-amd64 Kali GNU/Linux Rolling

1 Processor Core
256 MB Memory

IP: 172.16.200.10
MAC: 00:0C:29:53:A3:5F

Hard Disks 9.7 GB Snapshots 0 bytes Reclaimable



malware_win7x64
Windows 7 Professional, 64-bit Service Pack 1 (Bu...

root:toor

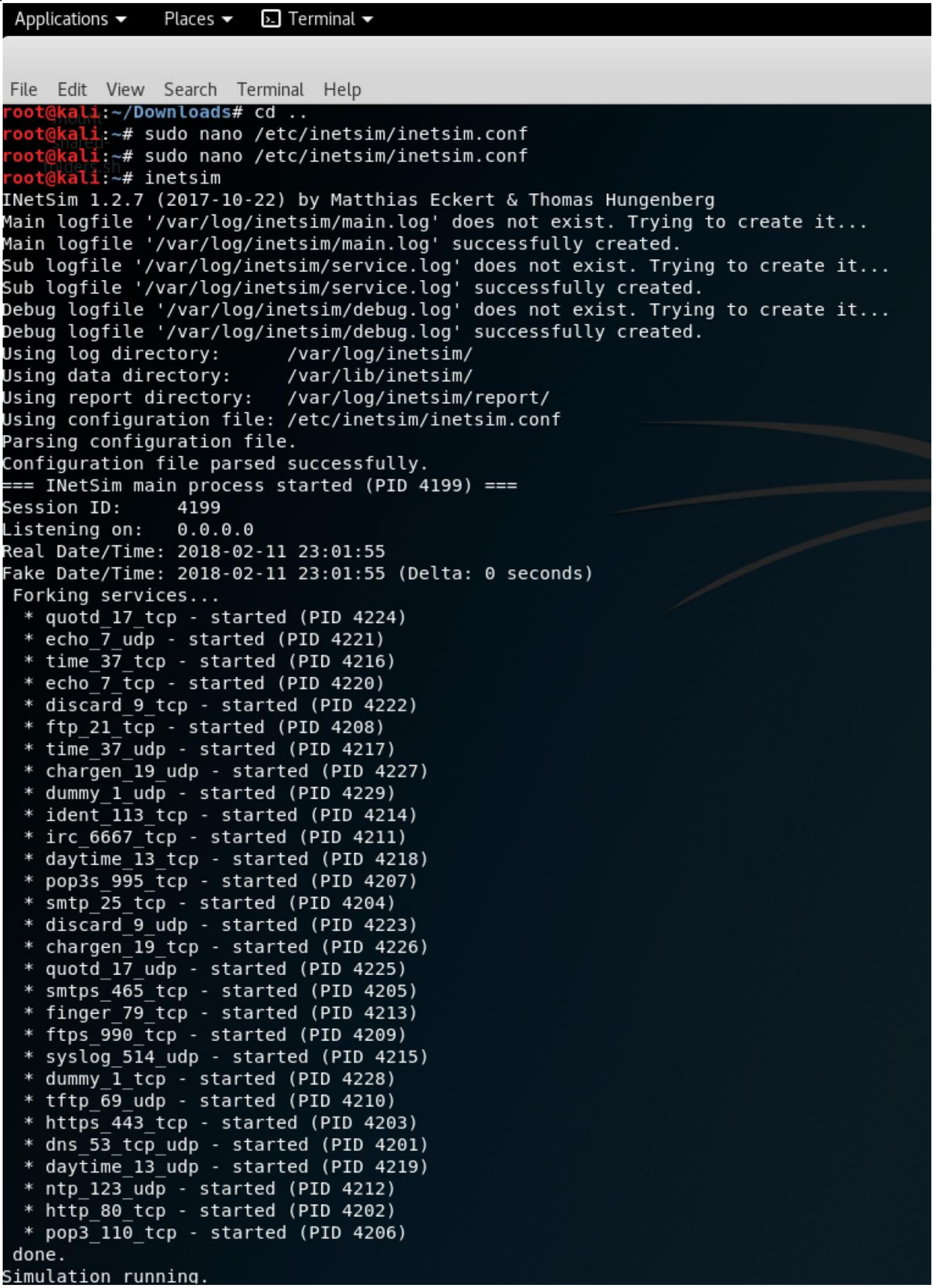
2 Processor Cores
4096 MB Memory

IP: 172.16.200.131
MAC: 00:0C:29:AD:81:E5

Hard Disks 31.8 GB Snapshots 62.1 KB Reclaimable 6.7 GB

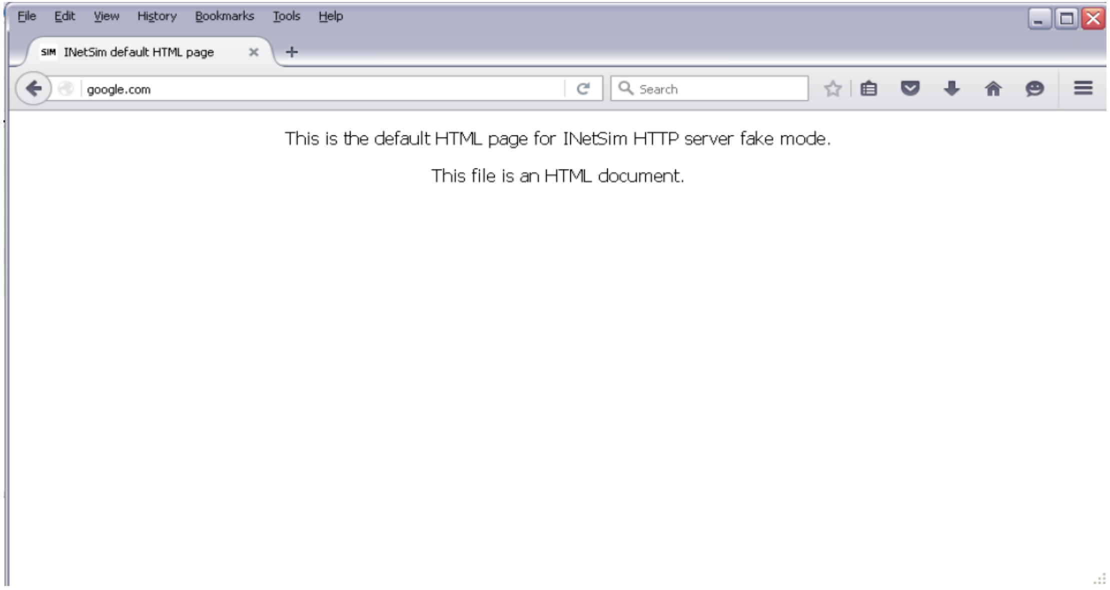
Clean Up Recommended

2)



