恶意代码分析与防治技术

第5章 基本动态分析

王志
zwang@nankai.edu.cn

南开大学 网络空间安全学院

2023-2024学年

知识点

- 基本动态分析
- 沙箱（Sandbox）
- DLL的动态分析
  - 难点：动态链接库的启动，服务程序的启动
- 进程动态监控
- 注册表动态监控 Regshot
- 网络动态监控
- 重点：Process Monitor、Process Explorer、Regshot、Wireshark

基本动态分析
Basic Dynamic Analysis

主观题 10分

设置

已经可以提取静态特征并基于Yara引擎开发杀毒软件，为什么还需要动态分析?

作答

为什么要进行动态分析

- Static analysis can reach a dead-end, due to
  - Obfuscation
  - Packing
  - Examiner has exhausted the available static analysis techniques
- Dynamic analysis is efficient and will show you exactly what the malware does

多选题 10分

设置

以下哪项可以用来隐藏程序中的字符串信息?

A UPX

B PEiD

C ELF

D DLL

提交

南開大學 Nankai University

沙箱
Sandboxes: The Quick-and-Dirty Approach

沙箱

- **All-in-one** software for basic dynamic analysis
- Virtualized environment that **simulates network services**
- Examples: Norman Sandbox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis
- They are expensive but easy to use
- They produce a nice PDF report of results

GFI SandBox™ Analysis # 2307

Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)

Table of Contents

主观题 10分

设置

有了沙箱的动态分析结果，计算机病毒还需要进行人工分析吗?

作答

沙箱

- 缺少命令交互
  - Without command-line options
  - Botnet C&C packets
- 分析时间限制
  - Not record all events
  - Stalling behaviors
- 反虚拟机技术
  - Anti-VM techniques
- 运行环境单一
  - Certain Environment

多选题 10分

设置

沙箱的优点？

A No command-line options

B All-in-one software for basic dynamic analysis

C Not record all events

D Fixed Environment

提交

多选题 10分

设置

此题未设置答案，请点击右侧设置按钮

沙箱的缺点有哪些?

A 缺少命令交互

B 分析时间限制

C 反虚拟机技术

D 运行环境单一

提交

动态链接库程序的动态分析
Launching DLLs

主观题 10分

设置

如何动态分析一个动态链接库程序?

作答

动态链接库程序的执行

- EXE files can be run directly, but DLLs can't
- Use rundll32.exe (included in Windows)

  rundll32.exe *DLLname, Export arguments*
- The *Export* value is one of the exported functions you found in Dependency Walker, PEview, or PE Explorer.

动态连接库程序的执行

- Example
  - rip.dll has these exports: **Install** and **Uninstall**

    rundll32.exe rip.dll, Install

- Some functions use **ordinal** values instead of names, like

  rundll32.exe xyzzy.dll, #5

- It's also possible to modify the PE header and convert a DLL into an EXE

服务的安装和启动

- Installed as a service
  - rpr32x.dll has the export: InstallService
  - 安装服务
    - rundll32 ipr32x.dll, InstallService ServiceName
  - 启动服务
    - net start ServiceName

主观题 10分

设置

Windows的服务程序和应用程序有哪些区别?

作答

服务与应用的区别

- 功能：通常提供后台运行的长期服务
  - 网络服务、数据备份等
- 用户交互：一般不与用户直接交互，在后台默默地运行。
- 权限：通常以系统管理员权限运行，可以访问系统的各种资源。
  - 应用程序则以普通用户权限运行，只能访问其所需的资源和文件。
- 生命周期：通常在系统启动时启动，直到系统关闭或该手动停止
  - 应用程序则由用户启动和关闭，生命周期由用户控制。
- 运行模式：服务程序通常以后台进程的形式运行，对用户不可见
  - 应用程序则以前台进程运行，提供给用户可见的界面和操作。

设置

如何启动服务？

A net start ServiceName

B rundll32.exe abc.dll #num arguments

C rundll32.exe abc.dll function arguments

D rundll32.exe abc.dll InstallService ServiceName

提交

进程的动态监控

主观题 10分

设置

哪些进程的行为可以进行动态监控?

作答

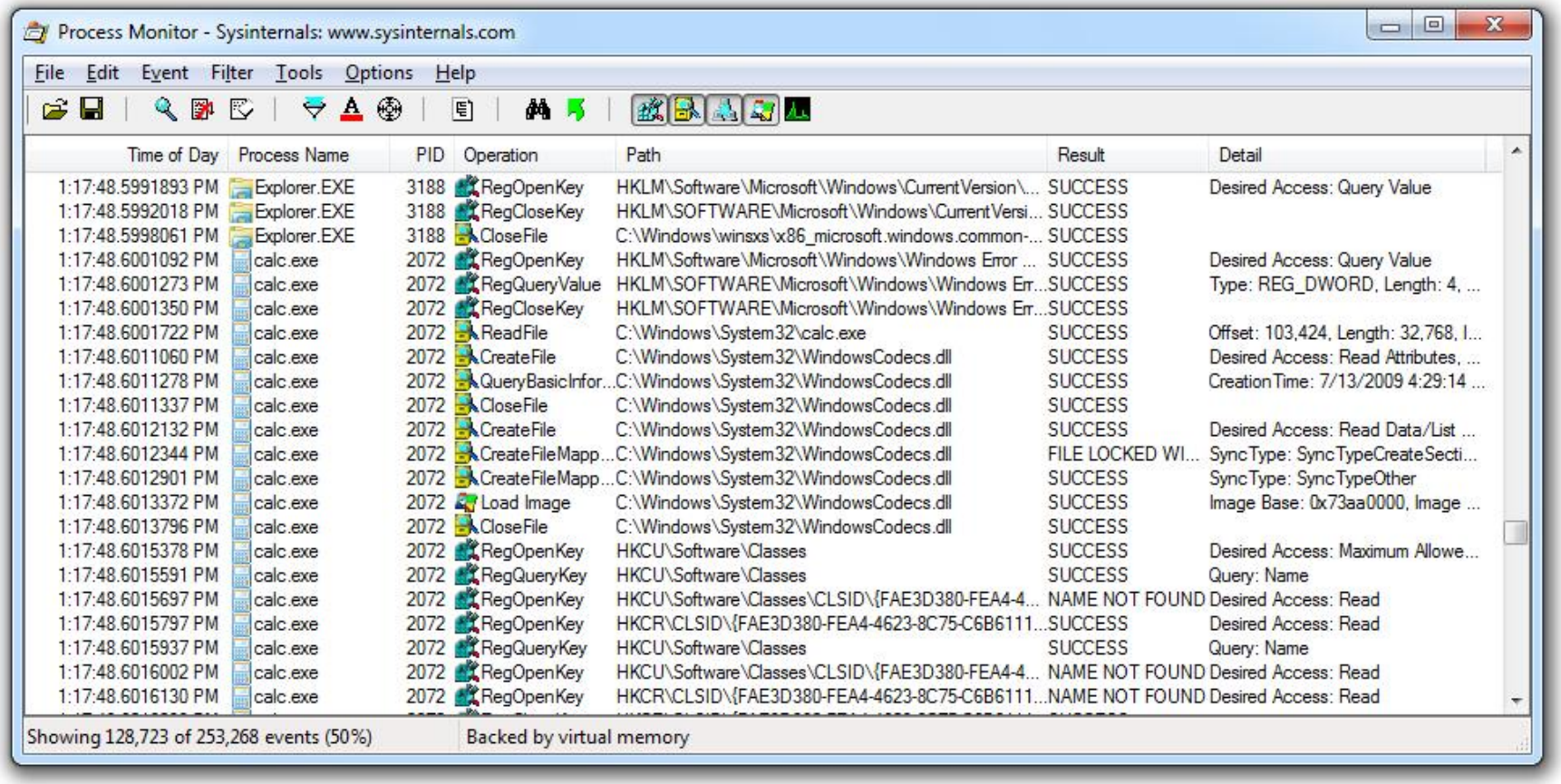
Process Monitor

- Monitors registry, file system, network, process, and thread activity
- All recorded events are kept, but you can filter the display to make it easier to find items of interest

