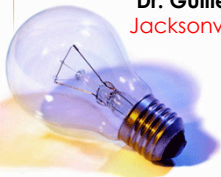


Log Processing Tools

Dr. Guillermo A Francia, III
Jacksonville State University



PS Tools Suite

- Developed by Mark Russinovich and Dave Solomon of SysInternals
- A collection of tools for viewing the detailed information about processes
- **Good news:** great tools for Sysadmins
- **Worst news:** hackers thrive with them
- Works on Windows NT, Windows 2000, Windows XP and Windows Server 2003



PSTools Suite

- [PsExec](#) - execute processes remotely
- [PsFile](#) - shows files opened remotely
- [PsGetSid](#) - display the SID of a computer or a user
- [PsInfo](#) - list information about a system
- [PsKill](#) - kill processes by name or process ID
- [PsList](#) - list detailed information about processes



PSTools Suite

- [PsLoggedOn](#) - see who's logged on locally and via resource sharing
- [PsLogList](#) - dump event log records
- [PsPasswd](#) - changes account passwords
- [PsService](#) - view and control services
- [PsShutdown](#) - shuts down and optionally reboots a computer
- [PsSuspend](#) - suspends processes





PSEXec

- PsExec is a utility that lets you execute processes on other systems, complete with full interactivity

Usage:

```
psexec [\\ \computer[,computer[...]] | @file ][-u user [-p psswd]][-n s][-l][-s | -e][-i][-x][-c [-f | -v]][-d][-w directory][-<priority>][-a n,n,...] cmd [arguments]
```



PSEXec

Computer -- Direct PsExec to run the application on the computer or computers specified. A computer name of "*" PsExec runs the applications on all computers in the current domain.

@file -- Directs PsExec to run the command on each computer listed in the text file specified.

-c -- Copy the specified program to the remote system for execution.

-d -- Don't wait for application to terminate.

-f -- Copy the specified program to the remote system even if the file already exists on the remote system.

-i -- Run the program so that it interacts with the desktop on the remote system.



PSEXec

- n -- Specifies timeout in seconds connecting to remote computers.
- p -- Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
- s -- Run remote process in the System account.
- u -- Specifies optional user name for login to remote computer.
- v -- Copy the specified file only if it has a higher version number or is newer on than the one on the remote system.



PSEXec

-priority -- Specifies -low, -belownormal, -abovenormal, -high or -realtime to run

Program -- Name of the program to execute.

Arguments -- Arguments to pass

You can enclose applications that have spaces in their name with quotation marks e.g. "psexec \\afrancia c:\long name\app.exe". Input is only passed to the remote system when you press the enter key, and typing Ctrl-C terminates the remote process.



PSEXec Examples

Launch a command console

- `psexec \\RemoteComp cmd`

Execute ipconfig on the remote system with the /all switch

- `psexec \\RemoteComp ipconfig /all`

Copy the program test.exe to the remote system and execute it interactively:

- `psexec \\RemoteComp -c test.exe`



PSEXec Examples

Run Regedit interactively in the System account to view the contents of the SAM and SECURITY keys:

- `psexec -i -d -s c:\windows\regedit.exe`

Run Internet Explorer with limited-user privileges:

- `psexec -l -d "c:\program files\internet explorer\iexplore.exe"`



PSLogList

- **PsLogList** is a utility that shows the contents of the System Event Log on the local computer in a user-friendly format. Command line options let you view logs on different computers, use a different account to view a log, or to have the output formatted in a string-search friendly way.

Usage:

```
psloglist [-?] [\computer[,computer[...]] | @file [-u
username [-p password]] [-s [-t delimiter]] [-m # | -n # | -
h # | -d # | -w][-c][-x][-r][-a mm/dd/yy][-b mm/dd/yy][-f
filter] [-i ID[,ID[...]] | -e ID[,ID[...]]] [-o event
source[,event source][,...]] [-q event source[,event
source][,...]] [-l event log file] <eventlog>
```



PSLogList Options

- @fileExecute the command on each of the computers listed in the file.
- a Dump records timestamped after specified date.
- b Dump records timestamped before specified date.
- c Clear the event log after displaying.
- d Only display records from previous n days.



