A

Project Report

on

KEYLOGGER

Submitted in partial fulfillment of the requirement for the IV semester

Bachelor of Technology (Com Engg with CS)

By

Tripti Singh (20012828)

Mahi Adhikari (20042188)

Under the Guidance of

Mr Shobhit Kumar

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

GRAPHIC ERA HILL UNIVERSITY, BHIMTAL CAMPUS

SATTAL ROAD, P.O. BHOWALI

DISTRICT- NAINITAL-263132

2021-22

STUDENT'S DECLARATION

We, **Tripti Singh (20012828), Mahi Adhikari (20042188)** hereby declare that the work, which is being presented in the project, entitled "KEYLOGGER" in partial fulfillment of the requirement for the award of the degree (B. Tech) in the session **2021-2022**, is an authentic record of our own work carried out under the supervision of **Mr Shobhit Kumar, Graphic Era Hill University, Bhimtal.**

Date: ……

CERTIFICATE

The project report entitled “KEYLOGGER” being submitted by TRIPTI SINGH (20012828), MAHI ADHIKARI (20042188) to Graphic Era Hill University, Bhimtal Campus for the award of bonafide work carried out by them. They have worked under my guidance and supervision and fulfilled the requirement for the submission of report.

(……) (……)

Project Guide HOD, CSE Dept.

ACKNOWLEDGEMENT

I take immense pleasure in thanking Honorable **"Mr Shobhit Kumar"** (GEHU Bhimtal Campus) to permit me and carry out this project work with his excellent and optimistic supervision. This has all been possible due to his novel inspiration, able guidance and useful suggestions that helped me to develop as a creative researcher and complete the research work, in time.

Words are inadequate in offering my thanks to GOD for providing me everything that I need. I again want to extend thanks to our President **"Prof. (Dr.) Kamal Ghanshala"** for providing us all infrastructure and facilities to work in need without which this work could not be possible.

Many thanks to Professor **"Dr. Manoj Chandra Lohani"** (HOD-CS&A, GEHU), and other faculties for their insightful comments, constructive suggestions, valuable advice, and time in reviewing this thesis.

Finally, yet importantly, I would like to express my heartiest thanks to my beloved parents, for their moral support, affection and blessings. I would also like to pay my sincere thanks to all my friends and well-wishers for their help and wishes for the successful completion of this research.

Tripti Singh

Mahi Adhikari

Table of Contents

ABSTRACT

Computer security specialists work every day solving security problems and handling intrusions. The experts try to avoid new security threats, but the intruders are trying to find new penetration methods and sophisticated attacking methods to compromise computers. The number of intruders is increasing in the computer world today. The usage of keylogging is being used for monitoring and logging what attackers are doing when performing attacks. Keylogging can log the entered keystrokes on hosts such as remote systems and in honeypots. Collecting keystrokes is an important step towards understanding the hackers and acquire knowledge about the attacks. Honeypots can tell security researchers how data is stolen and where hackers hide their stolen data or which methods the hackers are using to take control over a remote machine. Originally keyloggers where developed for servers with operating systems accessing the hardware directly. However, the usage of visualization and virtual machines is increasing rapidly for service providers in small and large organizations. Keylogging in bare-metal technology and in virtual technologies can be different since the keystrokes might be interpreted differently depending on the hypervisor technology. The results of this thesis show that with respect to keylogging there are differences between bare-metal and virtual environments for Linux systems.

INTRODUCTION

A computer keyboard distinguishes each physical key from every other and reports all key presses to the controlling software.

Physical keyboards are used to type text and numbers into a word processor, text editor or other programs. In a modern computer, the interpretation of keystrokes is generally left to the software.

A command-line interface is a type of user interface operated entirely through a keyboard. In computer environment it exists both hardware keyloggers and software keyloggers.

The hardware keylogger can only log from the only one physical machine the hardware keylogger is installed on. A keylogger with a lot of features to capture all necessary information can be used in honeypots in a honeynet.

A typical honeypot is a host machine, acting like a useful and normal host. Several honeypots in a network are called honeynet.

The honeynet consist of technology for watching honeypots that are running with the primary intent of luring attackers and collect information about attacks and tracking attacking methods.

What is a Keylogger?

A keylogger is a form of malware or hardware that keeps track of and records your keystrokes as you type. It takes the information and sends it to a hacker using a command-and-control (C&C) server. The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.

Keystroke logging has become an established method used by hackers for fetching passwords and other confidential data. Not only for hackers, but also for others such as: system administrators for systems, detecting suspicious users.

In research for different areas such as for research by parents for monitoring children for detecting special behaviors and criminals to name a few areas. Keystroke logging can also be a very useful method to detect attacks and their attack mechanisms, when setting up keylogger in honeypots.

An important part of this research will be to find out how keylogging works under different technologies and set up a

honeypot to log the keystrokes, entered as commands or executable scripts entered by the attackers. With the purpose to viewing exactly what the hackers are doing. This will monitor which method that is going to be used.

This may also successfully cause interaction with the hacker. To detect keystrokes might prepare against such attacks in the future.

What does a Keylogger do?

The basic functionality of a keylogger is that it records what you type and, in one way or another, reports that information back to whoever installed it on your computer.

Since much of your interactions with your computer – and with the people you communicate with via your computer – are mediated through your keyboard, the range of potential information the snooper can acquire by this method is truly vast from passwords and banking information to private correspondence.