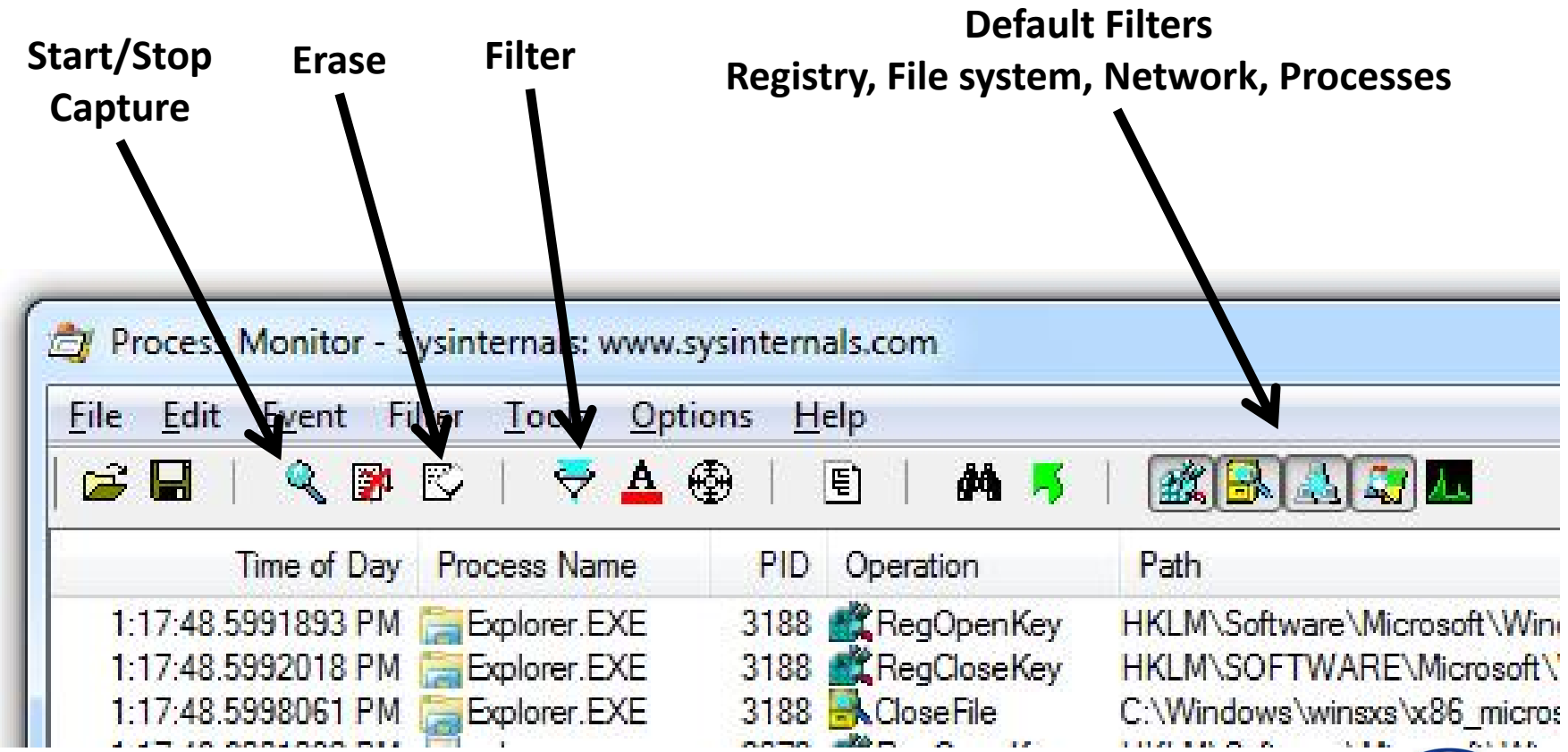
Process Monitor

- Don't run it too long or it will fill up all RAM and crash the machine
  - Use RAM to log events until it is told to stop capturing
  - run out memory to crash the system
  - limited periods of time
  - File->Capture Events
  - File->Clear Display

Launching Calc.exe



Process Monitor Toolbar

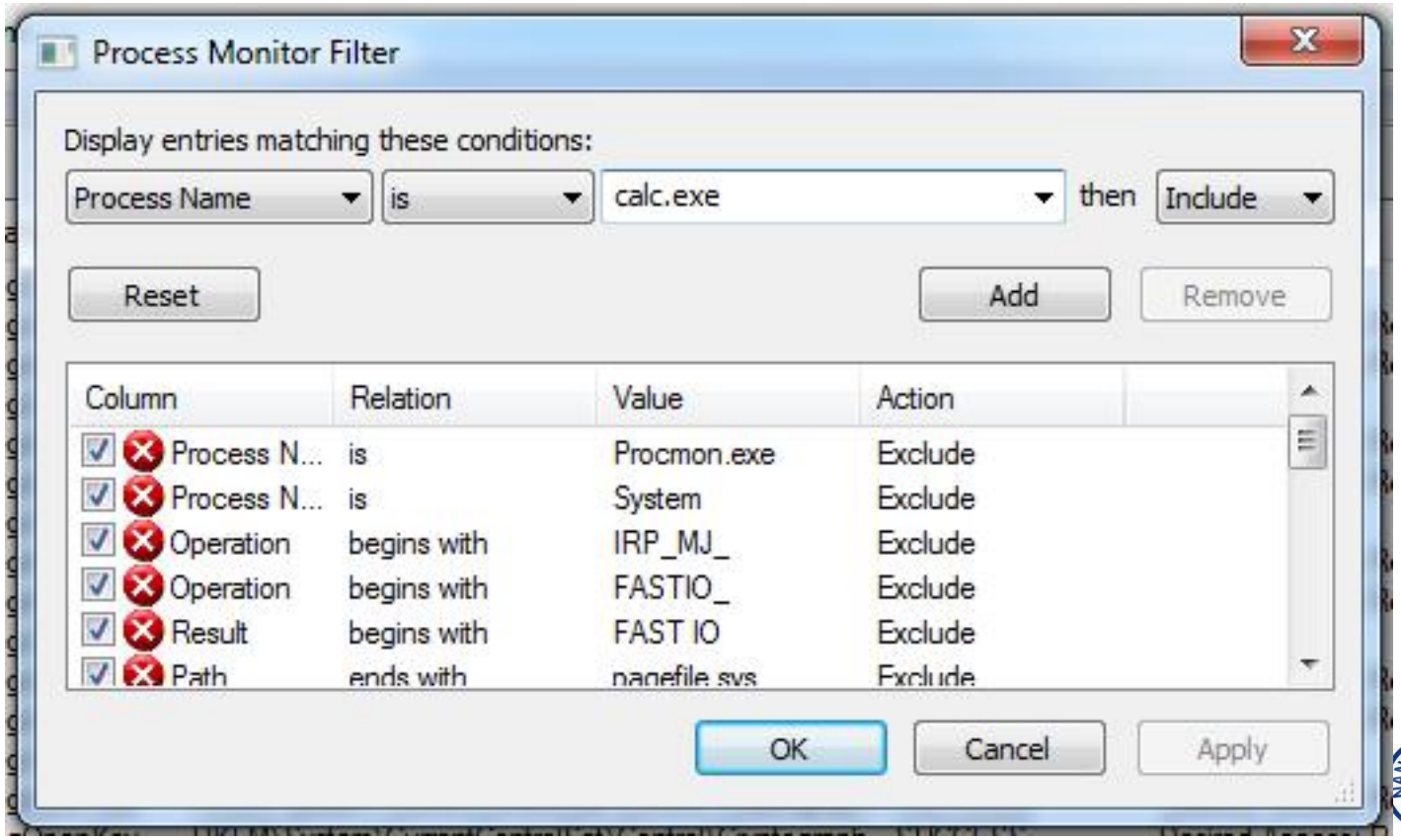


Filtering with Exclude

- One technique: hide normal activity before launching malware
- Filter on process name
- Filter on system calls
- Right-click each Process Name and click **Exclude**

Filtering with Include

- Most useful filters: Process Name, Operation, and Detail



多选题 10分

设置

Process Monitor可以动态监控哪些进程的操作行为?