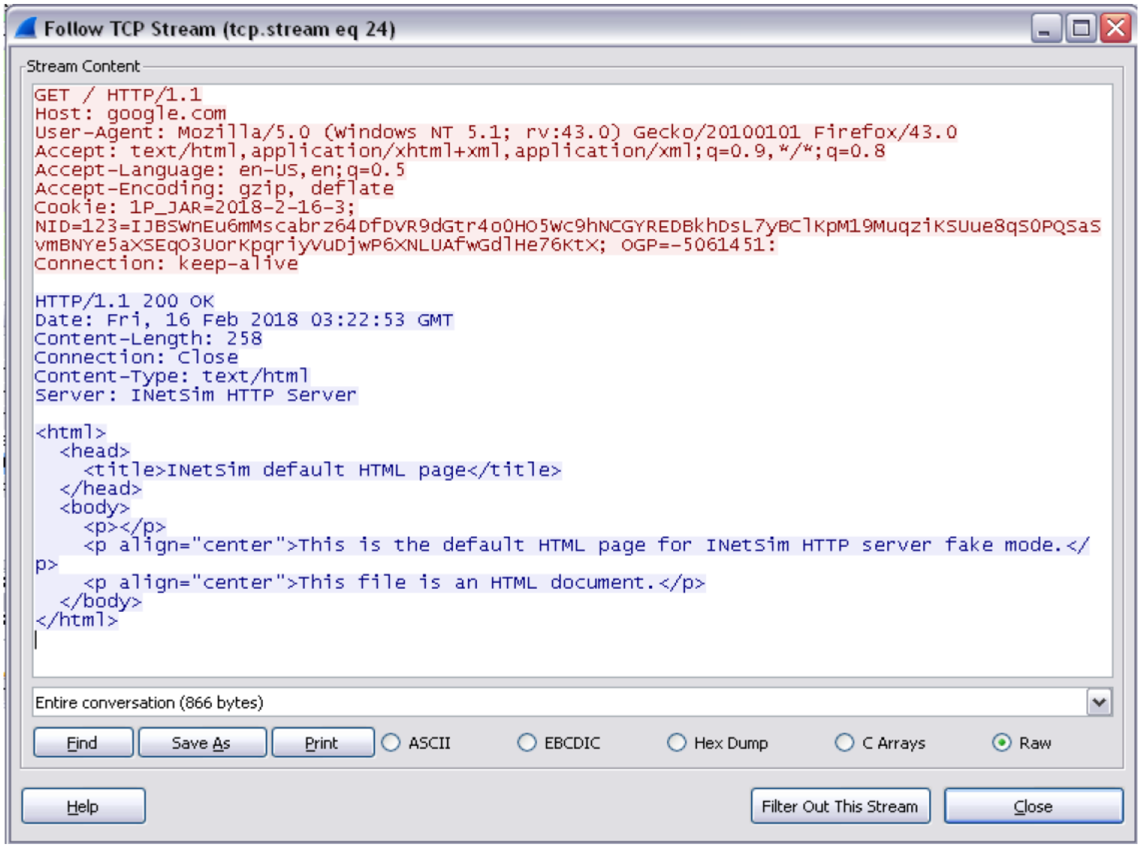
```
root@kali:~/Downloads# cd ..
root@kali:~# sudo nano /etc/inetsim/inetsim.conf
root@kali:~# sudo nano /etc/inetsim/inetsim.conf
root@kali:~# inetsim
INetSim 1.2.7 (2017-10-22) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it...
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create it...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 4199) ===
Session ID:     4199
Listening on:   0.0.0.0
Real Date/Time: 2018-02-11 23:01:55
Fake Date/Time: 2018-02-11 23:01:55 (Delta: 0 seconds)
 Forking services...
  * quotd_17_tcp - started (PID 4224)
  * echo_7_udp - started (PID 4221)
  * time_37_tcp - started (PID 4216)
  * echo_7_tcp - started (PID 4220)
  * discard_9_tcp - started (PID 4222)
  * ftp_21_tcp - started (PID 4208)
  * time_37_udp - started (PID 4217)
  * chargen_19_udp - started (PID 4227)
  * dummy_1_udp - started (PID 4229)
  * ident_113_tcp - started (PID 4214)
  * irc_6667_tcp - started (PID 4211)
  * daytime_13_tcp - started (PID 4218)
  * pop3s_995_tcp - started (PID 4207)
  * smtp_25_tcp - started (PID 4204)
  * discard_9_udp - started (PID 4223)
  * chargen_19_tcp - started (PID 4226)
  * quotd_17_udp - started (PID 4225)
  * smtps_465_tcp - started (PID 4205)
  * finger_79_tcp - started (PID 4213)
  * ftps_990_tcp - started (PID 4209)
  * syslog_514_udp - started (PID 4215)
  * dummy_1_tcp - started (PID 4228)
  * tftp_69_udp - started (PID 4210)
  * https_443_tcp - started (PID 4203)
  * dns_53_tcp_udp - started (PID 4201)
  * daytime_13_udp - started (PID 4219)
  * ntp_123_udp - started (PID 4212)
  * http_80_tcp - started (PID 4202)
  * pop3_110_tcp - started (PID 4206)
 done.
Simulation running.
```

