STUDY AND DESIGN OF HACKER DETECTION SYSTEM ON LOCAL AREA NETWORK (LAN) FOR INTERNAL SECURITY

Prepared by: Lai Yan Chang

ABSTRACT

There are two major hacking programs in use now. NetBus and Back Orafice (BO). These programs do a legitimate use in network security and analysis, but they can easily be sued to snoop your PC network connection. These programs can be disguised as harmless programs. These are often those goofy programs or screen savers people always send through files or mails. When you click on the executable file and watch something pretty or any funny animation across the screen, it will unwittingly let the Trojan program onto the system. These programs are buried deep in the system files, often hidden from detection or cloaked at as harmless files. When you log on into network connections, these programs force TCP ports open and allow virtually anyone with BO or NetBus administrator programs to detect your PC and access your files. Therefore, the author will come out with a system that can detect hacker or hacking program across the Local Area Network (LAN). For an example, if any PC tries to hack other PC in the LAN, the main security PC system will capture hacker IP address, hacking time and store the information in log file. Besides that, a warning signal will appear on main security PC in any hacking activities appears. With this system, it will make your PC more secure when you are logging in the network.