

Experiment 13

Study of malicious software using different tools: Keylogger attack using a keylogger tool.

--

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO5: Demonstrate the network security system using open source tools.

Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.

Introduction:

Keyloggers:

Keyloggers, also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved to a file, and that file is accessed by the person using this malware. Keylogger can be software or can be hardware.

Working:

Mainly key-loggers are used to steal passwords or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware keylogger and first software key-logger was developed in 1983.

1. Software key-loggers :

Software key-loggers are computer programs which are developed to steal passwords from the victim's computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft Windows 10 also has a key-logger installed in it.

JavaScript based keylogger –

It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.

Form Based Keyloggers –

These are key-loggers which activate when a person fills a form online and when clicking the button submit all the data or the words written are sent via file on a computer. Some key-loggers work as an API in a running application. It looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers :

These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard is pressed it gets recorded.

USB keylogger :

There are USB connector key-loggers which have to be connected to a computer and steal the data. Also some circuits are built into a keyboard so no external wire is used or shows on the keyboard.

Smartphone sensors –

Some cool android tricks are also used as keyloggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%.

Nowadays crackers are using keystroke logging Trojan, a malware which is sent to a victim's computer to steal the data and login details.

So key-loggers are software malware or hardware which is used to steal , or snatch our login details, credentials , bank information and many more.

Some keylogger application used are:

1. Kidlogger
2. Best Free Keylogger
3. Windows Keylogger
4. Refog Personal Monitor
5. All In One Keylogger

Prevention from key-loggers :

1. Anti-Key-logger –

As the name suggests these are the software which are anti / against keyloggers and main task is to detect key-loggers from a computer system.

2. Anti-Virus –

Many anti-virus software also detect keyloggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.

3. Automatic form filler –

This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .

4. One-Time-Passwords –

Using OTP's as password may be safe as every time we login we have to use a new password.

5. Patterns or mouse-recognition –

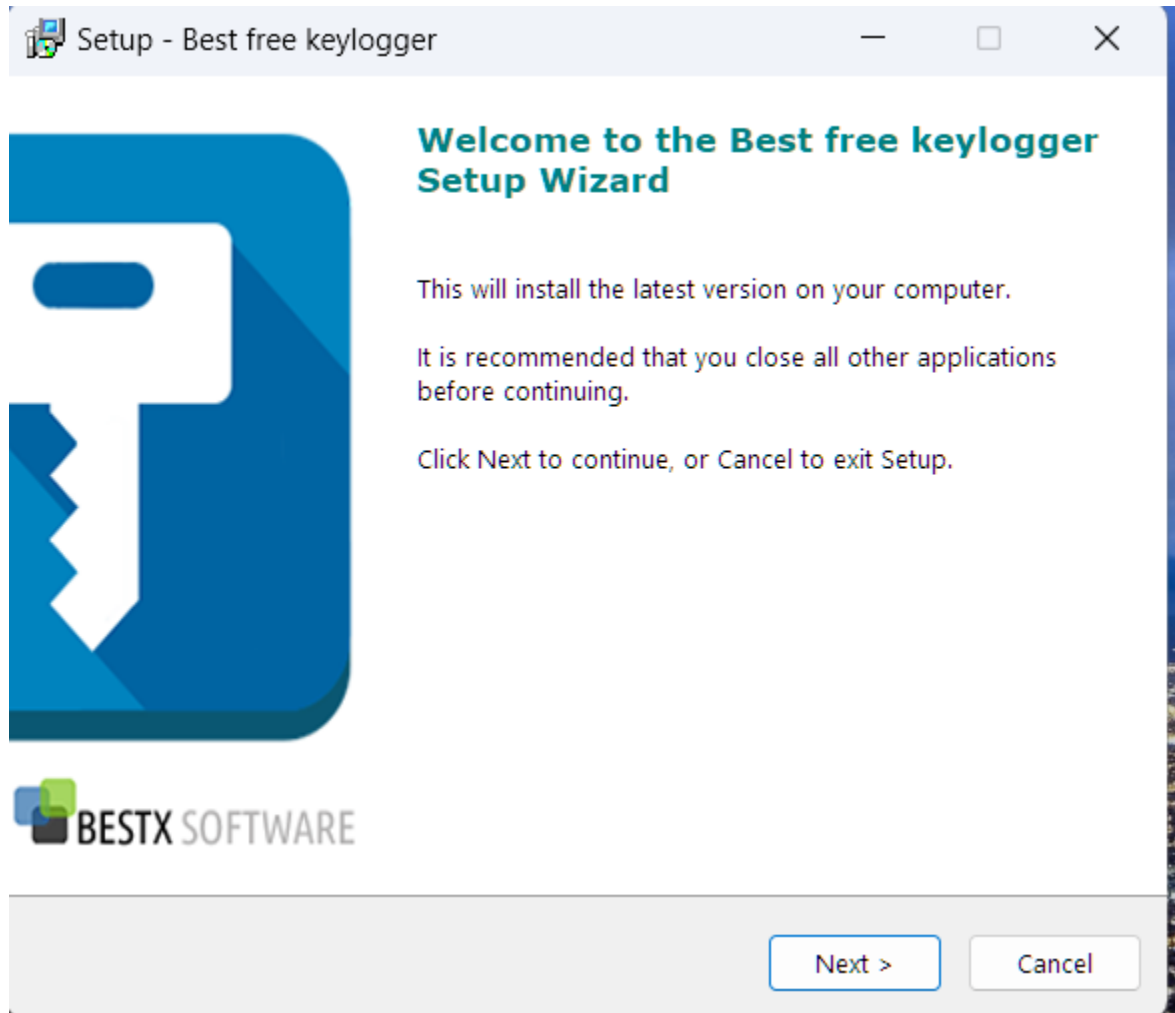
On android devices use pattern as a password of applications and on PC use mouse recognition,mouse programs use mouse gestures instead of stylus. These techniques are less common but are very helpful against key-loggers.

