Auditing Tools for Windows Systems

Institutional Affiliation

Students Name

Date

**Introduction**

Security controls are major tools in an organization but the best way that helps in having an efficient auditing tool is by comparing all the accessible security controls tools for Windows systems in an organization. The Microsoft Security Baseline Analyzer (MBSA) that is in Graphical User Interface (GUI) version has been one of the most replicated techniques used by IT professional in handling security malware issues. They are compatible with most computers and they profiled with more than one baseline. But not forgetting Shavlik NetChk Protect, Security Configuration and Analysis and Secunia Security Analyzers which also provide extended scanning abilities. In regard to this, MBSA in GUI version is the most efficient, easy and secure security controls tools to use in handling suspected malware scenarios in any given organization as much the other auditing tools play handy.

**Windows Systems Auditing Tools in Suspected Malware Scenarios**

In the first scenario, whereby a schedule weekly analysis has to be created in a data center to enable a command that should run as a scheduled job and report any available patches for the Windows Server 2012 R2 operating system that have not been installed. This includes the Internet information services (IIS) Web server and the structured query language (SQL) server that have also not been installed. Regarding Rountree (2011), MBSA-GUI has one button away ability in Windows operating systems and even other operating systems such as Ubuntu since its compatible that is situated in the Windows key where dialog boxes are the real help. MBSA-GUI systems have dialog help boxes that enhance to program a scanning schedule in the designated or the chosen computers’ for a daily, weekly or customized days’ time frame. They check for IIS vulnerabilities, SQL vulnerabilities, security updates and most importantly they generate an automatic report. Therefore, a weekly schedule analysis will be created and with the help of the MBSA-GUI automatic program, it will generate an automatic weekly scan and report. Which makes it the best auditing tool to be used in such a doubted malware situation.

In the second scenario, whereby there is a need for scanning available vulnerabilities in old version products of Windows, inclusive of Microsoft office 2000. With the guiding and automatic tools that MBSA uses in its scanning process for operating systems, Shavlik NetChk Protect will be efficient in helping to profile such a windows computer. This is because Shavlik NetChk Protect has the capabilities of patching malware issues with a single agent for a machine. This means that the software will autorun with the help of the MBSA commanding line thus identifying the vulnerabilities of the older version programs in windows virtual machines through the setup wizard and updating them to the latest but giving out reports of the susceptibilities.

In the third scenario, where an organization is encouraging its employees and contractors to be using malware scanners both at home and at work thus the need for selecting a single vendor able to process scanning software for home and work virtual machines. In such a situation of suspected malware, Secunia Security Analyzers are the best auditing tools to be used since a single vendor is able to streamline resulted in reports from different computers. According to Rountree (2011), Secunia Security Analyzer has the capability of surpassing hard to identify malware with its super technique of fuzzing and binary analysis. They also provide reports and they are compatible with Windows computers. The last scenario, which is, comparing several types of computer settings to a conforming template developed created to analyze if any configuration settings will change while in use. In such a situation, the best tool to use is the Security Configuration Analysis which has the aptitude of snapping in more saved configurations in different kinds of computers. It also has the capability of storing complex configurations making it the best tool to be used in such a scenario

**Conclusion**

The windows systems have quite a variety of auditing tools that help in reducing the vulnerabilities of systems in many organizations. It depends on the complexity and the type of scenario that an organization falls in, in order to choose the most efficient auditing tool that helps in clearing vulnerable malware in computer systems.

References

Rountree, D., (2011) Security for Microsoft Windows System Administrators: *Introduction to*

*Key Information Security Concepts*. Elsevier Inc., USA