



Dynamic/Behavioural Analysis

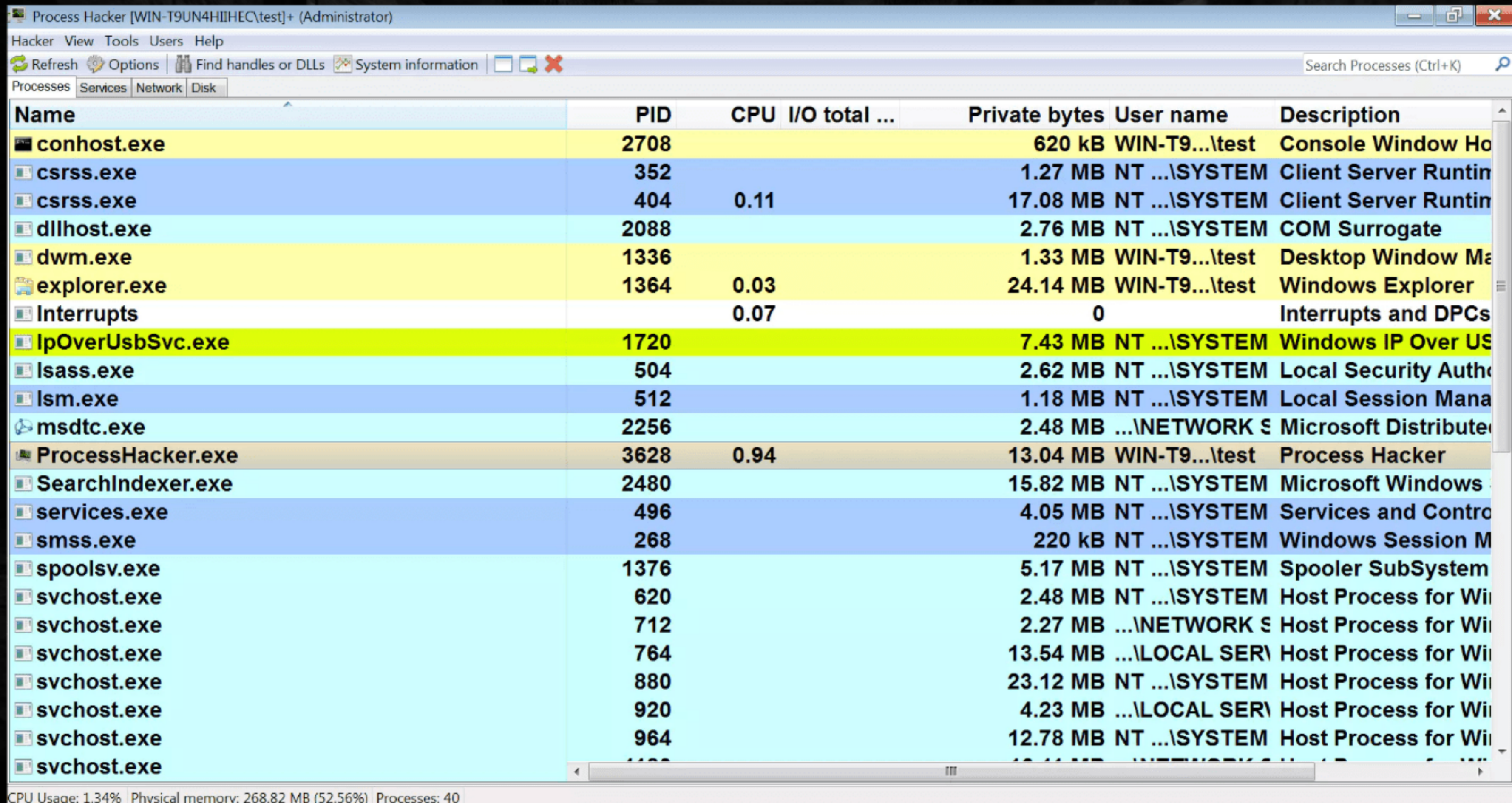
Dynamic/Behavioral Analysis Steps

- Run Monitoring tools
- Run the malware
- Stop the malware process
- Stop the monitoring tools
- Analyze the results

Dynamic Analysis Tools

- **Process Hacker:** list the process and examine process attributes
- **Process Monitor:** Monitor process interaction with the system
- **Wireshark:** Network sniffer which allows you to capture packets
- **Noriben:** Python script that works in conjunction with Process Monitor to collect, analyze, and report on run-time indicators of malware
- **Fakedns:** Gives fake DNS response, useful in redirecting network traffic to your lab system
- **InetSim:** Simulates Network Services

Process Hacker is an open source multi-purpose tool that helps in examining the system resources and process attributes.