A Registry

B File system

C Network

D Process

E Thread

提交

Process Explorer

主观题 10分

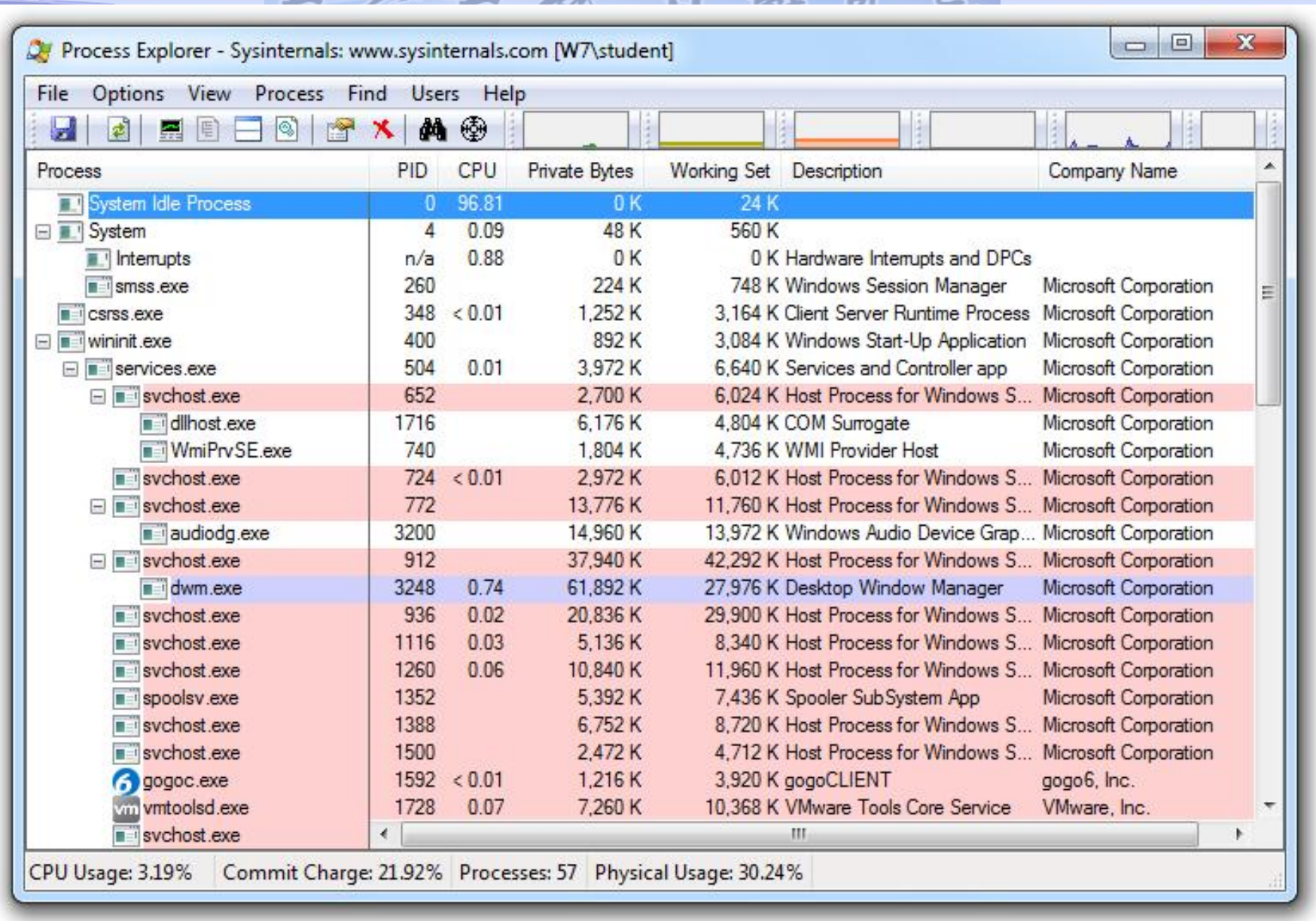
设置

进程和进程之间有哪些行为需要进行监控?

作答

Process Explorer

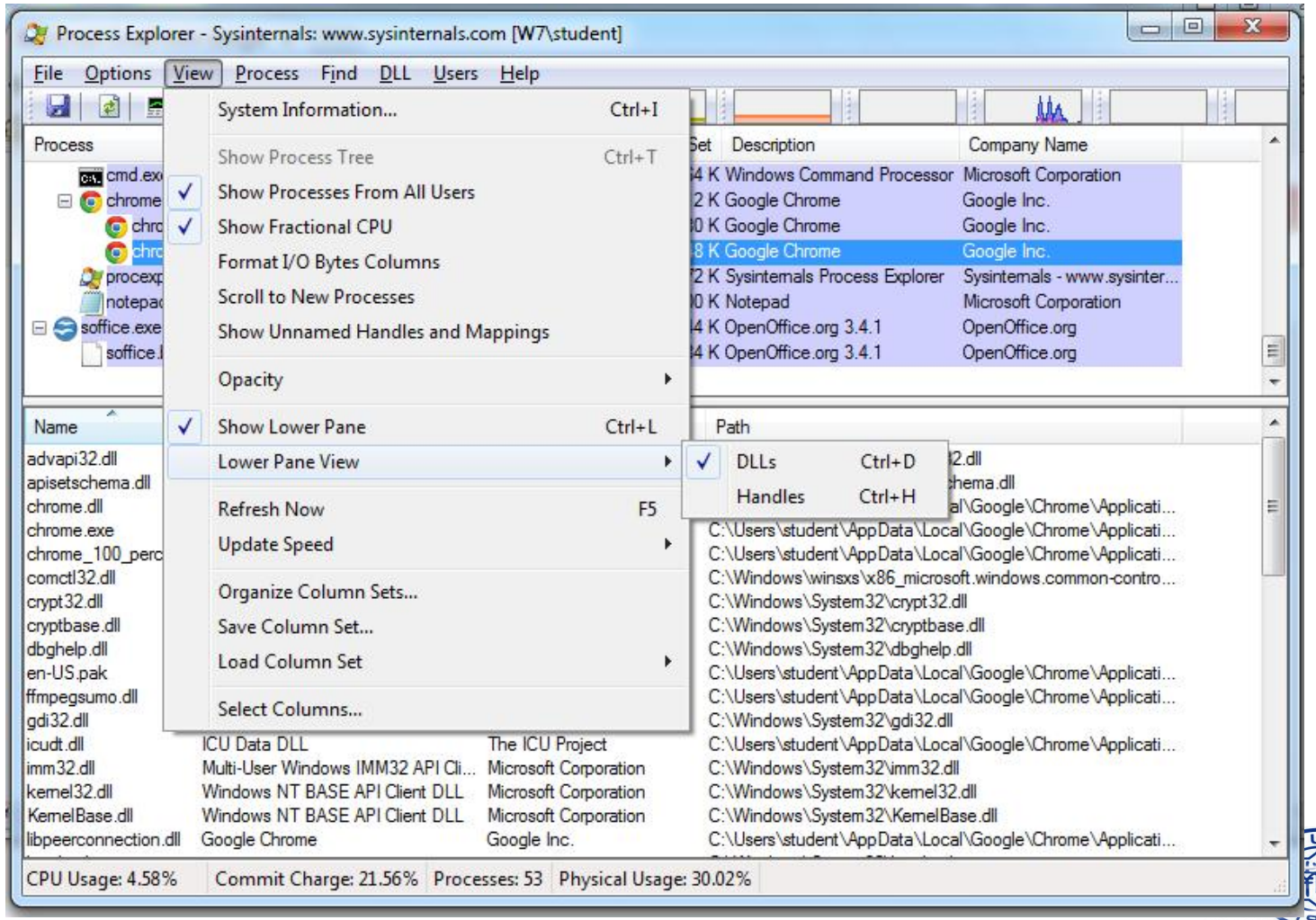
- List all processes currently running on the system
  - Dlls loaded
  - Various process properties
  - Overall system information