Methods:

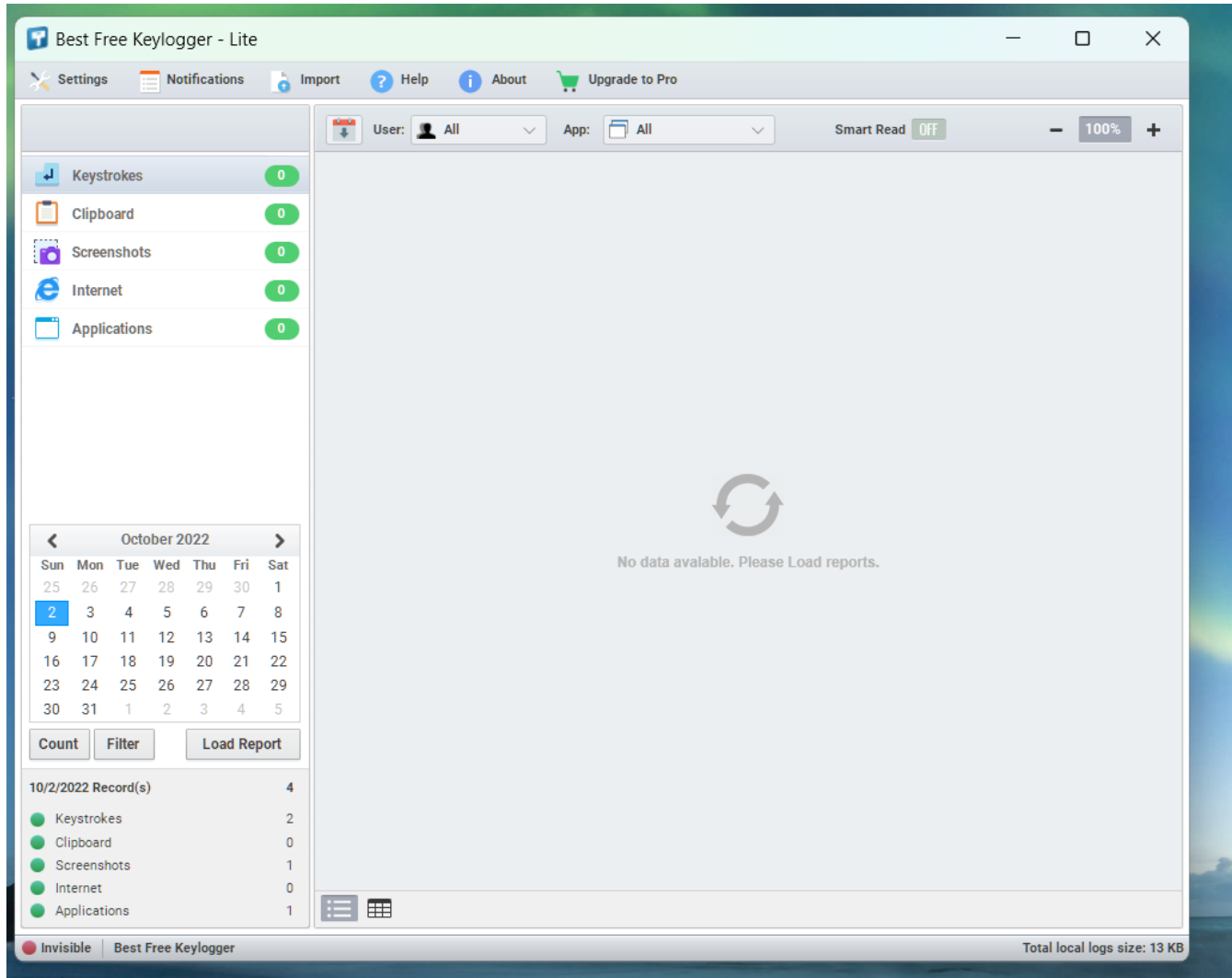
Step 1: Firstly we will install one of the keylogger “**Best Free Keylogger**” from this website: <https://bestxsoftware.com/download.html>