The screenshot shows the Process Hacker application window. The title bar reads "Process Hacker [WIN-T9UN4HIIIHEC\test]+ (Administrator)". The menu bar includes "Hacker", "View", "Tools", "Users", and "Help". Below the menu bar is a toolbar with icons for "Refresh", "Options", "Find handles or DLLs", and "System information". A search bar on the right says "Search Processes (Ctrl+K)". The main area is a table with columns: "Name", "PID", "CPU", "I/O total ...", "Private bytes", "User name", and "Description". The table lists various system processes, with "ProcessHacker.exe" highlighted in orange. The status bar at the bottom shows "CPU Usage: 1.34% Physical memory: 268.82 MB (52.56%) Processes: 40".

Name	PID	CPU	I/O total ...	Private bytes	User name	Description
conhost.exe	2708			620 kB	WIN-T9...\test	Console Window Ho
csrss.exe	352			1.27 MB	NT ...\SYSTEM	Client Server Runtin
csrss.exe	404	0.11		17.08 MB	NT ...\SYSTEM	Client Server Runtin
dllhost.exe	2088			2.76 MB	NT ...\SYSTEM	COM Surrogate
dwm.exe	1336			1.33 MB	WIN-T9...\test	Desktop Window Ma
explorer.exe	1364	0.03		24.14 MB	WIN-T9...\test	Windows Explorer
Interrupts		0.07		0		Interrupts and DPCs
IpOverUsbSvc.exe	1720			7.43 MB	NT ...\SYSTEM	Windows IP Over US
lsass.exe	504			2.62 MB	NT ...\SYSTEM	Local Security Autho
lsm.exe	512			1.18 MB	NT ...\SYSTEM	Local Session Mana
msdtc.exe	2256			2.48 MB	...\NETWORK S	Microsoft Distribute
ProcessHacker.exe	3628	0.94		13.04 MB	WIN-T9...\test	Process Hacker
SearchIndexer.exe	2480			15.82 MB	NT ...\SYSTEM	Microsoft Windows
services.exe	496			4.05 MB	NT ...\SYSTEM	Services and Contro
smss.exe	268			220 kB	NT ...\SYSTEM	Windows Session M
spoolsv.exe	1376			5.17 MB	NT ...\SYSTEM	Spooler SubSystem
svchost.exe	620			2.48 MB	NT ...\SYSTEM	Host Process for Wi
svchost.exe	712			2.27 MB	...\NETWORK S	Host Process for Wi
svchost.exe	764			13.54 MB	...\LOCAL SER\	Host Process for Wi
svchost.exe	880			23.12 MB	NT ...\SYSTEM	Host Process for Wi
svchost.exe	920			4.23 MB	...\LOCAL SER\	Host Process for Wi
svchost.exe	964			12.78 MB	NT ...\SYSTEM	Host Process for Wi
svchost.exe	1100			10.11 MB	...\NETWORK S	Host Process for Wi

Process Monitor shows the real-time interaction of the processes with the system (like the File system, registry, process activity). It can be noisy but the filters can help you reduce the noise.

The screenshot shows the Process Monitor application window with a list of events. The columns are: Time, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show Explorer.EXE (PID 1364) performing various registry and file system operations.

