Inventory Assets on Network and Identify Vulnerabilities

Student’s Name

Institution

Date

**Inventory Assets on Network and Identify Vulnerabilities**

Network vulnerability is critical aspect for the security of network infrastructure and an organization data security (Ossi, 2018). Vulnerability is caused by several factors include ignorance or recklessness of employees. However, the determination of vulnerability is based on the level of risk, since the precaution is taken based on the risk. The scan of the vulnerability indicates that cento 6/7 Firefox is one of the most venerable in the organization and therefore, the risk factor is high (Ahmad, 2018). The scan score indicates that that the CVSS Scare of 9.3 and CVSS had a temporal score of 6.9 and the CVSS vector sectors. It is therefore, evident that the vulnerability is on the access at the end points of the network. The system vulnerability by loose application of system and lack of proper protection and security policies hence the system can be attacked by hackers, and virus attack (King, 2014). These threats are usually get entry into the system based on the vulnerability, which are created by uses. The implementation of network security would be the best ideal method to product the system.

The network security can be implemented in there levels on the network infrastructure. It can be implemented at the backbone, servers, and at the computer. At the backbone level, the network security is installed at router, gateway, and switches to prevent any unauthorized access to the system (Kumar & Malhotra, 2015). This is to ensure that the entry point to the system is protected and it becomes difficult to gain entry into the system or the network. Besides installation of security at the gateway and switches, it is important to install strong firewall hardware and set software as well. This will limit access to the system to ensure that unauthorized person does not get access to the network. However, it would be important to ensure that there is a clear security policy, to prevent the data from being accessed

# References

Ahmad, N. (2018). Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of. 2-31.

King, T. (2014). CompTIA Security+ Exam: Devices, Media, and Topology Security. 2-3.

Kumar, A., & Malhotra, S. (2015). Network Security Threats and Protection Models. *Technical Report – CSE-101507* , 2-34.

Ossi, V. (2018). 2 EVALUATION OF FIREWALLS AND RESEARCH. *Degree Programme in Information Technology* , 5-38.

Salah, A. (2018). Design and Implementation of a Network Security Model for Cooperative Network. *https://www.researchgate.net/publication/50367393\_Design\_and\_Implementation\_of\_a\_Network\_Security\_Model\_for\_Cooperative\_Network* , 2-35.