Laboratory works nr 1

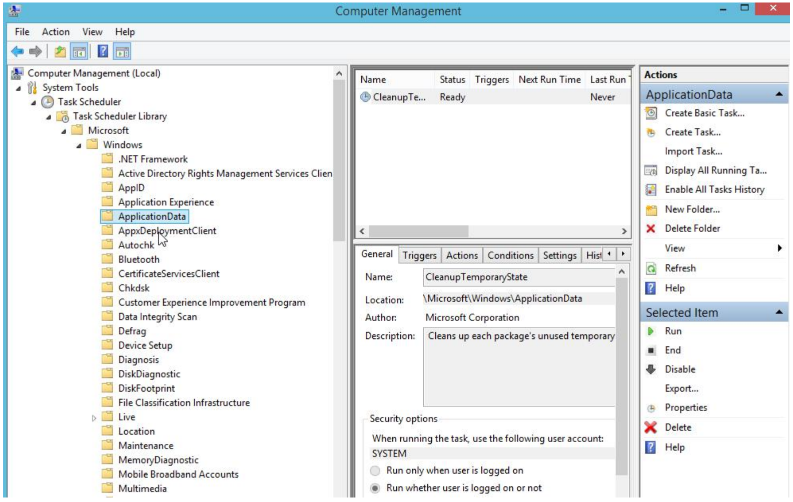
Workstation auditing with MS Windows

Security audits for an operating system can be internal or external and can be performed continuously or asynchronously.
SE will use the virtual machine available on the station to install and test each of the tools that will be shown below.
In this laboratory we will focus on the analysis of instruments that can be used for internal security audits

1. Analyze security settings in the internal Windows registry. (mscoonfig)
2. Analysis of active connections with tcpview or netstat (also test Microsoft Network Monitor, GlassWire and Wireshark)
3. Antivirus Analysis
4. IDS

Windows Scheduling

Tweaking it allows performance optimization, as well as tracking the status of direct or collateral applications that track various aspects of the system.



Name	Status	Triggers	Next Run Time	Last Run
CleanupTe...	Ready			Never

Name: CleanupTemporaryState

Location: \Microsoft\Windows\ApplicationData

Author: Microsoft Corporation

Description: Cleans up each package's unused temporary

Security options

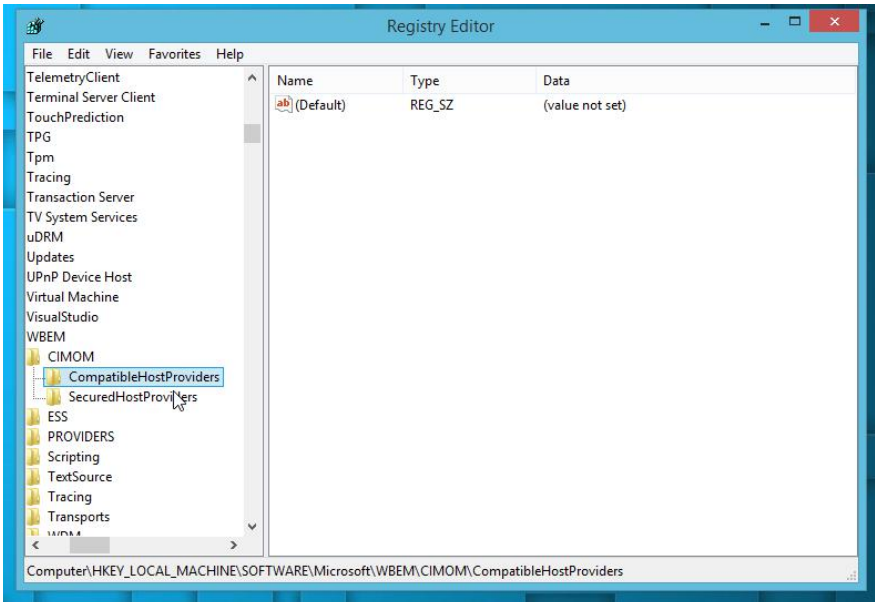
When running the task, use the following user account:
SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

Regedit

With Regedit we can check/analyze/check most of the keys and settings used by Windows. This is where additions and or changes are made by many unwanted friends of all sorts (electronic app or real guys).



Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\CompatibleHostProviders

Intrusion Detection Systems – Windows supported also

1. Snort

It is a utility provided by CISCO, in the category "oldest but goldest" that can be installed on both on Windows and Linux. Although it is slightly outdated compared to Suricata, which has a number of advantages, it is still a presence worth considering both in terms of the latest improvements that have given it a “new breath” and due to a fairly large knowledge base in terms of the user experience in its use. For many people his skills cannot be used completely because it requires knowledge of Ruby language.

When installing on Windows, it will also require WinPcap to be installed because it is necessary to be able to complete network traffic monitoring. Windows will install in the default snort directory on drive C if another path is not provided. It can be launched from the bin subdirectory. Since initially it was only for Linux, the interaction is all console type and given the previous observations it remains recommended only for users who have decent knowledge in the field of information security. It also allows the development of custom detectors using Lua-c which will probably keep it active for a long time on the market.

2. OSSEC

Another free and "open source" IDS that was designed for servers but allows you to install a client and on a Windows machine. It is based on the IDS log-based concept and allows us to develop custom applications that analyze the logs generated by it. It also allows us to check the integrity of files on both Linux and Windows, check the registry for Windows, as well as *rootkit* analyses for Linux or even counter actions if configured/programmed properly.

It supports a wide variety of plugins that in the case of IDS are called decoders. At the client level outside of network traffic monitoring will generate alerts (by monitoring logs) about e-mail or questionable activity of some executables active in the system. Custom decoder development is done using XML files but also requires knowledge of using the *regex* for more complicated analysis of log files.

3. Suricata

He can be seen as the Successor of Snort but with a series of assets that the previous one has not yet acquired. Moreover, the level of its integration with cloud services and tools is native, which gives it a great advantage over it. Unfortunately being relatively new the support provided by the community is relatively low and then for many administrators its use is relatively limited to the use of the console or additional components that allow visual management.

These things do not diminish its current value but make it cumbersome to develop more customized tools for the user's needs. It is oriented towards network monitoring but the level of reactivity to attacks it possesses is superior to the snort. It is in the category "real time intrusion detection", "inline intrusion detection", "network monitoring" but also "pcap processing".

For the detection of more complex threats there is support for Lua scripts. Because it uses YARL and JSON for input and output files it is compatible with tools such as SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases.

4. Zeek Network Security Monitor

It was originally called Bro and remained free BSD licensed software. It takes a slightly different approach to standard IDSs. One advantage is that it was built for maximum flexibility. As a result it will allow, with the help of script languages that are domain-specific, to develop modules that allow custom monitoring for each site under control.

It is dedicated to managing high-performance networks and sites and loading. Because is not based on classical approaches to signature sets or certain standard detection schemes result that it is not recommended for average users either.

As in the previous case it provides detailed logs on network activities while allowing us top-level semantic analyses on them through dedicated modules made available. It also extensively monitors the application level in the ISO-OSI model. It has been designed with open interfaces which allows almost unlimited interoperability including real-time exchange of information with other profile applications.

5. Sagan

It is a log monitoring tool that can integrate data generated by the snort. The following no longer require special presentations:

- **Comodo**
- **Kaspersky Total Security 2018**
- **Cylance Smart Antivirus**
- **Trend Micro Business Solution**
- **Norton Internet Security**

Laboratory job

Use NAT in network configuration for virtual machines

In the minimal Machine of Windows 8 available install test and possibly configure the utilities shown above.

Homework

Resume these tests on your personal laptop and report on its behavior for each application in the lab (in terms of additional system-induced load - a comparative table tracking memory, processor, file handle, virtual memory, etc.). The report will also specify the hardware/software features of the system used for testing.