PSLogList Options

- e Exclude events with the specified ID or IDs (up to 10).
- f Filter event types with filter string (e.g. "-f w" to filter warnings).
- g Export an event log as an evt file. This can only be used with the -c switch (clear log).
- h Only display records from previous n hours.



PSLogList Options

- l Dump records from the specified event log file.
- m Only display records from previous n minutes.
- n Only display the number of most recent entries specified.
- o Show only records from the specified event source (e.g. "\"-o cdrom\"").
- p Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.



PSLogList Options

- q Omit records from the specified event source or sources (e.g. "\"-o cdrom\"").
- r Dump log from least recent to most recent.
- s This switch has *PsLogList* print Event Log records one-per-line, with comma delimited fields. This format is convenient for text searches, e.g. `psloglist | findstr /i text`, and for importing the output into a spreadsheet.
- t The default delimiter is a comma, but can be overridden with the specified character.



PSLogList Options

- u Specifies optional user name for login to remote computer.
 - w Wait for new events, dumping them as they generate.
 - x Dump extended data.
- eventlog** By default *PsLogList* shows the contents of the System Event Log. Specify a different event log by typing in the first few letters of the log name, application, system, or security.

PSLogList Examples

```

C:\Malta\Tools>psloglist -i 624,625,626,627,628,644 -s security

PsLoglist v2.64 - local and remote event log viewer
Copyright (C) 2008-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Security log on \\FRANCIATABLET:
686 Security,Security,AUDIT SUCCESS,FRANCIATABLET,2/7/2007 6:40:33 AM,628,gfranc
ia,FRANCIATABLET,User Account password set: Target Account Name: Sony Target
Domain: FRANCIATABLET Target Account ID: %S-1-5-21-375897639-1085621266-164882867-1019 Caller User Name: gfrancia Caller Domain: FRANCIATAB
LET Caller Logon ID: 0x0,0x3d6a
603 Security,Security,AUDIT SUCCESS,FRANCIATABLET,2/7/2007 6:36:05 AM,628,gfranc
ia,FRANCIATABLET,User Account password set: Target Account Name: Sony Target
Domain: FRANCIATABLET Target Account ID: %S-1-5-21-375897639-1085621266-164882867-1019 Caller User Name: gfrancia Caller Domain: FRANCIATAB
LET Caller Logon ID: 0x0,0x3d6a
496 Security,Security,AUDIT SUCCESS,FRANCIATABLET,2/7/2007 6:35:26 AM,626,gfranc
ia,FRANCIATABLET,User Account Enabled: Target Account Name: Sony Target
Domain: FRANCIATABLET Target Account ID: %S-1-5-21-375897639-1085621266-164882867-1019 Caller User Name: gfrancia Caller Domain: FRANCIATAB
LET Caller Logon ID: 0x0,0x3d6a
495 Security,Security,AUDIT SUCCESS,FRANCIATABLET,2/7/2007 6:35:26 AM,624,gfranc
ia,FRANCIATABLET,User Account Created: New Account Name: Sony New Domain:
FRANCIATABLET New Account ID: %S-1-5-21-375897639-1085621266-164882867-1019 Caller User Name: gfrancia Caller Domain: FRANCIATABLET Caller
Logon ID: 0x0,0x3d6a

C:\Malta\Tools>psloglist -i 624,625,626,627,628,644 -s security > sample

PsLoglist v2.64 - local and remote event log viewer
Copyright (C) 2008-2006 Mark Russinovich
Sysinternals - www.sysinternals.com
    
```

Log Parser

- A Microsoft tool that provides universal query access to log files, XML files, CSV files, and key system resources such as the event logs, the registry, the file system, and Active Directory
- Its output can be formatted into text delimited, grid data, or a chart.
- It is a free utility and can be downloaded from:

<http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.msp>

Log Parser Examples

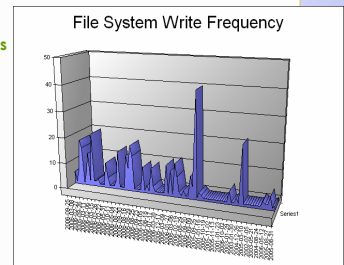
LogParser "SELECT TimeGenerated, EventTypeName INTO report.txt FROM Security WHERE EventID = 528 OR EventID=529"

```

report - Notepad
File Edit Format View Help
2007-02-07 04:38:02 failure Audit event
2007-02-07 04:38:03 success Audit event
2007-02-07 04:38:03 failure Audit event
2007-02-07 04:38:03 success Audit event
2007-02-07 04:38:12 success Audit event
2007-02-07 04:38:16 success Audit event
2007-02-07 04:38:16 success Audit event
2007-02-07 04:38:16 success Audit event
2007-02-07 04:38:17 success Audit event
TimeGenerated EventTypeName
-----
2007-02-07 06:40:12 failure Audit event
2007-02-07 06:40:13 failure Audit event
2007-02-07 08:13:35 success Audit event
2007-02-07 12:05:20 success Audit event
2007-02-07 12:05:21 success Audit event
2007-02-07 12:05:25 failure Audit event
2007-02-07 12:05:28 success Audit event
2007-02-07 12:05:31 success Audit event
2007-02-07 12:05:37 success Audit event
TimeGenerated EventTypeName
-----
2007-02-07 12:05:37 success Audit event
2007-02-07 12:05:39 success Audit event
2007-02-07 12:05:41 success Audit event
2007-02-07 12:05:54 success Audit event
    
```

Log Parser Examples

SELECT TO_DATE(LastWriteTime) as LastWriteDate, COUNT(*) as WriteFrequency INTO C:\TempChart.gif FROM C:/Temp/*.* GROUP BY LastWriteDate





Log Parser SQL-like Engine Core

- Processes the SQL-like language that includes common SQL clauses (SELECT, WHERE, GROUP BY, HAVING, ORDER BY), aggregate functions (SUM, COUNT, AVG, MAX, MIN), and a rich set of functions (e.g. SUBSTR, CASE, COALESCE, REVERSEDNS, etc.);



Log Parser Output Formats

- Write data to text files in different formats (CSV, TSV, XML, W3C, user-defined, etc.)
- Send data to a SQL database
- Send data to a SYSLOG server
- Create charts and save them in either GIF or JPG image files
- Display data to the console or to the screen



Input Format Fields and Data Types

- Data Types Supported
 - Integer
 - Real
 - String
 - Timestamp



The EVT Input Format

- To determine the input format of Windows Event type (EVT):

C:\>LogParser -h -i:EVT

Fields:

EventLog (S)	RecordNumber (I)
TimeGenerated (T)	TimeWritten (T)
EventID (I)	EventType (I)
EventTypeName (S)	EventCategory (I)
EventCategoryName (S)	SourceName (S)
Strings (S)	ComputerName (S)
SID (S)	Message (S) Data (S)



Log Parser Basic Query

LogParser -i:EVT -o:NAT "SELECT * FROM System"

-i:EVT input format is Windows Event log
 -o:NAT output format is tabulated values
 Select * * is a wildcard indicating all fields
 From System input data coming from System
 event log



Log Parser Basic Query

LogParser -i:EVT -o:NAT "SELECT * INTO Sample.txt FROM System"

Sample.txt specified output file



Log Parser Basic Query

More sample queries:

SELECT * FROM SecurityWHERE Message LIKE '%logon%'

SELECT * FROM SecurityWHERE EventID IN (547; 541; 540; 528)

SELECT * FROM SecurityWHERE EventID BETWEEN 528 AND 547

LogParser -i:FS -o:NAT "SELECT Path, Size FROM C:\MyDirectory*.*
ORDER BY Size"

LogParser -i:FS -o:NAT "SELECT Path, Size FROM
C:\MyDirectory*.* ORDER BY Size DESC"



Calling LogParser from a C# Program

```
Process myProc = new Process();
myProc.StartInfo.FileName = "Logparser.exe";
myProc.StartInfo.Arguments =
    "-i:EVT file:C:\\logon.sql";
myProc.StartInfo.WorkingDirectory =
    "C:\\Program Files\\Log Parser 2.2";
myProc.Start();
myProc.WaitForExit();
myProc.Close();
```



The Logon.sql File

```
SELECT SID, EventTypeName,  
       EventCategoryName, COUNT(*) as TotalLogons  
INTO "C:\\junk.txt"  
FROM Security  
   WHERE EventID BETWEEN 528 AND 547  
Group by SID, EventTypeName,  
         EventCategoryName  
Order by TotalLogons DESC
```