**Windows**

**Event Logging API (Windows 2003, XP, 2000)**

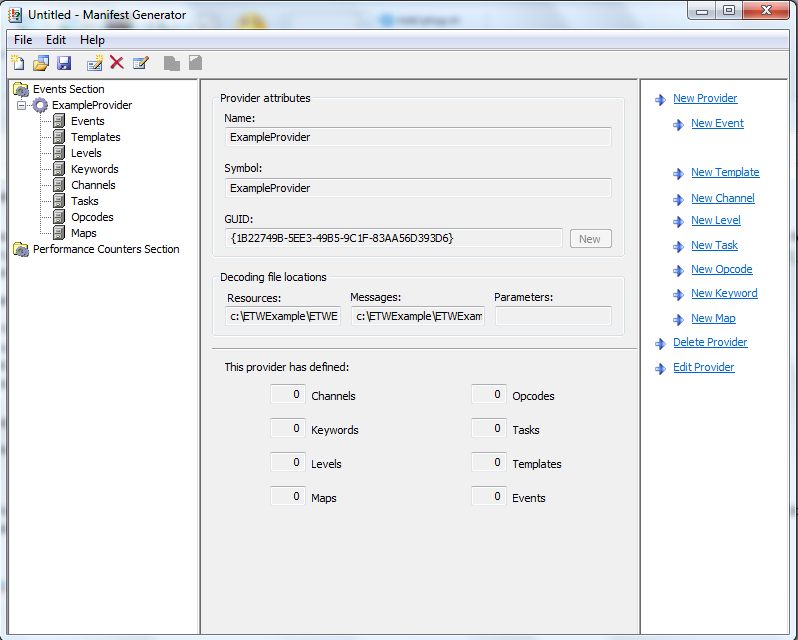
* Use the following C++ code to query for events logged in API
  + <https://msdn.microsoft.com/en-us/library/windows/desktop/bb427356(v=vs.85).aspx>
  + Puts all logged events on a buffer and prints the contents of the buffer
* Use the following C++ code to receive notifications of event logs
  + <https://msdn.microsoft.com/en-us/library/windows/desktop/aa363677(v=vs.85).aspx>
  + Loops through all event logs and if a new event appears, displays a notification

**Windows Event Log (Vista-Win10)**

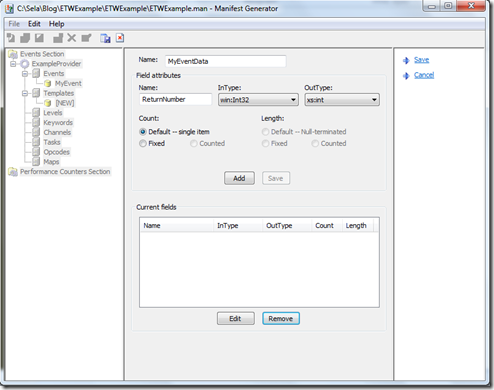
* Download Windows SDK
  + <https://www.microsoft.com/en-us/download/details.aspx?id=8279>
  + Windows tool kit that allows users to create applications. We’ll use this to create an application for log monitoring
* Choose which events your event manifest will record
  + Recommended:
    - Authentication successes/ failures
    - Authorization failures
    - Application and related systems start-ups and shut-downs, and logging initialization (starting, stopping or pausing)
    - Use of higher-risk functionality e.g. network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, etc.
* Create an event manifest
  + Run ECManGen.exe from Windows SDK \bin directory

1. **Create a new event provider.** This step requires two actions:

* First, select the “Events Section” node in the far left pane and then “New Provider” in the far right pane.
* Second, give the provider a name, symbol, and GUID. Set the Resources and Messages boxes to the full path where the application will be installed. Click “Save” in the far right pane.
  + Use the example from the example section for each of the events you are going to be putting in your event manifest

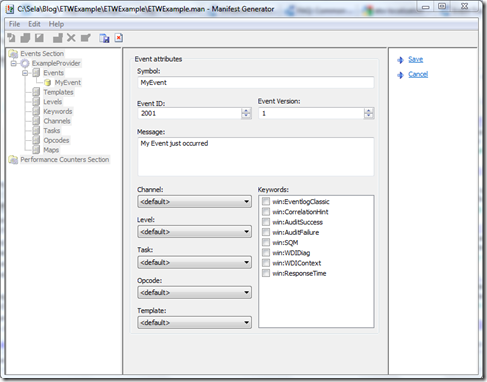


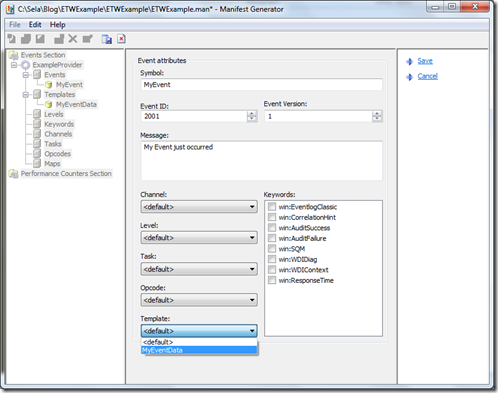
2. **Create a new template to define parameter types for each message that requires input parameters.**