Time	Process Name	PID	Operation	Path	Result	Detail
1:49...	Explorer.EXE	1364	RegQueryValue	HKCU\Software\Microsoft\Windows\Current...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 00 00 00 ...
1:49...	Explorer.EXE	1364	RegSetValue	HKCU\Software\Microsoft\Windows\Current...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 00 00 00 ...
1:49...	Explorer.EXE	1364	RegSetValue	HKCU\Software\Microsoft\Windows\Current...	SUCCESS	Type: REG_BINARY, Length: 1,612, Data: 00 00 ...
1:49...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 1620, User Time: 0.0000000, Kernel ...
1:49...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 2932, User Time: 0.0000000, Kernel ...
1:49...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 1160, User Time: 0.0156001, Kernel T...
1:49...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 3812, User Time: 0.0000000, Kernel ...
1:49...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 3792, User Time: 0.0000000, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 2596, User Time: 0.0000000, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 1788, User Time: 0.0312002, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 3224, User Time: 0.0156001, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 2600, User Time: 0.0624004, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 1664, User Time: 0.0000000, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 2792, User Time: 0.0000000, Kernel ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 2564, User Time: 0.0156001, Kernel ...
1:50...	Explorer.EXE	1364	RegQueryValue	HKCU\Software\Microsoft\Windows\Current...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 00 00 00 ...
1:50...	Explorer.EXE	1364	RegSetValue	HKCU\Software\Microsoft\Windows\Current...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 00 00 00 ...
1:50...	Explorer.EXE	1364	RegSetValue	HKCU\Software\Microsoft\Windows\Current...	SUCCESS	Type: REG_BINARY, Length: 1,612, Data: 00 00 ...
1:50...	Explorer.EXE	1364	Thread Exit		SUCCESS	Thread ID: 1636, User Time: 0.0000000, Kernel ...
1:50...	Explorer.EXE	1364	QueryNameInform...	C:\softwares\SysinternalsSuite\Procmon.exe	SUCCESS	Name: \softwares\SysinternalsSuite\Procmon.exe
1:50...	Explorer.EXE	1364	CreateFile	C:\softwares\SysinternalsSuite\Procmon.exe	SUCCESS	Desired Access: Read Attributes, Disposition: ...
1:50...	Explorer.EXE	1364	QueryBasicInform...	C:\softwares\SysinternalsSuite\Procmon.exe	SUCCESS	CreationTime: 5/26/2015 9:38:52 AM, LastAcces...
1:50...	Explorer.EXE	1364	CloseFile	C:\softwares\SysinternalsSuite\Procmon.exe	SUCCESS	
1:50...	Explorer.EXE	1364	CreateFile	C:\softwares\SysinternalsSuite	SUCCESS	Desired Access: Read Data/List Directory, Sync...
1:50...	Explorer.EXE	1364	QueryDirectory	C:\softwares\SysinternalsSuite\Procmon.exe	SUCCESS	Filter: Procmon.exe, 1: Procmon.exe
1:50...	Explorer.EXE	1364	CloseFile	C:\softwares\SysinternalsSuite	SUCCESS	
1:50...	Explorer.EXE	1364	CreateFile	C:\Users\test\Desktop	SUCCESS	Desired Access: Read Attributes, Read Control,...
1:50...	Explorer.EXE	1364	QuerySecurityFile	C:\Users\test\Desktop	BUFFER O...	Information: Label
1:50...	Explorer.EXE	1364	QuerySecurityFile	C:\Users\test\Desktop	SUCCESS	Information: Label
1:50...	Explorer.EXE	1364	CloseFile	C:\Users\test\Desktop	SUCCESS	
1:50...	Explorer.EXE	1364	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:50...	Explorer.EXE	1364	RegOpenKey	HKCU\Software\Classes\Drive\shell\Folde...	NAME NOT...	Desired Access: Enumerate Sub Keys
1:50...	Explorer.EXE	1364	RegOpenKey	HKCR\Drive\shell\FolderExtensions	SUCCESS	Desired Access: Enumerate Sub Keys
1:50...	Explorer.EXE	1364	RegQueryKey	HKCR\Drive\shell\FolderExtensions	SUCCESS	Query: Name
1:50...	Explorer.EXE	1364	RegOpenKey	HKCU\Software\Classes\Drive\shell\Folde...	NAME NOT...	Desired Access: Maximum Allowed
1:50...	Explorer.EXE	1364	RegEnumKey	HKCR\Drive\shell\FolderExtensions	SUCCESS	Index: 0, Name: {fbeb8a05-beee-4442-804e-409d...
1:50...	Explorer.EXE	1364	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:50...	Explorer.EXE	1364	RegOpenKey	HKCU\Software\Classes\Drive\shell\Folde...	NAME NOT...	Desired Access: Query Value
1:50...	Explorer.EXE	1364	RegOpenKey	HKCR\Drive\shell\FolderExtensions\{fbeb...	SUCCESS	Desired Access: Query Value
1:50...	Explorer.EXE	1364	RegOpenKey	HKCR\Drive\shell\FolderExtensions\{fbeb...	SUCCESS	Query: Name