3) I performed this question on Windows XP



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.



```
GET / HTTP/1.1
Host: google.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: 1P_JAR=2018-2-16-3;
NID=123=IJBSWnEu6mMscabrz64DfDVR9dGtr4oOHO5Wc9hNCGYREDBkhDsL7yBClKpM19MuqziKSUue8qS0PQSaS
vmBNYe5aXSEqO3UorKpqriyVuDjwP6XNLUAfwGdlHe76KtX; OGP=-5061451:
Connection: keep-alive

HTTP/1.1 200 OK
Date: Fri, 16 Feb 2018 03:22:53 GMT
Content-Length: 258
Connection: Close
Content-Type: text/html
Server: INetSim HTTP Server

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</
p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Entire conversation (866 bytes)

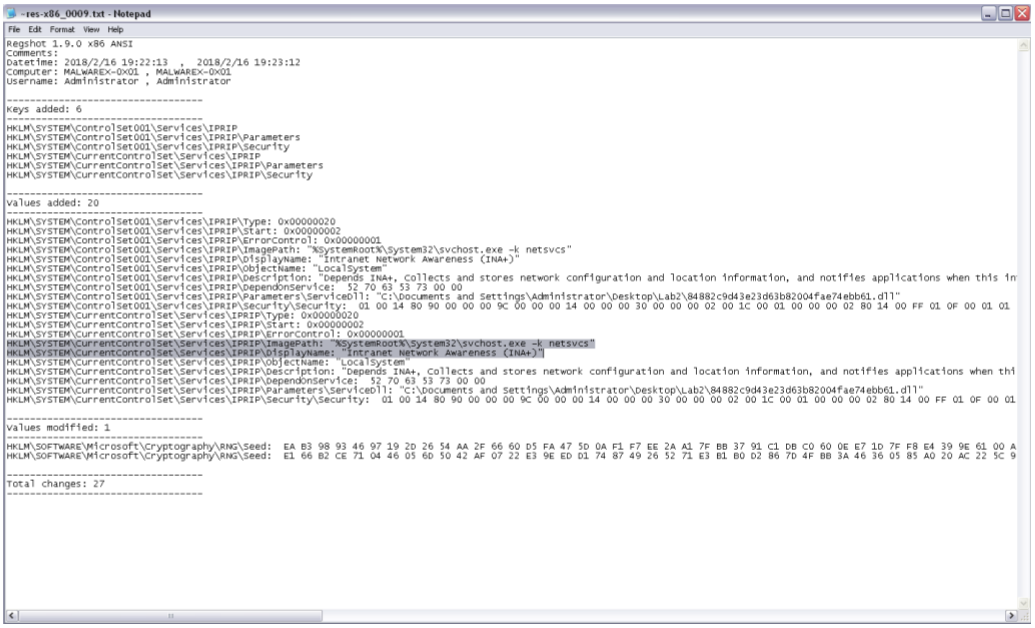
84882c9d43e23d63b82004fae74ebb61

1) This is an unpacked DLL file. This needs to be executed with the command prompt. We first need to install it and then execute it. So, we must check the functions in the dll file to understand the command it needs to be installed. Therefore, I ran the DLL file thru IDA Pro to check for the functions and I found install and installA.

2) To install the malware, we need to run the command as below:

    rundll32 84882c9d43e23d63b82004fae74ebb61.dll, installA

3) Before installing, I took a shot using Regshot. The comparisons of the shots before and after installation is shown below:



```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2018/2/16 19:22:13  ,  2018/2/16 19:23:12
Computer: MALWAREX-0X01 , MALWAREX-0X01
Username: Administrator , Administrator

