Report Introduction: Working Draft

There is no such thing as a machine with absolute security (one which is connected to the internet) but there are steps to make a machine as secure as possible. Most machines have their own built-in Firewall these days (hardware and/or software). Yet there are many ways to breach their security. A Firewall any hardware or software that is used to prevent and/or remove malware from entering or accessing a computer system that has an active connection to the internet. Internet connection leaves a machine vulnerable to hackers who can access financial data, personal information, remote login and much more. A Firewall behaves as a shield between you machine and the internet. When a machine is connected to the internet it is constantly uploading and downloading information. On the internet, information is sent and received in packets. A machine does not directly send and receive packets itself, the Firewall does that on behalf of the machine and filters and/or checks each packet for its proper protocol (to make sure that the packet is authentic) and free of malware. After the Firewall is finished filtering out the packets, it blocks any packet that does not match with the given security criteria. The threat of malware can be found everywhere on the internet, from e-mails, games, IMs, etc. The threat is higher when using an application that is connected to a server (example: multiplayer gaming) because the machine is visible and accessible (up to a certain limit) to a variety of users. The purpose of this report is to inspect the vulnerability of the computer systems taken with and without the use of different types of Firewall. There will be 4 different computer systems considered; Machine 1, Machine 2, Machine 3 and Machine 4. All systems will have the same specifications excluding the Firewall. The variance in levels of security achieved using different settings of Firewall is the main focus of the inspection. Whether the inspection will be conducted on virtual machines or real ones is yet to be decided as some malwares can corrupt a machine permanently. The evaluation is not based just based on whether malware can infiltrate a machine but how much damage can be prevented in each variation of Firewall. There will be a glossary at the beginning of the report for the reader to have a thorough understanding of the inspection. After the tests are done for each machine (Machine 1-4), they will be evaluated based on the functionality of the machine compared to before and after the malware attack and how much data is safe, recoverable, and permanently damaged. There will be some sort margin where the machines will be graded with either ranks or percentage, etc. This report is meant to help its readers have a better insight on Firewall and the internet and helps them to have a safer browsing experience of the internet.