It is an essential network security management process to grasp the network security status precisely and rapidly by identifying the vulnerabilities on the network. Manual check-up method by security experts and automatic vulnerability assessment tools can be used to check the network security. But it is an inevitable option to use the automatic vulnerability assessment tools to cover large-scale network. There are lots of automatic vulnerability assessment tools available in the market. But the vulnerability assessment tool cannot find an acceptable percentage of vulnerabilities by itself. When multiple vulnerability assessment tools are used, integrating and analyzing the results can be a time-consuming job. This research set out to develop an automated network vulnerability assessment model (AADRA), which can integrate various kinds of vulnerability assessment tools with the purpose of complementing each other. A log parser application was developed and forms an integral part of this research. The log parser is used to analyze the data that is produced by the vulnerability assessment tools. It takes a large data file as input and depending on the selected action gives output accordingly. After implementing the prototype experimentation was undertaken to compare the time it could take to do a manual interpretation of the data from the Network vulnerability assessment tool and the log parser analysis. Through evaluation tests done using the prototype on the University of Nairobi network, it showed that the Log parser application improved the analysis process by a factor of fourteen.