----------------------------------
Keys added: 6
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

----------------------------------
Values added: 20
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies applications when this in
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService:  52 70 63 53 73 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Desktop\Lab2\84882c9d43e23d63b82004fae74ebb61.dll"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies applications when thi
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService:  52 70 63 53 73 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Desktop\Lab2\84882c9d43e23d63b82004fae74ebb61.dll"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01

----------------------------------
Values modified: 1
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  EA B3 98 93 46 97 19 2D 26 54 AA 2F 66 60 D5 FA 47 5D 0A F1 F7 EE 2A A1 7F BB 37 91 C1 DB C0 60 0E E7 1D 7F F8 E4 39 9E 61 00 A
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  E1 66 B2 CE 71 04 46 05 6D 50 42 AF 07 22 E3 9E ED D1 74 87 49 26 52 71 E3 B1 B0 D2 86 7D 4F BB 3A 46 36 05 85 A0 20 AC 22 5C 9

----------------------------------
Total changes: 27
----------------------------------
```

This shows us that s service IPRIP needs to be started to run the malware. Therefore, I used the command:

    net start IPRIP

which is how the file runs.

4) I used two filters for:
    - process name which contains “rundll32.exe”
    - path which contains “IPRIP”

5) Host base signatures:
    - IPRIP
    - cmd.exe
    - Windows XP 6.11

6) Network based signatures:
    - practicalmalwareanalysis.com
    - server.html
    - GET
    - HTTP/1.1

7) To inspecting this malware I used, Regshot, ApateDNS, Command Prompt, Process Explorer and Process Monitor. On ApateDNS we see that when we try to run the malware by starting the IPRIP service, it contacts

practicalmalwareanalysis.com. Considering this and the fact that we see strings such as cmd.exe we can assume the malware is requesting the command prompt for the remote host: http://practicalmalwareanalysis.com

e2bf42217a67e46433da8b6f4507219e

1) When running the exe file, Process Monitor detects that it generates svchost.exe. This process runs in the background even though it shows an error to the user while opening the malware.

2) There are live memory modifications. We know this because, when combing thru the properties of service svchost.exe, we look under strings tab and find that when toggling between Memory and Image there are differences in the strings. This means that there have been some modifications with the memory.

3) Host base signatures:

   practicalmalwareanalysis.log

4) When we open the malware, we see that it creates a file practicalmalwareanalysis.log next to the malware. When combing thru the strings in the memory section of "svchost.exe" we find strings such as

   - practicalmalwareanalysis.log
   - [ENTER]
   - [CAPS LOCK]
   - [SHIFT]
   - [CTRL]
   - [DELETE]

   This mean that the malware is a keylogger. The file practicalmalwareanalysis.log, starts to build whenever a key is presses. This logs all the keys pushed and saves them on the .log file created.

b94af4a4d4af6eac81fc135abda1c40c

1) When I try to run the file, it disappears. When Going thru process monitor we find a process created to call cmd.exe and then and instruction to delete the malware from the c drive.

   ```
   "C:\WINDOWS\system32\cmd.exe" /c del C:\DOCUME~1\ADMINI~1\Desktop\Lab2\B94AF4~1.EXE >> NUL"
   ```

2) The set back is that the program deletes itself from the hard drive.

3) Another way to run the malware is to debug it using IDA Pro and ollydbg. By locating the delete instruction, we can code to jump to the next instruction instead of executing the delete command.

4) There are several strings found in this malware:

   - http://www.practicalmalwareanalysis.com
   - command.com
   - Manager Service.exe
   - cmd.exe
   - UPLOAD
   - DOWNLOAD
   - /c del

All these strings suggest that the malware is being used to remotely access the command prompt and possibly connect to http://www.practicalmalwareanalysis.com from where it can UPLOAD or DOWNLOAD malware. The remote attacker could also control the Service Manager and install services and or remove them.