Coloring

- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

DLL Mode

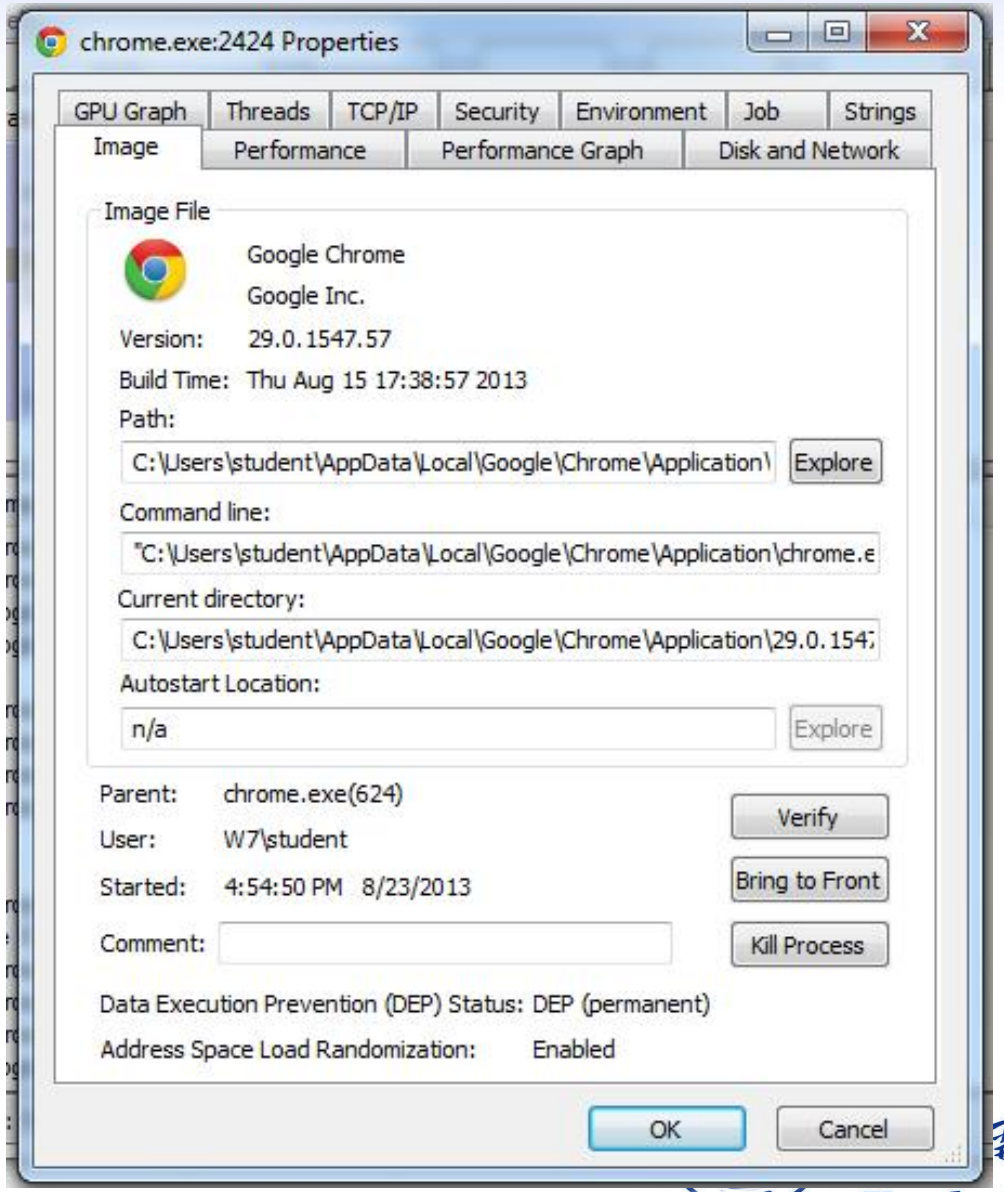

Process Explorer - Sysinternals: www.sysinternals.com [W7\student]
File Options View Process Find DLL Users Help
System Information... Ctrl+I
Show Process Tree Ctrl+T
Show Processes From All Users
Show Fractional CPU
Format I/O Bytes Columns
Scroll to New Processes
Show Unnamed Handles and Mappings
Opacity
Show Lower Pane Ctrl+L
Lower Pane View
Refresh Now F5
Update Speed
Organize Column Sets...
Save Column Set...
Load Column Set
Select Columns...
DLLs Ctrl+D
Handles Ctrl+H
Process
Description
Company Name
Name
Path
CPU Usage: 4.58%
Commit Charge: 21.56%
Processes: 53
Physical Usage: 30.02%

Handle Mode

Type	Name
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\crypt32LogoffEvent
Event	\BaseNamedObjects\userenv: User Profile setup event
Event	\BaseNamedObjects\userenv: Machine Group Policy has been applied
Event	\BaseNamedObjects\userenv: User Group Policy has been applied
File	C:\Tools\ProcessExplorer
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	\Device\KsecDD
File	C:\Documents and Settings\xpbot\Local Settings\Temp\Perflib_Perfdata_25...
File	\Device\PROCEXP152
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	\Device\Tcp
File	\Device\Tcp
File	\Device\Ip
File	\Device\Ip
File	\Device\Ip

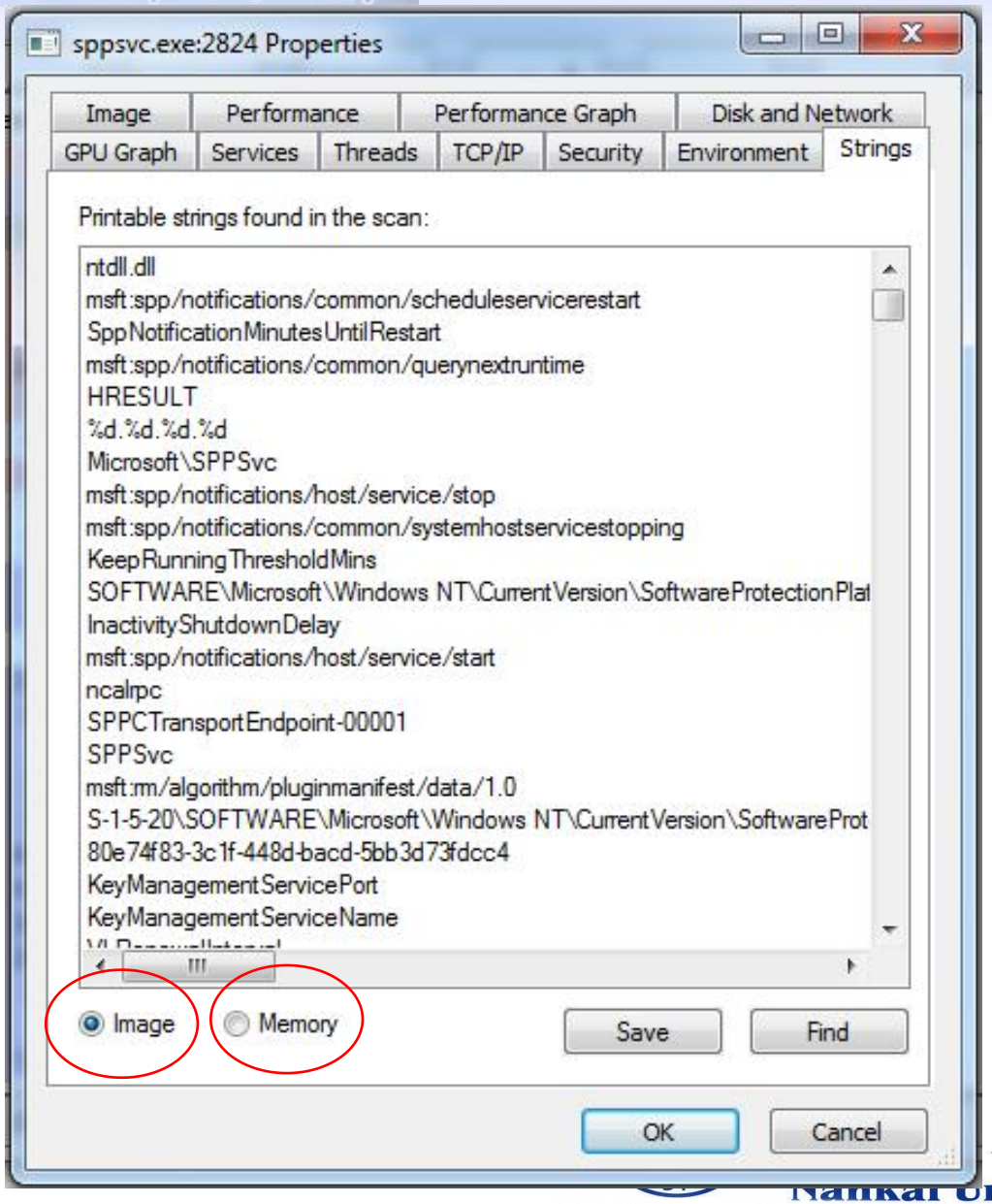
Properties

- Shows DEP and ASLR status
- Verify button checks the disk file's Windows signature
  - But not the RAM image, so it won't detect **process replacement**



Strings

- Compare Image to Memory strings, if they are very different, it can indicate process replacement



Detecting Malicious Documents

- Open the document (e.g. PDF) on a system with a vulnerable application
- Watch Process Explorer to see if it launches a process
- The Image tab of that process's Properties sheet will show where the malware is

注册表的动态监控

主观题 10分

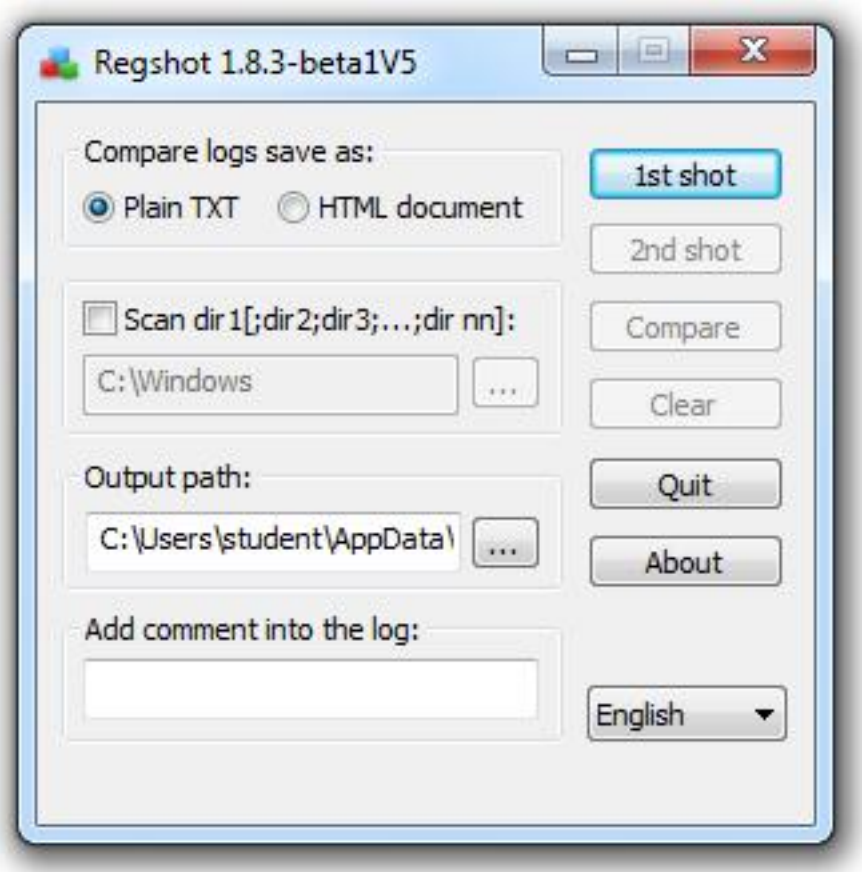
设置

如何监控恶意代码修改了系统的哪些注册表项?

