Honeypots and firewalls

Technology, Information Technology

Honeypots and Firewalls Honeypots and firewalls Multiple screen subnet architecture vs. dual homed host Multiple screen subnet architecture offers or runs it provisions originating from a host linked to manifold grids. Its source is however switched off. The source of the network ought to be linked to the heart of the grid by the use of an isolated router. This design permits packages to pass through the network into the heart of the grid. In contrast, a dual homed design is created in a manner that does not permit these packages to pass through. The dual homed host is created about two or more grids crossing each other. A dual homed host can be deployed when services needs to be deliver through proxy whereas a multiple screen subnet can be deployed where packages or packets are required to pass through the network into the grid (Zwicky, Cooper and Chapman, 2000).

2. Worms, Malware, and Viruses

Worms, malware, and viruses are common issues facing companies every day. These can be prevented through the use of antiviruses. An antivirus is software that identifies threats and hence blocks them from attacking a computer, an antivirus is also able to delete viruses, worms, and malware that has already attacked a computer system. Worms, viruses, and malware are sometimes used by hackers to illegally access other peoples’ computers. Ensuring all computers within an organization is therefore important as it will prevent unauthorized individuals from accessing private and confidential information in other peoples’ computers.

3. How to sell a Honeypot to a CIO

The value of a honeypot can be sold to a CIO through elucidating its benefits, values, as well as the potential issues and downsides. Based on its simple design, a honeypot has the capability to gather and assemble trivial and minute cliques and arrays of statistics and information. Honeypots are created with the main objective of intermingling and networking with aggressors of the system. Therefore, through assembling and gathering each and every information and statistics, novel gizmos used by hackers and other attackers are identified and dealt with amicably. One of the downside off a honeypot is the fact that it can only identify threats that networks or associates with it. Honeypots can also be hijacked by aggressors and hence be used to cause more damage to the system (The Government off the Hong Kong Special Administrative Region, 2008).

4. Honeypots and Firewalls

There are diverging characteristics associated with firewalls and honeypots. According to Zwicky, Cooper and Chapman (2000), a firewall is characterized by diverse security ranks on the basis of the position and situation of the computer, security or safeguarding of wireless grids and systems such as Wi-Fi. A firewall is used within an organization to stipulate the kind of drivers and packages fitted in a particular computer that should contact the complex system, stops intrudes or aggressors trying to attack the computer, and as well blocks any unwanted programs. Firewalls can be deployed in small or medium sized organizations. Honeypots on the other hand are characterized by their ability to identify minute and trivial data, encryptions, is created in such a way that aggressors or hackers cannot differentiate them form the grid, and also simple processes and procedures. Since they can identify unauthorized packages trying to access the grid, they are ideal for big organizations.

5. A response plan centered on a honeypot technology

According to The Government of the Hong Kong Special Administrative Region (2008), a honeypot technology permits and consents the ordering and ranking of connected warnings and signals. This is made possible through substantiation and validation of the honeypot system. An alert is considered as useable and binding when it has connected in both the honeypot and the computer grid or system. This is followed by the documentation of a letdown and hence the system amicably responds by sojourning the impeding attack or lessening the consequence of the attack. Once an attack has been identified, the honeypot reacts by tricking and misleading the aggressor that the honeypot is a genuine or authentic grid. Subsequently, as the aggressor tries to circumvent through the honeypot, his or her IP address is identified and hence prized statistics and data regarding the attack is scrutinized. If need be, the aggressor can be therefore be tracked. It is also of significance to posit that honeypots can also slow down the aggressor by directing to him or her acknowledgement package of nil magnitude. Through accessing the aggressor's IP dress, the honeypot is therefore able to update information regarding the hacking processes and procedures of the aggressor.

References

The Government of the Hong Kong Special Administrative Region. (2008). Honeypot Security. Retrieved from http://www. infosec. gov. hk/english/technical/files/honeypots. pdf

Zwicky, E. D., Cooper, S., & Chapman, D. B. (2000). Building Internet Firewalls. Sebastopol, CA: O'Reilly.