Download and install it , I am doing it for Windows Operating System.

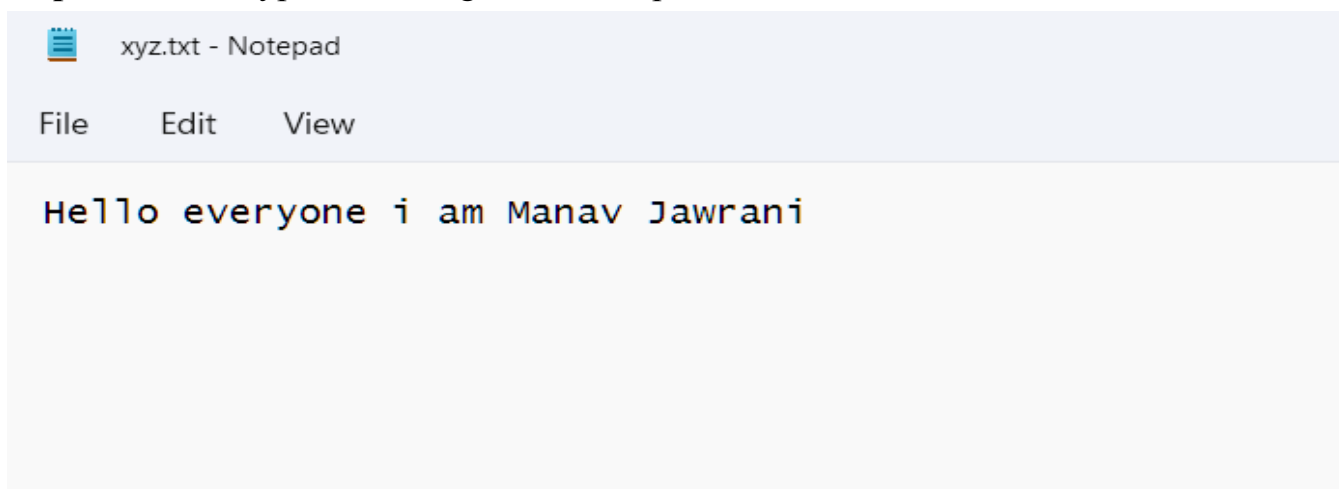
NOTE: Please turn off the antivirus before installing.