作答

Regshot

- An open source registry comparison tool
  - Take registry snapshots
  - Compare two registry snapshots


Regshot 1.8.3-beta1V5
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
...
Output path:
C:\Users\student\AppData\
...
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English

主观题 10分

设置

Windows注册表有哪些功能?

正常使用主观题需2.0以上版本雨课堂

作答

南開大學 Nankai University

网络动态监控

主观题 10分

设置

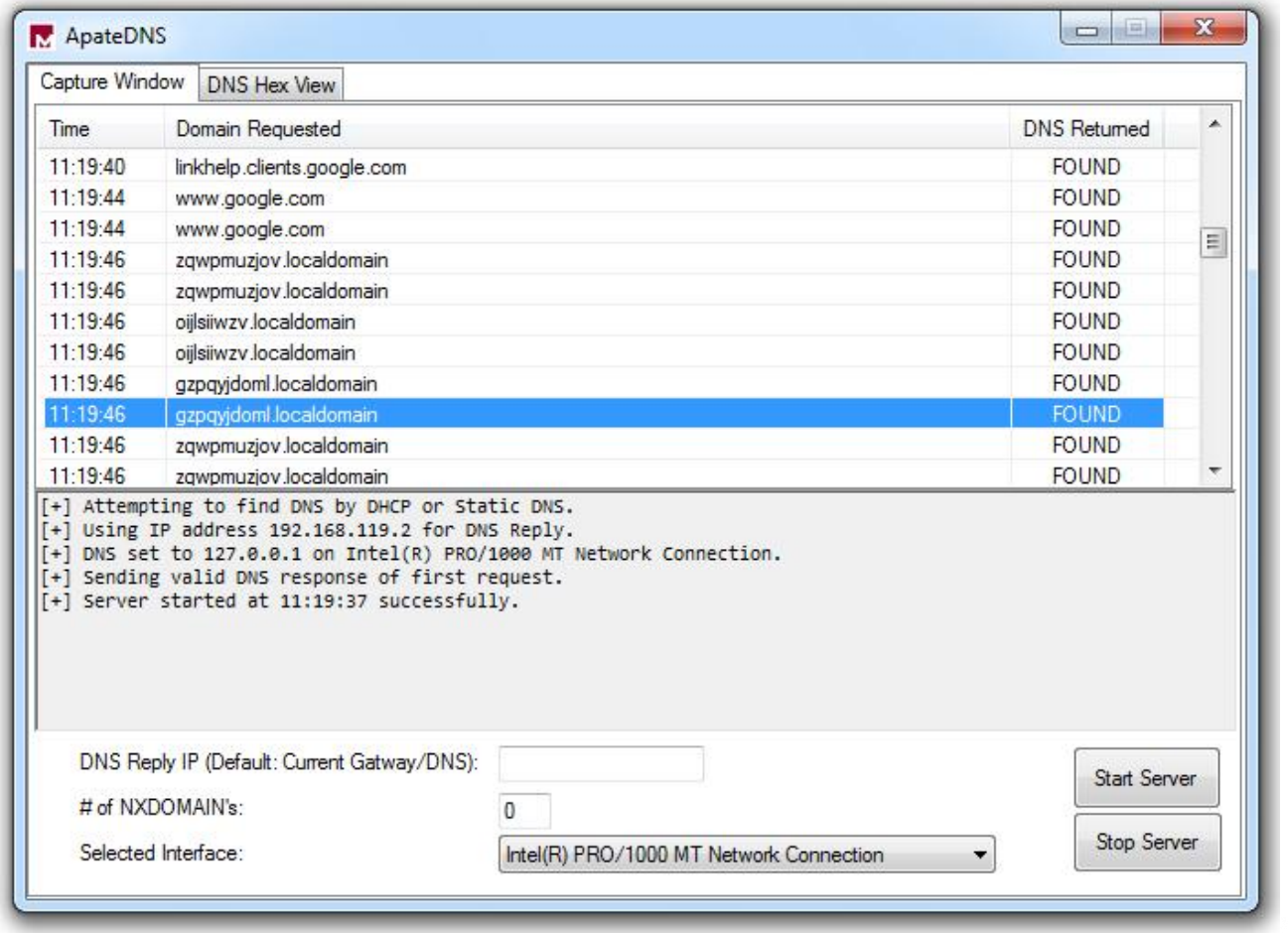
计算机病毒分析一般会进行网络隔离，隔离后如何进行网络的动态监控?

作答

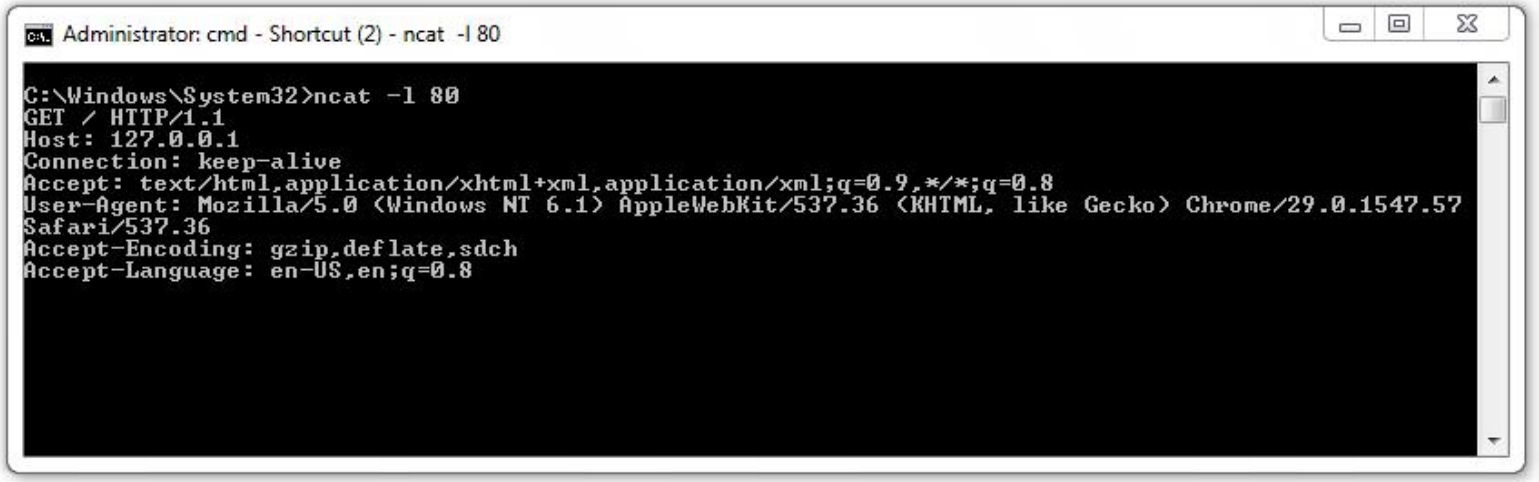
Faking a Network

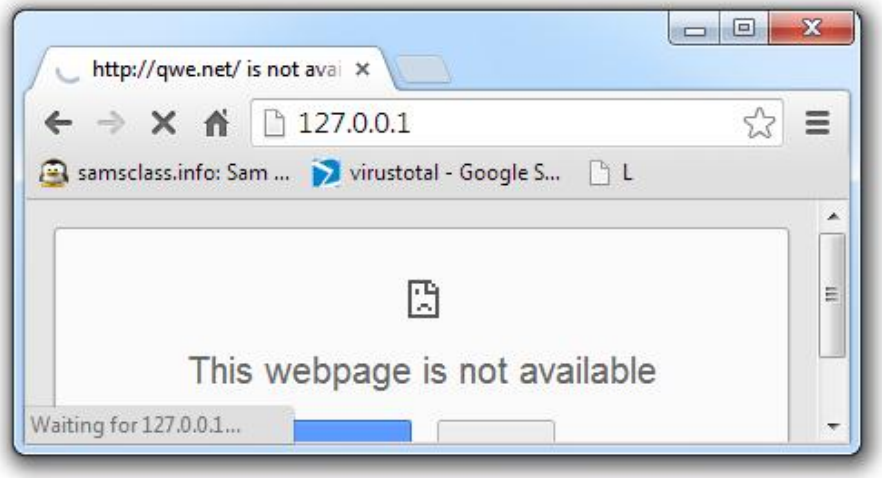
- Malware:
  - beacons out
  - communicate with a C&C server
- Fake Network
  - obtain network indicators
  - airgap between VM and Internet

