CIS 333 – Networking Security FundamentalsAssignment 1: Identifying Potential Malicious Attacks, Threats, and VulnerabilitiesNovember 3rd2013Many organizations have invested vast amount of money in computer networks, only to find out that although it is providing means of improving the efficiency and productivity of the organization but it also exposes the Organization to possible attacks and threats. Such attacks have been the most challenging issue for most network administrators and a worrying topic for administrators.The network structure of the company has two firewalls, one is external firewall and the other is internal firewall. The CIO Company will use firewalls, intrusion detection systems, virus scanners and other protective software to provide some assurance that the security policies for the site are properly implemented. Firewalls are the basis of computer and network security defense. They are widely deployed. They are very hard to configure properly, and people who configure them may not know the current threats and attacks. For example, an administrator

***Subscribe*** to view the full document.

Subscribe to Unlock

**Identifying Potential Malicious Attacks, Threats, and Vulnerabilities** maybe working on some task and might leave something open in a firewall where attackers can enter through. Some firewalls have the vulnerability that enables attackers and be defeated.The second vulnerability is the email server. Although very well controlled for been within the Demilitarized Zone (DMZ), this is always a vulnerability with which most companies have to deal with (Hamelin). This vulnerability opens the way for phishing attack. One way to mitigate this vulnerability is configuring the email server so that only authorized email may enter. This is difficult because our video game company has a large list of customers and suppliers that are in constant change. The best option is to alert users about the security measures and company policies regarding private and unknown emails.The location of the file servers in the network is totally unprotected against internal attacks. Any successful attack in the LAN would leave the data servers exposed. The establishment of a demilitarized zone with a completely different set of log on names and password than any other machines would give these servers better security. The LAN can be compromised but the data still remain in a safer area of the network.The most vulnerable point of our network is the Wireless Access Point. It is located inside the LAN, which reduces network security, being away from the protection of firewalls. The only protection it has is the internal configuration. This vulnerability provides various attacks like Snooping, Brute-Force and Eavesdropping. Do not think it's necessary to have a WAP in the company but if necessary I suggest that should be installed inside the DMZ, after the external firewall, IDS just before, if someone unauthorized gets through it will be detected and we have the safety of the internal firewall.