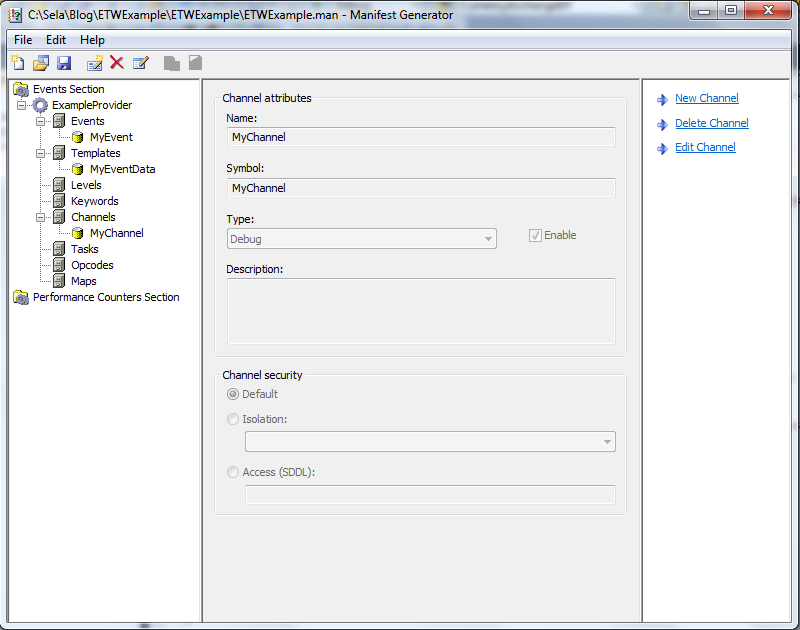
3. **Define metadata used to tag events.**

4. **Create events by giving each a symbol, event ID, message text and template.** When you write the message text, use %1, %2, %3, …, %12 to specify the positions of each parameter. Make sure the event template matches the format of the message text with parameters. Assign any channels, levels, tasks, keywords, and opcodes which apply to the event. Save the event. Do the same for all remaining event messages your application will produce.





5. **Save the event manifest to your project directory.**



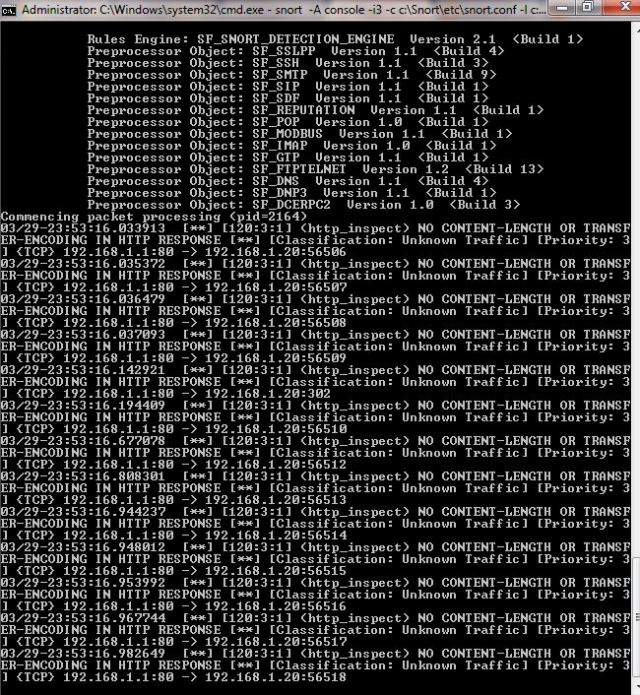
**Windows Defender**

* Download most recent version
  + Note:this will not run on anything earlier than Windows XP SP2
  + https://www.microsoft.com/en-us/windows/comprehensive-security
* Set up a more frequent scan to search for malware
  + Search for and open schedule tasks
  + In the left pane, expand **Task Scheduler Library** > **Microsoft** > **Windows** and then scroll down and double click the **Windows Defender** folder
  + In the top center pane, double click **Windows Defender Scheduled Scan**
  + Select the **Triggers** tab, and then select **New**
  + Set your time and frequency (every half hour?) and then select **OK**