Some keyloggers go beyond just logging keystrokes and recording text and snoop in several other ways as well. It's possible for advanced keyloggers to:

- Log clipboard text, recording information that you cut and paste from other documents
- Track activity like opening folders, documents, and applications
- Take and record randomly timed screenshots

- Request the text value of certain on-screen controls, which can be useful for grabbing passwords

Types of Keylogger

There are generally two types of keylogger:

1. Hardware Keylogger
2. Software Keylogger

Hardware Keylogger: The hardware keylogger is a device that is connected between the keyboard and the input/output(I/O) input unit on the computer's hardware for logging keystrokes entered in the computer. Some of hardware keyloggers works at BIOS level while some are based on keyboard level.

The hardware keyloggers does not require any driver or software and will work with all Linux based operating systems as well as with Windows operating systems. Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

Hardware keyloggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between

the computer keyboard and the computer, typically in line with the keyboard's cable connector. There are also USB based Hardware keyloggers as well as ones for laptop computers.

Software Keylogger: A Software keylogger in installed on a computer, directly or by remote installation. The software keylogger is invisible to the human eye, while hardware keylogger is easy to spot if a user checks what is connected to the computer.

Software-based keyloggers use the target computer's operating system in various ways, including imitating a virtual machine, hypervisor based or virtual machine manager, acting as the keyboard driver (kernel based), to watch keyboard strokes.

Within software keylogger there are also two different types: user-level and kernel-level keyloggers. A kernel level-based keylogger is a program on the machine that gets administrator permissions and hides itself in the operating system, and starts intercepting keystrokes, because keystrokes always go through the kernel.

A keylogger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system. A user level-based keylogger are the easiest to create, but also the easiest to detect. This is the most common method used when creating keyloggers.

- A hardware keylogger has an advantage over a software keylogger solution: it is not dependent on being installed on the target computer's operating system and therefore will not interfere with any program running on the target machine or be detected by any software.

Usage of Keyloggers

Both hardware keyloggers and software keyloggers have their advantages and disadvantages. It is depending on what purpose one will use the keylogger. Keyloggers are used in many different areas.

There is a lot of legitimate software which is designed to allow system administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers.

Keyloggers are also used in information technology organizations to troubleshoot technical problems with computers and business networks.

Keyloggers can also be used by a family or business to monitor the network usage of people without their direct knowledge.

Malicious individuals, also called hackers may use keyloggers on public computers to steal passwords or confidential informative entered to the computer via the keyboard.

Hackers are using keyloggers for cyber espionage, identity theft, fraud and several more methods.

Other areas for usage are: Detecting users, parents watching children, computer cyber criminals, private detectives, law enforcement, spouses and family members, employers, system administrators and in research for different areas.

Keyloggers are also using for this research to detect hackers and attackers. Keyloggers are also used in honeypots. For example, we can log the keystrokes of an interactive session even if encryption is used to protect the network traffic.

Visibility for Keyloggers

A hardware keylogger is easy to spot if a user checks what is connected between the keyboard and hardwrae the hardware on a computer, but software keyloggers are more difficult to detect, because they are software inside a computer.

A good feature for a keylogger is that the keylogger is invisible and hard to detect on the current system. Especially if the purpose is to hide the keylogger from the users.

Features for Keyloggers

Keylogger have different performances to log the interactivity. In Linux server environment only, the keystrokes are logged. In windows environments a lot more than keystrokes is logged.

Here is a list of features for keyloggers:

- **Keystrokes Logging** : Record all keystrokes.
- **Clipboard Record** : Record any words or texts which are copied and pasted on the clipboard or other file editing programs. The purpose of this is to be able to view the record in detail about which user at what time have selected and copied what exact text information.
- **Application Tracking** : All attempts to run any program can be logged. The purpose is to easily understand what time which user is running what applications in the computer.
- **Websites Visited**: All the web activity like site titles, clicking links, visiting web-pages URLs could be monitored and recorded by Keylogger. The logs are accurate to the exact time hence you can know what the user was involved in the specific computer activities.
- **Screen Capture**: Screen shot allows you to understand what's going on with the computer without logging keystrokes. For the screen shot, you can customize with

capture interval and capture quality one the screen shot taken.

- **Time / date tracking**: It allows you to pinpoint the exact time a window received a keystroke.
- Easy to install

Conclusion

- Keyloggers are a very important tool within the computer security.
- Keyloggers are dangerous weapons when doing hacking and for detecting attackers on the other hand.
- A keylogger can record instant messages, email, and any information you type at any time using your keyboard.
- The log file created by the keylogger can then be sent to a specified receiver.
- There are two types of keyloggers namely, Hardware Keyloggers and Software Keyloggers.
- Hardware Keylogger starts its applications when it is been plugged in. It is a physical device that is used for capturing keystrokes.
- Software Keylogger is something that is installed on the hard drive. This type of software is also called spy software.

Bibliography

- UiO: Department of Informatics (Keylogging of user interaction in physical and virtual environments and its implications for honeypot analysis)
- Wikipedia
- Dieter Gollman. "Computer Security ". John. Wiley and Sons, Inc., 2011.
- Hafez Barghouthi, Keystroke Dynamics, how typing characteristics differ from one application to another, 2009.