Wireshark is a packet sniffer. It allows you to capture the network traffic while you are executing the malware

Capturing from eth0 [Wireshark 1.6.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3	0.000159	192.168.1.60	192.168.1.22	DNS	Standard query A mail.upgoogle.com
4	0.009285	192.168.1.22	192.168.1.60	DNS	Standard query response A 192.168.1.22
5	0.013110	192.168.1.60	192.168.1.22	TCP	49164 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
6	0.013165	192.168.1.22	192.168.1.60	TCP	80 > 49164 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=
7	0.013287	192.168.1.60	192.168.1.22	TCP	49164 > 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8	0.015043	192.168.1.60	192.168.1.22	TCP	[TCP segment of a reassembled PDU]
9	0.015055	192.168.1.22	192.168.1.60	TCP	80 > 49164 [ACK] Seq=1 Ack=123 Win=14608 Len=0
10	0.015077	192.168.1.60	192.168.1.22	HTTP	POST /image/image.php HTTP/1.1
11	0.015080	192.168.1.22	192.168.1.60	TCP	80 > 49164 [ACK] Seq=1 Ack=216 Win=14608 Len=0
12	0.050992	192.168.1.22	192.168.1.60	TCP	[TCP segment of a reassembled PDU]
13	0.052975	192.168.1.22	192.168.1.60	HTTP	HTTP/1.1 200 OK (text/html)
14	0.053841	192.168.1.60	192.168.1.22	TCP	49164 > 80 [ACK] Seq=216 Ack=410 Win=65280 Len=0

▶ Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

▶ Ethernet II, Src: 00:0c:29:0f:9f:67 (00:0c:29:0f:9f:67), Dst: 00:0c:29:34:d2:69 (00:0c:29:34:d2:69)

▶ Internet Protocol Version 4, Src: 192.168.1.60 (192.168.1.60), Dst: 192.168.1.22 (192.168.1.22)

▶ Transmission Control Protocol, Src Port: 49164 (49164), Dst Port: 80 (80), Seq: 216, Ack: 410, Len: 0

0000	00 0c 29 34 d2 69 00 0c 29 0f 9f 67 08 00 45 00	..)4.i..)..g..E.
0010	00 28 01 27 40 00 80 06 76 06 c0 a8 01 3c c0 a8	.(.'@... v....<..
0020	01 16 c0 0c 00 50 9b f4 46 c1 58 e7 3b c2 50 11P.. F.X.;.P.
0030	00 ff f3 75 00 00 00 00 00 00 00 00	...u....

Noriben

- Python script Works in conjunction with Process Monitor
- Helps in collecting, analyzing and reporting runtime indicators of malware
- Comes with pre-defined filters which help in reducing noise

Running Noriben - Copy *procmon.exe* and run the python script

Computer > Local Disk (C:) > noriben

Name	Date modified	Type	Size
Noriben.py	6/19/2015 12:27 ...	Python File	49 KB
Noriben_18_Feb_17_19_28_55_391000.p...	2/18/2017 7:29 PM	ProcMon Log File	28,672 KB
Procmon.exe	5/26/2015 9:38 AM	Application	1,999 KB
README.md	4/28/2015 10:17 ...	MD File	9 KB

```
Administrator: C:\Windows\system32\cmd.exe - python Noriben.py
C:\noriben>python Noriben.py
[!] Python module "requests" not found. Internet functionality is now disabled.
--===[ Noriben v1.6.2 ]===--
--===[ @bbaskin ]===--
[!] Filter file ProcmonConfiguration.PMC not found. Continuing without filters.
[+] Features: (Debug: False YARA: False VirusTotal: False)
[*] Using procmon EXE: procmon.exe
[*] Procmon session saved to: Noriben_18_Feb_17__19_28_55_391000.pml
[*] Launching Procmon ...
[*] Procmon is running. Run your executable now.
[*] When runtime is complete, press CTRL+C to stop logging.
```