Using ApateDNS to Redirect DNS Resolutions



Monitoring with Ncat (included with Nmap)

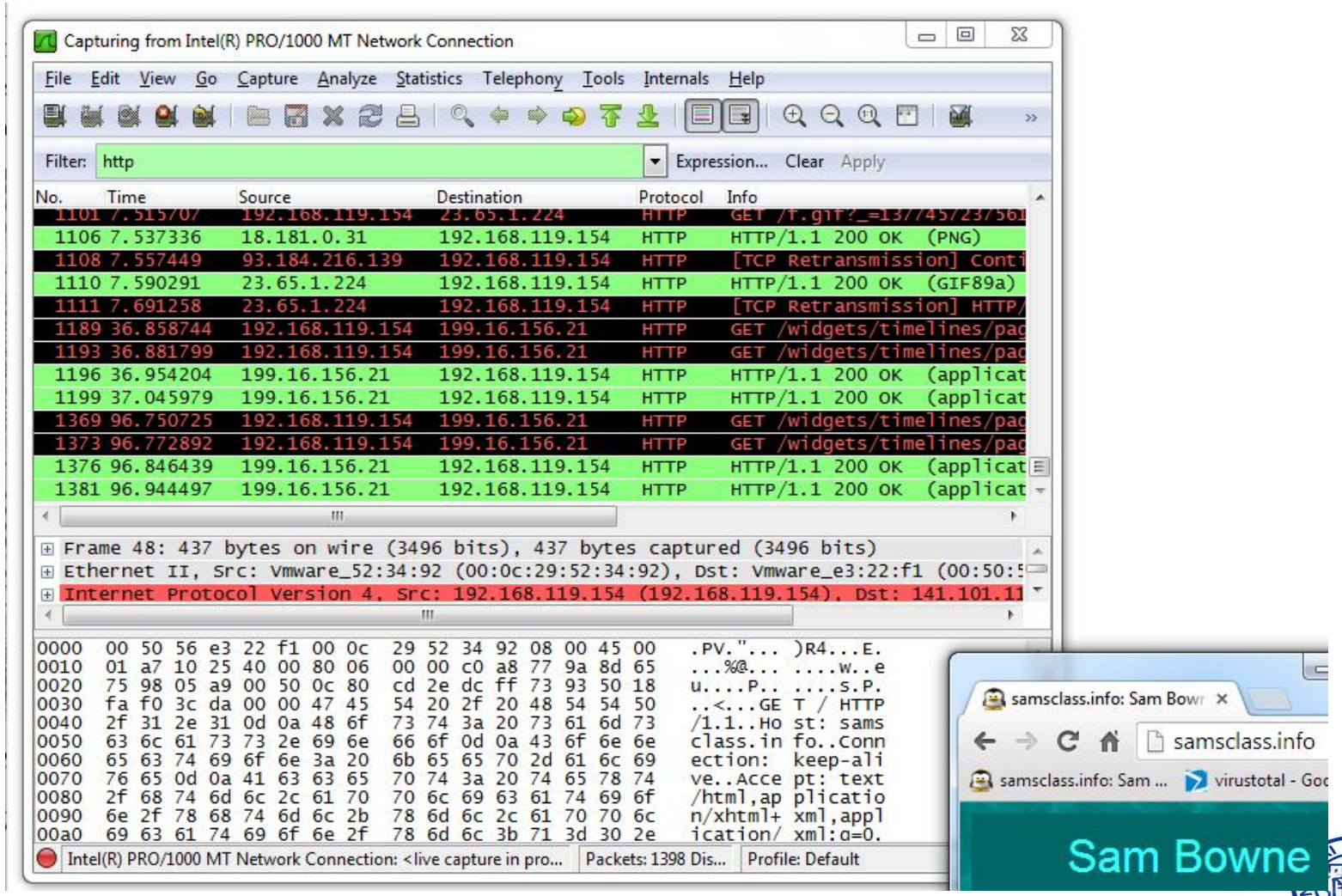




Wireshark

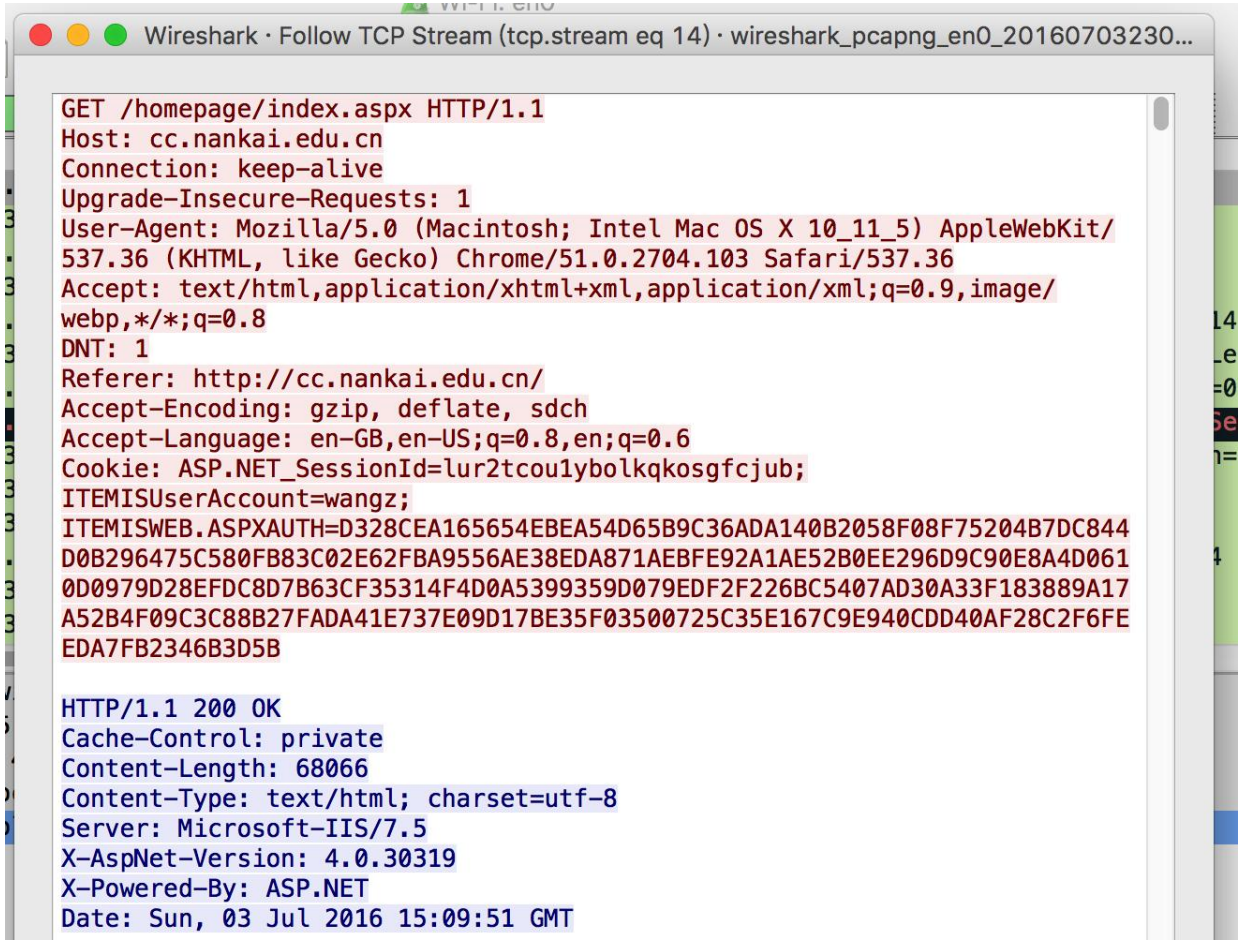
- Open source sniffer
  - capture packets
  - intercepts and logs network traffic
- Understand malware network communication
- Chapter 14 discusses protocol analysis and additional uses of Wireshark.

