G PULLA REDDY ENGINEERING COLLEGE

DEPARTMENT OF CSE

MINI PROJECT - 1

ABSTRACT

Title: BLACKCAT KEYLOGGER

Keyloggers are the type of rootkit malware that capture typed keystroke events of the keyboard and save them into the log file, therefore, it can intercept sensitive information such as usernames, PINs, and passwords, thus transmits into malicious attacker without attracting the attention of users. Using this approach, an attacker can obtain valuable data without cracking into a hardened database or file server. Keylogging presents a special challenge to security managers. Unlike traditional worms and viruses, certain types of keyloggers are all but impossible to detect. A keylogger is a tool that is implemented to acquire the keystrokes entered by using a keyboard. It is also a battery sized tool which is connected between keyboard and computer. The main purpose of the keylogger tool is to keep monitor that work computers are used for business and other purposes. Keyloggers present a major threat to business transactions and personal activities such as E-commerce, online banking, email chatting, and system database. Keyloggers have been widely used by hackers as a tool to steal information and passwords from users in e-commerce. A password is a secret word or phrase that must be used to gain access to the website. That password access can either be an application, a network, documents, and data in a computer system. Generally, a password should consist of something hard to guess, so that it will remain a secret. We can authorize that password with our keylogger program. This paper presents an overview of keylogger programs, types, characteristics of keyloggers, we look at the various types of keyloggers and how they differ, and the methodology they use.

Keywords: Keylogger, Software, virtual keyboard.

Signature of the Guide:

Ms. Y. Supriya Reddy

Assistant Professor

CSE

Group B-19

Team Members:

D. Venkata Karthik Reddy
[189X1A0536]

S. Sai Sreekanth
[189X1A05A7]

V. Venkata Sai
[189X1A05G4]