Fakedns

- It runs DNS Service
- Resolves every domain to the IP of the machine on which it runs
- Useful in redirecting network traffic to your lab system

Below screenshot shows *fakedns* resolving the domains to the IP address of the system on which it is running

```
File Edit Tabs Help
remnux@remnux:~$ myip
192.168.1.22 ←
remnux@remnux:~$ fakedns
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.22
Respuesta: 2.2.2.4.in-addr.arpa. -> 192.168.1.22
Respuesta: yahoo.com. -> 192.168.1.22
Respuesta: yahoo.com. -> 192.168.1.22
Respuesta: 2.2.2.4.in-addr.arpa. -> 192.168.1.22
Respuesta: google.com. -> 192.168.1.22
Respuesta: google.com. -> 192.168.1.22
Respuesta: 2.2.2.4.in-addr.arpa. -> 192.168.1.22
Respuesta: cysinfo.com. -> 192.168.1.22
Respuesta: cysinfo.com. -> 192.168.1.22
```

INetSim

- Simulates common internet services in a lab environment
- Useful in redirecting all the communication to your lab system
- Easy to configure and the configuration file is ***inetsim.conf***

Below screenshot shows *InetSim* simulating all the internet services

```
File Edit Tabs Help
remnux@remnux:~$ inetsim
INetSim 1.2.4 (2013-08-15) by Matthias Eckert & Thomas Hungenberg
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 3000) ===
Session ID: 3000
Listening on: 192.168.1.22
Real Date/Time: 2016-07-27 00:36:25
Fake Date/Time: 2016-07-27 00:36:25 (Delta: 0 seconds)
Forking services...
* ident_113_tcp - started (PID 3015)
* irc_6667_tcp - started (PID 3012)
* finger_79_tcp - started (PID 3014)
* quotd_17_udp - started (PID 3026)
* daytime_13_tcp - started (PID 3019)
* echo_7_udp - started (PID 3022)
* discard_9_udp - started (PID 3024)
* syslog_514_udp - started (PID 3016)
* chargen_19_tcp - started (PID 3027)
* chargen_19_udp - started (PID 3028)
* echo_7_tcp - started (PID 3021)
* time_37_udp - started (PID 3018)
* time_37_tcp - started (PID 3017)
* daytime_13_udp - started (PID 3020)
```

Below screenshot shows the https traffic intercepted using **INetSim**

```
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: POST /webmail.php HTTP/1.1
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Connection: Keep-Alive
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Content-Type: application/x-www-form-
urencoded; Charset=UTF-8
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Accept: */*
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: User-Agent: (RF) : <exe> :(PC-Name: WIN-
T9UN4HIIHEC : Username: Administrator ; AV: NoAV)
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Content-Length: 80
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Host: webmail.duia.in
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: <(POSTDATA)>
[2016-11-14 12:04:27] [192.168.1.60:49166] info: POST data stored to: /usr/share/inetsim/
data/http/postdata/6ba1e7ed0791c196aac167563c26b9f6f92a1e7f

POSTDATA: action=getfiles&username=000C290F9F67-WIN-T9UN4HIIHEC-Administrator&filename=exe
```

<https://cysinfo.com/malware-actors-using-nic-cyber-security-themed-spear-phishing-target-indian-government-organizations/>

Demo 1 - Analysis of SpyBot

Lab 2- The case of Remcos RAT (contd.)

This is the continuation of Lab 1, analyze the sample host.exe and answer the below questions

- What is the name of the file dropped by the malware?
- Where does it drop this file?
- Does the malware copies itself or does it drop a different component?
- How does malware execute this dropped file?
- What is the name of the C2 domain?
- What is the port on which malware is communicating?
- Do you see anything suspicious in the network traffic?
- How is Malware persisting on the system?