Network security and applications

Web 2. 0 security Securing a network is a becoming a major issue, and in the past only tackled by skilled and qualified people. On the other hand, as increasingly the people become ``wired'', an increasing number of people need to recognize the fundamentals of security in a networked world. Additionally, at present a lot of people get chances to work from home and connect to systems distantly, in this regard network security becomes a significant subject for the companies. In this regard, the most excellent way to keep away from inconsequential security issues and threats is that education of end-user though the right software can help diminish the threat. Thus, this is very important to train the basic computer users and information systems manager in mind, teaching the ideas required to read through the hype in the marketplace and recognize threats associated with the computer security and how to cope with them (Network Security, 2010; Curtin, 1997). In addition, the network security is turning out to be more and more significant in view of the fact that people spend more and more time connected. In this scenario, compromise on network security is frequently much easier than compromise on physical or local security, and is much more frequent. However, there are numerous good tools available to help improve network security, as well as majority of them are shipping with Windows features (The Linux Documentation Project, 2010). The new web based or web-supported tools offer a range of effective software features and services to the consumers, workers and business associates. These services could be easily managed and handled. Additionally, the new information technology offers access to a major business resource such as the web server, which gives the capability to access various other useful information resources, for instance database servers (ITSecurity). The major

examples of Web 2. 0 includes social networking websites such as wikis, blogs, hosted services, video-sharing websites, mashups, web applications and folksonomies. Cloud computing (a broad term for anything that engages distributing hosted services over the internet) also integrates Web 2. 0 utilities for the distribution and coordination of data across a range of tools and devices. In spite of these Web 2. 0 advantages and technology based solutions, there is an expenditure that is further than the cost of the systems and software: major security contests. In current years, websites like that Gmail, Yahoo! Mail, Facebook along with MySpace have all been overwhelmed by hateful code. However, the absolute openness of today's computing setting is outstanding. In this regard, consumers, human resources and business associates utilize a range of systems, comprising smartphones and other portable units to beat someone delicate or intellectual possessions, personal data, credit card details, health care records and more (Greengard) and (TechTarget). With the capability of adware, malware and spam dispensers to utilize the websites as delivery mediums for their newest effort for cyber-hackers to expertise tremendously overwhelmed attacks through the information gathered from individual outlines placed on web pages of Web 2. 0 characteristics. In such type of situation social networking is quickly turning out to be a serious pain position, investigators uphold (Hines). In Web 2. 0 based environment a user can face following attacks and assaults: (Perez) 1. Injection mistakes 2. Inadequate Authentication Controls 3. Reliability of Information 4. Inadequate Anti-automation 5. Outflow of Information 6. Phishing 7. Cross Site Scripting (XSS) 8. Cross Site Request Forgery (CSRF) These possible security susceptibilities are more aligned to the web 2. 0 based environment.

In this current web based business and working arrangement such categories of safety and privacy assaults are turning out to be more frequent. Therefore there is a dire need for even much better ways and techniques to deal with such type of attacks. The section below is aimed to offer such type of ways or mechanisms for better protection and privacy administration (Perez). In case of web 2. 0 based setting we can take the following efficient steps for the better management of security associated vulnerabilities (SpamLaws) Validation of User-Input: In web applications there is vital need for the validation of all the data that is entered by various users. This can be done by implementing proper login and password based security mechanism (SpamLaws). Default Configurations: In Web2. 0 based arrangement we need to overlook the requests for rearrangement of web servers by setting their default configurations. In this way hackers will not be able to change the configurations to perform or to launch a security attack (SpamLaws). Encryption: It is a very useful technique for the protection of the data and information in the Web2. 0 based arrangement. It can efficiently protect from the outsider attacks (SpamLaws). Protected Servers: By making web based server protected against the outsider attacks we can implement better security and privacy management. This can be done through the establishment of highly sophisticated firewall systems or intrusion detection system (SpamLaws). Web 2. 0 is becoming a very useful tool for the businesses. It is very helpful for improving the performance of the corporations. However, there are lots of security related issues in Web 2. 0. This paper has presented a brief overview of some of the main aspects regarding the Web 2. 0 security. This paper has also suggested possible mitigation actions those can be taken for an effective Web 2. 0 security

management. Works Cited Curtin, Matt. Introduction to Network Security. March 1997. 06 February 2011 . Greengard, Samuel. Web 2. 0 Security Strategy. 12 October 2010. 09 February 2011 . Hines, Matt. Experts hammer Web 2. 0 security. 21 February 2008. 09 February 2011 . ITSecurity. Best Practices for Web 2. 0 Security. 2011. 09 February 2011 . Network Security. Education: Basic Foundation to Business Network Security. 03 October 2010. 07 February 2011 . Perez, Sarah. Top 8 Web 2. 0 Security Threats. 17 February 2009. 09 February 2011 . SpamLaws. 5 Best Methods for Web 2. 0 Security . 2009. 09 February 2011 . TechTarget. Cloud Computing. 28 December 2007. 09 February 2011 . The Linux Documentation Project. Network Security. 2010. 08 February 2011