Auditing Tools

This Auditing Tools reference lists the tools that can be used for editing audit policies and viewing event logs.

Auditpol.exe (for Windows XP and 2003)

```
    AuditPol [\\computer] [/enable | /disable] [/help | /?] [/Category:Option]

       /Enable   = Enable audit (default).

       /Disable  = Disable audit.

       Category  = System    : System events
                   Logon     : Logon/Logoff events
                   Object    : Object access
                   Privilege : Use of privileges
                   Process   : Process tracking
                   Policy    : Security policy changes
                   Sam       : SAM changes

       Option    = Success   : Audit success events
                   Failure   : Audit failure events
                   All       : Audit success and failure events
                   None      : Do not audit these events
```

Samples are as follows:

```
       AUDITPOL \\MyComputer
       AUDITPOL \\MyComputer /enable /system:all /object:failure
       AUDITPOL \\MyComputer /disable
       AUDITPOL /logon:failure /system:all /sam:success /privilege:none

    AUDITPOL /HELP | MORE displays Help one screen at a time.
```

Auditpol.exe (for Windows 7)

```
    Usage: AuditPol command [<sub-command><options>]

         Commands (only one command permitted per execution)
           /?                Help (context-sensitive)
           /get              Displays the current audit policy.
           /set              Sets the audit policy.
           /list             Displays selectable policy elements.
           /backup           Saves the audit policy to a file.
           /restore          Restores the audit policy from a file.
           /clear            Clears the audit policy.
           /remove           Removes the per-user audit policy for a user account.
```

```
  /resourceSACL    Configure global resource SACLs


Use AuditPol <command> /? for details on each command
```

(You can get this on a command line on your windows 7 machine by just running the command “auditpol.”)

EVENTQUERY.vbs

```
EVENTQUERY.vbs [/S system [/U username [/P password]]] [/FI filter]
               [/FO format] [/R range] [/NH] [/V] [/L logname | *]
```

Description:
The EVENTQUERY.vbs script enables an administrator to list the events and event properties from one or more event logs.

```
Parameter List:
    /S     system          Specifies the remote system to connect to.

    /U     [domain\]user   Specifies the user context under which the
                           command should execute.

    /P     password        Specifies the password for the given
                           user context.

    /V                     Specifies that the detailed information
                           should be displayed in the output.

    /FI    filter          Specifies the types of events to
                           filter in or out of the query.

    /FO    format          Specifies the format in which the output
                           is to be displayed.
                           Valid formats are "TABLE", "LIST", "CSV".

    /R     range           Specifies the range of events to list.
                           Valid Values are:
                               'N' - Lists 'N' most recent events.
                              '-N' - Lists 'N' oldest events.
                           'N1-N2' - Lists the events N1 to N2.

    /NH                    Specifies that the "Column Header" should
                           not be displayed in the output.
                           Valid only for "TABLE" and "CSV" formats.

    /L     logname         Specifies the log(s) to query.

    /?                     Displays this help/usage.

    Valid Filters  Operators allowed   Valid Values
```

```
        -------------  ------------------  ------------
        DATETIME       eq,ne,ge,le,gt,lt   mm/dd/yy(yyyy),hh:mm:ssAM(/PM)
        TYPE           eq,ne               ERROR, INFORMATION, WARNING,
                                           SUCCESSAUDIT, FAILUREAUDIT
        ID             eq,ne,ge,le,gt,lt   non-negative integer
        USER           eq,ne               string
        COMPUTER       eq,ne               string
        SOURCE         eq,ne               string
        CATEGORY       eq,ne               string
```

NOTE: Filter "DATETIME" can be specified as "FromDate-ToDate"
  Only "eq" operator can be used for this format.

```
    Examples:
        EVENTQUERY.vbs
        EVENTQUERY.vbs /L system
        EVENTQUERY.vbs /S system /U user /P password /V /L *
        EVENTQUERY.vbs /R 10 /L Application /NH
        EVENTQUERY.vbs /R -10 /FO LIST /L Security
        EVENTQUERY.vbs /R 5-10 /L "DNS Server"
        EVENTQUERY.vbs /FI "Type eq Error" /L Application
        EVENTQUERY.vbs /L Application
                /FI "Datetime eq 06/25/00,03:15:00AM-06/25/00,03:15:00PM"
        EVENTQUERY.vbs /FI "Datetime gt 08/03/00,06:20:00PM"
                /FI "Id gt 700" /FI "Type eq warning" /L System
        EVENTQUERY.vbs /FI "Type eq error OR Id gt 1000 "
```

PsLogList.exe

```
PsLogList dumps event logs on a local or remote NT system.

Usage: psloglist [\\computer[,computer2[,...] | @file] [-u username [-p
password]]] [-s [-t delimiter]] [-m #|-n #|-d #|
-h #|-w][-c][-x][-r][-a mm/dd/yy][-b mm/dd/yy] [-f filter] [-i ID,[ID,...]] | -e
ID,[ID,...]] [-o event source[,event so
urce[,...]]] [-q event source[,event source[,...]]] [[-g|-l] event log file]
<event log>
     @file     Psloglist will execute 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 event log after displaying.
     -d        Only display records from previous n days.
     -e        Exclude events with the specified ID or IDs (up to 10).
     -f        Filter event types, using starting letter
               (e.g. "-f we" to filter warnings and errors).
     -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.
     -i        Show only events with the specified ID or IDs (up to 10).
     -l        Dump the contents of the specified saved event log file.
```

```
-m        Only display records from previous n minutes.
-n        Only display n most recent records.
-o        Show only records from the specified event source or sources
          (e.g. "-o cdrom").
-p        Specifies password for user name.
-q        Omit records from the specified event source or sources
          (e.g. "-q cdrom").
-r        Dump log from least recent to most recent.
-s        Records are listed on one line each with delimited
          fields, which is convenient for string searches.
-t        The default delimiter for the -s option is a comma,
          but can be overriden with the specified character. Use "\t"
          to specify tab.
-u        Specifies optional user name for login to
          remote computer.
-w        Wait for new events, dumping them as they generate (local system
          only.)
-x        Dump extended data.
eventlog  Specifies event log to dump. Default is system. If the
          -l switch is present then the event log name specifies
          how to interpret the event log file.
```

Recommended Internet Sites

- Windows Security Log Events: https://web.archive.org/web/20160726161728/https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.