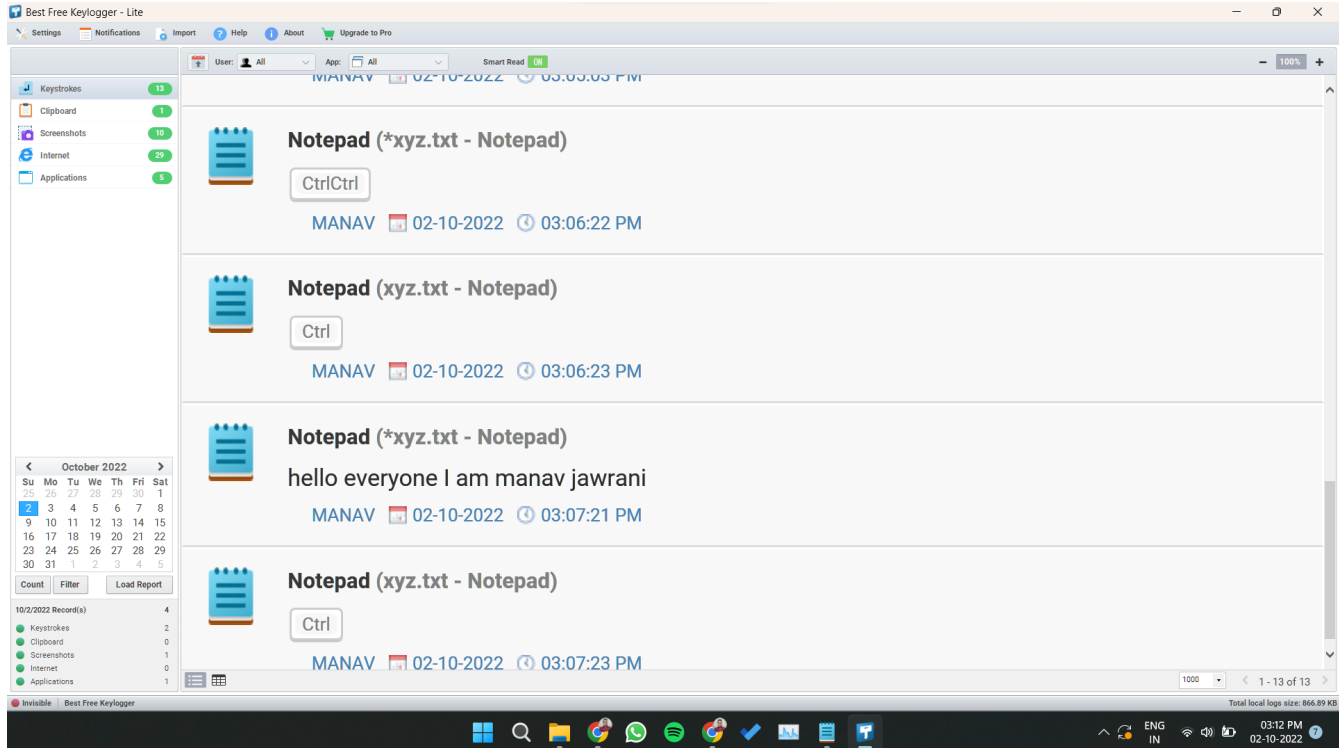


After Successfully installing the Software you will see such an interface.



Step 2: We will type something on the notepad.



Step 3: Check the logs on the home screen of the software.

And this is how keyloggers work , they capture your keystrokes and many more things.

Conclusion:

Thus, we have studied the malicious software tool using the Keylogger tool.