Packet Sniffing with Wireshark

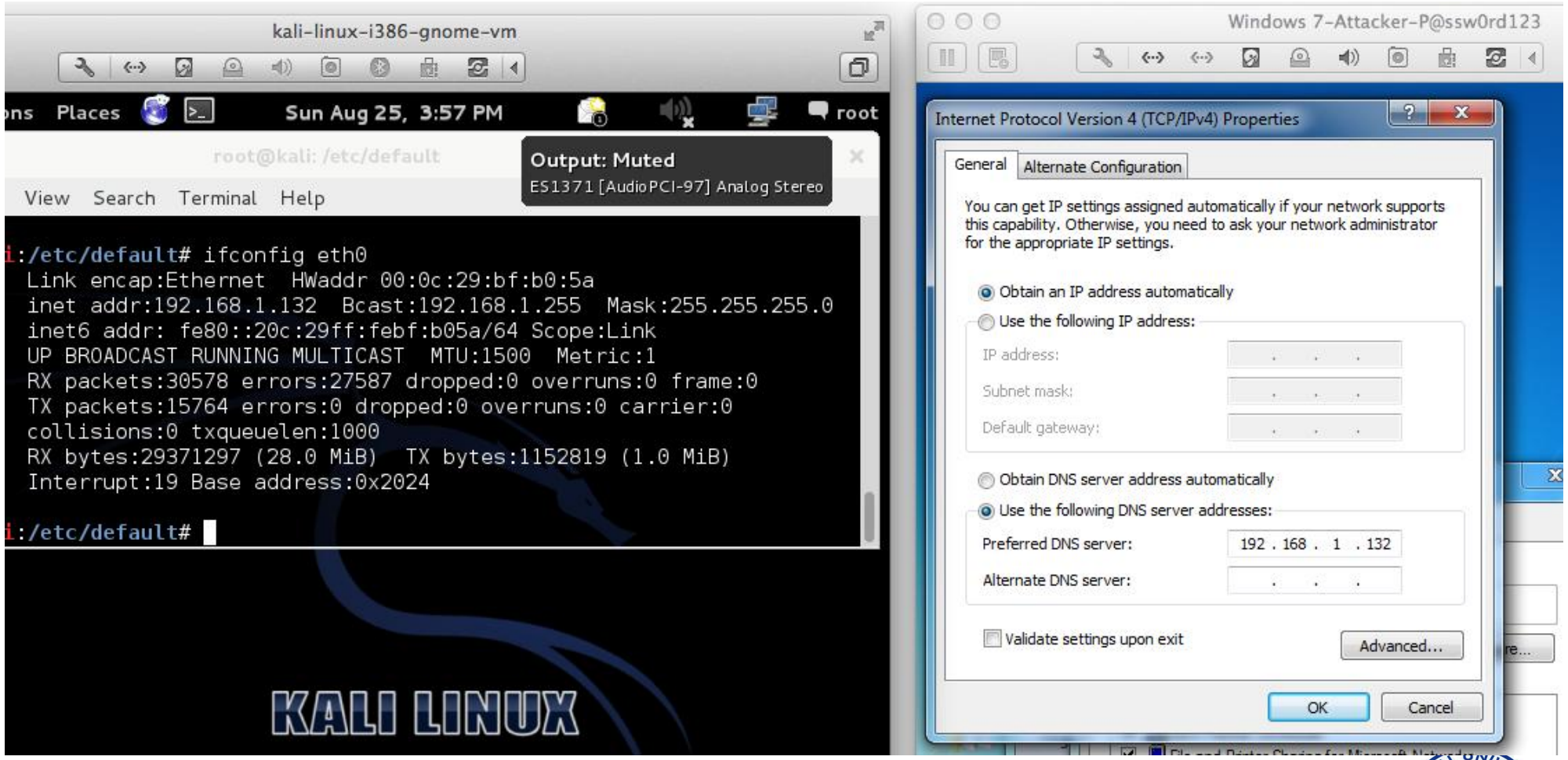


Follow TCP Stream

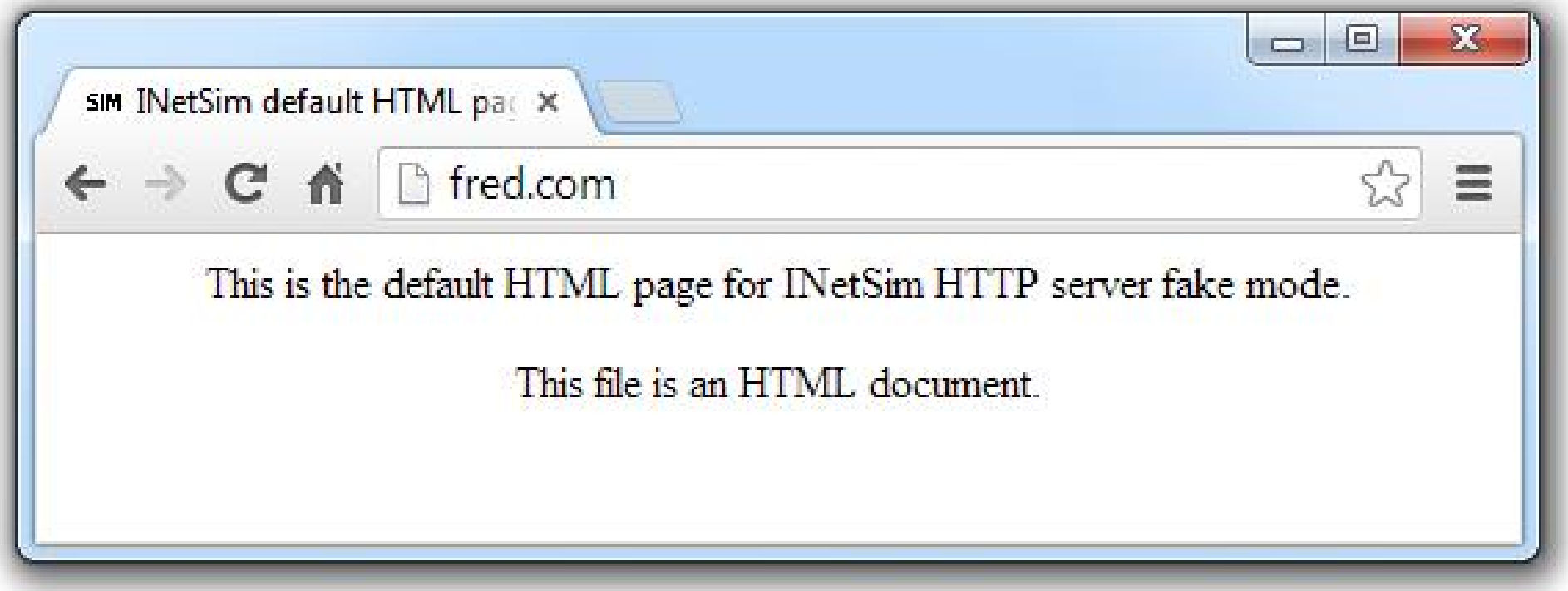
- Can save files from streams here too



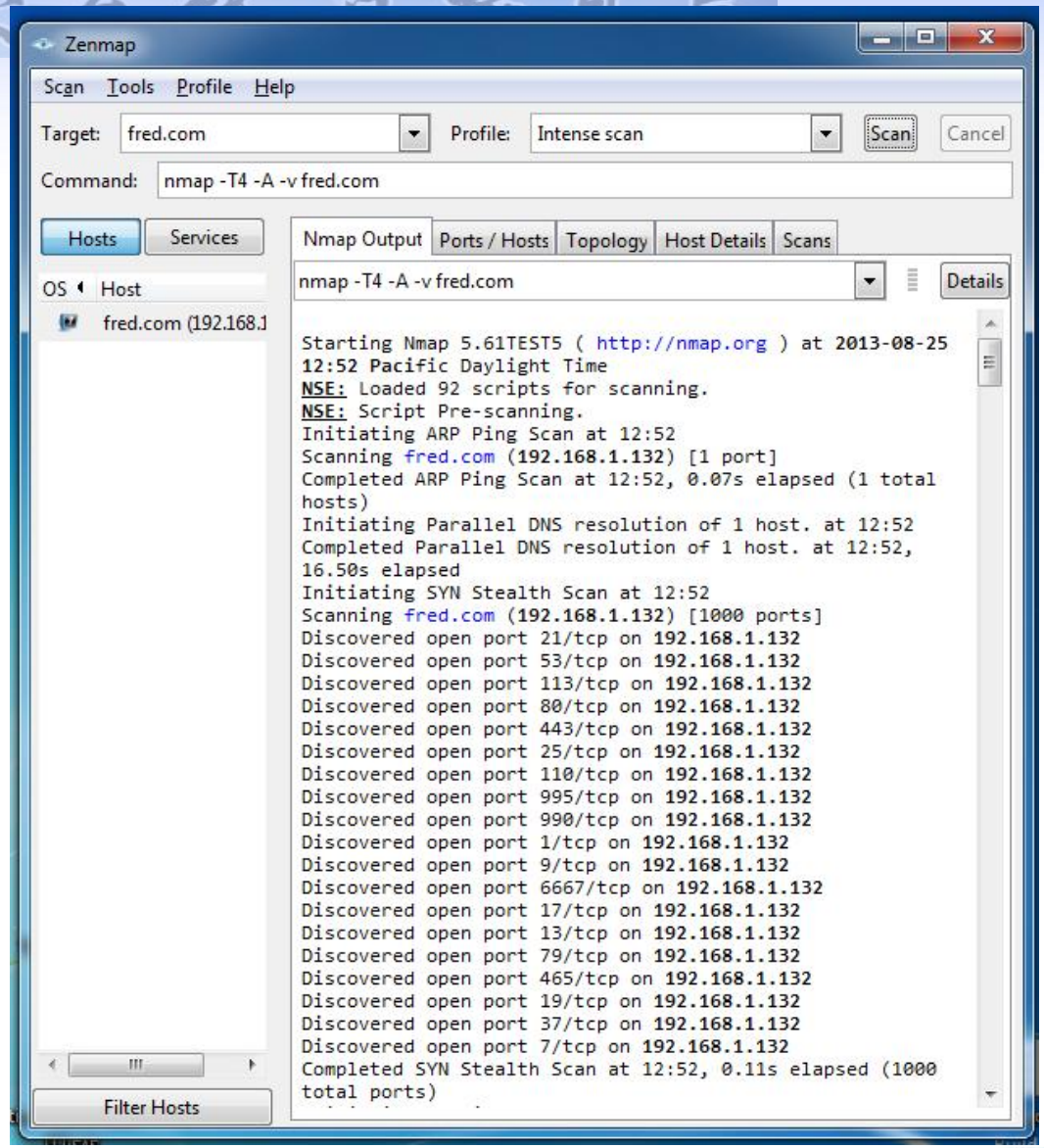
inetsim


kali-linux-i386-gnome-vm
Places
Sun Aug 25, 3:57 PM
root
root@kali: /etc/default
Output: Muted
ES1371 [AudioPCI-97] Analog Stereo
View Search Terminal Help
i:/etc/default# ifconfig eth0
Link encap:Ethernet HWaddr 00:0c:29:bf:b0:5a
inet addr:192.168.1.132 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:febf:b05a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:30578 errors:27587 dropped:0 overruns:0 frame:0
TX packets:15764 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:29371297 (28.0 MiB) TX bytes:1152819 (1.0 MiB)
Interrupt:19 Base address:0x2024
i:/etc/default#
KALI LINUX
Windows 7-Attacker-P@ssw0rd123
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 132
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

INetSim Fools a Browser



INetSim Fools Nmap



多选题 10分

设置

以下哪些技术可以用于计算机病毒网络行为的动态分析?

A Sniffing Traffic

B Simulating Services

C DNS Spoofing

提交

南開大學 Nankai University

计算机病毒动态分析实践

Using the Tools

- Procmon
  - Filter on the malware executable name and clear all events just before running it
- Process Explorer
- Regshot
- Virtual Network with INetSim
- Wireshark

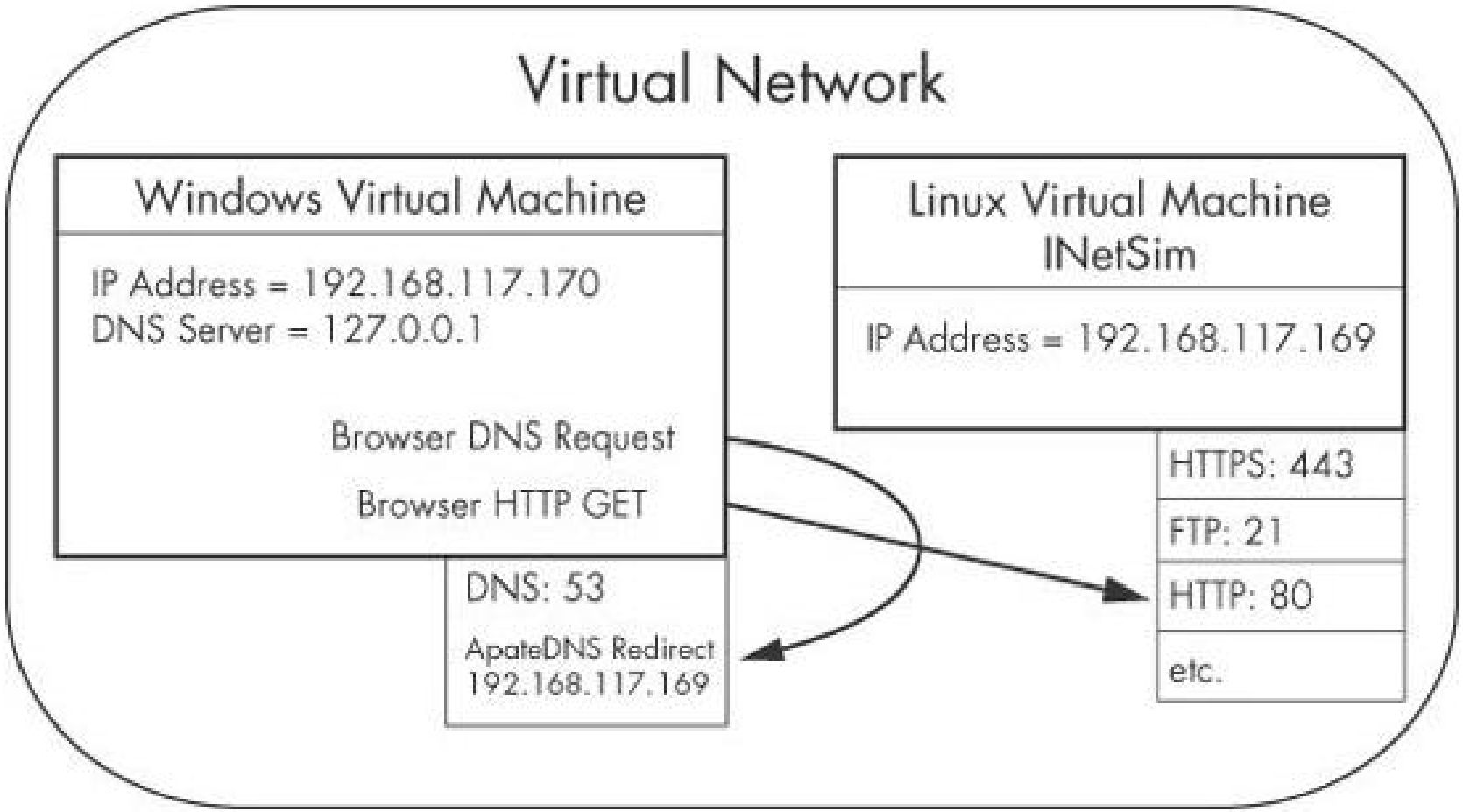


Figure 4-12. Example of a virtual network

多选题 10分

设置

Which tool reveals the services hosted by scvhost?

A Procmon

B Process Explorer

C Dependency Walker

D Regshot

E INetSim

提交

南開大學 Nankai University

设置

Which tool is specifically intended to aid analysis of the network traffic from malware?

A Procmon

B Process Explorer

C Dependency Walker

D Regshot