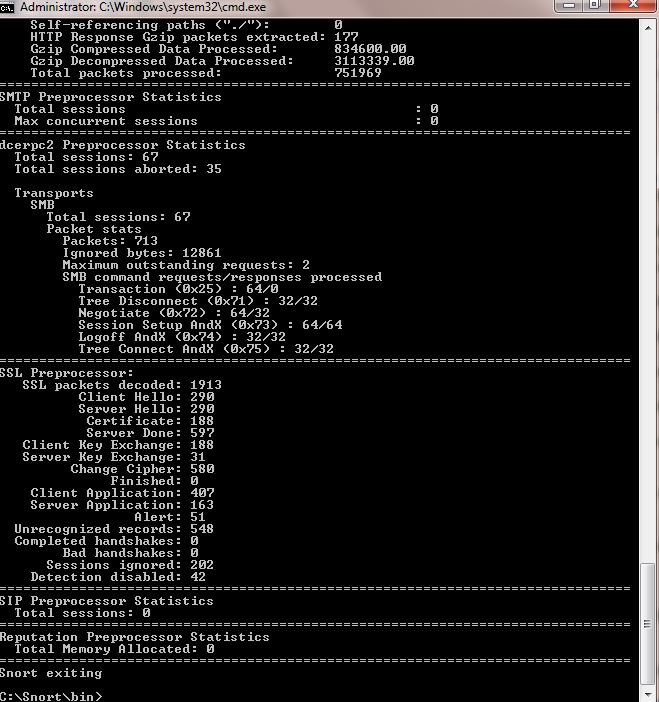
**Snort (IDS mode)**

* Ensure you have WinPcap installed
  + https://www.winpcap.org/install/
* Download most recent version from snort.org/snort-downloads
* Download Rules
  + <https://www.snort.org/snort-rules>
  + Extract Rules file
  + Copy and paste extracted files to C:\Snort\rules
  + Copy the “snort.conf” file from the “etc” folder of the extracted folder into “C:\Snort\etc”
* Edit the conf file
  + var HOME\_NET 192.168.1.0/24
    - Change the address on this line to your network address
  + Repeat for DNS servers
* Open a command prompt and navigate to “C:\Snort\bin”
* Change the RULE\_PATH variable to the path of rules folder.
  + It should now read “var RULE\_PATH c:\snort\rules”
* Change the path of all library files with the name and path on your system. and you must change the path of snort\_dynamicpreprocessorvariable.
* C:\Snort\lib\snort\_dynamiccpreprocessor
  + Do this to all library files in the “C:\Snort\lib” folder. The old path might be: “/usr/local/lib/…”. you will need to replace that path with your system path. Using C:\Snort\lib
* Change the path of the “dynamicengine” variable value in the “snort.conf” file
* Add the paths for “include classification.config” and “include reference.config” files.
  + include c:\snort\etc\classification.config
  + include c:\snort\etc\reference.config
* Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.
  + include $RULE\_PATH/icmp.rules
* You can also remove the comment of ICMP-info rules comment, if it is commented.
  + include $RULE\_PATH/icmp-info.rules
* To add log files to store alerts generated by snort, search for the “output log” test in snort.conf and add the following line:
  + output alert\_fast: snort-alerts.ids
* Comment (add a #) the whitelist $WHITE\_LIST\_PATH/white\_list.rules and the blacklist
* Change the nested\_ip inner , \ to nested\_ip inner #, \
* Comment out (#) following lines:
  + #preprocessor normalize\_ip4
  + #preprocessor normalize\_tcp: ips ecn stream
  + #preprocessor normalize\_icmp4
  + #preprocessor normalize\_ip6
  + #preprocessor normalize\_icmp6
* Save snort.conf file
* Run on command line
* snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3

Example output:



After done scanning:



**(Windows Hardening)**

* Change all default passwords
* Have firewall filter on port 445
  + Defends against ms08\_067\_netpai
* In the Security Policy Editor under “Local Policies->User Rights Assignment” there is a policy called “Deny access to the computer from this network”
  + Ensure this is enabled to defend against remote access to local accounts, specifically admin
* Set the RunAsPPL registry key for the LSA
  + Prevents code injection that can compromise credentials
    - Prevents code injection that can compromise credentials
      * Open the registry editor (regEdit.exe) and navigate to the registry key that is located at: HKEY\_LOCAL\_MACHINES\SYSTEM\CurrentControlSet\Control\Lsa
      * Set value of the registry key to “RunAsPPL”=dword:00000001.