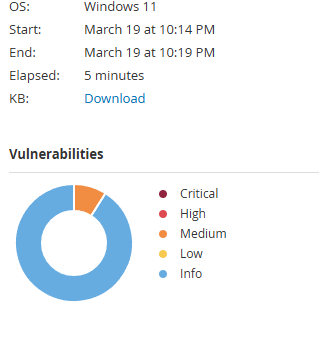
**Observations**

The current network that is being utilized has a gateway router that is in between the wireless access point and the modem provided by spectrum. The routers are of the same brand GLiNet. Both routers have been configured prior to conducting this SOHO project and are up to date with firmware. Some quick configurations, not utilizing a default password and wireless network security consists of WPA2/WPA3. The gateway router is focused on routing and not providing wireless access. The routers do not have any firewall rules applied to them at this moment in time. The main focus is on the desktop computer. There is more of a home office network, but still upholding the regards of a SOHO network setup. In regards to the desktop computer, it is currently up to date with Windows. Outside of being up to date with the operating system is that it lacks a host based firewall and an intrusion prevention system (IPS). There is only one firewall rule applied to the desktop and that is a rule on port 23 in blocking telnet access. The desktop does not have a virtual machine created on it. Virtual box is currently installed, but there is no virtual machine image setup. The virtual machine consideration would be a Linux OS, Ubuntu.

**Vulnerability Scanner Results**



For further observations, Nessus Essentials was installed and utilized to get a better understanding of the current vulnerability level of the desktop computer. A plugin had to be installed called terrascan in order for Nessus to conduct scans. Presently displayed on the scanner are 225 vulnerabilities. Of the 225 vulnerabilities, 223 are info based with the rest being at the value of medium. These severity values utilize CVSS v3.0 scoring system. The two medium level vulnerabilities relate to Secure Sockets Layer (SSL) certificate cannot be trusted and Server Message Block (SMB) signing not required. The SSL certificate concern is for the certificate authority (CA). Typically, this is in regards to websites. The other vulnerability is more of an insurance of integrity of a message to a server. The current desktop is not connected with any servers at this time. The majority of the vulnerabilities stem from the port scan within Nessus. This gives an idea in regards to modifying a host based firewall and reviewing used ports and unused ports. While this scanner can check if an application is up to date, it cannot verify if a browser has good security levels to it.

**Browser Configuration**

There are three browsers that this computer utilizes: google chrome, edge, and Firefox. Of the three present, the one with the most browser configuration would be that of Firefox. It has a significant amount of extensions to help enhance security to it. Such as uBlock origin and configurations like saving passwords and history off. It is also a browser that can be easily transferred to Linux as the settings can be saved and copied over. As for Google chrome and edge, these two browsers have minimal to no configurations present on them. The weak configurations make it more at risk of an attack such as man in the middle, cross site request forgery, or even cross site scripting. Since, Firefox is easily configurable it will be the configured browser within the virtual machine.