E INetSim

提交

Conclusion

- Assist and conform basic static analysis findings
- Most of tools are free and easy to use
- Next chapter is **Advanced Static Analysis** using reverse engineering.

Labs

Lab 3-1

Analyze the malware found in the file *Lab03-01.exe* using basic dynamic analysis tools.

Questions

1. What are this malware's imports and strings?
2. What are the malware's host-based indicators?
3. Are there any useful network-based signatures for this malware? If so, what are they?

Labs

Lab 3-2

Analyze the malware found in the file *Lab03-02.dll* using basic dynamic analysis tools.

Questions

1. How can you get this malware to install itself?
2. How would you get this malware to run after installation?
3. How can you find the process under which this malware is running?
4. Which filters could you set in order to use procmon to glean information?
5. What are the malware's host-based indicators?
6. Are there any useful network-based signatures for this malware?

Labs

Lab 3-3

Execute the malware found in the file *Lab03-03.exe* while monitoring it using basic dynamic analysis tools in a safe environment.

Questions

1. What do you notice when monitoring this malware with Process Explorer?
2. Can you identify any live memory modifications?
3. What are the malware's host-based indicators?
4. What is the purpose of this program?

Labs

Lab 3-4

Analyze the malware found in the file *Lab03-04.exe* using basic dynamic analysis tools. (This program is analyzed further in the Chapter 9 labs.)

Questions

1. What happens when you run this file?
2. What is causing the roadblock in dynamic analysis?
3. Are there other ways to run this program?

恶意代码分析与防治技术

第5章 基本动态分析

王志
zwang@nankai.edu.cn

南开大学 网络空间安全学院

2023-2024学年